Zurich Security Management

Última atualização: 11/11/2025

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

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

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

Tradução automática

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

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Índice

Operações de segurança **5**

Explorando Operações de segurança 7

Now Assist para Resposta a incidentes de segurança 13

Explorar 15

Configurar 19

Usar Now Assist para fechar incidentes de segurança 27

Use fluxos de trabalho do agentic 43

Now Assist para resposta a vulnerabilidades 58

Explorar 59

Configurar 62

Use habilidades de IA generativa 66

Use fluxos de trabalho do agentic 75

Referência 80

Aplicações de gestão de superfície de ataque 82

Resposta a vulnerabilidades 83

Resposta a vulnerabilidades de aplicações 883

Contêiner de Resposta a vulnerabilidades 1090

Conformidade de configurações 1169

Resposta a vulnerabilidades Espaços de trabalho 1437

Lista de materiais de software 1638

Aplicações de gestão de casos de segurança empresarial 1681

Resposta a incidentes de segurança 1683

Inteligência contra ameaças 3201

Controle de posturas de segurança 3452

Explorar 3454

Use o espaço 3470

Use controles de mitigação 3491

Referência 3515

Painel executivo de cibersegurança 3529

Aceite pontuações de benchmark 3547

Definir metas 3548

Simulação de segurança e integração de treinamento para operações de segurança 3548

Painel de risco e conformidade para GRC: Metrics 3551

Central de segurança de inteligência contra ameaças 3560

Explorar 3561

Configurar 3566

Integrar 3570

Administrar 3656

Referência 3702

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uso....3710
Data Loss Prevention Incident Response....3905
Explorar....3907
Configurar....3910
Administrar....3911
Gerenciar incidentes....3966
Integração de entrada....3988
Integrar....3990
Operações de segurança funcionalidade comum....4060
Criar e definir grupos de filtros em Operações de segurança....4063
Transformação de dados compartilhados....4065
Operações de segurança processamento de e-mail....4068
Operações de segurança mapeamento de campo....4079
Operações de segurança transformações de valor do campo....4083
Operações de segurança mapeamento de dados de aprimoramento....4084
Operações de segurança escalação definida pelo usuário....4087
Crie substituições de propriedade separadas por domínio....4088
Crie um grupo de sistemas operacionais....4090
Configurar grupos de marcadores de segurança e marcadores....4091
Anotações de segurança....4095
Componentes instalados com Security Support Common....4097
Pesquisar Operações de segurança....4098
Referência do Security Operations Integrations....4099
Operações de segurança gatilhos de fluxo de trabalho....4199
Orquestração do Security Operations....4201
Operações de segurança e o ServiceNow Store....4202
Baixar uma aplicação do ServiceNow Store pela primeira vez....4202
Instale um Operações de segurança integração....4208
Atualize uma aplicação baixada anteriormente do ServiceNow Store....4212
Atualize sua instância para a próxima versão da família....4213

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança

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

Escolha um desses blocos para começar.

Aplicações de operações de segurança e seus espaços de trabalho



Saiba como Operações de segurança as aplicações podem ajudar você a melhorar sua postura de segurança.

Now Assist para resposta a incidentes de segurança



Saiba como o Now Assist for Security Incident Response oferece suporte ServiceNow® Habilidades de IA generativa (IA generativa) no Espaço de resposta a incidentes de segurança e na IU principal (UI16).

Now Assist para resposta a vulnerabilidades



Saiba como Now Assist para resposta a vulnerabilidades suporte ServiceNow® Habilidades de IA generativa (IA generativa) no Espaço de resposta a vulnerabilidades e na IU principal (UI16).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de gestão de superfície de ataque



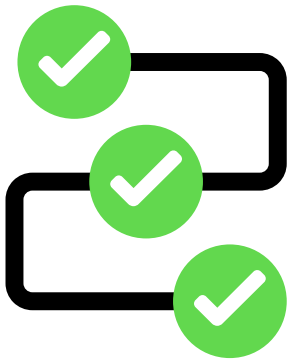
Saiba mais sobre as aplicações no Resposta a vulnerabilidades que ajudam você a identificar e corrigir vulnerabilidades em sua superfície de ataque cibernético.

Aplicações de gestão de casos de segurança empresarial



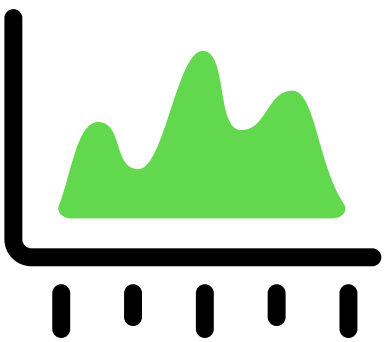
Saiba mais sobre as aplicações em Resposta a incidentes de segurança que ajudam você a analisar, isolar e corrigir incidentes de segurança críticos à medida que eles evoluem.

Aplicações de controle de postura de segurança



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

Painel executivo de cibersegurança



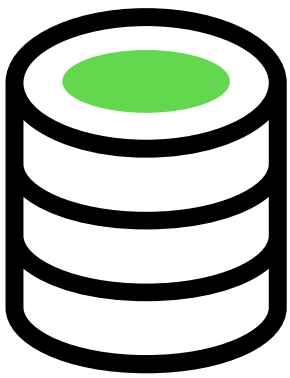
Saiba como o Painel executivo de segurança cibernética consolida dados de vários produtos SecOps em um painel unificado.

Central de segurança de inteligência contra ameaças



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

Data Loss Prevention Incident Response

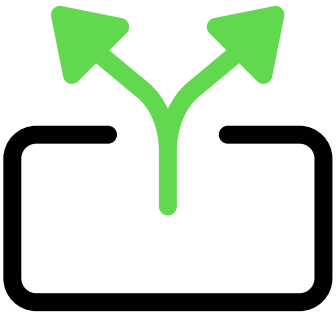


Saiba como você pode gerenciar informações confidenciais para seus clientes e identificar e proteger seus canais de perda de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança compartilhadas



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

Cenários e exemplos de operações de segurança



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

Solucionar problemas e obter ajuda

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

Explorando Operações de segurança

Proteja seus ativos e o ambiente empresarial com a ServiceNow Operações de segurança e o poder do ServiceNow AI Platform®. Conecte suas equipes de segurança e TI para ajudar você a priorizar e resolver ameaças com base no impacto que elas representam para sua organização.

Visão geral Operações de segurança

. Operações de segurança o pacote de aplicações ajuda você a proteger seus ativos, melhorando sua postura geral de segurança. Por exemplo, integrando aplicações como Resposta a incidentes de segurança, Resposta a vulnerabilidades e Controle de posturas de segurança Com suas ferramentas de segurança existentes, os analistas, gerentes e equipes de TI do Centro de operações de segurança (SOC) podem:

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

Tradução automática

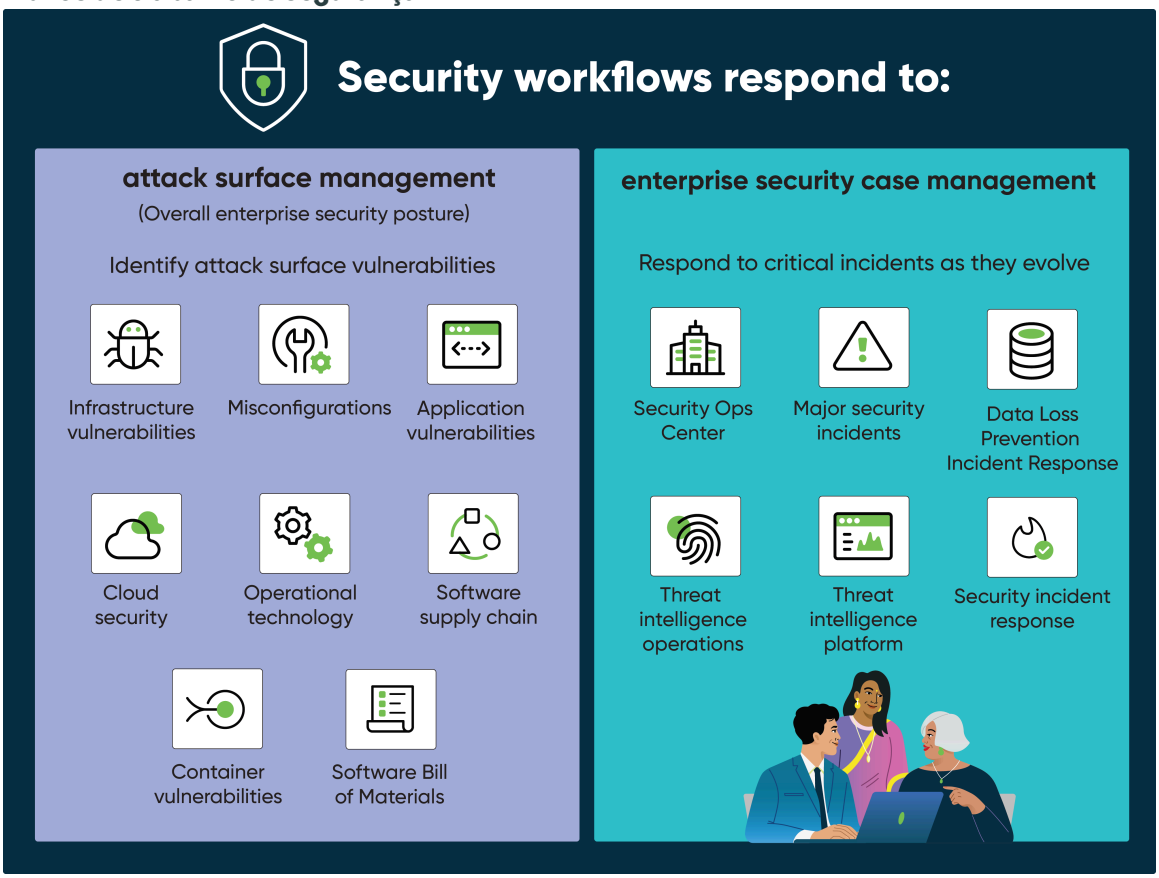
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança aplicações para fluxos de trabalho

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

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

Fluxos de trabalho de segurança



As duas categorias de aplicações de operações de segurança e os casos de uso que elas ajudam você a lidar em seu ambiente empresarial.

Benefícios do Operações de segurança aplicações

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

- O ciclo de vida dos incidentes de segurança, desde uma análise inicial até contenção, erradicação e recuperação.
- As vulnerabilidades com as quais eles mais se importam para que possam decidir estrategicamente quais vulnerabilidades serão enviadas para as equipes DE TI corrigirem.
- Principais informações e principais casos de uso para cobertura de ferramentas de segurança e higiene de ativos que relatam e monitoram informações importadas sobre seus ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de gestão de superfície de ataque

Aplicações que ajudam você a prever ameaças e identificar vulnerabilidades

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações que ajudam você a prever ameaças e identificar vulnerabilidades

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

Aplicações de gestão de casos de segurança empresarial

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

Aplicação	Descrição	Usuários
Resposta a incidentes de segurança	Simplifique o processo de identificação de incidentes críticos aplicando ferramentas avançadas de fluxo de trabalho e automação que aceleram a correção. Integre suas ferramentas existentes do Gerenciador de eventos e informações de segurança (SIEM) com Resposta a incidentes de segurança E Operações de segurança para importar dados de ameaças de várias fontes e criar automaticamente incidentes de segurança priorizados.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças
Gestão de incidentes graves de segurança	Os recursos de gestão de incidentes de segurança graves funcionam com os recursos de produto de resposta a incidentes de segurança existentes. Isso inclui a capacidade de	• CISO • Analista de segurança da informação • Gerente de operações de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Aplicação	Descrição	Usuários
	um analista de segurança escalar um incidente de segurança padrão para um incidente de segurança grave, para que os novos recursos do produto estejam disponíveis para oferecer suporte ao processo de correção. Rastreie o andamento do incidente de segurança grave (MSI) da descoberta à análise. Propor soluções, promover e vincular incidentes de segurança e fechamento.	• Engenheiro de operações DE TI • Responsável pelo serviço (persona do responsável pela correção) • conselho Geral
Data Loss Prevention Incident Response	A Resposta a incidentes de prevenção contra perda de dados (DLP IR) permite revisar e gerenciar o fluxo de trabalho de correção de incidentes de DLP de várias origens, como endpoint, rede, e-mail e nuvem. Com a aplicação DLP, você pode identificar, responder e proteger seus canais de perda de dados.	• CISO • Analista de segurança da informação • Gerente de operações de segurança
Inteligência contra ameaças	Permite que as equipes de resposta a incidentes automatizem pesquisas, pesquisas e correlação de ameaças. A integração com o MITRE ATT&CK permite medir e entender a cobertura de detecção e mitigação e ajuda na busca de ameaças.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças
Centro de segurança de inteligência contra ameaças (TISC)	Agregue, organize e gerencie a inteligência contra ameaças de várias fontes e conduza a gestão de casos de inteligência contra ameaças. Rastreie campanhas, operacionalize a inteligência contra ameaças e responda à inteligência acionável.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que explorar a seguir

Selecione um bloco para começar a usar Operações de segurança Espaços de trabalho.

Espaço de resposta a incidentes de segurança



Saiba mais sobre o Espaço de resposta a incidentes de segurança

Espaço para gerentes de vulnerabilidades



Saiba mais sobre o Espaço do gerenciador de vulnerabilidades

Espaço de controle de postura de segurança



Saiba mais sobre o Espaço de controle de postura de segurança

Espaço de avaliação de vulnerabilidade



Saiba mais sobre o Espaço de avaliação de vulnerabilidades

Espaço de correção de TI



Saiba mais sobre o Espaço de correção de TI

Espaço da lista de materiais do software



Saiba mais sobre o Espaço de lista de materiais do software

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Solucionar problemas e obter ajuda

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

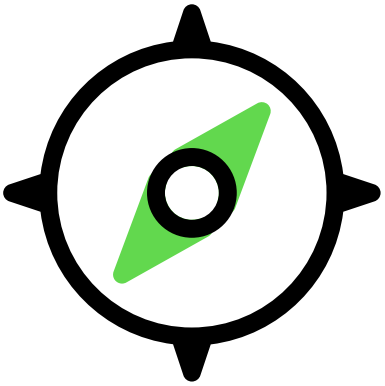
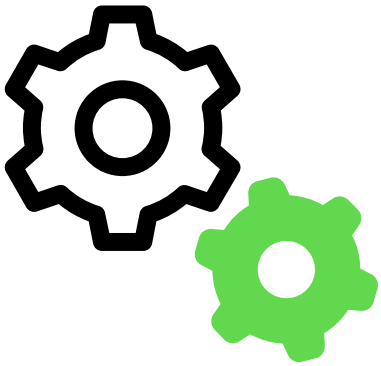
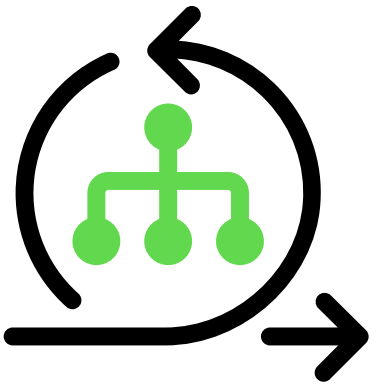
Now Assist para Resposta a incidentes de segurança

Os analistas de segurança podem usar fluxos de trabalho inteligentes e. ServiceNow Habilidades de IA generativa para ajudá-los a resolver incidentes de segurança. Os gerentes de segurança podem revisar o contexto de incidentes de segurança e anotações de fechamento rapidamente em um formato conciso e fácil de ler, exiba dados de análise pós-incidente e veja as etapas de correção recomendadas com Now Assist para Resposta a incidentes de segurança aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

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

Importante:

- Nem todos os provedores de modelos estão disponíveis para clientes com SKUs no país, e alguns produtos/recursos do Now Assist estão indisponíveis no momento para clientes no país. Para obter mais informações, consulte KB1584492 artigo na Base de conhecimento do Now Support. Certifique-se de verificar se há atualizações de disponibilidade do provedor de modelos em versões futuras.
- Alguns Now Assist No momento, os produtos/recursos não estão disponíveis para clientes nos datacenters protegidos pelo FedRAMP, NSC DOD IL5 ou IRAP da Austrália, clientes auto-hospedados ou em outros ambientes restritos. Para obter mais informações, consulte o artigo KB0743854 na Now Support Base de conhecimento. Certifique-se de verificar se há atualizações de disponibilidade em versões futuras.
- Alguns Now Assist no momento, os produtos/recursos estão disponíveis somente para clientes em algumas regiões. Certifique-se de verificar se há atualizações de disponibilidade em versões futuras.

Solucionar problemas e obter ajuda

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

Limitações de IA

Esta aplicação usa inteligência artificial (IA) e aprendizado de máquina, que são campos de estudo em rápida evolução que geram previsões com base em padrões de dados. Como resultado, esta aplicação nem sempre produz informações precisas, completas ou

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

apropriadas. Além disso, não há garantia de que esta aplicação tenha sido totalmente treinada ou testada para o seu caso de uso. Para mitigar esses problemas, é sua responsabilidade testar e avaliar o uso desta aplicação quanto à precisão, dano e adequação para seu caso de uso, empregar supervisão humana da saída e evitar depender exclusivamente de saídas geradas por IA para fins de tomada de decisão. Isso é especialmente importante se você optar por implantar esta aplicação em áreas com impactos importantes, como saúde, finanças, jurídico, emprego, segurança ou infraestrutura. Você concorda em cumprir Política de uso aceitável de IA da ServiceNow , Que pode ser atualizado pela ServiceNow.

Processamento de dados

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

Coleta de dados

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

Para obter mais informações, consulte Documentação do Now Assist .

Explorando Now Assist para Resposta a incidentes de segurança

Seus analistas de segurança podem usar fluxos de trabalho inteligentes e. ServiceNow Habilidades de IA generativa para ajudá-los a fazer a triagem, investigar e fechar incidentes de segurança no fluxo de trabalho com o. Now Assist para Resposta a incidentes de segurança aplicação.

Visão geral Now Assist para Resposta a incidentes de segurança

Com habilidades de IA generativa e fluxos de trabalho do agente, seus analistas de segurança têm a opção de:

- Resuma os detalhes do incidente de segurança e revise o contexto rapidamente em um formato conciso e fácil de ler.
- Gere as próximas etapas recomendadas para um incidente de segurança.
- Gerar dados de análise pós-incidente.
- Gerar anotações de fechamento.
- Gerar informações de correlação

Os analistas de segurança podem compartilhar descobertas, detalhes de incidentes e anotações de fechamento com outros analistas, gerentes e principais partes interessadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Now Assist para Resposta a incidentes de segurança usuários

Usuários

Usuário	Descrição
Analistas e gerentes de segurança	Visualize os detalhes do incidente de segurança, veja o possível impacto e exiba as principais ações de correção já realizadas com resumos de incidentes de segurança usando IA generativa. Resumos e próximas etapas recomendadas (ações) dê aos analistas e gerentes uma vantagem inicial com suas investigações e ajude a encerrar incidentes de segurança. Gere automaticamente um rascunho de anotações de fechamento usando a IA generativa. As anotações de fechamento para incidentes de segurança são criadas rapidamente com base nas atividades de correção e contenção, além de outros detalhes relevantes relacionados ao fechamento.

Benefícios do Now Assist para Resposta a incidentes de segurança

Recursos do Now Assist para Resposta a incidentes de segurança

Benefício	Recurso	Usuários
Agilize a triagem de incidentes de segurança com fluxos de atividades longos, revisando anotações de trabalho e informações contextuais rapidamente em um formato conciso e fácil de ler.	Gere resumos de incidentes de segurança que incluem as seguintes informações: • Ocorrência • Detalhes • Observações • Principais ações realizadas • Detalhes do fechamento	• Analistas de segurança • Gerentes de segurança
Gere automaticamente um rascunho de anotações de fechamento para um incidente de segurança quando ele estiver pronto para fechamento. Os analistas podem modificar qualquer conteúdo gerado pela habilidade de IA editando-o, removendo-o ou adicionando suas próprias anotações antes de fechar o incidente de segurança.	Gerar anotações de fechamento de incidente de segurança	• Analistas de segurança • Gerentes de segurança
Gere as próximas etapas recomendadas no fluxo de trabalho mediante solicitação para ajudar você a fechar um incidente de segurança.	Gerar ações recomendadas de incidente de segurança	• Analistas de segurança • Gerentes de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos do Now Assist para Resposta a incidentes de segurança

Benefício	Recurso	Usuários
Gere uma análise pós-incidente que inclua uma análise de causa raiz, avaliação de impacto e lições aprendidas no fluxo de trabalho de fechamento de um incidente de segurança.	Gerar análise pós-incidente	• Analistas de segurança • Gerentes de segurança
Conecte incidentes atuais a eventos anteriores que envolvem os mesmos usuários afetados, itens de configuração (ICs) ou observáveis.	Gerar informações de correlação	• Analistas de segurança • Gerentes de segurança
Saiba mais sobre os detalhes de um incidente de segurança rapidamente acessando resumos e anotações de fechamento do Now Assist painel.	Acesse o resumo da IA generativa e as anotações de fechamento do Now Assist painel. Digite solicitações de informações mais básicas sobre incidentes de segurança no painel.	• Analistas de segurança • Gerentes de segurança
Personalize as habilidades de IA generativa para resumos e anotações de fechamento para atender às suas necessidades.	Copie uma habilidade e modifique os campos da tabela relacionada selecionada, defina a disponibilidade da habilidade e escolha onde a habilidade será exibida.	administrador

O que explorar a seguir

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

- Configuração da Now Assist para Resposta a incidentes de segurança
- Resuma um incidente de segurança com Now Assist para Resposta a incidentes de segurança
- Gere anotações de fechamento para um incidente de segurança com Now Assist para Resposta a incidentes de segurança
- Gere informações de correlação no Now Assist painel com Now Assist para Resposta a incidentes de segurança
- Gere ações recomendadas para um incidente de segurança com Now Assist para Resposta a incidentes de segurança
- Gere uma análise pós-incidente para um incidente de segurança com Now Assist para Resposta a incidentes de segurança
- Entradas e gatilhos do Now Assist para Resposta a incidentes de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações de suporte para Now Assist para Resposta a incidentes de segurança

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

Versões com suporte

Versão 2.0.1 de Now Assist para Resposta a incidentes de segurança compatível com:

- legado IU (UI16): Resposta a incidentes de segurança aplicação principal, v13.6.4
- Espaço de resposta a incidentes de segurança(Espaço SIR v1.7.0
- Now Assist para ServiceNow AI Platform® v6.0.1

Interfaces do usuário compatíveis

. Now Assist para Resposta a incidentes de segurança Inclui as habilidades de IA generativa listadas na tabela a seguir.

Now Assist para Resposta a incidentes de segurança interfaces e habilidades compatíveis

Interface	Recursos
Resposta a incidentes de segurança	• Resumo do incidente de segurança. • Geração de próximas etapas recomendadas para um incidente de segurança. • Geração de análise pós-incidente que inclui análise de causa raiz, avaliação de impacto e lições aprendidas. • Now Assist painel. • Geração de anotações de fechamento. • Informações de correlação do Now Assistpainel.
Legado UI16	• Resumo do incidente de segurança • Geração de próximas etapas recomendadas para um incidente de segurança. • Geração de análise pós-incidente que inclui análise de causa raiz, avaliação de impacto e lições aprendidas. • Now Assist painel. • Geração de anotações de fechamento. • Informações de correlação do Now Assistpainel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração da Now Assist para Resposta a incidentes de segurança

. Now Assist para Resposta a incidentes de segurança a aplicação é compatível com Espaço de resposta a incidentes de segurança e no legado IU principal (UI16). Você pode usar a configuração assistida no Administração do Now Assist console a ser configurado Now Assist para Resposta a incidentes de segurança.

Visão geral da configuração

Compartilhando dados com ServiceNow® Programa de desenvolvimento de IA, você fornece dados relevantes para ajudar a melhorar a precisão da previsão, a experiência do usuário, personalizar produtos de acordo com suas necessidades de negócios e reduzir alucinações para seu ativado Now Assist habilidades.

Você pode optar por recusar um ServiceNow instância do compartilhamento de dados do Administração do Now Assist console se você não quiser participar. Consulte Recusar o compartilhamento de dados para Now Assist . Repita o processo de recusa para todas as instâncias que usam Now Assist funcionalidade.

Use o console do Administração do Now Assist para configurar Now Assist para Resposta a incidentes de segurança. Este console contém tudo o que você deve instalar os aplicativos e configurar as habilidades de IA generativa. Para obter informações adicionais, confira Configurando Now Assist configurações e recursos .

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

Now Assist para Resposta a incidentes de segurança recursos e habilidades no Administração do Now Assist console

Produto Now Assist Technology	Habilidades em incidentes de segurança
Now Assist para Resposta a incidentes de segurança	Resumo do incidente de segurança **Nota:** O resumo de incidentes oferece suporte a incidentes de segurança em qualquer estado diferente de **Rascunho** .
	Geração de anotações de resolução.
	Ações recomendadas de incidente de segurança A habilidade Ações recomendadas de incidente de segurança oferece suporte a incidentes de segurança em qualquer estado diferente de **Encerrado** e. **Cancelado** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Now Assist para Resposta a incidentes de segurança recursos e habilidades no Administração do Now Assist console

Produto Now Assist Technology	Habilidades em incidentes de segurança
	Nota: A aplicação Pesquisa com IA deve ser habilitada para que a habilidade Ações recomendadas funcione para incidentes de segurança. Para verificar se a Pesquisa com IA está habilitada em sua instância, navegue até **Tudo** > **Pesquisa com IA** > **Status da Pesquisa com IA**. Se a página indicar que a Pesquisa com IA não está habilitada, entre em contato com o suporte. As informações de correlação oferecem suporte a incidentes de segurança em todos os estados.
	Geração de análise pós-incidente

1. Instalar plug-ins de Now Assist .

   Instale o. Now Assist para Resposta a incidentes de segurança aplicação (sn_sec_gen_ai) e. Resposta a incidentes de segurança Principais [sn_si] aplicações.

2. Configure e ative uma habilidade para Now Assist para Resposta a incidentes de segurança

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

Usando Configuração assistida para implementar Now Assist para Resposta a incidentes de segurança

Configuração assistida fornece uma sequência de tarefas que ajudam você a configurar Now Assist para Resposta a incidentes de segurança em seu ServiceNow instância. Para abrir o. Configuração assistida para Now Assist para Resposta a incidentes de segurança, navegue até **Tudo** > **Administrador do Now Assist** > **Recursos**.

Para mais informações, consulte Configure e ative uma habilidade para Now Assist para Resposta a incidentes de segurança.

Configure e ative uma habilidade para Now Assist para Resposta a incidentes de segurança

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

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Administrador do Now Assist** > **Recursos**.
2. Com **Tecnologia** selecionado no painel de navegação, selecione **Operações de segurança** da lista.
   Estas habilidades de Incidente de segurança são exibidas no cartão Incidente de segurança:
   - Ações recomendadas de incidente de segurança

     A aplicação Pesquisa com IA deve ser habilitada para que a habilidade Ações recomendadas funcione para incidentes de segurança. Para verificar se a Pesquisa com IA está habilitada em sua instância, navegue até **Tudo** > **Pesquisa com IA** > **Status da Pesquisa com IA**. Se a página indicar que a Pesquisa com IA não está habilitada, entre em contato com o suporte.
   - Análise pós-incidente
   - Geração de informações de correlação
   - Resumo do incidente de segurança
   - Geração de anotações de resolução
3. Selecione **Exibir detalhes**.
   Não é possível editar as habilidades incluídas com a aplicação. Para editar as configurações padrão, você deve fazer uma cópia. Para obter mais informações sobre como personalizar uma habilidade, consulte Personalizar uma habilidade do Now Assist para Resposta a incidentes de segurança.
4. Selecione **Ativar habilidade** para a habilidade que você deseja.
5. Siga as etapas para configurar e ativar uma habilidade usando Configuração assistida.

   Nota: Algumas habilidades não exigem todas as etapas de configuração listadas abaixo. Selecione as únicas tarefas exibidas no painel esquerdo e siga as instruções. Depois de concluir as tarefas, ative a habilidade.

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

      Ou todos os seguintes os modelos de entrada para a habilidade são listados: **Trabalho em andamento** , **Revisão** e **Encerrado** . . **Trabalho em andamento** o modelo está selecionado.

      Você pode preferir deixar esses modelos de entrada em suas configurações padrão até se familiarizar com como as habilidades para Now Assist para Operações de segurança trabalho.

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

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Salve e continue** para ir para a próxima etapa em Configuração assistida.
7. **Opcional:** Teste o prompt em um registro de incidente de segurança.
8. Selecione **Salve e continue** para ir para a próxima etapa em Configuração assistida.
9. **Opcional:** Escolha uma das seguintes opções para definir a disponibilidade.

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

10. Selecione **Salve e continue** para ir para a próxima etapa em Configuração assistida.
11. Escolha **Selecione exibir** para determinar onde você deseja exibir a habilidade.

Opção	Descrição
No produto	Now Assist as habilidades são exibidas em formulários e espaços de trabalho.
Funções de usuário	Selecione o ícone Expandir ( )
Painel do Now Assist	Now Assist as habilidades estão disponíveis em Now Assist painel. **Nota:** Se você não vir esta opção, deverá ativar o painel do Now Assist. Para obter mais informações, consulte Ligue o. Now Assist painel . As ações recomendadas de incidente de segurança e as habilidades de análise pós-incidente não estão disponíveis no Now Assist painel.

12. Selecione **Salvar e continuar** para prosseguir para a próxima etapa.
13. **Opcional:** Adicionar ou remover funções.

    (Optional) Por padrão, as funções sn_si.analyst e sn_si.manager são adicionadas e podem ver os resultados da geração automatizada de habilidades. Você poderá adicionar ou remover funções somente se você Personalizar uma habilidade do Now Assist para Resposta a incidentes de segurança.

14. Revise suas escolhas e selecione **Ativar** para concluir a configuração da habilidade.
15. Selecione **Retornar ao Incidente de segurança** .
    A habilidade é exibida na seção Habilidades ativas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Personalizar uma habilidade do Now Assist para Resposta a incidentes de segurança

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

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Tudo** > **Administrador do Now Assist** > **Recursos** . Administração do Now Assist console.
2. Com **Tecnologia** selecionado no painel de navegação, selecione **Operações de segurança** da lista. Estas habilidades de incidente de segurança são exibidas:
   - Ações recomendadas de incidente de segurança
   - Análise pós-incidente
   - Geração de informações de correlação
   - Resumo do incidente de segurança
   - Geração de anotações de resolução
3. Crie uma cópia de uma habilidade e personalize os campos de entrada.

   a. No cartão Recurso de incidente de segurança, selecione **Exibir detalhes** .

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

   c. Selecione **Faça uma cópia** .

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

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

   f. Prossiga para a próxima etapa selecionando **Salve e continue** .

   g. Selecione **Escolha a entrada** .

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

   Você pode configurar alguns dos campos da tabela de entrada de base, as condições e as listas relacionadas para os modelos. Selecione Somente a partir das tabelas relacionadas compatíveis com as listas para seus dados de entrada.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

i. Prossiga para a próxima etapa em Configuração assistida Para o modelo Trabalho em andamento, selecionando **Salve e continue** .

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

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

- **Selecione exibir** :

Opção	Descrição
No produto	Mostre o resumo do incidente de segurança em todos os produtos de segurança. Now Assist as habilidades são exibidas em formulários e espaços de trabalho.
Funções de usuário	Selecione o ícone Expandir ( )
Painel do Now Assist	Now Assist as habilidades estão disponíveis em Now Assist painel. **Nota:** Se você não vir esta opção, deverá ativar o painel do Now Assist. Para obter mais informações, consulte Ligue o. Now Assist painel .

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

k. Selecione o modelo Revisar.

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

m. Selecione **Salve e continue** para prosseguir para a próxima etapa em Configuração assistida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

o. Selecione **Revise e ative** para revisar sua habilidade e fazer modificações adicionais.

4. Selecione **Ativar**.
   Sua habilidade é exibida na página Incidente de segurança na seção Todas as habilidades de incidente de segurança disponíveis.
5. Selecione **Ativar habilidade** .

Entradas e gatilhos para Now Assist para Resposta a incidentes de segurança

Você pode configurar algumas das entradas ou gatilhos para uma habilidade de IA generativa. Entradas ou gatilhos permitem determinar como e quando uma habilidade é usada.

Entradas e gatilhos

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

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

Habilidade de resumo de incidentes de segurança

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

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident].
Campos de entrada	• Descrição resumida • Descrição • Estado • Prioridade • Anotações de trabalho • Comentários adicionais
Tabelas de entrada relacionadas	• ICs afetados - Item de configuração • Usuários afetados - Usuários • Resposta a incidentes de segurança Tarefa - Descrição resumida

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entrada	Descrição
	• Estado - Qualquer estado diferente de **Cancelado** . • Observáveis associados - A descoberta do observável é mal-intencionada ou suspeita.

Habilidade de geração de anotações de resolução

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

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

Habilidade de geração de ações recomendadas de incidente de segurança

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident].

Habilidade de geração de análise pós-incidente

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident].

Habilidade de geração de informações de correlação

Suas informações de correlação para um incidente de segurança podem conter registros das tabelas a seguir, mas você deve ter permissão para acessar essas tabelas e registros.

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident]. Tabela Item de configuração [cmdb_ci]. Tabela Incidente [incidente].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entrada	Descrição
	Tabela Solicitação de mudança [change_request]. Tabela Problema [Problema]. Tabela Item vulnerável [sn_vul_vulnerable_item]. Associar tabela Observable [sn_ti_observable].

Usando Now Assist para Resposta a incidentes de segurança para fechar incidentes de segurança

Os analistas de segurança podem fechar incidentes de segurança rapidamente de dentro do fluxo de trabalho com as habilidades de IA generativa compatíveis com Now Assist para Resposta a incidentes de segurança.

Visão geral do Now Assist para Resposta a incidentes de segurança

Com habilidades de IA generativa com Now Assist para Resposta a incidentes de segurança seus analistas de segurança têm a opção de:

- Resuma os detalhes do incidente de segurança e revise o contexto rapidamente em um formato conciso e fácil de ler.
- Gerar anotações de fechamento (resolução).
- Gere ações recomendadas para um incidente de segurança
- Gerar dados de análise pós-incidente
- Gere informações de correlação para acelerar a investigação de incidentes.

Gerentes e analistas de segurança podem solicitar resumos de incidentes de segurança e anotações de fechamento dos seguintes locais:

- Registros de incidentes de segurança
- Resposta a incidentes de segurança Espaço
- . Now Assist painel.

> **Nota:** As ações recomendadas de incidente de segurança e as habilidades de análise pós-incidente não estão disponíveis no Now Assist painel.

Os gerentes e analistas de segurança podem gerar as próximas etapas recomendadas e dados de análise pós-incidente dos seguintes locais:

- Registros de incidentes de segurança
- Resposta a incidentes de segurança Espaço

Gerentes e analistas de segurança podem criar tarefas de correção a partir de ações recomendadas geradas somente de incidentes de segurança no Resposta a incidentes de segurança Espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Resuma um incidente de segurança com Now Assist para Resposta a incidentes de segurança

   Gere um resumo de um incidente de segurança que inclua o problema subjacente, detalhes do incidente, dados de listas relacionadas (observáveis) e ações-chave já realizadas.

2. Gere ações recomendadas para um incidente de segurança com Now Assist para Resposta a incidentes de segurança
3. Gere uma análise pós-incidente para um incidente de segurança com Now Assist para Resposta a incidentes de segurança
4. Gere informações de correlação no Now Assist painel com Now Assist para Resposta a incidentes de segurança
5. Gere anotações de fechamento para um incidente de segurança com Now Assist para Resposta a incidentes de segurança

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

6. Solicite habilidades de IA generativa no Now Assist painel para Now Assist para Resposta a incidentes de segurança

   Gere resumos e anotações de fechamento do Now Assist painel.

   Nota: As ações recomendadas de incidente de segurança e as habilidades de análise pós-incidente não estão disponíveis no Now Assist painel.

7. Personalizar uma habilidade do Now Assist para Resposta a incidentes de segurança

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

Resuma um incidente de segurança com Now Assist para Resposta a incidentes de segurança

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

Antes de Iniciar

Você pode resumir um incidente de segurança no legado IU principal (UI16) e no Espaço de resposta a incidentes de segurança. Deve haver um mínimo de 50 palavras nos campos que são usados para os dados de entrada para resumir um incidente usando IA generativa. Para obter mais informações sobre os campos de entrada, consulte Entradas e gatilhos para Now Assist para Resposta a incidentes de segurança.

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Procedimento

1. Em legado IU principal, navegue até **Tudo** > **Incidente de segurança** > **incidentes** e abra um incidente de segurança atribuído a você.
2. Como alternativa, navegue até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
3. Em **Visão geral** , selecione **Resumir** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O resumo gerado é exibido em uma faixa na parte superior do registro de incidente de segurança em legado UI16 principal.
- O resumo gerado é exibido no **Visão geral** no Espaço de resposta a incidentes de segurança.

4. **Opcional:** Depois que o resumo for gerado, selecione uma das seguintes opções.

(Optional) Os resumos gerados pela IA podem perder detalhes importantes. Antes de prosseguir, você pode preferir revisar o resumo quanto à precisão e integridade.

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

Gere anotações de fechamento para um incidente de segurança com Now Assist para Resposta a incidentes de segurança

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

Antes de Iniciar

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se os campos Código de fechamento ou Anotações de fechamento já estiverem atualizados para um incidente de segurança, o Now Assist não modificará esses campos, independentemente do estado atual do incidente. Para habilitar o Now Assist para atualizar esses campos, certifique-se de que os campos Código de fechamento e Anotações de fechamento sejam deixados em branco.

Procedimento

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

Opção	Descrição
Feche o incidente de segurança em legado UI16 principal	**a.** Mude **Estado** campo para **Encerrado** . O modal de fechamento é exibido. **b.** Clique em **Anotações de encerramento** seção. As anotações de encerramento serão geradas automaticamente se não houver texto, ou você pode modificar o texto existente conforme necessário es–colhendo a opção necessária no NACM. **Nota:** Revise o texto gerado e certifique-se de que ele seja preciso antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias. Você também pode **Elaborar** ou **Encurtar** o texto gerado. **c.** Selecione a opção necessária no menu de contexto do Now Assist. **Elaborar** ajudará você a elaborar o texto e substitui o texto de resolução selecionado. Se você quiser encurtar o texto de resolução, selecione **Encurtar** Opção do menu de contexto para tornar o texto mais conciso. **d.** Atualize o código de fechamento e selecione **Fechar incidente** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

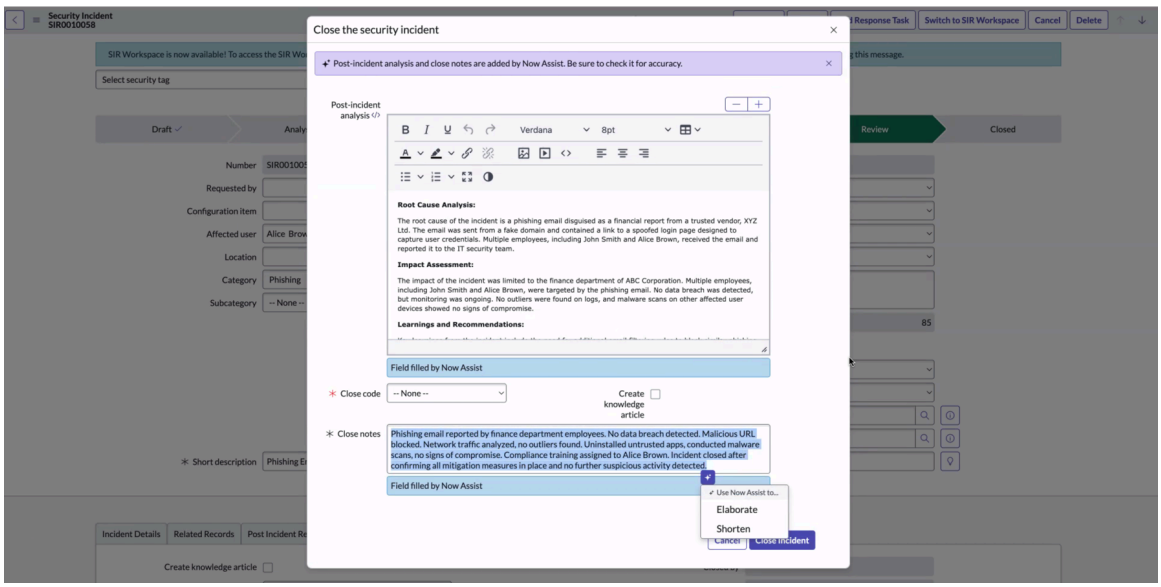
Opção	Descrição
	O resumo da resolução é exibido na seção Informações de resolução no registro de incidente de segurança. **Nota:** Usando o menu de contexto do Now Assist, você pode adicionar ou gerar diretamente as anotações de resolução no **Anotações de encerramento** no próprio registro de incidente, quando o incidente está em **Revisão** estado. Para obter mais informações, consulte a captura de tela abaixo.
Feche o incidente de segurança do Espaço de resposta a incidentes de segurança	**a.** Em **Detalhes** do espaço, altere **Estado** campo para **Encerrado** . O modal de passo é exibido. **b.** Revise cada etapa e selecione **Próximo** . **c.** Selecione **Forneça detalhes da resolução** **d.** Clique em **Anotações de encerramento** seção. As anotações de fechamento serão geradas automaticamente se não houver texto, ou você poderá modificar o texto existente conforme necessário usando as opções do NowAssist. **Nota:** Revise o texto gerado e certifique-se de que ele seja preciso antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias. Você também pode **Elaborar** ou **Encurtar** o texto gerado. **e.** Selecione a opção necessária no menu de contexto do Now Assist. **Elaborar** ajudará você a elaborar o texto e substitui o texto de resolução selecionado. Se você quiser encurtar o texto de resolução, selecione **Encurtar** Opção do menu de contexto para tornar o texto mais conciso. **f.** Atualize o código de fechamento e selecione **Fechar incidente** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	O resumo da resolução é exibido no **Detalhes** no registro de incidente de segurança no espaço. **Nota:** Usando o menu de contexto do Now Assist, você pode adicionar ou gerar diretamente as anotações de resolução no **Anotações de encerramento** no próprio registro de incidente, quando o incidente está em **Revisão** estado. Para obter mais informações, consulte a captura de tela abaixo.

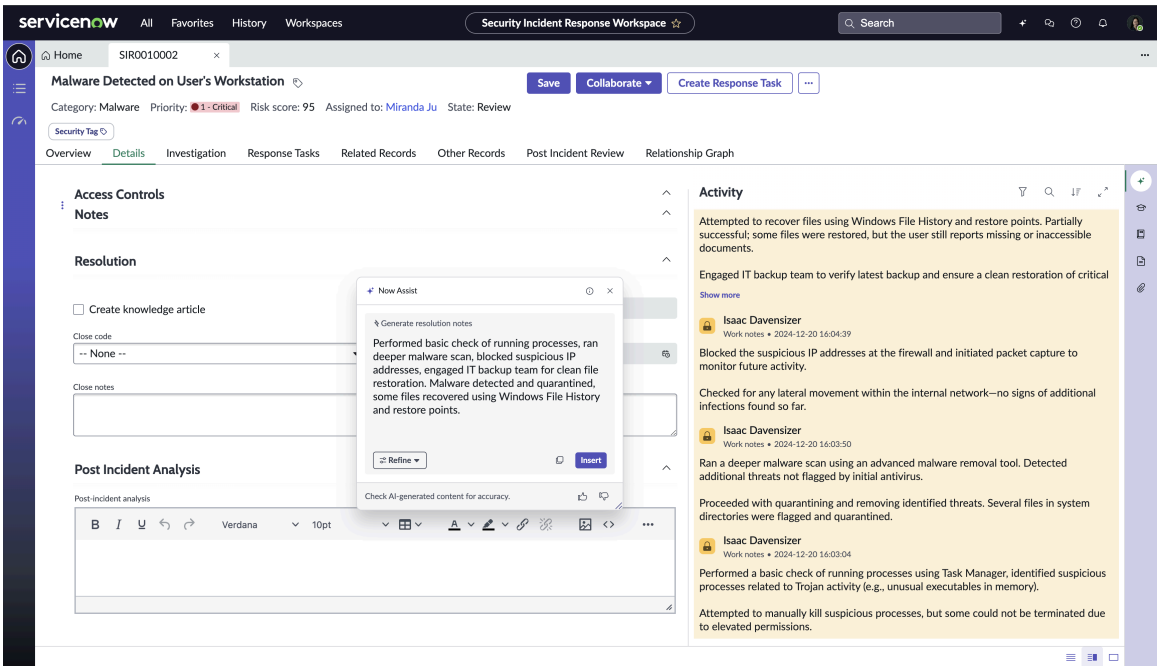
A captura de tela a seguir descreve as anotações de resolução geradas para fechar o incidente de segurança no Core UI16.



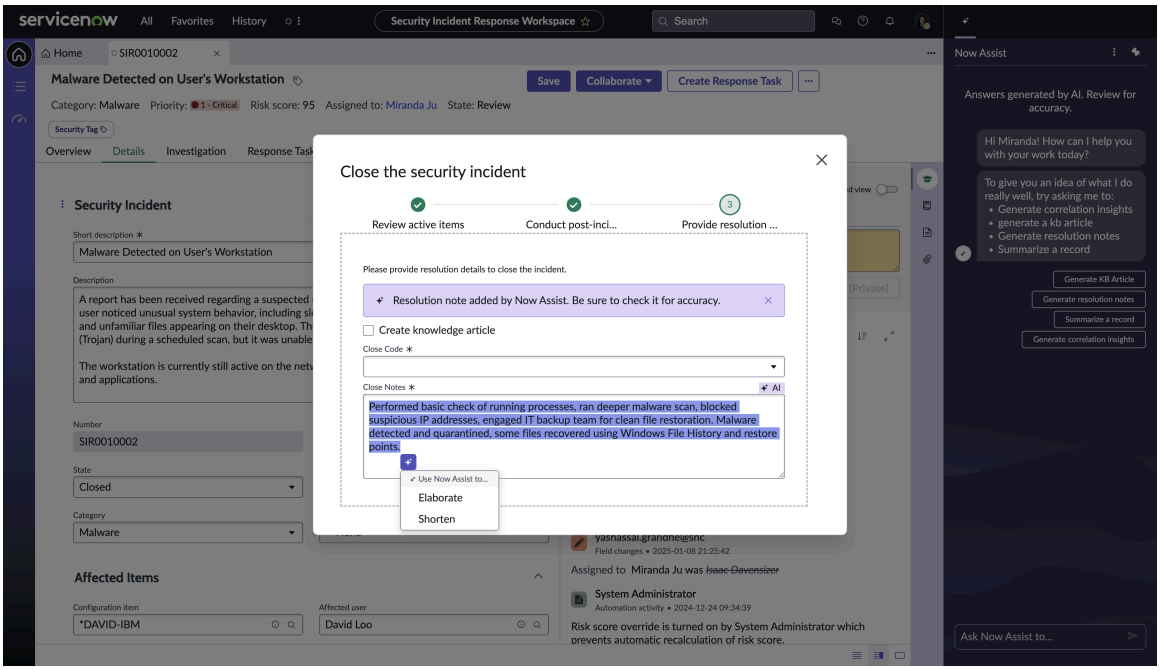
Anotações de resolução geradas automaticamente no Espaço de resposta a incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Edite as anotações de resolução geradas usando o menu de contexto do Now Assist no espaço Resposta do incidente de segurança.



Gere ações recomendadas para um incidente de segurança com Now Assist para Resposta a incidentes de segurança

Gere automaticamente as próximas etapas que seus analistas podem executar para ajudá-los a fechar um incidente de segurança no Espaço de resposta a incidentes de segurança. As etapas recomendadas são baseadas em incidentes de segurança e artigos de conhecimento existentes.

Antes de Iniciar

As próximas etapas recomendadas funcionam para incidentes de segurança ativos em qualquer estado diferente de **Encerrado** ou **Cancelado** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A aplicação Pesquisa com IA deve ser habilitada para que a habilidade Ações recomendadas funcione para incidentes de segurança. Para verificar se a Pesquisa com IA está habilitada em sua instância, navegue até **Tudo** > **Pesquisa com IA** > **Status da Pesquisa com IA**. Se a página indicar que a Pesquisa com IA não está habilitada, entre em contato com o suporte.

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
2. Selecione **Ações recomendadas** ícone ( ) na barra lateral contextual.



3. Selecione **Obter recomendações** .
4. No modal Verificar conteúdo gerado por IA, selecione **Reconheço** .
   As ações recomendadas geradas são exibidas em cartões. Até quatro referências para as ações são exibidas na parte superior. Essas referências podem ser qualquer combinação de artigos de conhecimento (KB) ou incidentes de segurança (nº SIR).
5. Em um cartão, escolha um.

Opção	Descrição
Exibir detalhes	Exiba os detalhes desta ação de correção.
Salvar nas anotações de trabalho	Revise as anotações de trabalho e tenha a opção de editá-las antes de salvá-las nas anotações de trabalho do incidente de segurança.
Selecione um link de referência	Exiba o incidente de segurança ou o artigo de conhecimento usado como as origens dessas ações.

6. **Opcional:** Selecione o ícone de atualização no painel Ações recomendadas para gerar novamente as ações recomendadas.

   As ações recomendadas permanecem em cache por uma hora. Você pode optar por atualizar as etapas recomendadas se:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você acredita que as informações relacionadas ao incidente de segurança mudaram desde a última vez que gerou as ações.
- Você sai da página, faz logout, faz login novamente e retorna em uma hora ao incidente de segurança.

Você deve gerar novamente as ações a partir da etapa 3 para exibi-las após uma hora.

7. Selecione **Criar tarefa de resposta** em um cartão.
   Uma nova guia é aberta no espaço . . **Descrição resumida** e o. **Descrição** os campos são preenchidos automaticamente a partir dos detalhes no cartão de ação recomendada que você selecionou.
8. Edite o formulário conforme necessário e selecione **Salvar** para criar a tarefa de resposta.
   Até que você mude o valor na propriedade do sistema, as duas opções em todas as ações recomendadas geradas permanecerão **Exibir detalhes** e. **Criar tarefa de resposta** .
9. **Opcional:** Crie uma tarefa de resposta a partir das ações recomendadas.
   Por padrão, o fluxo de trabalho fornece a opção de salvar as ações recomendadas em anotações de trabalho dos cartões. Se você quiser ter a opção de criar uma tarefa de resposta a partir de um cartão de ação em vez de salvá-la em anotações de trabalho, altere o campo Valor do **Ação recomendada de SecOps** propriedade do sistema [sn_sec_ra.card_action_config].

   a. Como um usuário com a função de Gerenciador de incidentes de segurança [sn_si.manager], navegue até sys_properties.LIST.

   b. Localize a propriedade do sistema Ação recomendada de SecOps [sn_sec_ra.card_action_config] e abra o registro.

   c. Altere o valor de `share_to_work_notes . create_task` .

   d. Salve o registro.

   e. Retorne ao registro de incidente de segurança e atualize a página.
   Os cartões de ação fornecem as opções para **Exibir detalhes** e. **Criar tarefa de resposta** .

Gere uma análise pós-incidente para um incidente de segurança com Now Assist para Resposta a incidentes de segurança

Gere automaticamente uma análise pós-incidente para um incidente de segurança que inclua uma análise de causa raiz, avaliação de impacto e informações de aprendizado e recomendações.

Antes de Iniciar

Você deve ter a habilidade de análise pós-incidente ativada se quiser que uma análise pós-incidente seja gerada automaticamente por Now Assist para Resposta a incidentes de segurança.

Se as anotações de fechamento já forem preenchidas manualmente antes de fechar o incidente de segurança, este conteúdo não será substituído por Now Assist para Resposta a incidentes de segurança Quando os analistas definem o campo Estado como **Encerrado** .

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Tradução automática

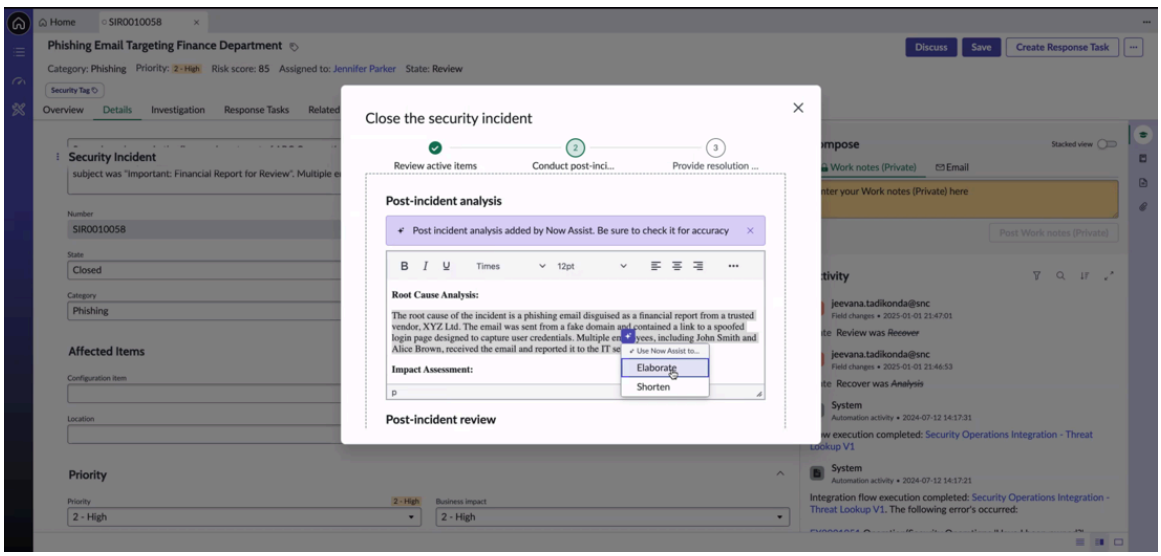
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
2. Em **Detalhes** , selecione **Encerrado** No campo Estado para fechar o incidente de segurança.
   O modal Fechar o incidente de segurança é aberto.
3. **Opcional:** Selecione **Revise tarefas ativas** para revisar todas as tarefas de correção ativas associadas a este incidente.
   Uma nova guia é aberta com registro(s) para sua revisão. Use esta opção para verificar se você está pronto para fechar o incidente de segurança, porque esta ação cancela todos os fluxos de trabalho e atividades associados e fecha o incidente em todas as tarefas de correção associadas.
4. Para gerar a análise pós-incidente, selecione **Próximo** .
   A análise pós-incidente é exibida no modal com três seções. Observe o ícone do Now Assist ( ) indica que o conteúdo é gerado por Now Assist para Resposta a incidentes de segurança.
   - Análise de Causa raiz
   - Avaliação de impacto
   - Aprendizados e recomendações

   Nota: Você pode usar o Menu de contexto do Now Assist em qualquer uma das opções de análise pós-incidente e elaborar ou encurtar a Análise de causa raiz/Avaliação de impacto/aprendizagens e recomendações e substituir o texto. **Elaborar** ajudará você a adicionar mais informações ao texto existente. **Encurtar** tornará o texto selecionado mais conciso.

   A captura de tela a seguir descreve como o Menu de contexto do Now Assist é usado para elaborar ou encurtar e substituir o texto de análise pós-incidente desejado.



5. Revise o relatório para verificar a precisão e fazer as edições necessárias.
6. **Opcional:** Selecione **Fazer avaliação** e. **Configurar/visualizar relatório** para executar a revisão pós-incidente.
   Todas as edições feitas na revisão pós-incidente serão preservadas por uma hora se você sair desta página para fazer a avaliação ou executar outra ação. Após uma hora, você deve definir o Estado como **Encerrado** novamente no incidente para gerar novamente a análise pós-incidente e fechar anotações.
7. Selecione **Próximo** para gerar as anotações de resolução.
   As anotações de resolução são exibidas no campo Anotações de fechamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione um na lista para o Código de fechamento.
9. Selecione **Fechar incidente** .
   A análise pós-incidente é salva no campo Análise pós-incidente na guia Detalhes e na guia Visão geral em Incidentes de segurança no Espaço de resposta a incidentes de segurança.

Explorar informações de correlação com Now Assist para Resposta a incidentes de segurança

Você pode gerar informações de correlação para ajudar a evitar a duplicação da investigação sobre usuários afetados, itens de configuração e observáveis e ajudar a resolver o incidente de segurança no qual está trabalhando mais rapidamente. Você seleciona os critérios de um incidente de segurança no qual deseja basear as informações de correlação.

Gerando informações de correlação no Espaço de resposta a incidentes de segurança

Começando com v 3.0.0 de Now Assist para Resposta a incidentes de segurança gere e exiba informações de correlação e exiba os resultados no Espaço de resposta a incidentes de segurança.

- Anteriormente, se você selecionasse um item de configuração (IC) ou um usuário afetado para basear suas informações, a pesquisa retornaria o usuário afetado primário ou o IC primário associado a um incidente de segurança. Começando com v3.0.0 O agente pergunta a qual IC ou usuário afetado você deseja correlacionar o incidente de segurança com as listas relacionadas.
- Você pode gerar informações de correlação do **Investigação** para um incidente de segurança em qualquer estado no Espaço de resposta a incidentes de segurança.
- Você pode gerar informações para vários itens simultaneamente para **Observáveis associados** , **Itens de configuração** e **Usuários afetados** .
- Os resultados são exibidos em uma caixa de diálogo não modal que você pode redimensionar e mover.
- Seu intervalo de tempo para a pesquisa de correlação é de 30 dias.

> **Nota:** Depois de gerar um observável associado a um incidente de segurança, as informações são armazenadas para esse observável até que você o gere novamente com um intervalo de tempo diferente. Suas informações para o novo intervalo de tempo são exibidas.

A habilidade de geração de informações de correlação deve ser ativada antes que você possa ver **Gerar informações de correlação** . Espaço de resposta a incidentes de segurança. Para obter mais informações, consulte Configure e ative uma habilidade para Now Assist para Resposta a incidentes de segurança.

Gerando informações de correlação a partir do Now Assist painel no Espaço de resposta a incidentes de segurança E na IU (UI16)

A habilidade de geração de informações de correlação deve ser ativada antes que você possa ver **Gerar informações de correlação** . Now Assist painel.

Se você não vir Now Assist, você deve ativá-lo. Para obter mais informações, consulte Ligue o. Now Assist painel .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode gerar informações de correlação a partir de um registro de incidente de segurança em qualquer estado no Espaço de resposta a incidentes de segurança ou em legado IU (UI16).
- Por padrão, as informações de correlação pesquisam registros correspondentes dos últimos 30 dias.
- Você pode localizar e revisar valores do **Item de configuração** , **Usuário afetado** e **Observáveis** filtros de informações de correlação no **Detalhes** no Espaço de resposta a incidentes de segurança Ou nas listas relacionadas Itens de configuração, Usuários afetados e Observáveis em legado IU (UI16).
- Seus critérios de pesquisa e resultados permanecem exibidos em Now Assist até redefinir a conversa. Para redefinir sua conversa, selecione Now Assistícone mais opções () no painel e selecione **Redefinir conversa** .
- Você deve ter acesso às seguintes tabelas para exibir esses registros nas informações de correlação geradas:
  - Tabela Item de configuração [cmdb_ci].
  - Tabela Incidente [incidente].
  - Tabela Solicitação de mudança [change_request].
  - Tabela Problema [Problema].
  - Tabela Item vulnerável [sn_vul_vulnerable_item].
  - Associar tabela Observable [sn_ti_observable].
- Seus resultados de informações de correlação são baseados nas tabelas às quais você tem acesso. Por exemplo, se você quiser exibir itens vulneráveis (VIT) em seus resultados de informações de correlação, deverá ter Resposta a vulnerabilidades aplicação instalada e a função de acesso de leitura (sn_vul.read_all).

Para obter as etapas para gerar informações de correlação, consulte Gere informações de correlação no Now Assist painel com Now Assist para Resposta a incidentes de segurança.

Gere informações de correlação do Espaço de resposta a incidentes de segurança com Now Assist para Resposta a incidentes de segurança

Gerar e exibir informações de correlação no Espaço de resposta a incidentes de segurança para ajudar você a conectar eventos anteriores ao incidente de segurança em que você está trabalhando.

Antes de Iniciar

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
2. Selecione **Investigação** no registro de incidente de segurança.
3. Selecione um ou mais filtros nos quais você deseja basear suas informações de correlação.

   Você pode selecionar mais de um observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Observáveis associados** : Registros vinculados por observáveis compartilhados que sugerem possíveis ataques contínuos ou uso repetido de infraestrutura mal-intencionada. Os exemplos podem incluir endereços IP, URLs ou hashes de arquivo.
- **Itens de configuração** (IC): Registros que têm os mesmos ICs para ajudar você a identificar possíveis vulnerabilidades em sistemas específicos. Um exemplo pode ser os laptops dos usuários.
- **Usuários afetados** Incidentes passados que têm os mesmos usuários para ajudar você a ver padrões como tentativas frequentes de phishing ou várias tentativas de acesso não autorizado. Um exemplo é o nome de um usuário específico.

Uma lista de itens correspondentes é exibida.

4. Selecione os itens na lista para os quais você deseja gerar informações.
5. Selecione **Gerar informações** .
   Uma caixa de diálogo é aberta. Depois de alguns momentos, suas informações de correlação são exibidas. Você tem as seguintes opções nesta caixa de diálogo:
   - Atualizar informações ( ) - Você pode mudar os itens na lista depois que suas informações iniciais forem geradas e atualizar seus resultados.
   - Expandir (Redimensionar a caixa de diálogo e arrastá-la na página.

   Você tem as seguintes opções para cada entrada de informações de correlação na caixa de diálogo.

   - **Intervalo de tempo de mudança** - Selecione um intervalo de tempo para recarregar a caixa de diálogo com informações correspondentes. Seus resultados para esta entrada serão gerados novamente automaticamente se você selecionar um novo intervalo de tempo. O intervalo de tempo de cada entrada é exibido ao lado da informação, por exemplo, (100 dias 35.35.35.35) .
   - Última geração - A data em que a informação foi gerada pela última vez.
   - Classifique o conteúdo - (e ( ).
   - Cópia - (Copie as informações para a área de transferência.
   - **Compartilhar em anotações de trabalho** - Edite o conteúdo e publique-o nas anotações de trabalho sobre o incidente de segurança.

   As informações de correlação são armazenadas para observáveis quando você as gera pela primeira vez com base no período de pesquisa padrão (30 dias). Essas informações são armazenadas até que você gere novamente informações para os observáveis com um período de pesquisa diferente. Modifique o limite de 30 dias da consulta seguindo estas etapas:

   a. Como um usuário com a função de Gerenciador de incidentes de segurança [sn_si.manager], navegue até sys_properties.LIST.

   b. Localize a propriedade do sistema Período de retrospectiva de correlação [sn_sec_gen_ai.correlation_lookback_period] e abra o registro.

   c. Insira um número em **Valor** campo até 360.

   d. Salve o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Retorne ao registro de incidente de segurança e atualize a página.

f. Gerar informações de correlação. Seus resultados são baseados no novo período de pesquisa.

Gere informações de correlação no Now Assist painel com Now Assist para Resposta a incidentes de segurança

Gere informações de correlação do Now Assist painel para ajudá-lo a conectar eventos anteriores ao incidente de segurança em que você está trabalhando.

Antes de Iniciar

Funções necessárias: sn_si.analyst, sn_si.manager ou sn_si.basic

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
2. Como alternativa, em legado IU (UI16), localize um incidente de segurança na tabela Incidentes de segurança [sn_si_incident] e abra-o.
3. Selecione Now Assistícone ( ) no cabeçalho superior para abrir o. Now Assist painel.
4. Selecione **Gerar informações de correlação** .

   As informações de correlação serão geradas se um ou mais dos seguintes valores puderem ser correspondidos. Os filtros a seguir para basear suas informações são exibidos em Now Assist painel. Somente os filtros que têm correspondências com outros incidentes de segurança são exibidos.

   Nota: Se você não tiver um registro de incidente de segurança aberto, será solicitado que insira o número de um registro de incidente de segurança depois de selecionar **Gerar informações de correlação** .

   - **Item de configuração** (IC): Registros que têm o mesmo IC para ajudar você a identificar possíveis vulnerabilidades em sistemas específicos. Um exemplo pode ser o laptop de um usuário.
   - **Usuário afetado** Incidentes anteriores que têm o mesmo usuário para ajudar você a ver padrões como tentativas frequentes de phishing ou várias tentativas de acesso não autorizado. Um exemplo é o nome de um usuário específico.
   - **Observáveis** : Registros vinculados por observáveis compartilhados que sugerem possíveis ataques contínuos ou uso repetido de infraestrutura mal-intencionada. Os exemplos podem incluir endereços IP, URLs ou hashes de arquivo. Você deve inserir um valor exato para um observável, por exemplo, um hash de arquivo completo.

   Se não houver dados correspondentes para nenhum desses filtros, nenhum será exibido. Você será solicitado a adicionar um desses valores ao incidente de segurança no qual está trabalhando, salvá-lo e redefinir sua conversa no painel e tentar novamente.

5. Para redefinir sua conversa, selecione Now Assistícone do menu mais opções ( ) no painel e selecione **Redefinir conversa** .
6. Selecione um filtro.

   Os resultados correspondentes são exibidos em Now Assist painel.

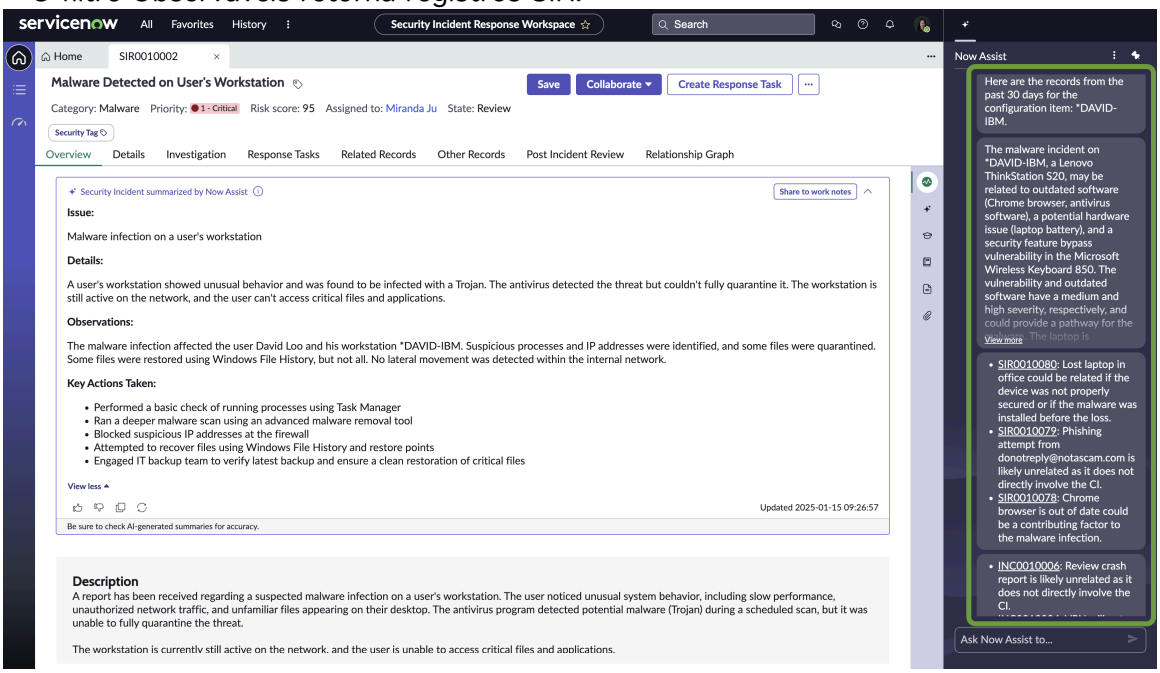
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No exemplo a seguir, **Item de configuração** solicitado. A pesquisa retornou um resumo de alto nível e links para registros que têm um item de configuração correspondente.

Os resultados são agrupados por tipo de registro: Registro de incidente de segurança (SIR), incidente (INC), solicitação de mudança (CHG), problema (PRB) e item vulnerável (VIT).

- O filtro Usuários afetados retorna: Registros SIR, INC e CHG.
- O item de filtro Configuração retorna: Registros SIR, INC, CHG, PRB e VIT.
- O filtro Observáveis retorna registros SIR.



7. **Opcional:** Modifique o limite de 30 dias da consulta seguindo estas etapas:

   a. Como um usuário com a função de Gerenciador de incidentes de segurança [sn_si.manager], navegue até sys_properties.LIST.

   b. Localize a propriedade do sistema Período de retrospectiva de correlação [sn_sec_gen_ai.correlation_lookback_period] e abra o registro.

   c. Insira um número em **Valor** campo até 360.

   d. Salve o registro.

   e. Retorne ao registro de incidente de segurança e atualize a página.

Solicite habilidades de IA generativa no Now Assist painel para Now Assist para Resposta a incidentes de segurança

Solicite um resumo de incidente de segurança ou anotações de fechamento do Now Assist painel.

Antes de Iniciar

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

Funções necessárias: si_analyst, si_manager ou sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login em uma instância em que Now Assist para Resposta a incidentes de segurança a aplicação está instalada.
2. Em legado IU principal, navegue até **Tudo** > **Incidente de segurança** > **incidentes** e abra um incidente de segurança atribuído a você.
3. Como alternativa, navegue até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
4. Selecione o ícone do Now Assist ( ) na faixa superior.

Opção	Descrição
Gerar anotações de resolução	No painel Now Assist, selecione **Gerar anotações de resolução**. As anotações de fechamento geradas no painel são idênticas às geradas quando você fecha um incidente de segurança a partir de um registro. As anotações de fechamento para incidentes de segurança são criadas com base em todas as ações tomadas para correção e contenção, além de outros detalhes relevantes relacionados ao fechamento. **Nota:** Revise o texto gerado e certifique-se de que ele seja preciso antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias. Para obter mais informações, consulte Gere anotações de fechamento para um incidente de segurança com Now Assist para Resposta a incidentes de segurança.
Resumir um incidente de segurança	No painel Now Assist, selecione **Resumir um registro**. O resumo gerado no painel é idêntico ao que você gera a partir de um registro de incidente de segurança. Os resumos gerados pela IA podem perder detalhes importantes. Antes de prosseguir, você pode preferir revisar o resumo quanto à precisão e integridade. Para obter mais informações, consulte Resuma um incidente de segurança com Now Assist para Resposta a incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Gerar informações de correlação	Em Now Assist painel, selecione **Gerar informações de correlação** . Informações de correlação do Now Assist painel para ajudá-lo a conectar eventos anteriores ao incidente de segurança em que você está trabalhando. Para obter mais informações, consulte Explorar informações de correlação com Now Assist para Resposta a incidentes de segurança e Gere informações de correlação no Now Assist painel com Now Assist para Resposta a incidentes de segurança.

Usando fluxos de trabalho do agente de IA no Now Assist para Resposta a incidentes de segurança

Use Resposta a incidentes de segurança Agentes de IA para concluir suas tarefas de forma autônoma.

Fluxos de trabalho do agente disponíveis para agentes de IA para Resposta a incidentes de segurança

Nome do fluxo de trabalho do Agentic	Descrição	Agentes de IA disponíveis
Encerrar incidente de segurança	Este fluxo de trabalho do agente ajuda os analistas de segurança a fechar um incidente de segurança usando linguagem natural no Now Assist painel.	Gerador de encerramento de incidentes de segurança
Analisar métricas de operações de segurança	Este fluxo de trabalho do agente ajuda um gerente do SOC (Security Operations Center, centro de operações de segurança) a analisar o desempenho de seus analistas de segurança. As métricas são geradas para resposta a incidentes de segurança (SIR) Registros para volume de casos, tempo médio de atribuição (MTTA) e tempo médio de resolução (MTTR).	• Agente de IA de recuperação de incidente de segurança • Agente de IA de análise de métricas de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos de trabalho do agente disponíveis para agentes de IA para Resposta a incidentes de segurança

Nome do fluxo de trabalho do Agentic	Descrição	Agentes de IA disponíveis
Resolução do incidente de segurança	Este fluxo de trabalho do agente ajuda os analistas de segurança a identificar um caminho de resolução de incidente de segurança. Este fluxo de trabalho também ajuda os analistas de segurança a fechar um incidente de segurança usando linguagem natural no Now Assist painel.	• Agente de IA de resolução do incidente de segurança • Integração do Exchange Online lidando com agente de IA • Agente de IA do gerador de encerramento de incidentes de segurança • Agente de IA de análise observável • Atividades de incidentes de segurança lidando com agentes de IA
Gerar relatório de entrega de turno SIR	Este fluxo de trabalho do agente adiciona detalhes de um incidente de segurança ao relatório de entrega de turno. O agente preenche as diferentes seções da entrega de turno com o conteúdo apropriado, identificando os detalhes relevantes do incidente de segurança.	Entrega de turno de incidente de segurança Agente de IA

Importante: Por padrão, todos os fluxos de trabalho do agente e registros do agente de IA são somente leitura.

Para modificar um fluxo de trabalho do agentic, você deve primeiro Duplicar um fluxo de trabalho do agentic e prossiga com as seguintes etapas:

- Ative o fluxo de trabalho.
- Ative todos os agentes de IA no fluxo de trabalho.
- Se necessário, você pode adicionar um gatilho para invocar o fluxo de trabalho automaticamente.

Procurando um agente de IA?

- Pode haver agentes de IA instalados com o. Now Assist aplicações que não são usadas em fluxos de trabalho agentivos. Para saber como ver todos os agentes disponíveis em sua instância, consulte Encontre agentes de IA .
- Para encontrar agentes que podem não estar instalados em sua instância, visite AI Agent Marketplace em ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança Fechar fluxo de trabalho do agente de IA do agente de segurança

O fluxo de trabalho Fechar agente de incidente de segurança permite que os analistas de segurança fechem um incidente de segurança.

Fechar visão geral do fluxo de trabalho do agente de incidente de segurança

Usando o fluxo de trabalho Fechar agente de incidente de segurança, cancele as tarefas de resposta associadas, gere anotações de resolução, anotações de encerramento, código de encerramento e análise pós-incidente (PIA) durante o fechamento de um incidente de segurança e forneça feedback e ajuste o conteúdo em linguagem naturaldo Now Assist painel.

Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a versão duplicada do fluxo de trabalho do agentic.

Agente usado no fluxo de trabalho do agente do agente de incidente de segurança encerrado

O especialista do gerador de encerramento de incidentes de segurança é usado no fluxo de trabalho Fechar agente de incidentes de segurança.

Feche um incidente de segurança

Bate-papo com um agente com IA no Now Assist painel para ajudar você a fechar um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst ou sn_si.manager

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança**.
2. Abra o incidente de segurança que você deseja fechar usando o agente de IA.
3. Selecione o Now Assist (ícone).
   . Now Assist o painel é exibido.
4. Feche o incidente de segurança usando uma das seguintes opções.

Opção	Descrição
Feche um incidente de segurança	Em Now Assist, peça ao agente para fechar o incidente de segurança em linguagem natural inserindo `Feche este incidente` , `Feche este incidente de segurança` ou `Feche o incidente de segurança: SIR0012345` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: ○ Ao inserir `Feche este incidente` ou `Feche este incidente de segurança` . Now Assist o painel seleciona o incidente de segurança no contexto. Quando você fornece um número de incidente de segurança específico, como `Feche o incidente de segurança: SIR0012345` , o fluxo de trabalho do agente executa uma ação para o incidente de segurança sugerido. ○ Você pode fechar qualquer incidente de segurança no Now Assist fornecendo o número do incidente de segurança em seu texto. ○ Quando você solicita o fechamento de um incidente de segurança, o fluxo de trabalho Fechar agente de incidente de segurança cancela a avaliação pós-incidente obrigatória, as ações de fluxo, as ações de playbook, as ações de fluxo de trabalho e as tarefas de resposta. No entanto, você pode fechar essas ações manualmente antes de iniciar a solicitação de fechamento do incidente de segurança. O fluxo de trabalho Fechar agente de incidente de segurança fornece conteúdo para cada um dos campos a seguir e solicita seu feedback. O fluxo de trabalho do agentic preenche seu feedback aceito. Depois de aceitar o conteúdo de um campo, o fluxo de trabalho do agente fornecerá conteúdo para o próximo campo. ○ **Análise pós-incidente** : Aceite o conteúdo sugerido respondendo com uma resposta positiva, como `bom visual` ou `OK` . Peça ao fluxo de trabalho do agentic para refinar o conteúdo e sugerir as mudanças necessárias. ○ **Anotações de encerramento** : Aceite o conteúdo sugerido respondendo com uma resposta positiva, como `bom visual` ou `OK` . Você pode solicitar que o fluxo de trabalho do agentic refine o conteúdo e também pode sugerir as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ **Código de fechamento** : Com base nos detalhes do incidente de segurança, o fluxo de trabalho do agente sugere um código de fechamento. Você pode aceitar o código de fechamento ou sugerir um código de fechamento alternativo para o incidente de segurança. O agente de IA fecha o incidente de segurança. **Nota:** Quando um campo é alterado, o fluxo de atividades anexa as palavras "AGENTE de IA:" com uma descrição da atualização feita pelo agente de IA. Por exemplo, AGENTE com IA: O código de fechamento foi atualizado .
Feche um incidente de segurança como falso-positivo	Em Now Assist, você pode solicitar ao agente de IA para fechar o incidente de segurança como falso-positivo. Por exemplo, Feche este incidente como falso-positivo ou feche este incidente de segurança como falso positivo . O fluxo de trabalho do agentic fornece o resumo do incidente de segurança. Para fechar o incidente de segurança, insira respostas positivas, como bom visual ou OK . O agente de IA fecha o incidente de segurança. Ele também atualiza as anotações de fechamento como Encerrado pelo agente de IA como falso-positivo E o código de fechamento como **Falso-positivo** e cancela todas as tarefas de resposta ativas.

Tradução automática

Resposta a incidentes de segurança Fluxo de trabalho do agente do agente de resolução de incidentes de segurança

Bate-papo com um agente com IA no Now Assist painel para ajudar você a criar um plano de resolução para um incidente de segurança e resolvê-lo.

Resolver incidente de segurança visão geral do fluxo de trabalho do agente

Use o fluxo de trabalho Resolver agente de incidente de segurança para buscar os detalhes do incidente, buscar os artigos de conhecimento e incidentes de segurança encerrados semelhantes, obter um plano de resolução e resolver o incidente de segurança.

Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a versão duplicada do fluxo de trabalho do agentic.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Agentes usados no fluxo de trabalho do agente Resolver incidente de segurança

O fluxo de trabalho Resolver agente de incidente de segurança contém os seguintes agentes:

- Agente de IA de resolução do incidente de segurança
- Integração do Exchange Online lidando com agente de IA
- Agente de IA do gerador de encerramento de incidentes de segurança
- Agente de IA de análise observável
- Atividades de incidentes de segurança lidando com agentes de IA

Resolva um incidente de segurança

Bate-papo com um agente com IA no Now Assist painel para resolver um incidente.

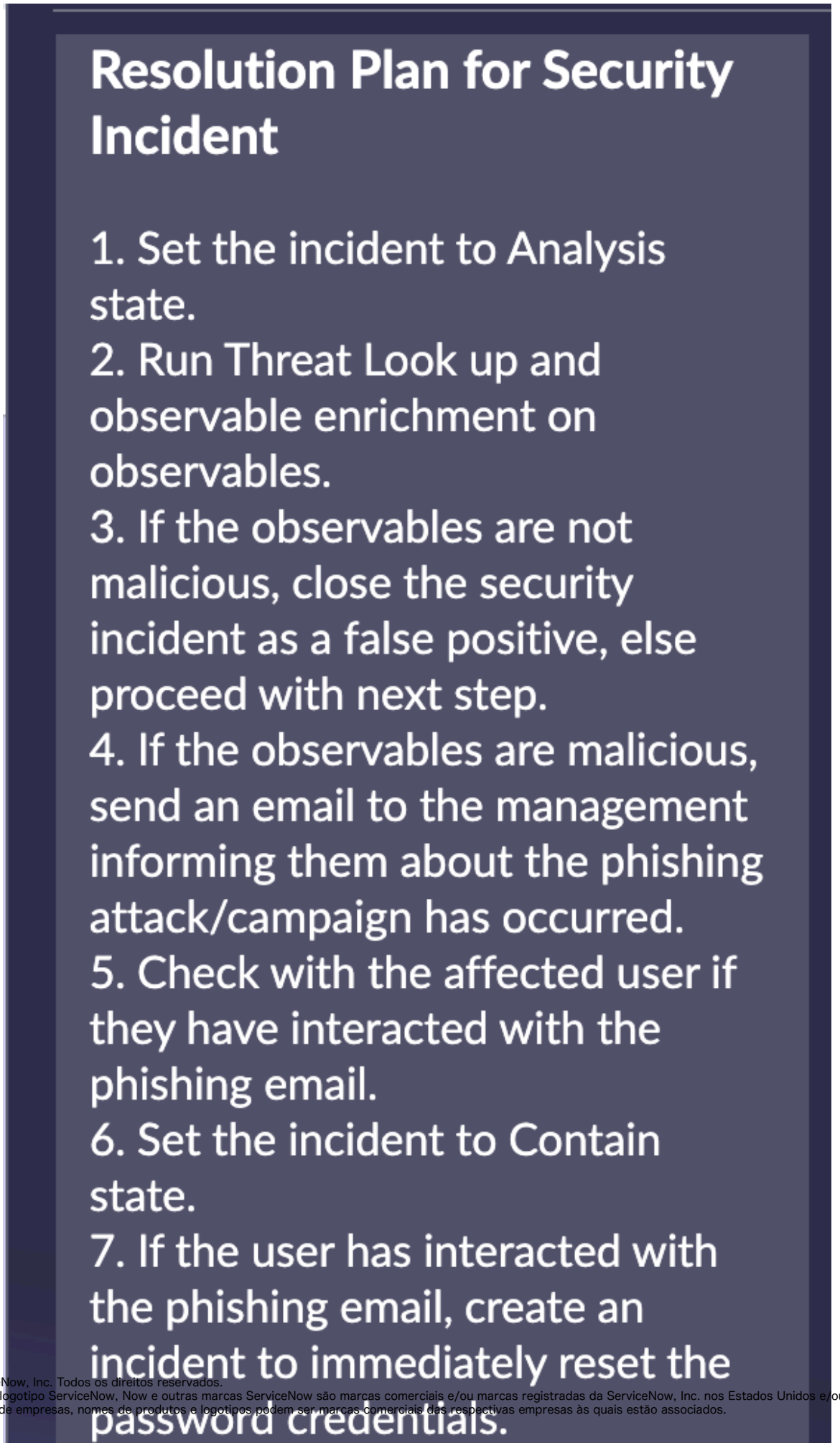
Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança**.
2. Abra o incidente de segurança que você deseja resolver usando o agente de IA.
3. Selecione Now Assist( ícone).
   O fluxo de trabalho Resolver agente de incidente de segurança é sob demanda. Você pode inserir uma consulta em linguagem natural para resolver um incidente de segurança usando este fluxo de trabalho do agente.
4. Em Now Assist, peça ao agente para resolver o incidente de segurança inserindo `Resolva este incidente` , `Resolva este incidente de segurança` ou `Resolva o incidente de segurança: SIR0012345` .
   . Now Assist o painel fornece todas as ações que você pode executar no incidente de segurança.
5. Selecione **Resolver incidente de segurança** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O agente de IA analisa o incidente de segurança e fornece um resumo do incidente e seu estado atual. Usando os detalhes do incidente, artigos de conhecimento e incidentes de segurança encerrados semelhantes, o agente de IA fornece um plano de resolução.

6. Insira respostas positivas, como `bom visual` ou `OK` se você concordar com o plano de resolução.
Para obter uma resposta positiva, o agente de IA investiga cada etapa no plano de resolução e ajuda o analista (o usuário com a função sn_si.analyst) a resolvê-la. Para cada etapa, o agente de IA fornece feedback e solicitações de intervenção do analista. Por exemplo, se o agente de IA identificar o incidente gerado para um e-mail de phishing, ocorrerá o seguinte fluxo de trabalho do agente:

Fluxo de trabalho do Agentic para resolver um incidente de e-mail de phishing

Tarefas para resolver um incidente de segurança	Descrição
Atualize o estado do incidente de segurança	O agente de IA atualiza o estado do incidente de segurança. Por exemplo, se o estado do incidente de segurança for Rascunho, o agente de IA o atualizará para Análise.
Execute a pesquisa de ameaças e o aprimoramento do observável no observable	O agente de IA inicia uma pesquisa de ameaças e um processo de aprimoramento de observável. Quando o analista confirma com uma entrada positiva, o agente de IA fornece a Análise observável e o resumo de aprimoramento.
Para observáveis mal-intencionados, envie e-mail para a gestão	O analista pode solicitar que o agente de IA envie um e-mail para a gestão. O agente com IA fornece um rascunho de e-mail e solicita os destinatários do e-mail. **Nota:** O analista pode verificar o e-mail enviado no **Outros registros** guia.
Verifique com o usuário afetado se ele interagiu com o e-mail de phishing	O analista verifica manualmente com o usuário afetado se ele interagiu com o e-mail de phishing.
Se o usuário interagiu com o e-mail de phishing, redefina suas credenciais de senha	Se o usuário afetado interagiu com o e-mail de phishing, o analista poderá solicitar ao agente de IA para criar um incidente para redefinir a senha do usuário. O agente de IA fornece um resumo do incidente e cria um incidente quando o analista aprova o resumo.
Bloquear o remetente/e-mail/URL no gateway de e-mail	O agente de IA solicita que o analista bloqueie o remetente/e-mail/URL no gateway de e-mail. O analista pode solicitar que o agente de IA crie uma tarefa de resposta para bloquear o remetente/e-mail/URL no gateway de e-mail. O agente de IA fornece as informações para as tarefas de resposta e cria uma tarefa de resposta depois que o analista a aprova.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas para resolver um incidente de segurança	Descrição
	Nota: O analista pode concluir a tarefa de resposta e marcar a tarefa de resposta como **Concluído** em **Tarefas de resposta** guia. O analista confirma ao agente de IA que a tarefa de resposta está concluída.
PESQUISE e exclua o e-mail de phishing de todas as caixas de entrada do usuário	O agente de IA informa o analista para excluir o e-mail de phishing de todas as caixas de entrada do usuário. O analista exclui o e-mail de phishing e confirma com o agente de IA.
Inscreva o usuário afetado em um treinamento de phishing obrigatório	Se o usuário afetado interagiu com o e-mail de phishing, o agente de IA informará o analista para inscrever o usuário afetado no treinamento obrigatório de phishing.
Execute a auditoria do incidente de segurança	O agente de IA executa a auditoria do incidente de segurança e fornece o resumo.
Encerrar o incidente de segurança	O agente de IA fecha o incidente. Para obter mais informações, consulte Feche um incidente de segurança.

Resposta a incidentes de segurança Coleção de agentes de IA para o fluxo de trabalho do agente Analisar métricas de operações de segurança

O fluxo de trabalho do agente Analisar métricas de operações de segurança ajuda os gerentes do centro de operações de segurança a analisar o desempenho de suas equipes de segurança.

Analisar métricas de operações de segurança Visão geral do fluxo de trabalho do agente

Os gerentes do SOC (Security Operations Center, centro de operações de segurança) podem analisar métricas de volume geral de casos, tempo médio de atribuição (MTTA) e tempo médio de resolução (MTTR) na resposta a incidentes de segurança (SIR) para fornecer informações sobre o desempenho dos analistas de segurança. Eles também podem solicitar recomendações sobre como melhorar as métricas.

Agentes usados no fluxo de trabalho do agente Analisar métricas de operações de segurança

- Agente de IA de recuperação de incidente de segurança
- Agente de IA de análise de métricas de segurança

Ferramentas mapeadas para o fluxo de trabalho do agente Analisar métricas de operações de segurança

As ferramentas a seguir são mapeadas para os agentes de IA usados no fluxo de trabalho do agente Analisar métricas de operações de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de ferramenta	Modo de execução	Nome	Descrição
Script	Autônomo	Pesquisar incidentes de segurança	Esta ferramenta invoca o script com a entrada correta da consulta do usuário para recuperar os incidentes de segurança do banco de dados.
Script	Autônomo	Análise	Fornece uma análise adicional para um tipo de métrica especificado, analista , grupo , StartDate , Data de término Para o desempenho do SOC.
Script	Autônomo	Cálculo	Calcula métricas de desempenho para gerentes de SOC, como tempo médio de resolução (MTTR) e tempo médio de atribuição (MTTA).
Script	Autônomo	Recomendar	Recomenda ações gerenciais que podem ser tomadas com base em uma análise de uma métrica.

Gatilhos para o fluxo de trabalho do agente Analisar métricas de operações de segurança

Não há gatilhos para este caso de uso. Se necessário, você pode adicionar um gatilho para invocar o caso de uso automaticamente.

Analise o fluxo de trabalho do agente das métricas de operações de segurança

Bate-papo com um agente com IA do Now Assist painel para ajudar você a obter informações sobre a eficiência com que seus analistas de segurança estão trabalhando com a resolução de incidentes de segurança.

Antes de Iniciar

Você deve ativar o. Now Assist Habilidade de análise de métricas de operações de segurança antes que você possa usar os agentes de IA com o fluxo de trabalho do agente Analisar métricas de operações de segurança. Para obter mais informações, consulte Configure e ative uma habilidade para Now Assist para Resposta a incidentes de segurança.

Função necessária: sn_si.manager

Procedimento

1. Selecione Now Assistícone ( ) de qualquer lugar em sua instância.
   . Now Assist o painel é exibido.
2. Selecione **Analisar métricas de operações de segurança** em Now Assist painel.
3. No prompt, selecione **Analise métricas de incidentes de segurança** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O caso de fluxo de trabalho do agente Analisar métricas de operações de segurança é sob demanda. Você pode inserir qualquer consulta em linguagem natural, mas considere usar os prompts descritos na tabela e nas etapas a seguir para se familiarizar com os dados de métricas disponíveis e o que você pode fazer com eles.

Sua solicitação ou resposta	Descrição
Insira um nome para um de seus grupos de analistas de segurança e métricas de solicitação, por exemplo: ○ **Analise as métricas de operações de segurança da equipe de analista L1.** ○ **Métricas de segurança da equipe de analista L1 nos últimos seis meses.** ○ **Como a equipe de analista L1 se saiu no mês passado?**	Especifique uma equipe por nome e indique um período de tempo.
Encerre a sessão ou **Parar** .	Encerre a conversa.

Você pode preferir ter o Resposta a incidentes de segurança espaço aberto em outra guia para que você possa consultar grupos de atribuição, datas e outras informações para seus prompts.

Sua conversa é salva até que você inicie um novo bate-papo. Para iniciar um novo bate-papo, selecione o ícone Novo bate-papo ( ).

Sua solicitação é repetida e exibida em texto realçado com mais informações.

Após alguns momentos, você será solicitado a fornecer mais informações sobre um analista específico ou um grupo de analistas.

4. Insira um nome de grupo de atribuição, por exemplo, **Equipe de analistas L1** .
5. No prompt, insira um intervalo de tempo, por exemplo, **Últimos seis meses** .
   Os resultados de Tempo médio de resolução (MTTR), Tempo médio de atribuição (MTTA) e o número total de incidentes de segurança que sua equipe manipulou são exibidos. Selecione o link para obter mais informações. Uma nova guia é aberta com uma lista em UI16.
6. Expanda **Origens** e selecione **Lista de incidentes de segurança** link.
   Uma lista de incidentes de segurança atribuídos ao grupo de analistas L1 é exibida em uma nova guia na IU 16. Na parte superior da lista, o intervalo de datas solicitado (**6 meses**) é exibido no seguinte formato: Aberto > 2024-09-23 > Aberto > 2025-03-23 . Você será solicitado se deseja ver uma análise mais detalhada para MTTR, MTTA ou volume de caso.

   Nesta lista, você pode selecionar um link para abrir incidentes de segurança individuais para revisão. Você pode inserir um número de registro na lista no bate-papo para o agente de IA resumir.

7. Retorne ao bate-papo e insira sua solicitação para uma métrica de desempenho em linguagem natural, por exemplo, Sim, mergulhe mais fundo no MTTR.
   São fornecidas mais informações para sua solicitação que incluem um resumo e dados organizados em seções para campos no incidente de segurança.
   - Análise de categoria - Detalhamento por categoria. Os exemplos podem incluir Acesso não autorizado , Vulnerabilidade sem patch , Falso-positivo e assim por diante.
   - Análise de prioridade - Detalhamento por gravidade: Crítica, Alta, Moderada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Análise da equipe - Detalhamento do MTTR por membros individuais da equipe.
- Análise de exceção - Detalhamento de incidentes de segurança que têm valores excepcionalmente altos, baixos ou outros exclusivos.

8. No prompt, insira uma resposta afirmativa à solicitação de sugestões de melhoria.
   Suas sugestões são exibidas. Com base nos resultados da avaliação, convém pesquisar mais informações sobre tipos específicos de incidentes de segurança.
9. No prompt, por exemplo, solicite em linguagem natural todos os incidentes de segurança na categoria de phishing que estão no estado **Análise** .
10. Selecione **Exibir resultados** link.
    Uma lista de incidentes de segurança que correspondem à sua solicitação é fornecida em uma nova guia no UI16.

    Nesta lista, você pode abrir incidentes individuais e solicitar resumos do agente de IA.
11. **Opcional:** Modifique as propriedades do sistema para os campos de origem que são usados para análise de métrica e o valor do fator de exceção.
    - sn_sec_gen_ai.aia_metric_analysis_dimensiones - O agente de IA divide a análise com base nos seguintes campos ao analisar métricas de MTTR e MTTA: **categoria** , **prioridade** , **close_code** , **assigned_to** , **alert_sensor** . Usuários com as funções sn_si.manager e sn_si.admin podem modificar esta lista.
    - sn_sec_gen_ai.aia_metric_analysis_outlier_factor - Esta propriedade determina o fator de exceção para MTTR e MTTA. O valor de exceção padrão é 2. Por padrão, um registro será um valor atípico se seu MTTR exceder 2 vezes o tempo médio que um grupo de atribuição leva para resolver incidentes de segurança para o intervalo de tempo solicitado. Usuários com as funções sn_si.manager e sn_si.admin podem modificar esse valor.

Gerar relatório de entrega de turno SIR

Bate-papo com um agente com IA no Now Assist Painel para usar o fluxo de trabalho do agente Gerar relatório de entrega de turno SIR para ajudar você a adicionar detalhes de um incidente de segurança a um relatório de entrega de turno.

Gerar visão geral do relatório de entrega de turno SIR

Use o fluxo de trabalho do agente Gerar relatório de entrega de turno SIR para adicionar detalhes de um incidente de segurança ao relatório de entrega de turno. O agente preenche as diferentes seções da entrega de turno com o conteúdo apropriado, identificando os detalhes relevantes do incidente de segurança.

O agente de IA identifica se o analista tem acesso a um registro de entrega de turno e gera conteúdo a partir dos detalhes do incidente de segurança para cada seção do relatório de entrega de turno. O analista pode fornecer feedback sobre o conteúdo, e o agente de IA gera o conteúdo atualizado e salva o conteúdo no relatório de entrega de turno quando o analista aprova.

Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a versão duplicada do fluxo de trabalho do agentic.

Visão geral Gerar relatório de entrega de turno SIR

O fluxo de trabalho do agente Gerar relatório de entrega de turno do SIR contém os seguintes agentes: Incidente de segurança Entrega de turno Agente de IA.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar incidente de segurança ao relatório de entrega de turno

Bate-papo com um agente com IA no Now Assist painel para adicionar detalhes de um incidente de segurança a um relatório de entrega de turno.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança**.
2. Abra o incidente de segurança que você deseja adicionar a um relatório de entrega de turno usando o agente de IA.
3. Selecione Now Assist( ícone).
   O fluxo de trabalho do agente Gerar relatório de entrega de turno SIR é sob demanda. Você pode inserir uma consulta em linguagem natural para adicionar um incidente de segurança a um relatório de entrega de turno.
4. Em Now Assist peça ao agente para adicionar um incidente de segurança a um relatório de entrega de turno `Adicione este incidente de segurança à entrega do turno` ou `Adicione este incidente à entrega do turno: SIR0012345` E pressione a tecla Enter.
   . Now Assist O painel aciona o fluxo de trabalho "Adicionar incidente de segurança para entrega de turno". Este fluxo de trabalho busca detalhes do incidente de segurança.

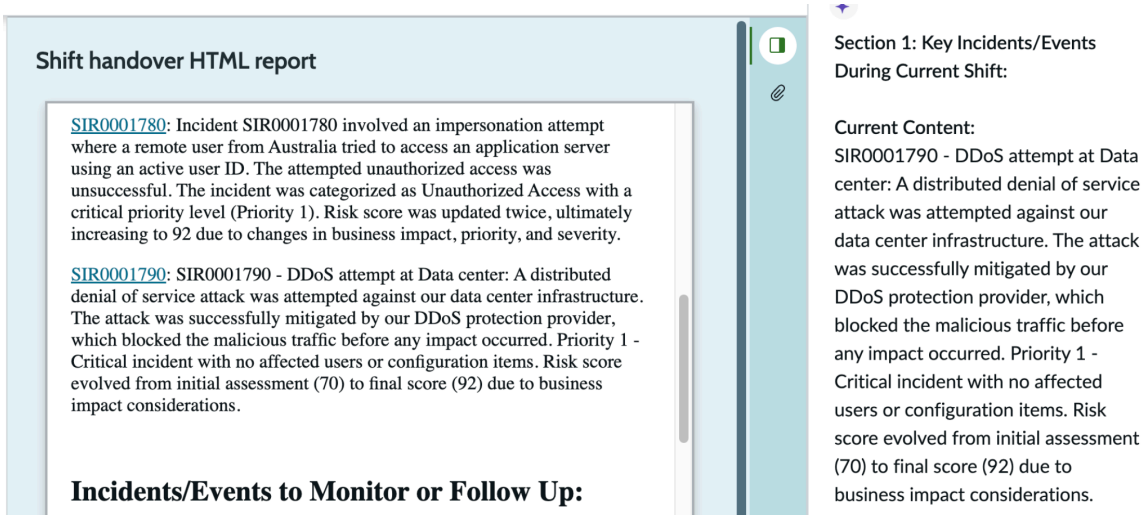
   O agente de IA encontra o registro de entrega de turno em andamento ao qual o analista tem acesso e adiciona os detalhes do incidente de segurança a ele. Se houver vários registros de entrega de turno em andamento aos quais o analista tem acesso, o agente de IA listará os cinco principais registros de entrega de turno para o analista selecionar.

   Se não houver registros de entrega de turno no estado "Andamento" e atribuídos ao grupo do usuário, ou não houver registros de entrega de turno, uma mensagem de notificação será exibida informando que não há registros de entrega de turno ativos para o usuário.
5. Forneça o número do registro de entrega de turno e pressione a tecla Enter.
   O agente de IA valida o registro de entrega de turno para identificar se o registro é válido e está em andamento, o analista conectado tem acesso ao registro de entrega de turno. Em uma validação bem-sucedida, o agente de IA gera o conteúdo do registro de entrega de turno e o fornece para aprovação.
6. Insira respostas positivas, como `bom visual` , `aprovado` ou `OK` se você concordar com o conteúdo.
   O agente de IA salva o conteúdo aprovado na seção relevante do relatório de entrega de turno.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para cada seção do relatório de entrega de turno, o agente de IA fornece o conteúdo e solicita feedback do analista. Se necessário, você pode ignorar para atualizar qualquer seção.



Resultado

O agente com IA exibe o resumo de todas as seções atualizadas e ignoradas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Shift Handover Report Update Complete

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

Summary of Processing:

Sections Saved (7 total):

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

Sections Skipped: None

All sections have been successfully

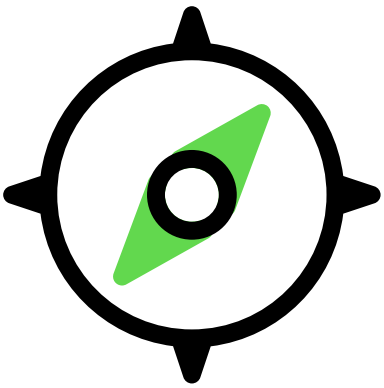
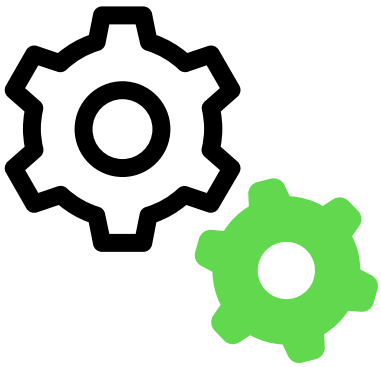
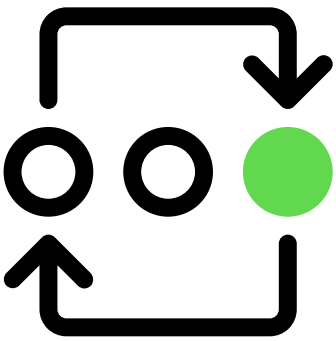
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Now Assist para resposta a vulnerabilidades

Use Now Assist para resposta a vulnerabilidades Aplicação para ajudar seus gerentes e analistas de vulnerabilidades a avaliar sua possível exposição a vulnerabilidades críticas e obter informações sobre a conformidade do Acordo de nível de serviço (ANS) para itens vulneráveis.

Iniciar

Explorar	Configurar	Uso
		
Saiba mais sobre Now Assist para resposta a vulnerabilidades	Saiba como configurar e ativar as habilidades de IA generativa e fluxos de trabalho do agente para Now Assist para resposta a vulnerabilidades	Saiba como usar Now Assist para resposta a vulnerabilidades

Coleção de agentes com IA



Obtenha informações sobre os agentes de IA e fluxos de trabalho do agente para Now Assist para resposta a vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

- Nem todos os provedores de modelos estão disponíveis para clientes com SKUs no país, e alguns produtos/recursos do Now Assist estão indisponíveis no momento para clientes no país. Para obter mais informações, consulte KB1584492 artigo na Base de conhecimento do Now Support. Certifique-se de verificar se há atualizações de disponibilidade do provedor de modelos em versões futuras.
- Alguns Now Assist No momento, os produtos/recursos não estão disponíveis para clientes nos datacenters protegidos pelo FedRAMP, NSC DOD IL5 ou IRAP da Austrália, clientes auto-hospedados ou em outros ambientes restritos. Para obter mais informações, consulte o artigo KB0743854 na Now Support Base de conhecimento. Certifique-se de verificar se há atualizações de disponibilidade em versões futuras.
- Alguns Now Assist no momento, os produtos/recursos estão disponíveis somente para clientes em algumas regiões. Certifique-se de verificar se há atualizações de disponibilidade em versões futuras.

Recursos úteis

Alguns ServiceNow os recursos que podem fornecer informações úteis são:

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

Processamento de dados

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

Coleta de dados

ServiceNow coleta e usa as entradas, saídas e edições nas saídas desta aplicação para desenvolver e melhorar tecnologias ServiceNow, incluindo modelos e produtos de IA ServiceNow. Além disso, esta aplicação coletará Os dados de vulnerabilidade que você importa, bem como informações sobre os itens de configuração no CMDB. Os clientes podem recusar a coleta futura de dados a qualquer momento, conforme descrito na página Now Assist Recusar .

Para obter mais informações, consulte Now Assist documentação .

Explorando Now Assist para resposta a vulnerabilidades

Obtenha informações sobre como seus gerentes e analistas de vulnerabilidades podem usar Now Assist habilidades E agentes de IA com Now Assist para resposta a vulnerabilidades.

Visão geral Now Assist para resposta a vulnerabilidades

Com Now Assist habilidades fornecidas com Now Assist para resposta a vulnerabilidades seus gerentes de vulnerabilidades e analistas têm a opção de identificar, revisar e fechar itens vulneráveis duplicados importados de seus scanners de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerentes e analistas também têm a opção de obter orientação clara sobre como resolver itens vulneráveis que incluem o fornecimento de possíveis soluções preferenciais importadas de fornecedores terceirizados Now Assist habilidades.

Com agentes de IA e fluxos de trabalho do agente fornecidos com Now Assist para resposta a vulnerabilidades Seus gerentes e analistas de vulnerabilidades têm a opção de determinar a exposição potencial do seu ambiente a vulnerabilidades recentes e conhecidas e exibir o quão bem seus destinos de correção estão em conformidade com seus Acordos de nível de serviço (ANS).

Now Assist para resposta a vulnerabilidades usuários

Usuários

Usuário	Descrição
Gerentes e analistas de vulnerabilidades	Determine sua exposição a vulnerabilidades em seu ambiente e seu possível impacto nos itens de configuração (ICs) e nos serviços de negócios.
Gerentes e analistas de vulnerabilidades	Obtenha informações sobre o quão bem você está atingindo suas metas de correção de vulnerabilidades de acordo com seus acordos de nível de serviço (ANS).
Gerentes e analistas de vulnerabilidades	Forneça etapas para que os analistas corrijam itens vulneráveis (Vits) atribuídos a eles com tópicos de observação e esforços de correção.
Gerentes e analistas de vulnerabilidades	Obtenha assistência clara de correção sobre como resolver tarefas de correção que incluem possíveis soluções preferenciais, se estiverem disponíveis.
Gerentes e analistas de vulnerabilidades	Identifique e revise itens vulneráveis duplicados que são importados por seus verificadores de vulnerabilidades. Identifique o item vulnerável primário associado a um item de configuração.

Benefícios do Now Assist para resposta a vulnerabilidades

Recursos do Now Assist para resposta a vulnerabilidades

Benefício	Recurso	Usuários
Identifique o item vulnerável primário (primeiro encontrado) de um item de configuração e remova itens vulneráveis do host (Vits) duplicados.	Habilidade de desduplicação de item vulnerável	Gerentes e analistas de vulnerabilidades
Obtenha orientação sobre como resolver tarefas de correção que incluem possíveis soluções preferenciais disponíveis de fornecedores de terceiros.	Solução preferencial recomendada para a habilidade VIT	Gerentes e analistas de vulnerabilidades
• Identificar ativos com vulnerabilidades e exposições comuns (CVEs). • Determine o número de itens de vulnerabilidade ativos (Vits) que correspondem aos CVEs. • Identificar serviços de negócio com vulnerabilidades conhecidas.	Avalie o fluxo de trabalho do agente de exposição a vulnerabilidades	Gerentes e analistas de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos do Now Assist para resposta a vulnerabilidades

Benefício	Recurso	Usuários
• Crie tópicos de observação para correção de item vulnerável (VIT) com base nas informações fornecidas. O agente de IA pode criar um esforço de correção para os Vits ativos associados ao tópico de observação.		
Obtenha informações sobre o andamento do resumo de conformidade do Acordo de nível de serviço (ANS) nos últimos 30 dias. Exiba grupos e tipos de ativos que não cumpriram SLAs para ajudar você a rastrear e ajustar metas.	Analisar o fluxo de trabalho do agente de status de correção de vulnerabilidade	Gerentes e analistas de vulnerabilidades
Recupere contexto e detalhes relevantes dos itens vulneráveis atribuídos a você. Analise, planeje e crie etapas para correção.	Etapas para resolução de problemas	Analistas de vulnerabilidades

O que explorar a seguir

Para saber mais sobre como configurar e usar a Now Assist para resposta a vulnerabilidades, consulte:

- Configuração da Now Assist para resposta a vulnerabilidades
- Usando fluxos de trabalho do agentic em Now Assist para Resposta a vulnerabilidades

Informações de suporte para Now Assist para resposta a vulnerabilidades

Obtenha uma visão geral rápida das informações importantes relacionadas à aplicação Now Assist para resposta a vulnerabilidades.

Versões compatíveis e aplicações necessárias

As seguintes aplicações são necessárias:

Aplicação	Versão
Now Assist para resposta a vulnerabilidades	1.0.4
Now Assist para plataforma [sn_genai_platform]	9.1.0
Resposta a vulnerabilidades Integração com CISA [sn_vul_cisa]	1.5.1
Resposta a vulnerabilidades [sn_vul]	26.2.1
Resposta a vulnerabilidades licenciamento e uso [sn_vul_licensing] (instalado com [sn_vul])	2.7.1
Resposta a vulnerabilidades Espaço comum [sn_vul_cmn_ws] (instalado com [sn_vul])	1.7.0
Estrutura de integração de resposta a vulnerabilidades [sn_vul_int_fw]	1.1.2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Versão
Gestão de soluções de vulnerabilidades [sn_vul_solution]	10.4.3

Interfaces do usuário compatíveis

Now Assist para resposta a vulnerabilidades Inclui as habilidades de IA generativa listadas na tabela a seguir.

Interfaces compatíveis do Now Assist para Resposta a vulnerabilidades

Interface	Recursos
Espaço para gerentes de vulnerabilidades	Now Assist habilidades: • Desduplicação de itens vulneráveis do host (Vits). • Assistência de correção que inclui o fornecimento de possíveis soluções preferenciais de fornecedores terceirizados. Agentes de IA: Gerentes e analistas de vulnerabilidades podem avaliar se seus itens de configuração (ICs) e seus serviços de negócios estão expostos a vulnerabilidades. Verifique se há novas vulnerabilidades exploráveis conhecidas da CISA (Cybersecurity and Infrastructure Security Agence, Agência de segurança cibernética e infraestrutura) e avalie seu possível impacto em seu ambiente. Os gerentes e analistas de vulnerabilidades podem obter informações sobre suas métricas de conformidade para entender a eficácia com que sua organização está cumprindo os objetivos de correção de vulnerabilidades com base em acordos de nível de serviço (ANS).
UI6	Links nas respostas no Now Assist abra novas guias no navegador.

Configuração da Now Assist para resposta a vulnerabilidades

. Now Assist para resposta a vulnerabilidades a aplicação é compatível com Now Assist e disponível sob demanda.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da configuração

Compartilhando dados com ServiceNow® Programa de desenvolvimento de IA, você fornece dados relevantes para ajudar a melhorar a precisão da previsão, a experiência do usuário, personalizar produtos de acordo com suas necessidades de negócios e reduzir alucinações para seu ativado Now Assist habilidades.

Você pode optar por recusar um ServiceNow instância do compartilhamento de dados do Administração do Now Assist console se você não quiser participar. Para obter mais informações, consulte Recusar o compartilhamento de dados para Now Assist . Repita o processo de recusa para todas as instâncias que usam Now Assist funcionalidade.

Antes da v1.0.4, use Estúdio de agentes de IA para configurar Now Assist para resposta a vulnerabilidades.

A partir da v1.0.4, use Administração do Now Assist console a ser configurado Now Assist para resposta a vulnerabilidades. Este console contém tudo o que você deve instalar os aplicativos e configurar as habilidades de IA generativa. Para obter informações adicionais, confira Configurando Now Assist configurações e recursos .

. Now Assist o painel deve ser ativado. Para obter mais informações, consulte Ligue o. Now Assist painel .

- Instalar plug-ins de Now Assist .

  Instale o. Now Assist para resposta a vulnerabilidades aplicação (sn_vul_ai).

- Configure e ative uma habilidade para Now Assist para resposta a vulnerabilidades

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

- Ative um fluxo de trabalho do agente para Now Assist para resposta a vulnerabilidades

  . Now Assist para resposta a vulnerabilidades Os agentes de IA incluídos com a aplicação são ativados por padrão. Você deve ativar os fluxos de trabalho do agentic no Estúdio de agentes de IA para usar Now Assist para resposta a vulnerabilidades. Para obter mais informações, consulte Ative um fluxo de trabalho do agente para Now Assist para resposta a vulnerabilidades.

  Configure e ative um fluxo de trabalho do agente no Configuração assistida.

Configure e ative uma habilidade para Now Assist para resposta a vulnerabilidades

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

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Administrador do Now Assist** > **Habilidades**.
2. Com **Tecnologia** selecionado no painel de navegação, selecione **Operações de segurança** da lista.
   . Now Assist A página Habilidades para Operações de segurança é exibida. Estes Now Assist para resposta a vulnerabilidades as habilidades são compatíveis com Now Assist para resposta a vulnerabilidades:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução preferencial recomendada para VIT
- Desduplicação de item vulnerável

3. Selecione **Ativar habilidade** para a habilidade que você deseja.
4. Siga as etapas para configurar e ativar uma habilidade usando Configuração assistida.

> **Nota:** Algumas habilidades não exigem todas as etapas de configuração listadas abaixo. Selecione as únicas tarefas exibidas no painel esquerdo e siga as instruções. Depois de concluir as tarefas, ative a habilidade.

5. Na página Detalhes gerais, selecione **Salve e continue** .
   Esta página é somente leitura.
6. **Opcional:** Escolha uma das seguintes opções para definir a disponibilidade.

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

7. Selecione **Salvar e continuar**.
8. Defina o acesso.

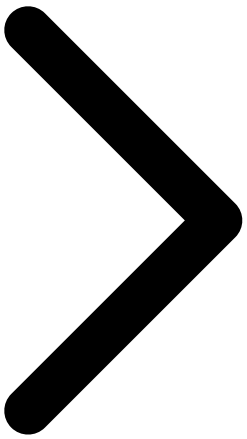
> **Nota:**
> - Para a habilidade de desduplicação de item vulnerável, a função sn_vul_ai.run_vi_dedup_job é exibida. Esta função é necessária para executar os trabalhos de desduplicação do espaço.
> - Para a solução preferencial recomendada para a habilidade VIT, a função sn_vul_ai.run_suggest_solution é exibida. Esta função é necessária para executar o recurso de solução recomendado para itens vulneráveis.
> - A função sn_vul_ai.read_suggest_solution_job é necessária para executar o trabalho agendado para tarefas de correção, exibir a tabela Recomendar trabalho de solução [sn_vul_ai_suggest_solution_job] e exibir o status da execução.
>
> Você pode editar essas funções, mas pode preferir deixá-las como as configurações padrão para esta etapa.

9. Selecione **Salvar e continuar**.
10. Determine onde você deseja exibir a habilidade e quem pode exibi-la no espaço.

Opção	Descrição
Desktop no produto	Now Assist as habilidades são exibidas em formulários e espaços de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Funções de usuário	Selecione o ícone Expandir ) A função da etapa Definir acesso é exibida na lista.

11. Selecione **Salvar e continuar**.
12. Revise suas escolhas e selecione **Ativar** para concluir a configuração da habilidade.
13. Selecione **Retorne para Operações de segurança** Para retornar à página Habilidades do Now Assist para Operações de segurança.
    Agora você está pronto para revisar Usando Now Assist para resposta a vulnerabilidades para correção de item vulnerável.

Ative um fluxo de trabalho do agente para Now Assist para resposta a vulnerabilidades

Você deve ativar os fluxos de trabalho do agentic no AI Agent Studio. . Now Assist para resposta a vulnerabilidades Os agentes de IA incluídos com a aplicação e usados nos fluxos de trabalho do agente são ativados por padrão.

Antes de Iniciar

. Now Assist o painel deve ser ativado. Para obter mais informações, consulte Ligue o. Now Assist painel .

Função necessária: aia-admin

Procedimento

1. Navegar até **Tudo** > **Studio do agente de IA** > **Visão geral**.
2. Selecione o cartão do fluxo de trabalho do agente que você deseja configurar e ativar.
   - **Avalie a exposição à vulnerabilidade**
   - **Analisar status de correção de vulnerabilidade do caso de uso**

   Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a duplicata.

   A Configuração assistida é exibida. A página Descrever e conectar é somente leitura.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Continuar**.
4. Para Definir gatilho, selecione **Continuar** .

   A página Definir gatilho é somente leitura.
5. Selecione **Exibição** Alterne para a página Selecionar exibição para que a conversa com o agente de IA seja exibida no Now Assist painel.
6. Selecione o ícone de seta para expandir a seção.
   As funções sn_vul.vulnerability_admin e sn_vul.vulnerability_analyst são exibidas. Essas funções são compatíveis com os fluxos de trabalho do agente no Now Assist para resposta a vulnerabilidades aplicação.
7. Para ativar o fluxo de trabalho do agentic, selecione **Salve e teste** .
   Agora você pode invocar os fluxos de trabalho do agente sob demanda.
8. **Opcional:** Selecione **Caso de uso** (fluxo de trabalho do agentic) e insira as informações que você deseja testar e selecionar **Iniciar teste** .

Usando Now Assist para resposta a vulnerabilidades para correção de item vulnerável

Gerentes e analistas de vulnerabilidades podem resolver tarefas de correção de dentro do fluxo de trabalho com as habilidades de IA generativa compatíveis com Now Assist para resposta a vulnerabilidades.

Visão geral de Now Assist para resposta a vulnerabilidades habilidades

Com habilidades de IA generativa com Now Assist para resposta a vulnerabilidades seus gerentes e analistas de vulnerabilidades têm a opção de:

Identificar e fechar itens vulneráveis duplicados.

Nota: A desduplicação só é compatível com VIT (Host Vulnerable Items) ativos

Exibir soluções de vulnerabilidade preferenciais recomendadas para itens vulneráveis.

Nota:

- Você deve instalar e ativar Solução de gestão de vulnerabilidade[sn_vul_solution] para importar e exibir soluções de vulnerabilidade preferenciais e disponíveis. Este aplicativo fornece soluções atuais com importações programadas. Solução de gestão de vulnerabilidade está disponível no ServiceNow® Store.
- Esta habilidade de IA generativa é compatível somente com Itens vulneráveis do host (Vits) ativos. Vits devem estar em **Aberto** , **Em investigação** , **Aguardando implementação** ou **Em Revisão** estados.
- As soluções atuais que resolvem vulnerabilidades com mais eficácia, também conhecidas como soluções de maior substituição, devem estar disponíveis para importação de fornecedores terceirizados. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre Solução de gestão de vulnerabilidade e integrações compatíveis para obter mais informações.
- . **Item de configuração** O campo em um VIT deve ser preenchido com um valor da tabela Item de configuração [cmdb_ci].
- . **Vulnerabilidade** O campo em um VIT deve ser preenchido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Identifique itens vulneráveis duplicados com Now Assist para resposta a vulnerabilidades

  Identifique e agrupe itens vulneráveis duplicados (Vits) criados a partir de vários scanners. Identificar o item vulnerável primário e remover (fechar) duplicatas.

- Sugira soluções de vulnerabilidade preferenciais com Now Assist para resposta a vulnerabilidades

  Identificar a solução preferencial mais apropriada para um determinado item vulnerável (VIT).

Identifique itens vulneráveis duplicados com Now Assist para resposta a vulnerabilidades

Crie ou execute um trabalho para identificar os itens vulneráveis primários (primeiros encontrados) para itens de configuração junto com itens vulneráveis duplicados que são importados por seus verificadores de vulnerabilidades.

Antes de Iniciar

Consulte Usando Now Assist para resposta a vulnerabilidades para correção de item vulnerável para obter mais informações sobre os requisitos para isso Now Assist habilidade. Consulte Configure e ative uma habilidade para Now Assist para resposta a vulnerabilidades para obter mais informações sobre como ativá-lo.

Funções necessárias:

Nota: Sn_vul.vulnerability_admin e sn_vul.vulnerability_analyst herdam as seguintes funções quando você instala o. Now Assist para resposta a vulnerabilidades aplicação.

- Exiba o módulo de desduplicação de item vulnerável no espaço - sn_vul_ai.now_assist_user
- Criar configurações de trabalho de desduplicação - sn_vul_ai.configure_vi_dedup
- Executar trabalhos de desduplicação - sn_vul_ai.run_vi_dedup_job
- Revise registros de trabalho duplicados - sn_vul_ai.review_duplicate_vi

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione Now Assist No painel de navegação.
   . **Todas as configurações de trabalho** , **Todos os trabalhos** e **Todas as revisões duplicadas** as guias são exibidas no Now Assist página. Você deve criar um trabalho de desduplicação como a primeira etapa para desduplicação de item vulnerável (Vits).

   Nota: Você deve ter a função sn_vul_ai.configure_vi_dedup para criar trabalhos.

3. Para criar um trabalho, selecione **Novo** e preencha os campos.

Campo	Descrição
Título	Nome exclusivo para ajudar você a identificar este trabalho de outros trabalhos.
Notificação por e-mail	Marque a caixa de seleção para receber notificações por e-mail quando este trabalho for concluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se selecionado, você poderá ver as seguintes informações em um e-mail: ○ Itens vulneráveis duplicados encontrados ○ Total de itens vulneráveis processados ○ Itens de configuração afetados ○ Selecione **Revise duplicatas** link para exibir a lista de duplicatas no espaço. Como alternativa, você pode selecionar o ícone Mostrar notificações (sino) na faixa superior para ver mensagens com os itens vulneráveis duplicados encontrados para trabalhos concluídos.
Definir condições	**a.** Selecione **Definir condições** link para filtrar os itens vulneráveis que você deseja revisar em busca de duplicatas. Um exemplo pode ser: **[Item de configuração] [contém] [server-based-vis]** . . **Definir condições** o link é atualizado e exibe uma contagem com seus resultados correspondentes. Você pode preferir renomear seu trabalho com base nos resultados retornados. Você pode selecionar **Exibir resultados correspondentes** Link para exibir itens vulneráveis que atendem às suas condições e mais detalhes, como um resumo, itens de configuração e classificações de risco no modal de condição. **b.** Quando estiver satisfeito com os resultados, selecione **Salvar** .

4. Depois de salvar o trabalho, o **Executar trabalho** o botão é exibido e ativado no registro.

Você está pronto para executar um trabalho.

Nota: Você deve ter a função sn_vul_ai.run_vi_dedup_job para exibir **Executar trabalho** e iniciar trabalhos.

a. Para executar um trabalho, navegue até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Now Assist** > **Todas as configurações de trabalho**.

b. Localize o trabalho desejado, selecione o registro na coluna Número para abri-lo e selecione **Executar trabalho** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mensagem informando que o trabalho está sendo executado em segundo plano é exibida. Para obter mais informações sobre o status do seu trabalho, selecione **Exibir andamento** link.

Depois de selecionar Executar trabalho, o trabalho Verificar conclusão do trabalho de desduplicação de item vulnerável é iniciado e executado em segundo plano.

Outro trabalho é executado a cada 30 minutos para verificar se os trabalhos ativos foram concluídos.

Depois que o trabalho for concluído com sucesso, você poderá revisar, avaliar e fechar os Vits duplicados encontrados por seu trabalho.

Nota: Você deve ter a função sn_vul_ai.review_duplicate_vi para revisar Vits duplicados.

5. Revisar Vits duplicados.

   a. Para revisar trabalhos concluídos e as listas de itens vulneráveis duplicados, navegue até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Now Assist** > **Todos os trabalhos**.

   b. Abra um registro (**TRABALHO Nº**) e selecione **Duplicar revisões de item vulnerável** lista relacionada.

   c. **Opcional:** Selecione os links para abrir o item vulnerável (**VIT Nº**) Registros para revisão antes de determinar se os Vits no registro são duplicados.

   d. Para obter uma comparação lado a lado dos registros VIT duplicados, selecione um (**NÚMERO DUP**) para abri-lo.

   - O número do trabalho e o estado (**Revisão necessária**) é exibido.
   - Os campos Confiança e Motivo fornecem mais informações. A coluna Motivo exibe o raciocínio da IA generativa e do serviço NOW LLM do motivo pelo qual esses Vits são considerados duplicados.
   - As informações sobre a VIT primária e a VIT duplicada estão lado a lado na seção de detalhes do item vulnerável.
   - Primeira data encontrada para os Vits primários e duplicados. Uma VIT primária normalmente tem a data de descoberta mais antiga.
   - Selecione as informações ⓘ Nos campos Detalhes do item vulnerável primário e Duplicado se você quiser abrir os registros de VIT nesta página.

   e. Escolha um.

Opção	Descrição
Marcar como não duplicado	Dois itens vulneráveis distintos que representam pelo menos duas vulnerabilidades exclusivas. Esses dois itens vulneráveis não serão considerados duplicados nos trabalhos que você criar daqui para frente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	As transições de Estado de **Revisão necessária** . **Não duplicado** para **NÚMERO DUP** registro.
Confirmar duplicata	Sua revisão indica que esses dois Vits são duplicados. O registro de VIT que é exibido no registro duplicado rotulado Duplicado transições para **Encerrado** . Uma anotação de trabalho com anotações de encerramento é adicionada ao registro de VIT encerrado. Todas as detecções associadas no VIT encerrado são movidas para o registro de VIT primário. As anotações de trabalho são adicionadas à VIT primária para indicar que uma duplicata foi encerrada e suas detecções foram vinculadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: A propriedade do sistema sn_vul_ai.duplicate_vi_confidence_threshold automatiza o fluxo de trabalho de desduplicação do item vulnerável. Esta propriedade do sistema é ativada por padrão, mas não tem valor limite para uma pontuação de confiança. Sem valor para o limite, o fluxo de trabalho automatizado não fecha duplicatas. **Nota:** Pontuações de confiança de 100 para Vits não são calculadas pelo Now Assist habilidade. Esta pontuação é calculada pela correspondência com a lógica determinística. Se você inserir um valor de limite, todas as duplicatas que tiverem pontuações de confiança maiores do que o valor especificado serão fechadas automaticamente e suas detecções serão acumuladas para o item vulnerável primário. Você pode preferir deixar esta propriedade do sistema em sua configuração padrão sem valor de limite até que você esteja familiarizado com o fluxo de trabalho e tenha algum tempo para estabelecer um valor preciso. Em sua configuração padrão, você pode manter o controle sobre as condições sob as quais seus Vits duplicados são revisados, marcados e processados. Você deve ter a função sn_vul_ai.configure_vi_dedup ou sn_vul_ai.review_duplicate_vi para modificar esta propriedade do sistema.

f. Opcional: Como alternativa, você pode revisar itens duplicados do **Todas as revisões duplicadas** guia lista de um **NÚMERO DUP** registro.
Esta lista permite que você execute uma edição em massa nos registros duplicados e seus registros de VIT associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sugira soluções de vulnerabilidade preferenciais com Now Assist para resposta a vulnerabilidades

Use o raciocínio da IA generativa com Now Assist para resposta a vulnerabilidades(Now Assist Com VR) para ajudar seus analistas a encontrar possíveis soluções preferenciais de fornecedores terceirizados para as vulnerabilidades em seus ativos.

Antes de Iniciar

Consulte Usando Now Assist para resposta a vulnerabilidades para correção de item vulnerável para obter mais informações sobre os requisitos para isso Now Assist habilidade. Consulte Configure e ative uma habilidade para Now Assist para resposta a vulnerabilidades para obter mais informações sobre como ativá-lo.

Funções necessárias:

Nota: Sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e sn_vul.remediation_owner herdam as seguintes funções quando você instala o. Now Assist para resposta a vulnerabilidades aplicação.

- sn_vul_ai.run_suggest_solution - necessário para executar o recurso de solução recomendado em itens vulneráveis.
- sn_vul_ai.read_suggest_solution_job - Necessário para executar o trabalho agendado para tarefas de correção e exibir a tabela Trabalho de solução recomendado [sn_vul_ai_suggest_solution_job] e o status de execução.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Abra um registro de item vulnerável (VIT) do host e selecione **Detalhes** guia.
3. Para usar Now Assist Com o raciocínio de VR para encontrar as soluções que melhor correspondem às suas vulnerabilidades, selecione **Solução recomendada** .
4. Como alternativa, abra uma tarefa de correção (RT) atribuída a você e selecione **Solução recomendada** .

As tabelas a seguir descrevem as mensagens e notificações exibidas e onde os dados são preenchidos depois que você seleciona **Solução recomendada** VIT e registros de tarefa de correção.

Nota: Now Assist Com VR não gera soluções de vulnerabilidade. As soluções são importadas de integrações de terceiros. Para você ver **Solução recomendada** Nos registros de VIT e de tarefa de correção, deve haver pelo menos uma solução de substituição mais alta disponível para a vulnerabilidade associada a essa VIT.

Registros de item vulnerável (VIT)

Mensagem ou notificação	Descrição
Uma possível solução foi encontrada pelo Now Assist para VR para ajudar você a corrigir esta vulnerabilidade. Verifique a seção Correção e o fluxo de atividades na guia Detalhes para obter mais informações.	As informações de uma solução preferencial são preenchidas na guia Detalhes de um VIT nos campos Solução preferencial e Resumo na seção Correção. As anotações de trabalho são inseridas no fluxo de atividades. Certifique-se de verificar as soluções quanto à precisão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem ou notificação	Descrição
	Nota: Se uma VIT tiver uma solução fornecida por Now Assist Para VR, a solução pode mudar se você importar mais soluções e executar novamente o trabalho (selecione **Solução recomendada**).
Uma solução para esta vulnerabilidade foi encontrada usando o Now Assist para VR com base no raciocínio a seguir.	Detalhes no fluxo de atividades no Vits sobre o motivo pelo qual esta solução foi determinada Now Assist VR ser uma solução preferencial. O raciocínio é exibido somente em Vits. As soluções preferenciais encontradas pela habilidade são acumuladas na guia Soluções em Tarefas de correção. Certifique-se de verificar as soluções quanto à precisão.
Uma solução não foi encontrada. Verifique a seção Correção e o fluxo de atividades na guia Detalhes para obter mais informações.	Resumo no fluxo de atividades na guia Detalhes em Vits sobre o motivo pelo qual nenhuma solução foi encontrada. O raciocínio é exibido somente em Vits.

Registros de tarefa de correção (RT)

Mensagem ou notificação	Descrição
Use o Now Assist para VR para ajudar você a encontrar possíveis soluções preferenciais para os itens vulneráveis nesta tarefa de correção. Seu desempenho poderá ser afetado se a tarefa de correção tiver um grande número de Vits.	○ O RT deve ter pelo menos um VIT. O padrão para o número máximo de Vits em um RT é 1 000. Você pode preferir manter esse valor em sua configuração padrão. **Nota:** Você pode modificar o valor máximo com a propriedade do sistema sn_vul_ai.max_vits_allowed_for_suggest_solution. ○ Revisa todos os Vits na tarefa de correção, mas as soluções são recomendadas somente para Vits na tarefa de correção que estão nos estados ativos, têm soluções de substituição mais alta e ainda não têm uma solução. **Nota:** Se você executar o trabalho novamente (selecione **Solução recomendada** Para uma tarefa de correção, por padrão, o trabalho avalia somente Vits sem soluções (verdadeiro). Para avaliar Vits com soluções, você deve mudar a propriedade do sistema sn_vul_ai.exclude_vits_with_solution para falso .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem ou notificação	Descrição
	○ Fornece um resumo da solução preferencial no fluxo de atividades na guia Detalhes da tarefa de correção. ○ As soluções preferenciais encontradas pela habilidade são acumuladas na guia Soluções em Tarefas de correção. ○ Rola as informações da solução para Vits correspondentes na tarefa de correção. As informações da solução são preenchidas nos campos Solução preferencial e Resumo e no fluxo Atividade nas guias Detalhes. ○ . Se um trabalho em segundo plano estiver em andamento e avaliando soluções para esse registro, o. **Solução recomendada** o botão não está visível na tarefa de correção. Você pode exibir o botão após a conclusão do trabalho. Certifique-se de verificar as soluções quanto à precisão.
Atualmente reunindo soluções para Vits. Selecione este link para rastrear o andamento.	Consulte Status do trabalho e um resumo que inclui as seguintes informações: ○ Número total de Vits na tarefa de correção: n ○ Número de Vits processados: n ○ Vits com soluções: n Vits Se não houver informações suficientes para sugerir com confiança uma solução, as soluções não serão fornecidas para o Vits. O resumo também é fornecido no fluxo de atividades depois que o trabalho é concluído.
As soluções não serão fornecidas para Vits se não houver informações suficientes para sugerir uma solução com confiança.	Não foram encontradas soluções para determinados Vits, porque não há informações suficientes ou não foram fornecidas soluções de maior substituição Now Assist para determinar uma solução. ○ Os campos Solução preferencial e Resumo permanecem vazios no VIT. ○ As anotações de trabalho são inseridas no fluxo de atividades na tarefa de VIT e correção. ○ O raciocínio é exibido somente em Vits.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando fluxos de trabalho do agentic em Now Assist para Resposta a vulnerabilidades

Use Resposta a vulnerabilidades Agentes de IA para concluir suas tarefas de forma autônoma.

Fluxos de trabalho do agente disponíveis para agentes de IA para Resposta a vulnerabilidades

Nome do fluxo de trabalho do Agentic	Descrição	Agentes de IA disponíveis
Avaliar a exposição à vulnerabilidade	• Determine se seus itens de configuração (ICs) e serviços de negócio estão expostos a vulnerabilidades conhecidas. • Determine o possível impacto que uma vulnerabilidade específica pode ter em todo o seu ambiente. • Verifique os ICs quanto a novas vulnerabilidades exploráveis (dia zero) da Agência de segurança cibernética e infraestrutura (CISA). • Crie tópicos de observação no espaço do Gerenciador de vulnerabilidades para corrigir itens vulneráveis.	• Agente de IA de análise de vulnerabilidade do CISA • Agente de IA de análise de exposição a vulnerabilidades • Assistir ao agente de IA de criação de tópico
Analisar o status de correção de vulnerabilidades	• Obtenha informações sobre suas métricas de conformidade e estatísticas sobre o quão bem você está cumprindo as datas de meta de correção em registros de item vulnerável (VIT). • Exiba os totais mensais de correção de registro de VIT e identifique metas perdidas. • Divida os dados de correção em Vits por **Gravidade** , **Grupo de atribuição** , **Item de configuração** e **Vulnerabilidade** Para	Agente de IA de análise de conformidade de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos de trabalho do agente disponíveis para agentes de IA para Resposta a vulnerabilidades

Nome do fluxo de trabalho do Agentic	Descrição	Agentes de IA disponíveis
	suas revisões mensais de conformidade do Acordo de nível de serviço (ANS).	

Importante: Por padrão, todos os fluxos de trabalho do agente e registros do agente de IA são somente leitura.

Para modificar um fluxo de trabalho do agentic, você deve primeiro Duplicar um fluxo de trabalho do agentic e prossiga com as seguintes etapas:

- Ative o fluxo de trabalho do agentic. . Now Assist para resposta a vulnerabilidades Os agentes de IA incluídos com a aplicação são ativados por padrão.
- Se necessário, você pode adicionar um gatilho para invocar o fluxo de trabalho do agentic automaticamente.

Procurando um agente de IA?

- Pode haver agentes de IA instalados com o. Now Assist aplicações que não são usadas em fluxos de trabalho agentivos. Para saber como ver todos os agentes disponíveis em sua instância, consulte Encontre agentes de IA .
- Para encontrar agentes que podem não estar instalados em sua instância, visite AI Agent Marketplace em ServiceNow Store.

- Avalie o fluxo de trabalho do agente de exposição a vulnerabilidades.

  Bate-papo com um agente com IA do Now Assist painel para ajudar você a avaliar se seus itens de configuração e seus serviços de negócios estão expostos a vulnerabilidades.

- Analisar o fluxo de trabalho do agente de status de correção de vulnerabilidade.

  Bate-papo com um agente com IA do Now Assist painel para ajudar você a obter informações sobre suas métricas de conformidade para resolver itens vulneráveis.

Avalie o fluxo de trabalho do agente de exposição a vulnerabilidades

Bate-papo com um agente com IA do Now Assist painel para ajudar você a avaliar a possível exposição de seus itens de configuração e seus serviços de negócios a vulnerabilidades.

Antes de Iniciar

. Now Assist o painel deve ser ativado. Para obter mais informações, consulte Ligue o. Now Assist painel .

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.vulnerability_analyst

Procedimento

1. Selecione Now Assistícone ( ) de qualquer lugar em sua instância.
   . Now Assist o painel é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O fluxo de trabalho do agente Avaliar exposição à vulnerabilidade é sob demanda. Você pode inserir qualquer consulta em linguagem natural, mas considere usar os prompts descritos na tabela e nas etapas a seguir para começar a se familiarizar com os dados de vulnerabilidade disponíveis e o que você pode fazer com eles. As etapas a seguir mostram como solicitar dados de vulnerabilidade atuais, criar um tópico de observação com base nos resultados retornados e determinar o impacto geral que uma vulnerabilidade pode ter em seu ambiente.

Sua solicitação ou resposta	Descrição
Quais são as vulnerabilidades recentes da CISA?	**Recente** em sua pergunta, refere-se a novas vulnerabilidades que surgiram durante os últimos sete dias. Sete dias (uma semana) é o período de tempo padrão para o fluxo de trabalho do agentic. Se você quiser pesquisar novas vulnerabilidades para um período de tempo específico diferente de sete dias, digite uma solicitação com um valor que ocorreu no passado, como, **Quais são as vulnerabilidades recentes nos últimos 30 dias?**
Sim, crie um tópico de observação para a vulnerabilidade CVE-2018-9065.	Quando perguntado se você deseja criar um tópico de observação, você pode preferir ser específico em sua resposta. Por exemplo, confirme a solicitação e digite uma vulnerabilidade específica no formato: **CVE-2018-9065** .
Você pode me fazer uma análise de impacto detalhada para a vulnerabilidade CVE-2018-9065?	A análise de possível impacto de vulnerabilidades é compatível somente com serviços de negócio afetados e classes de item de configuração.
Mostrar saída da pergunta anterior.	Solicite que o agente revise sua pergunta anterior se ela não fornecer uma resposta.
Encerre a sessão ou **Parar** .	Encerre a conversa.

Sua conversa é salva até que você inicie um novo bate-papo. Se a conversa terminar inesperadamente, inicie um novo bate-papo. Para iniciar um novo bate-papo, selecione o ícone Novo bate-papo ( ).

2. Insira uma solicitação em linguagem natural para ver se você está exposto a alguma vulnerabilidade recente, por exemplo, **Quais são as vulnerabilidades recentes da CISA?**

   Como sua entrada não especifica um intervalo, o agente coleta, por padrão, dados de vulnerabilidade exploráveis da Agência de segurança cibernética e infraestrutura (CISA) sobre seus ativos e retorna informações dos últimos sete dias.

   As vulnerabilidades CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) que afetam seus ativos e têm itens vulneráveis associados a eles em seu ambiente são listadas.

   Você pode ver que o agente também retorna aliases que correspondem às CVEs. Os aliases serão relatados se você estiver usando scanners de terceiros para importar seus dados de vulnerabilidade. Por exemplo, CVE-2018-8627 (alias: TEN-119686, TEN-119596) com gravidade Média tem 4 itens vulneráveis (Vits). Esta resposta indica que a vulnerabilidade foi descoberta e importada pelo produto de scanner Tenable (DEZ).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. **Opcional:** Selecione o link Vulnerabilidades exploráveis conhecidas da CISA para obter informações sobre todos os CVEs retornados.
   A lista é aberta em uma nova guia no UI16.
4. Retorne ao bate-papo e insira uma solicitação para que o agente crie um tópico de observação para um CVE no prompt, por exemplo, **Sim, crie um tópico de observação para a vulnerabilidade CVE-2018-9065.**
   O agente propõe um nome para o tópico de observação e solicita confirmação. Você pode mudar o nome.
5. Insira **OK** .
6. Selecione o link para exibir o tópico de observação no espaço do Gerenciador de vulnerabilidades e exibir mais detalhes, bem como os itens vulneráveis associados ao CVE.
   A lista é aberta em uma nova guia no UI16. Depois de revisar os dados, você pode decidir que deseja obter mais informações sobre o impacto que o CVE tem em seus outros ativos.
7. Retorne ao Now Assist e insira e solicite ao agente uma análise de impacto detalhada, por exemplo, **Você pode me fazer uma análise de impacto detalhada para a vulnerabilidade CVE-2018-9065?**
   Esta solicitação retorna informações sobre seus itens de configuração e serviços de negócio que são afetados por este CVE. Ele fornece um detalhamento de criticalidade, uma lista de serviços de negócio afetados e uma lista das classes de itens de configuração afetados. Há também um link para obter informações mais detalhadas.
8. **Opcional:** Solicite uma avaliação geral de exposição a vulnerabilidades para um serviço de negócios específico.
   As informações sobre o serviço de negócios incluem itens vulneráveis associados, criticidade (risco) e os itens de configuração por classe são listadas.

Analisar o fluxo de trabalho do agente de status de correção de vulnerabilidade

Bate-papo com um agente com IA do Now Assist painel para ajudar você a obter informações sobre suas métricas mensais de conformidade de correção para itens vulneráveis.

Antes de Iniciar

. Now Assist o painel deve ser ativado. Para obter mais informações, consulte Ligue o. Now Assist painel .

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.vulnerability_analyst admin

Procedimento

1. Selecione Now Assistícone ( ).
   . Now Assist o painel é exibido.

   O fluxo de trabalho do agente Analisar status de correção de vulnerabilidade é sob demanda. Você pode inserir qualquer consulta em linguagem natural, mas considere usar os prompts descritos na tabela e nas etapas a seguir para se familiarizar com os dados disponíveis e o que pode ser feito com eles.

   Essas etapas fornecem informações sobre suas métricas de conformidade de quão bem suas equipes atendem às datas de meta de correção mensais para registros de itens vulneráveis, conforme relatado no Acordo de nível de serviço (ANS).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua solicitação ou resposta	Descrição
Qual é minha conformidade para correção para o mês de outubro de 2024?	Por padrão, a pesquisa é baseada no grupo de atribuição. Se você não especificar um mês, o agente de IA procurará o mês atual e começará a retroceder no tempo, um mês de cada vez. Como alternativa, você pode solicitar ao agente um detalhamento por classe de item de configuração ou vulnerabilidade. Por exemplo, digite **Qual é a minha conformidade para o mês de outubro de 2024 para servidores Windows?**
Quais tipos de ativos foram responsáveis pelos SLAs mais perdidos?	Os resultados são organizados com base nos dados do mês da solicitação original por tipo de ativo.
Qual grupo de atribuição teve o menor número de SLAs críticos perdidos?	Obtenha o grupo de atribuição que teve os SLAs mais ou menos perdidos com base na gravidade do item vulnerável (VIT): Crítico , Alto , Médio e Baixo . Além disso, você pode solicitar que o agente de IA pesquise SLAs perdidos por categoria de VIT.
Mostrar saída da pergunta anterior.	Solicite que o agente revise sua pergunta anterior se ela não fornecer uma resposta.
Encerre a sessão ou **Parar** .	Encerre a conversa.

Sua conversa é salva até que você inicie um novo bate-papo. Se a conversa terminar inesperadamente, inicie um novo bate-papo. Para iniciar um novo bate-papo, selecione o ícone de novo bate-papo ( ).

2. Insira uma solicitação em linguagem natural para ver suas métricas de correção para um determinado mês e ano, por exemplo, Qual é minha conformidade para correção para o mês de outubro de 2024?

   Os resultados são organizados em seções.

   - Total de registros que tinham metas de correção de ANS para o mês e ano solicitado e o percentual total de datas de meta perdidas e atendidas.
   - Detalhamento por gravidade - Os itens vulneráveis que não atingiram as metas de correção são divididos por gravidade crítica, alta, média e baixa.
   - Detalhamento por grupos de atribuição - Porcentagem do total de registros com metas perdidas divididas por grupos de atribuição.
   - Link Conformidade de correção para outubro de 2024 - Exibir mais informações sobre os dados. Uma nova guia é aberta no UI16.

3. Você pode solicitar informações mais específicas sobre ANS perdidos, por exemplo, Quais tipos de ativos foram responsáveis pelos SLAs mais perdidos?
   Os resultados são organizados para os dados do mês da sua solicitação original por tipo de ativo, por exemplo, Servidor Windows, Banco de dados, Servidor Linux, e assim por diante.

4. Você pode solicitar informações mais específicas sobre a produtividade de suas equipes durante esse mês, por exemplo, Qual grupo de atribuição teve o menor número de SLAs críticos perdidos?

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É retornado o grupo de atribuição que tinha o menor número de Crítico Vits que perderam o ANS.

5. Você pode comparar esses resultados com outro mês, por exemplo, Como esses dados se comparam com novembro de 2024?
   Os resultados são organizados em seções.
   - Resumo da comparação - Total de registros que tinham metas de correção de ANS para o período solicitado pela primeira vez (**Outubro de 2024** em comparação com sua solicitação mais recente (**Novembro de 2024**).
   - Detalhamento por gravidade - Itens vulneráveis que não foram atingidos pelas metas de correção são divididos por gravidade: Crítico , Alto , Médio e Baixo .
   - Análises - Análise de dados e informações sobre tendências de dados com base na comparação.
   - Link Conformidade de correção para novembro de 2024 - Exibir mais informações sobre os dados usados para a comparação. Uma nova guia é aberta no UI16.

Now Assist para resposta a vulnerabilidades informações de referência

Ferramentas, agentes e informações de coleta de agentes de IA para Now Assist para resposta a vulnerabilidades.

Referências

Exiba visões gerais dos seguintes fluxos de trabalho do agente.

- Resposta a vulnerabilidades Coleção de agentes de IA para o fluxo de trabalho do agente Avaliar exposição à vulnerabilidade
- Resposta a vulnerabilidades Coleção de agentes de IA para o fluxo de trabalho do agente Analisar status de correção de vulnerabilidade

Resposta a vulnerabilidades Coleção de agentes de IA para o fluxo de trabalho do agente Avaliar exposição à vulnerabilidade

As ferramentas e os agentes de IA para o fluxo de trabalho do agente Avaliar exposição à vulnerabilidade.

Visão geral do fluxo de trabalho do Agentic

Os seguintes fluxos de trabalho do agente estão incluídos com a aplicação Now Assist for Vulnerability Response:

- Avalie o fluxo de trabalho do agente de exposição a vulnerabilidades
- Analisar o fluxo de trabalho de status de correção de vulnerabilidade

Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a versão duplicada do fluxo de trabalho do agentic.

Avaliar exposição a vulnerabilidades Fluxo de trabalho do agente Visão geral do fluxo de trabalho do agente

Use o fluxo de trabalho do agente Avaliar exposição à vulnerabilidade do Now Assist painel para ajudá-lo a:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Determine se seus itens de configuração (ICs) e serviços de negócio estão expostos a vulnerabilidades conhecidas.
- Determine o possível impacto que uma vulnerabilidade específica pode ter em todo o seu ambiente.
- Verifique os ICs quanto a novas vulnerabilidades exploráveis (dia zero) da Agência de segurança cibernética e infraestrutura (CISA).
- Crie tópicos de observação no espaço do Gerenciador de vulnerabilidades para corrigir itens vulneráveis.
- Ajustar conteúdo em linguagem natural.

Agentes usados no fluxo de trabalho do agente Avaliar exposição à vulnerabilidade

- Executor de ação de resposta a vulnerabilidades
- Analisador de vulnerabilidades exploradas conhecidas da CISA
- Consultor de avaliação de exposição a vulnerabilidades

Resposta a vulnerabilidades Coleção de agentes de IA para o fluxo de trabalho do agente Analisar status de correção de vulnerabilidade

As ferramentas e os agentes de IA para o fluxo de trabalho do agente Analisar status de correção de vulnerabilidade.

Analisar visão geral do fluxo de trabalho do agente de status de correção de vulnerabilidade

Use o fluxo de trabalho do agente Analisar status de correção de vulnerabilidade do Now Assist painel para ajudá-lo a:

- Obtenha informações sobre suas métricas de conformidade e estatísticas sobre o quão bem você está cumprindo as datas de meta de correção em registros de item vulnerável (VIT).
- Exiba os totais mensais de correção de registro de VIT e identifique metas perdidas.
- Divida os dados de correção em Vits por **Gravidade** , **Grupo de atribuição** , **Item de configuração** e. **Vulnerabilidade** Para suas revisões mensais de conformidade do Acordo de nível de serviço (ANS).

Se você quiser modificar este fluxo de trabalho do agente, você pode duplicado ajuste as configurações para atender às suas necessidades específicas e ative a versão duplicada do fluxo de trabalho do agentic.

Agente usado no fluxo de trabalho do agente do agente Analisar status de correção de vulnerabilidade

O Provedor de informações de conformidade de correção é usado pelo fluxo de trabalho do agente Analisar status de correção de vulnerabilidade.

Tradução automática

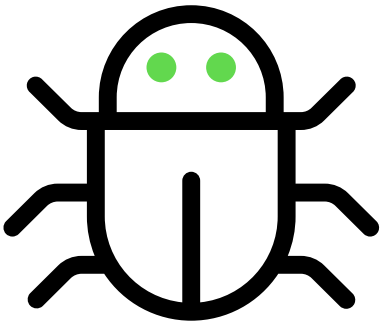
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de gestão de superfície de ataque

. Resposta a vulnerabilidades e outras aplicações que compõem a gestão de superfícies de ataque ajudam você a priorizar seus ativos vulneráveis e adicionar contexto para ajudar a determinar quando os sistemas críticos para os negócios estão ameaçados. Usando o CMDB, suas equipes de segurança também podem identificar facilmente as dependências entre sistemas e avaliar rapidamente o impacto das mudanças ou dos tempos de inatividade nos negócios.

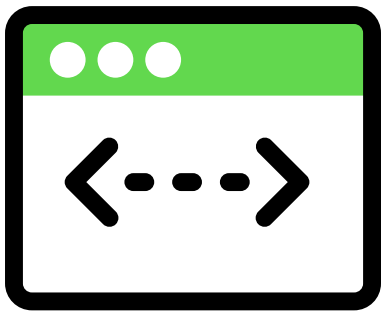
Resposta a vulnerabilidades aplicações

Resposta a vulnerabilidades



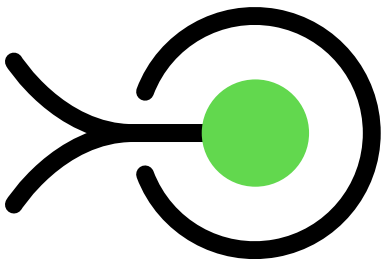
Saiba mais sobre a aplicação Resposta a vulnerabilidades

Resposta a vulnerabilidades de aplicações



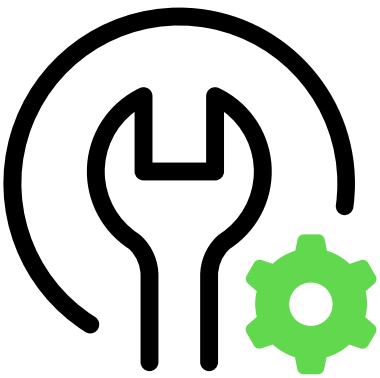
Saiba mais sobre a aplicação Resposta a vulnerabilidades da aplicação

Resposta a vulnerabilidades do contêiner



Saiba mais sobre a aplicação Resposta a vulnerabilidades do contêiner

Conformidade de configurações



Saiba mais sobre a aplicação Conformidade de configuração

Lista de materiais de software



Saiba mais sobre as aplicações de Lista de materiais de software

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades Espaços de trabalho

Espaço para gerentes de vulnerabilidades	Espaço de correção de TI	Espaço de avaliação de vulnerabilidade
		
Saiba mais sobre o Espaço do gerenciador de vulnerabilidades	Saiba mais sobre o Espaço de correção de TI	Saiba mais sobre o Espaço de avaliação de vulnerabilidades

Solucionar problemas e obter ajuda

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

Resposta a vulnerabilidades

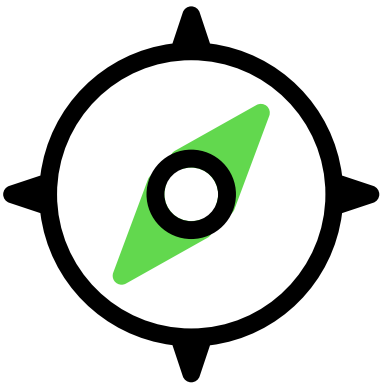
O National Vulnerability Database (NVD) e outras fontes coletam informações sobre vulnerabilidades conhecidas. Essas vulnerabilidades podem incluir pontos fracos no software, sistemas operacionais que o malware pode explorar e outros ataques. . ServiceNow® Resposta a vulnerabilidades a aplicação ajuda você a rastrear, priorizar e resolver essas vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

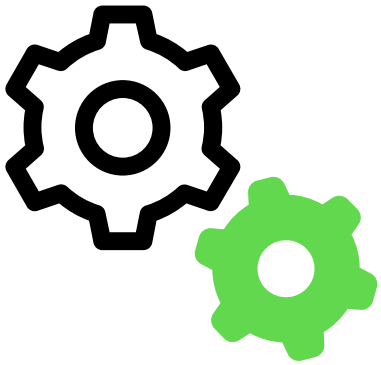
Resposta a vulnerabilidades

Explorar



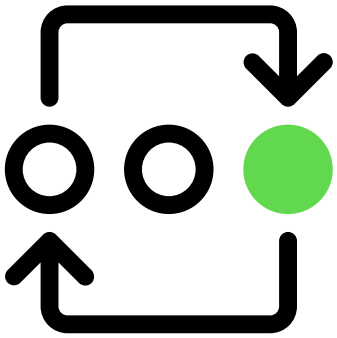
Saiba mais sobre os recursos do Resposta a vulnerabilidades

Configurar e Configurar



Instale e configure sua aplicação de Resposta a vulnerabilidades

Integrar



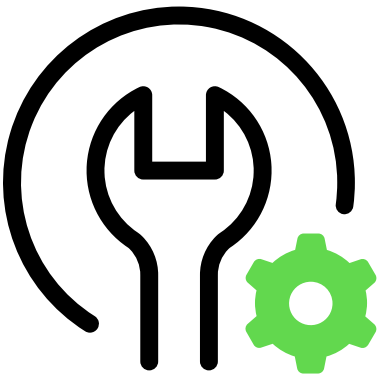
Integre o Vulnerability Response a outras aplicações

Use os Espaços de resposta a vulnerabilidades



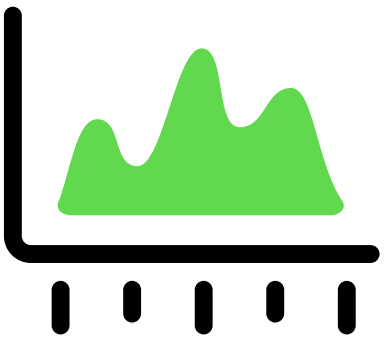
Saiba como monitorar, gerenciar e corrigir Vits nos espaços de trabalho do Gerenciador de vulnerabilidades, Correção de TI e Avaliação de vulnerabilidades.

Corrigir



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

Análise e emissão de relatórios

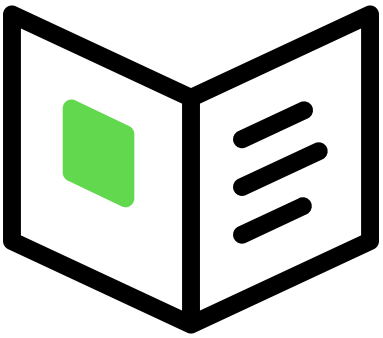


Monitorar o andamento da correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referência



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

Solucionar problemas e obter ajuda

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

Explorar o. Resposta a vulnerabilidades aplicação

. ServiceNow® Resposta a vulnerabilidades a aplicação importa e agrupa automaticamente itens vulneráveis de acordo com regras que permitem corrigir vulnerabilidades rapidamente. Os dados de vulnerabilidade são extraídos de fontes externas, como o National Vulnerability Database (NVD) e integrações de terceiros, e processados com aplicações desenvolvidas por ServiceNow®.

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

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

Resposta a vulnerabilidades e seu ambiente empresarial

Em um ambiente empresarial, as organizações usam scanners de vulnerabilidade e ferramentas de avaliação para identificar e gerenciar os riscos que as vulnerabilidades representam para seus ativos. As vulnerabilidades identificadas por essas ferramentas se traduz em riscos para as equipes de segurança e TI responsáveis por manter e proteger os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ativos de uma organização. Alguns riscos podem incluir, entre outros, os seguintes tipos de vulnerabilidades identificadas:

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

À medida que esses riscos potenciais são expostos, as equipes de segurança e TI geralmente enfrentam desafios no processamento e manipulação do volume de informações de vulnerabilidade geradas por suas ferramentas de verificação e avaliação. Essas equipes se veem sobrecarregadas ao gerenciar um alto volume de vulnerabilidades identificadas e elaborar esforços de resposta acionáveis para mitigar os possíveis riscos que suas organizações enfrentam.

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

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

Resposta a vulnerabilidades, Operações de segurança e o. ServiceNow AI Platform®

. Resposta a vulnerabilidades a aplicação faz parte do Operações de segurança pacote. Juntos, esses aplicativos ajudam você a proteger seus ativos, melhorando sua postura geral de segurança.

. ServiceNow Resposta a vulnerabilidades a aplicação tem dois objetivos primários:

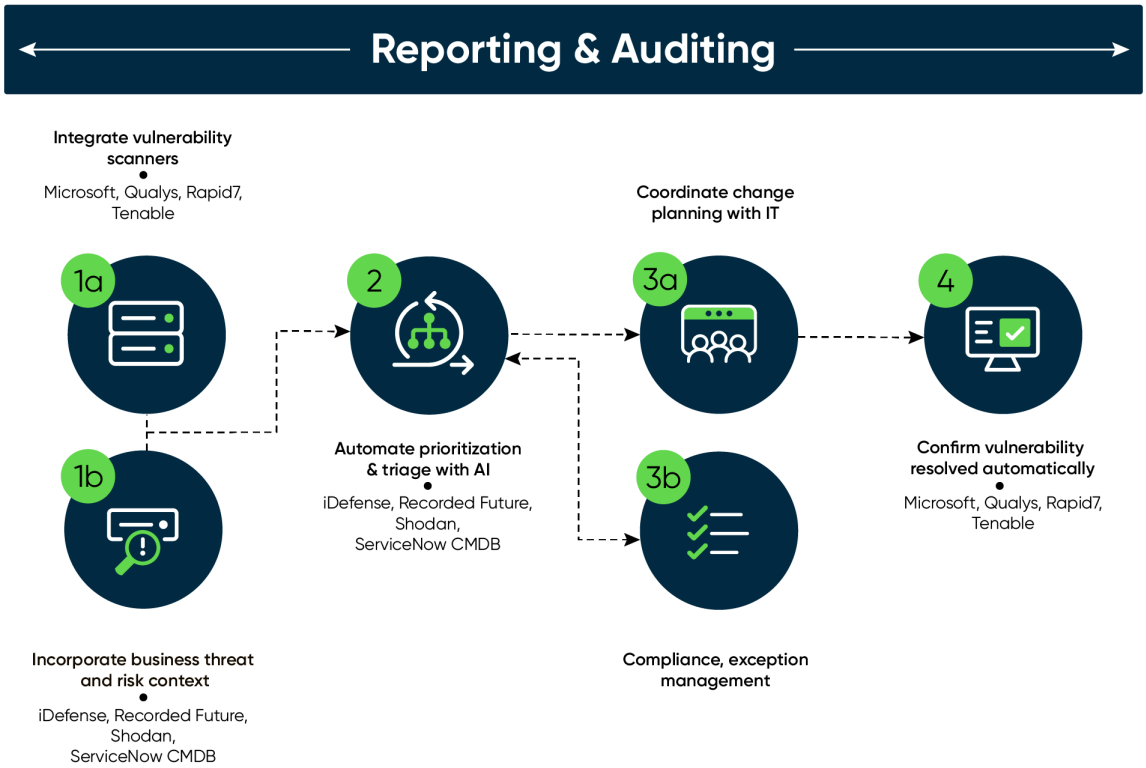
- Ajude as equipes de segurança desafiadas a lidar com enormes quantidades de dados de vulnerabilidade.
- Ajude as equipes de operações encarregadas de resolver vulnerabilidades.

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



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

Quem pode usar Resposta a vulnerabilidades em sua organização

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

Analista de vulnerabilidades

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

Importante: O analista de vulnerabilidades usa principalmente o. Espaço do gerente de vulnerabilidade para monitorar e criar tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Responsável pela correção

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

Importante: O responsável pela correção trabalha principalmente em tarefas de correção de no Espaço de correção de problemas de TI.

Resposta a vulnerabilidades de aplicações

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

Versões disponíveis

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

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

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações. Para obter mais informações, consulte Resposta a vulnerabilidades aplicações e. CSDM tabelas.

Instalação de Resposta a vulnerabilidades e aplicações compatíveis

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas para configuração básica

. Resposta a vulnerabilidades a aplicação é necessária como primeira etapa. Para obter mais informações sobre como instalá-lo, consulte Check-list de implementação do Resposta a vulnerabilidades aplicação e. Instale o Vulnerability Response aplicação.

- Após a conclusão da instalação, você pode Configure a Resposta a vulnerabilidades usando o Assistente de configuração .

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

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

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

- Selecione uma aplicação de análise, quando aplicável. O Pacote de conteúdo do Performance Analytics para a aplicação Resposta a vulnerabilidades contém relatórios que cobrem todas as fases do ciclo de vida da gestão de vulnerabilidades.

  [Opcional] Instale e configure o. Performance Analytics para Resposta a vulnerabilidades Aplicação [PA] aplicação.

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

  Nota:

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

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

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

Outras tarefas de configuração que você pode executar

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas avançadas fora da configuração básica

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

Resposta a vulnerabilidades personas e funções granulares

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

Uma das primeiras etapas de configuração necessárias para Resposta a vulnerabilidades a aplicação é atribuir funções a usuários e grupos. As funções definem o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidades e todas as integrações de terceiros com Resposta a vulnerabilidades.

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

Nota:

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para Resposta a vulnerabilidades aplicação. O acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário da correção anteriores à 10.3 não foi alterado.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver no Resposta a vulnerabilidades no nível da tarefa, você pode preferir usar funções granulares. Para obter mais informações, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

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

Funções de persona e funções granulares iniciando

Principais termos.

Função

As funções definem o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação.

Grupo

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

Função de persona

Uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidades, Analista de vulnerabilidades, Proprietário da correção, Gerenciador de item de configuração, e o Exception Manager são projetados para corresponder a cargos comuns para gerentes, analistas e responsáveis pelo serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Funções herdadas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

ACL (Access Control List, lista de controle de acesso)

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

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

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

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

As tabelas a seguir são listadas Resposta a vulnerabilidades funções de persona instaladas com a aplicação .

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

Funções granulares e funções de persona

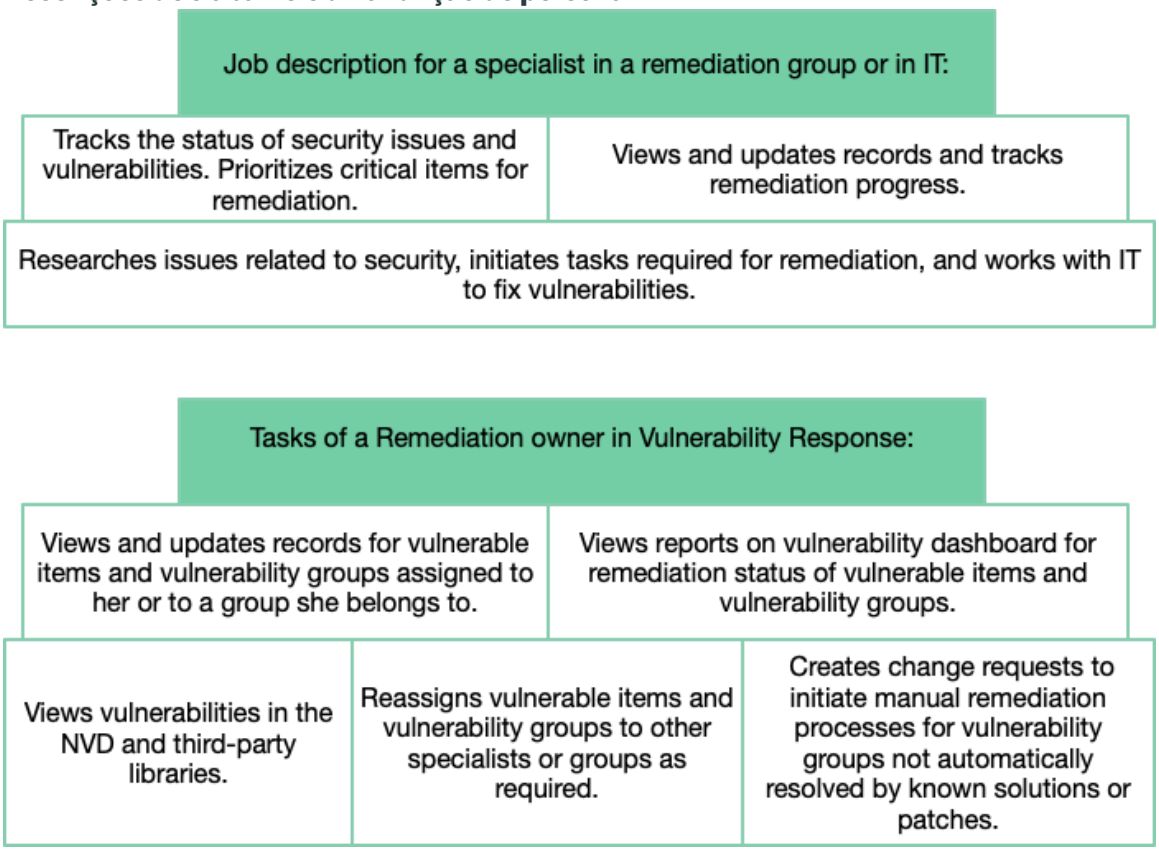
Uma maneira de pensar sobre as funções de persona é considerar como suas descrições podem estar relacionadas às descrições de trabalho para várias posições de correção de vulnerabilidades ou de TI em sua organização. A figura a seguir ilustra uma possível

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

descrição do trabalho para um especialista em correção em TI e como as tarefas associadas a este trabalho se relacionam com as tarefas de uma função de persona do responsável pela correção no Resposta a vulnerabilidades aplicação.

Descrições de trabalho e uma função de persona



A descrição do trabalho e a função da persona do responsável pela correção podem ser definidas como uma série de tarefas de correção. Na imagem anterior, uma descrição de trabalho e uma função de persona em blocos verdes ficam acima das tarefas que as descrevem. Alguns dos requisitos de trabalho típicos para um especialista em um grupo de correção correspondem diretamente às tarefas que compõem a persona do responsável pela correção em Resposta a vulnerabilidades: Revise e atualize registros, rastreie o status de correção de vulnerabilidades, priorize itens para correção e aplique correções e patches com ELES.

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

As funções granulares definem as tarefas

Os nomes das funções granulares em Resposta a vulnerabilidades geralmente descreva o que os usuários podem fazer e ver no Resposta a vulnerabilidades aplicação. Por exemplo, na imagem anterior, usuários e grupos com a persona de responsável pela correção atribuída têm as funções granulares sn_vul.read_assigned e sn_vul.write_assigned. Essas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

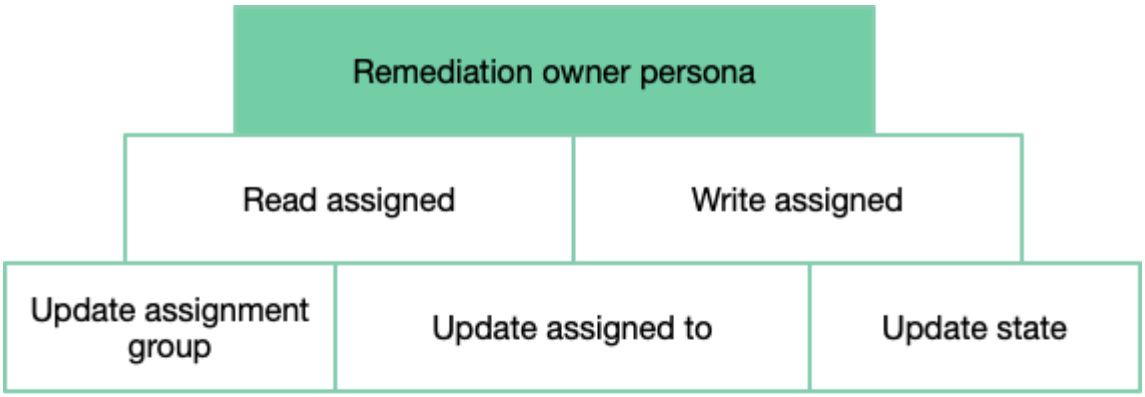
funções granulares permitem que usuários ou grupos exibam e atualizem itens vulneráveis e registros de tarefa de correção atribuídos a eles. Para exibir descrições de funções granulares específicas, como um usuário com a função de administrador do sistema, navegue até **Administração de Usuários** > **Funções** e localize a função desejada. As funções que são herdadas automaticamente quando uma função é atribuída são listadas. Além disso, quando uma função depende de outras atribuições de função, todas as funções necessárias também são listadas.

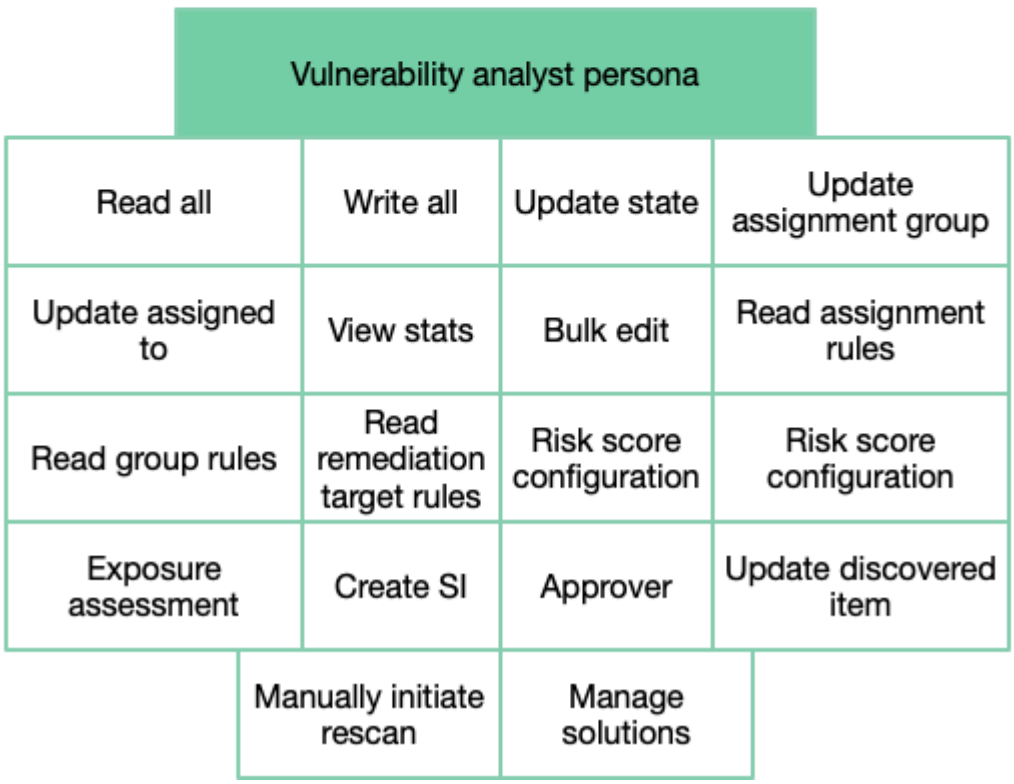
Na imagem a seguir, as funções granulares da persona do responsável pela correção e da persona do analista de vulnerabilidades são ilustradas. Observe que a persona do responsável pela correção não inclui as permissões read_all e write_all da persona do analista de vulnerabilidades. As funções granulares,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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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





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

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

Funções granulares com acesso de script

As seguintes funções fornecem acesso de script às tabelas listadas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função	Tabela	Aplicação
sn_vul.manage_auto_close_stale_vi	sn_vul_cmn_auto_close_rule	Resposta a vulnerabilidades
sn_vul.app_manage_auto_close_rule		Resposta a vulnerabilidades
sn_vul_container.manage_auto_close_stale_vi		Resposta a vulnerabilidades do contêiner
sn_vul_container.manage_assignment_rules	sn_vul_assignment_rule	Resposta a vulnerabilidades do contêiner
sn_vul.app_manage_assignment_rules		Resposta a vulnerabilidades de aplicações
sn_vul.manage_assignment_rules		Resposta a vulnerabilidades
sn_vul_agile.write	sn_vul_agile_tool	Resposta a vulnerabilidades
sn_vul_int_fw.configure_integrations	sn_vul_int_fw_integration	Resposta a vulnerabilidades

Funções granulares no módulo Administração de usuários

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

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

Resposta a vulnerabilidades visão geral das regras de atribuição

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

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

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

Tipo de atribuição, se **Manual** ou **Regra** Está disponível no formulário VIT e na exibição de lista. Qualquer VIT originalmente atribuída por uma regra, mas posteriormente reatribuída manualmente contém uma referência à regra original.

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

Os grupos de atribuição definidos por regras de atribuição são usados por **Regras da tarefa de correção** Para atribuir responsáveis a tarefas de correção (VULs).

Nota: Para fazer Rapid7 InsightVM Etiquetas de ativo disponíveis para uso no filtro de condição para Regras de atribuição, você deve executar o. Rapid7 InsightVM Integração da lista de ativos antes da outra Rapid7 InsightVM integrações.

A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuir itens vulneráveis automaticamente

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

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

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

Processo de avaliação da regra de atribuição

As regras de atribuição são usadas para avaliar e atribuir um VIT quando um novo VIT é aberto, ou seja, importado, criado manualmente ou reaberto. A menos que você reaplique manualmente as regras de atribuição após a VIT ou suas mudanças de estado, uma VI será avaliada uma vez.

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

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

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

> **Nota:** A regra padrão é a regra com o valor de ordem de execução mais alto. Uma regra final a ser usada que é uma boa abordagem é verdadeiro . Se não houver uma regra padrão, o VIT permanecerá sem atribuição quando a regra da tarefa de correção fizer a atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reaplicar regras de atribuição

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

Nota:

. *`Reapply all vulnerability assignment rules`*o trabalho agendado não foi executado antes do primeiro uso **Aplicar mudanças** , Em seguida, ele executa todas as regras de atribuição em todos os Vits abertos, exceto os VIS que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** execute novamente somente as regras alteradas e todas as regras dependentes. Mudanças em uma regra podem resultar em uma VIT correspondente a uma regra não modificada diferente. Reaplicar regras de atribuição não reagrupa os itens vulneráveis.

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

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

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

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

Para habilitar a propriedade do sistema:

1. Navegar até **Tudo** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Abra a propriedade do sistema sn_vul.rerun_task_rules.
3. Em **Valor** , defina o valor como verdadeiro.

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

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

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

Para habilitar a regra de negócio:

1. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.
2. Regra de negócio Abrir Link para tarefas de correção.
3. Selecione **Ativo** caixa de seleção para ativar a regra de negócio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Nota:

- Os itens vulneráveis são removidos dos grupos sem excluir os grupos.
- São removidos somente os itens que são criados usando regras de tarefa de correção ou esforço de correção.
- O reagrupamento é feito automaticamente somente quando o grupo de atribuição muda como parte de uma regra de atribuição e não quando é alterado manualmente.
- As regras de atribuição não se aplicam a Vits no estado Adiado. Se uma VIT for adiada, você deverá atribuí-la manualmente, se necessário.

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

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

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

Acompanhamento de contagens de adiamentos para itens vulneráveis e tarefas de correção

Rastreie o número de vezes que um item vulnerável, um item vulnerável à aplicação, um item vulnerável ao contêiner ou uma tarefa de correção é adiada. Um trabalho agendado, **definir contagens de adiamentos** É executado diariamente para contabilizar contagens para os registros que são adiados mais de uma vez na coluna Contagem de adiamentos. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Atualizando itens vulneráveis automaticamente

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

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

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

Você pode marcar a caixa de seleção novamente manualmente no estado Em investigação. **Atualizar automaticamente itens vulneráveis relacionados** não é desabilitado quando a tarefa de correção é movida para **Aguardando implementação** estado. No estado Aguardando implementação, nenhum novo item vulnerável poderá ser adicionado à tarefa existente, nem os itens vulneráveis existentes poderão ser removidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Atualizando itens vulneráveis manualmente

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

Tarefas de correção criadas manualmente usando **Condição** ou **Grupo de filtros** os tipos de filtro são atualizados uma vez por hora.

Noções básicas sobre as regras de tarefa de correção

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

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

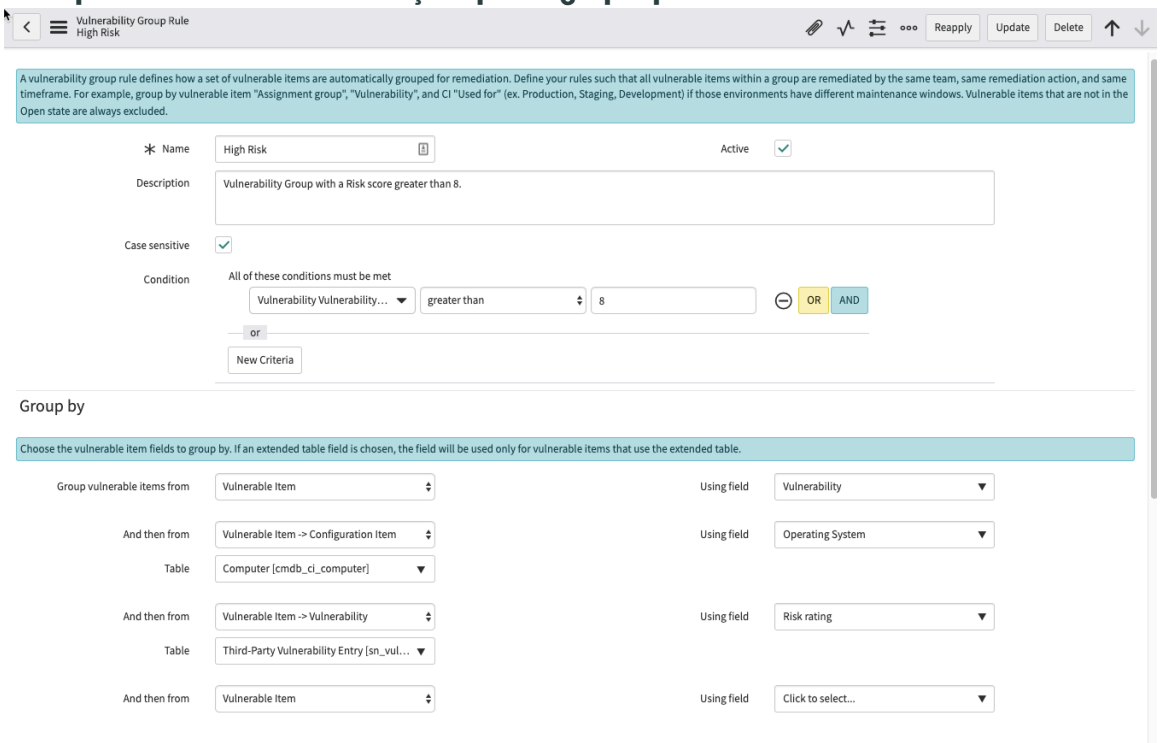
Nota: Para fazer Rapid7 InsightVM Etiquetas de ativo disponíveis para uso no filtro de condição para Regras de tarefa de correção, você deve executar o. Rapid7 InsightVM Integração da lista de ativos antes da outra Rapid7 InsightVM integrações.

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

Um conjunto diferente de regras pode ser usado para itens vulneráveis que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado à regra da tarefa de correção **Agrupar por** valores para fazer a descrição resumida do novo registro. Consulte Crie manualmente uma tarefa de correção em Resposta a vulnerabilidades para obter mais informações sobre os campos disponíveis.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de construtor de condições para Agrupar por entradas



Quando um novo item vulnerável é criado, importado ou reaberto após ser encerrado, as regras de vulnerabilidade são avaliadas em relação a ele. Uma VI só é avaliada uma vez, automaticamente, a menos que seja reaberta após ser fechada ou as regras sejam reaplicadas manualmente.

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

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

  Nota: O campo Descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidades mais longos estão truncados.

  A regra verifica se há uma correspondência **Aberto** Tarefa de correção atribuída ao mesmo grupo de atribuição que o VI.
  - Se a tarefa for encontrada, o VI será adicionado à tarefa existente no **Aberto** estado.
  - Se não houver tarefa no **Aberto** encontrado, a regra cria um **Alto risco: QID-32342** A atribui ao mesmo grupo de atribuição que o VI e coloca o VI na tarefa de correção.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras em **Regras de atribuição** módulo. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Quando uma regra de tarefa é excluída, na exibição de formulário ou de lista, você tem a opção de excluir tudo **Aberto** tarefas criadas por essa regra. Tarefas que não estão no **Aberto** estão excluídos.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use **Reaplicar** botão na página de regra da tarefa de correção para executar novamente a regra alterada em todos os ativos **Aberto** tarefas de correção criadas por essa regra. Exclui e recria tarefas de correção com base na regra alterada automaticamente.

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

Resposta a vulnerabilidades regras de destino de correção

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

Os gerentes de vulnerabilidades podem criar regras de destino de correção definindo:

- O destino de correção
- O destino do lembrete
- O lembrete e os destinatários da notificação: Quem devem ser notificados quando os itens vulneráveis (VIS) ultrapassarem a data de destino de lembrete ou correção e não tiverem sido corrigidos.

Os analistas e gerentes de vulnerabilidades podem ver a data de destino de correção no formulário de item de vulnerabilidade e nas exibições de lista, desde que os itens vulneráveis não estejam em **Adiado** , **Resolvido** ou **Encerrado** estado. As regras de destino de correção são executadas na importação e executadas novamente se uma VI for reaberta.

. **Data de destino de correção** É codificado por cores na exibição de lista de VI como pontos, da seguinte forma:

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de destino de correção atuais para o VIS ao qual ela foi aplicada são apagadas. Se uma VI atender a qualquer regra ativa, essa regra será aplicada, caso contrário, a VI não terá regra ou data de destino e seu status será **Nenhum destino** .

Quando as regras são excluídas, o **Destino de correção** Os campos de data e relacionados em VIS Encerrado, Adiado ou Resolvido são preservados. . **Destino de correção** Os campos de data e relacionados em VIS não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário de regra de destino de correção

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

Nota: As metas de correção são calculadas a partir de **Aberto pela última vez** data mais o número de dias (medido como incrementos de 24 horas).

A partir da V17.1, os destinos de correção são calculados a partir do **Destino de (data)** . O valor padrão permanece **Data da última abertura** .

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

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

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

Nesse cenário, a regra de destino de correção 2 se aplica ao item vulnerável, pois ele tem a data mais restritiva. 10 dias desde que o item vulnerável foi identificado pela primeira vez versus 15 dias.

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

Sobre o trabalho agendado Avaliar metas de correção

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

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

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

`Evaluate remediation targets` adiciona uma data de destino de correção, se não houver uma ou se uma regra resultar em uma data anterior à data no registro, ela atualiza a data de destino existente. Por fim, ele atualiza o. **Destino de correção** e. **Status de correção** campos no formulário de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma vez que *Evaluate remediation targets*as notificações disponíveis são enviadas.

Evaluate remediation targets Limpa os campos de correção no VI e interrompe o envio de notificações.

. *sn_sec_cmn.evaluate_targetmissed_records*a propriedade, quando habilitada, impede *Remediation Target Rules*Trabalho agendado da avaliação de Vs perdidos. Esta propriedade está habilitada por padrão.

Reaplicando regras de destino de correção

Ao alterar uma regra de destino de correção, use **Aplicar mudanças** Botão na página de lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os VIS abertos ativos, exceto aqueles em **Encerrado** , **Adiado** ou **Resolvido** estado. Dependendo de quantos VIS você tiver, isso pode levar tempo.

Nota:

Se o trabalho agendado, *Evaluate remediation targets*não é possível iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho agendado acionado por ele, eles serão executados em paralelo.

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

Importante: Como administrador e analista de vulnerabilidades, você pode obter a data de destino de correção mais recente para itens vulneráveis selecionados em Espaço do gerente de vulnerabilidade. Este método é mais eficiente do que executar as Regras de destino de correção para todos os itens vulneráveis no clássico IU, que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Tópicos relacionados

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Exiba o status de destino de correção de um Resposta a vulnerabilidades item vulnerável

Criar ou editar notificações de destino de correção

Grupos e regras de classificação de vulnerabilidades

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

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

- Classificação de itens descobertos
- Classificação de entrada de vulnerabilidade

Sempre que vulnerabilidades e itens descobertos são importados, as regras de classificação de vulnerabilidade nos respectivos grupos são executadas. Com base nas condições definidas na regra, os registros são classificados no grupo de classificação relevante. Você pode criar, editar, excluir ou reaplicar essas regras a uma vulnerabilidade existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

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

Para obter mais informações, consulte Criar e editar uma regra de classificação, Aplique uma regra a uma vulnerabilidade existente e Desative ou exclua uma regra de classificação.

Soluções de aprendizado de máquina para Resposta a vulnerabilidades

Recomendações de atribuição de vulnerabilidade usos ServiceNow® Inteligência preditiva E aprendizado de máquina para recomendar grupos de atribuição para itens vulneráveis (VIS) e tarefas de correção (VULs ou RTS). Você pode reduzir o tempo gasto na identificação dos responsáveis por descobertas de vulnerabilidade não atribuídas ou atribuídas incorretamente. Você também pode ver uma pontuação de confiança gerada pelo sistema que avalia se o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade.

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

Para obter mais informações, consulte Inteligência preditiva .

Recomendações de atribuição de vulnerabilidade

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

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

Para obter mais informações, consulte Inteligência preditiva .

Pontuações de confiança

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

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

Tópicos relacionados

Inteligência preditiva

Criar e treinar uma solução de classificação

Criação e treinamento de uma solução de semelhança

Criar e treinar uma solução de cluster

Definir configurações avançadas para suas soluções DE ML

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

A partir da versão 19,0, navegue até **Operações de segurança** > **CMDB** > **Regras de pesquisa** para localizar a lista em sua instância.

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

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

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

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

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

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

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

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

As regras de pesquisa de IC são enviadas com os plug-ins de integração correspondentes.

Alguns dos Qualys As regras de pesquisa de IC são:

- ID DE HOST DA QUALYS
- FQDN

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- NetBIOS
- DNS
- IP

Alguns dos Rapid7 As regras de pesquisa de IC são:

- MACAddress
- FQDN
- HostName
- IP

Algumas das regras de pesquisa de IC do Tenable.io são:

- FQDN
- NETBIOS
- HOSTNAME
- MACAddress
- DNS

Nota: As regras de pesquisa de IC do Tenable.io priorizam e preenchem os valores de interface de rede não vazios (FDQN, IPV4 e MacAddress) sobre os valores regulares FDQN, IPV4 e MacAddress para um item descoberto. Quando esses valores de interface de rede estão vazios, os valores regulares de FDQN, IPV4 e MacAddress são preenchidos para um item descoberto.

Algumas das regras de pesquisa de IC do Tenable.sc são:

- MACAddress
- FQDN
- NETBIOS

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

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

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

Aplicar novamente as regras de pesquisa de IC atualizadas

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

Hardware não classificado

Se um ativo não encontrar uma correspondência no Configuration Management Database (CMDB) Por regras de pesquisa de IC, o ativo é denominado como um hardware não classificado.

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

Se o mecanismo de Identificação e reconciliação (IRE) estiver ativado, a opção Reclassificar de itens descobertos não será compatível.

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

```
"className": "cmdb_ci_unclassed_hardware",

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

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

```
"className": "cmdb_ci_cmdb_ci_win_server"

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nesse caso, o IC de hardware não classificado existente não é reclassificado para o servidor Windows e, em vez disso, um novo IC no servidor Windows é criado. A regra de identificação depende do nome do IC de hardware. Se você notar as cargas, o nome na carga de Resposta a vulnerabilidadesÉ igual a FQDN/NETBIOS, mas é apenas o nome do host da carga Descoberta.

Tópicos relacionados

Reclassificar hardware não classificado

ICs incompatíveis

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

Se você acha que um IC incompatível pertence a uma classe existente no CMDB, Revise suas regras de pesquisa de IC . Caso contrário, considere reclassificação do item de configuração .

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

Se o mecanismo de Identificação e reconciliação (IRE) estiver ativado, a opção Reclassificar de itens descobertos não será compatível.

Tópicos relacionados

Exibir e reclassificar itens de configuração incompatíveis

Reconciliar itens descobertos sem correspondência

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

Desduplicação de itens de configuração existentes

Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação

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

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

Usando IRE para criação de IC

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

A partir da v24.0.6 de Resposta a vulnerabilidades Se o IRE encontrar exceções que impeçam a criação de ICs, as especificações dessas exceções serão registradas no campo Informações adicionais. Ao examinar os detalhes neste campo, você pode determinar a causa raiz e implementar as correções necessárias para garantir que o IC seja criado com sucesso.

Começando com Resposta a vulnerabilidades V12.2 a v18.0, se nenhuma correspondência for encontrada quando as regras de pesquisa de IC forem aplicadas, as informações do ativo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Classes de IC do CMDB

Nota: Para usar as novas classes, ative CMDB Plug-in Modelos de classe de IC. Caso contrário, os ICs serão criados na classe de IC incompatível.

Se o host importado de um scanner de terceiros não puder ser encontrado na lista de itens descobertos ou CMDB. criado em um dos novos a seguir CMDB Classes de IC.

Classes de IC do CMDB

CMDB **Classe de IC**	**Descrição**
Dispositivo identificado por IP incompleto (*cmdb_ci_incomplete_ip*)	O IC será criado nesta tabela se somente o endereço IP estiver disponível nas informações do host recebidas do scanner.
Hardware não classificado (*cmdb_ci_unclassed_hardware*)	O IC será criado nesta tabela se qualquer uma das seguintes informações estiver disponível nas informações do host recebidas do scanner: • Nome do host • Endereço IP • DNS • NETBIOS • Endereço MAC **Nota:** Se o endereço MAC estiver disponível, a entrada do adaptador de rede será criada e relacionada ao IC de hardware não classificado. Se os endereços IP e MAC estiverem disponíveis, o IC do endereço IP também será criado e relacionado ao IC de hardware não classificado.
Recurso de nuvem (*cmdb_ci_cmp_resource*)	O IC será criado nesta tabela se *Cloud Resource ID*está disponível nas informações do host recebidas do scanner. **Nota:** Se o Tipo de ativo de uma integração de scanner for *Híbrido* e o. *sn_sec_cmn.unmatched_cloud_resource_enabled*A propriedade do sistema é falsa, os ICs são criados no *Hardware não classificado* classe, mas não em *Recurso de nuvem* classe.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o mecanismo de Identificação e reconciliação (IRE) estiver ativado, a opção Reclassificar de itens descobertos não será compatível.

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

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

Para obter mais informações, consulte ICs incompatíveis .

Tópicos relacionados

Aplicação da Store dos Modelos de classe de IC do CMDB

Mecanismo de Identificação e Reconciliação (IRE)

Atualizando classe de IC para ativos de nuvem incompatíveis

Começando com Resposta a vulnerabilidades v20.0, você pode categorizar os ativos de nuvem incompatíveis de Qualys, Rapid7 e Tenable scanners em `Hardware não classificado` usando o. `sn_sec_cmn.unmatched_cloud_resource_enabled`propriedade do sistema.

Esta propriedade do sistema com `falso` como um valor padrão, é enviado com o sistema de base. Ele classifica os ativos de nuvem incompatíveis em um `Hardware não classificado` (`cmdb_ci_unclassed_hardware`ou `Recurso de nuvem` (`cmdb_ci_cmp_resource`classe para as integrações que trazem ativos de infraestrutura e nuvem.

Começando com Resposta a vulnerabilidades V20.0, a coluna Tipo de ativo é adicionada em Integrações de terceiros (`sn_sec_int_integration` tabela) para identificar as integrações compatíveis com ativos de infraestrutura e nuvem. A coluna Tipo de ativo tem o valor, `Híbrido` para os scanners que trazem ativos de infraestrutura e nuvem. Por exemplo, Qualys, Rapid7 e as integrações Tenable têm o valor como `Híbrido` Na coluna Tipo de ativo.

- Para nova instalação de Resposta a vulnerabilidades v20.0 e superior, todos os ativos de nuvem incompatíveis são categorizados em:
  - `Hardware não classificado` classe por padrão.
  - `Recursos de nuvem` se você mudar `sn_sec_cmn.unmatched_cloud_resource_enabled`propriedade do sistema para `verdadeiro` .
- Para upgrades para Resposta a vulnerabilidades v20.0:
  - Se houver ativos no `Recurso de nuvem` . `sn_sec_cmn.unmatched_cloud_resource_enabled` a propriedade do sistema é definida como verdadeira para que os ativos de nuvem incompatíveis continuem a ser adicionados ao `Recurso de nuvem` (`cmdb_ci_cmp_resource`).
  - Caso contrário, o `sn_sec_cmn.unmatched_cloud_resource_enabled` a propriedade do sistema é definida como falsa para que os ativos de nuvem incompatíveis sejam categorizados em `Hardware não classificado` classe.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens descobertos

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

Itens descobertos são considerados **Correspondido** , **Incompatível** ou **Reclassificado** . Os ICs identificados estão no **Correspondido** estado.

Para facilitar a localização de possíveis problemas correspondentes, a Regra de pesquisa de IC que correspondeu ao IC aparece em **Regra de correspondência de IC** campo.

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

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

Mudanças de IC para itens descobertos

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

A partir da v24.0.6 de Resposta a vulnerabilidades, Você pode exibir as atualizações de um IC na tabela Item descoberto. As informações, incluindo o IC anterior, o IC atualizado e o usuário que fez as mudanças, são documentadas na lista relacionada Histórico de auditoria.

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

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

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

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

Reavaliando itens descobertos

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você também pode optar por executar este trabalho agendado diariamente. Para obter mais informações sobre como iniciar este trabalho, a frequência do trabalho e como exibir o número de registros que ele processa, consulte KB1695110 Resposta a vulnerabilidades: Aplique novamente as regras de pesquisa de IC nos itens descobertos alterados .

Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável

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

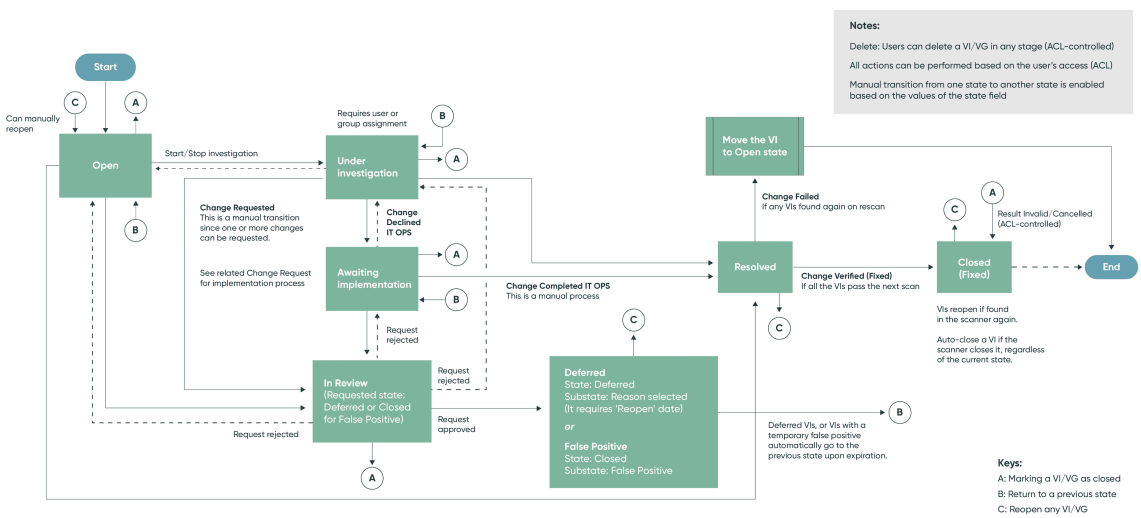
estados da tarefa de correção

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

Nota: A partir da v23.0 de Resposta a vulnerabilidades. **Aprovação do estado do item vulnerável** O fluxo de trabalho foi descontinuado e substituído pela Mudança de aprovação do estado de vulnerabilidade de fluxo no designer de fluxo.

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

Fluxo de estado de Resposta a vulnerabilidades



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

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

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

Para obter mais informações sobre a tarefa de correção e os estados de VI, consulte Tarefas de correção e estados de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Cálculo e exibição de idade do item vulnerável

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

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

- Configure regras no módulo Regras de exclusão automática para direcionar e excluir registros de VI específicos por Dias/Horas/Minutos. Remover registros com mais precisão pode aumentar seu desempenho, especialmente se você tiver um grande número de registros de VI em sua instância.
- Exiba relatórios com detalhes mais específicos na Análise de desempenho do Resposta a vulnerabilidades aplicação.
- Crie filtros que identifiquem somente o VIS desejado.
- Remova as exibições de lista para exibir somente o VIS desejado.
- Referência com pontos com mais facilidade.

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

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

A coluna de idade e os campos não são editáveis. Um gerente de vulnerabilidades com a permissão sn_vul.vulnerability_read ou a persona Administrador de vulnerabilidades pode exibir esse valor, e os responsáveis pela correção de TI com a função sn_vul.remediation_owner podem exibi-lo nos registros atribuídos a eles.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

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

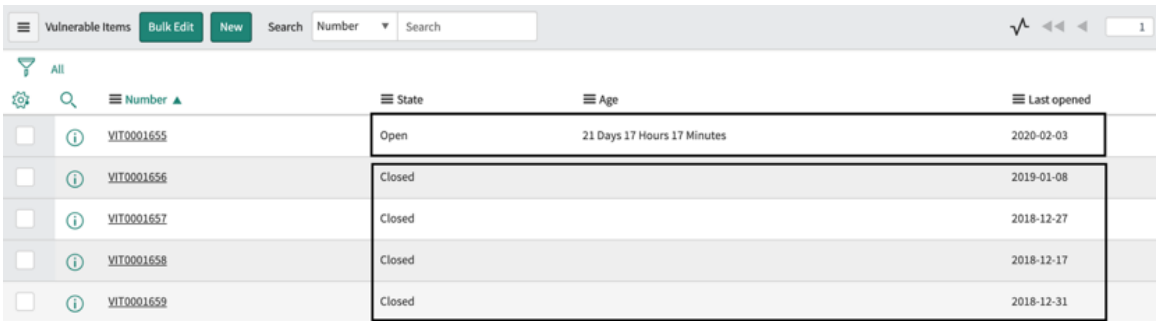
Lista de itens vulneráveis

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

Tradução automática

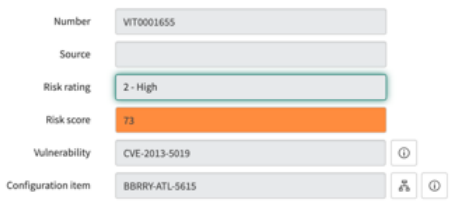
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

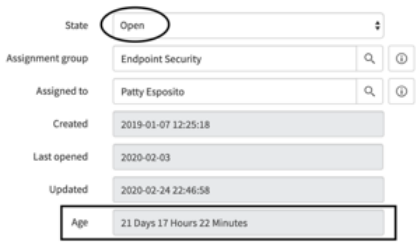
A idade não é exibida para VIS no estado "Encerrado". Anteriormente em um estado "Encerrado" e reaberto, o valor representa o número de dias que o VI esteve ativo desde a data em que foi aberto pela última vez.



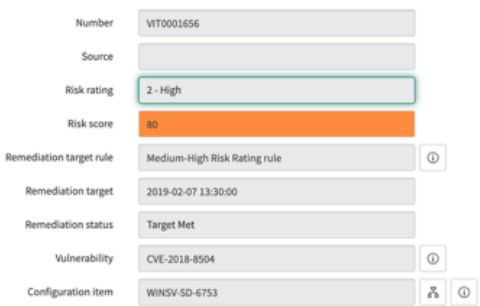
Idade nos registros VI

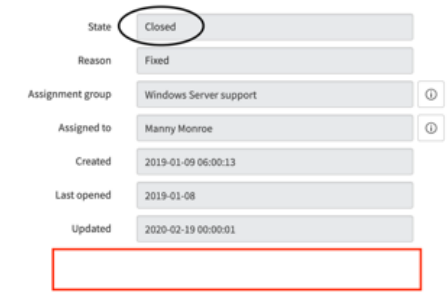
Nos registros de VI, o valor da coluna Idade na exibição de lista fica visível para VIS ativos no campo Idade.





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





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

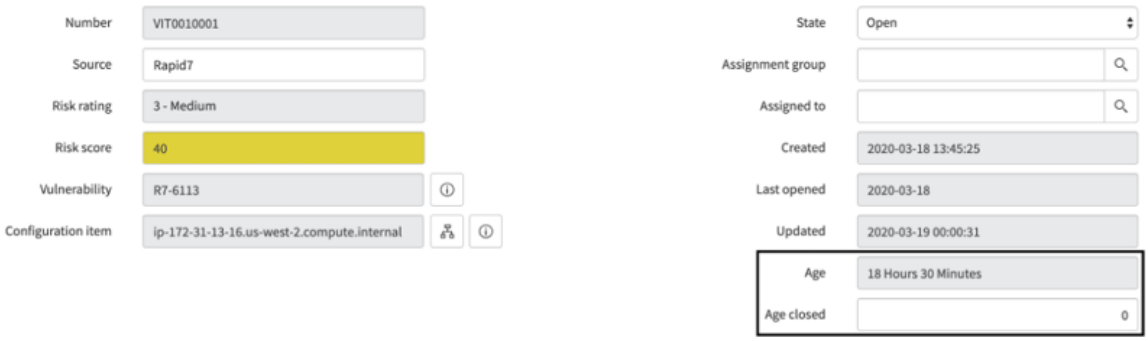
Quando um VI está no estado "Encerrado", o campo Idade não é exibido. Quando o VI faz a transição para "Encerrado", o valor em Número de dias da coluna Idade é exibido no campo Encerrado envelhecido (9), conforme mostrado na figura a seguir. Este valor representa o número de dias em que o VI estava ativo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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



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



Para obter mais informações sobre como personalizar os cálculos Idade e Idade encerrada, consulte KB1703270 artigo.

Removendo atribuições de itens vulneráveis e tarefas de correção

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

Visão geral do fluxo de trabalho

Os responsáveis pela correção e os analistas de vulnerabilidades podem limpar **Atribuído a.** e. **Grupo de atribuição** e atualizar registros para reatribuição com **Cancelar atribuição** Ação de IU.

Caso de uso

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

Ação de IU Cancelar atribuição e menu Mais opções

Você pode **Cancelar atribuição** Os registros a seguir com uma ação de IU ou no menu Mais opções (⋮) Em qualquer estado diferente de Encerrado ou Resolvido:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tarefas de correção (VULs, AVULs e CVULs) no ambiente clássico e nos espaços de trabalho.

  Se uma tarefa de correção for atualizada com este recurso, o **Atribuído a.** e. **Grupo de atribuição** Os campos em todos os seus Vits associados que têm os mesmos grupos de atribuição também são limpos.

  Nota: Se qualquer VIT, AVIT ou CVIT em uma tarefa de correção tiver um grupo de atribuição diferente da tarefa de correção, ela não terá atribuição cancelada. Na maioria dos casos, esses itens vulneráveis foram atribuídos manualmente.

- Itens vulneráveis (Vits, AVITs e CVITs) no ambiente clássico e nos espaços de trabalho.

Todos os registros para os quais você atualiza atribuições com a ação de IU ou manualmente são exibidos no módulo Não atribuído em seus respectivos módulos de produto.

Para as etapas para limpar **Atribuído a.** e. **Grupo de atribuição** campos em registros com *Unassigned*Ação de IU, consulte Remova atribuições de itens vulneráveis e tarefas de correção para obter mais informações.

Propriedades do sistema e notificações

Se você selecionar **Cancelar atribuição** em um registro, por padrão, o *sn_vul.unassign_vr.approval_required*e a propriedade do sistema aciona o fluxo de aprovação e cria um registro de aprovação de mudança de estado no estado de revisão e a solicitação de aprovação é gerada para o aprovador que é exibida no **Minhas aprovações** lista.

Nota: Como administrador de vulnerabilidades [sn_vul.vulnerability_admin], você pode definir *sn_vul.unassign_vr.approval_required*propriedade do sistema para **falso** para desabilitar o processo de aprovação.

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

  Nota: Se você mudar este valor, as notificações para todos os Vits, AVITs e CVITs não atribuídos são enviados para o grupo especificado.

- Se sua solicitação for rejeitada, o motivo será exibido em **Anotações** guia.

Se *sn_vul.default_assignment_group*Não está configurado para um grupo específico. Por padrão, os usuários que você adiciona ao grupo de usuários de notificação Cancelar atribuição são alertados quando os registros não são atribuídos. . *sn_vul.default_assignment_group*a propriedade do sistema determina as notificações para este grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O tipo de atribuição, seja **Manual** , **Regra** ou **Não atribuído** Está disponível nos registros de VIT e na exibição de lista. . **Não atribuído** o tipo de atribuição é exibido nos registros após **Atribuído a.** e. **Grupo de atribuição** os campos são limpos pela propriedade do sistema.

Consulte Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades para obter mais informações sobre como aprovar solicitações.

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

Um trabalho agendado diariamente conta os registros quando eles fazem a transição para **Não atribuído** tipo de atribuição. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar quaisquer regras de atribuição que possam não estar tendo um bom desempenho com base em regras de atribuição que tenham contagens mais altas de VIS não atribuídos.

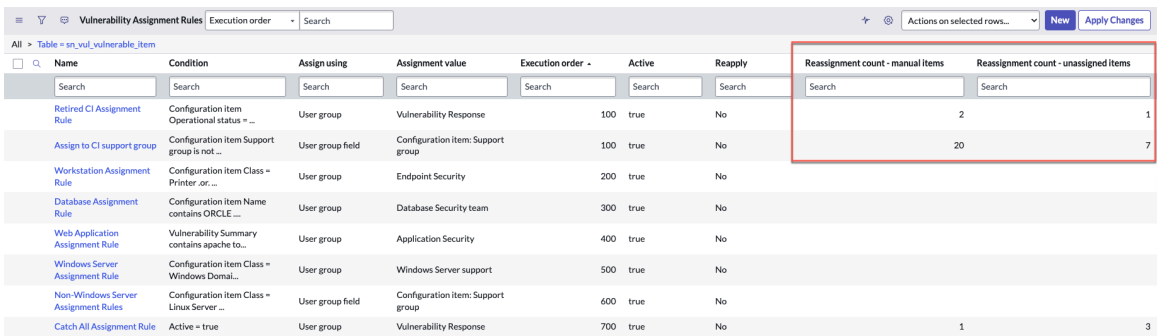
. *`Reassignment count for assignment rules`*O trabalho agendado é executado diariamente e publica o número total de VIS que não estão atribuídos por este recurso para uma regra de atribuição específica.

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

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

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

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



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

Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de Vulnerabilidade

. Resposta a vulnerabilidades o sistema de base inclui duas calculadoras de vulnerabilidade que definem a base **Pontuação de risco** no item vulnerável.

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

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

Além disso, você pode usar atributos em configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco de resposta a vulnerabilidades. Se, por exemplo, você determinar que os ICs voltados para o exterior em sua organização são mais vulneráveis e podem exigir correção imediata, poderá atribuir atributos como *`Internet Facing`*Para esses ICs. E outros atributos estão listados nas notas da versão do Modelo de dados de serviço comum . Para obter informações e orientações atuais sobre CMDB, consulte os seguintes tópicos:

- Modelo conceitual do Modelo de dados de serviço comum
- Modelo de esquema do CMDB
- Resposta a vulnerabilidades: Cálculo de pontuação de risco (KB1169927)

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

. **Gravidade da vulnerabilidade** a calculadora calcula o. **Pontuação de risco** para itens vulneráveis que usam a gravidade da vulnerabilidade normalizada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Apenas uma calculadora por campo de destino (**Pontuação de risco**) pode estar ativo por vez. **Gravidade da vulnerabilidade** está desabilitado por padrão.
- Sempre que a pontuação de risco é atualizada em um VIT, o. **Anotações** a seção é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadora
  - Nome da calculadora: Dependendo se a regra da calculadora é baseada em um modelo ou script, o nome é anexado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, clique em qualquer regra e selecione **Exibição avançada** caixa de seleção. Em **Tipo de valor** caixa suspensa, selecione a opção necessária. Se o Modelo for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se Script for selecionado, você poderá adicionar ou atualizar o script existente.

    A propriedade do sistema `sn_sec_cmn.risk_score_changes_add_worknotes`ajuda a preencher a seção de anotações de trabalho. A partir da v25.0.3 de Resposta a vulnerabilidades, a propriedade do sistema está inativa por padrão. Somente então você poderá ver todas as mudanças relacionadas à pontuação de risco.

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um item vulnerável é criado, quando um IC associado ou vulnerabilidade muda ou quando o **Calcular pontuação de risco** o link relacionado em um item vulnerável é usado. Por exemplo, a Pontuação de risco é atualizada automaticamente em registros de item vulnerável quando o valor de Severidade é atualizado em uma vulnerabilidade importada. Depois que uma importação de vulnerabilidade atualiza uma pontuação de vulnerabilidade, o sinalizador recalcular é habilitado para essa vulnerabilidade. As pontuações de risco dos itens vulneráveis que têm o sinalizador recalcular habilitado (verdadeiro) com essa vulnerabilidade são recalculadas.

De um item vulnerável existente, se você clicar em **Calcular pontuação de risco** e qualquer uma das calculadoras está habilitada, o **Pontuação de risco** o campo no item vulnerável foi atualizado.

Nota:

- . **Calcular pontuação de risco** o link relacionado só fica visível quando pelo menos uma calculadora de vulnerabilidade está habilitada.
- Você pode atualizar a pontuação de risco de um item vulnerável no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI selecionando **Calcular pontuação de risco** em sua exibição de registro.
- Sempre que a pontuação de risco em uma VIT muda, os seguintes detalhes são documentados na seção Anotações da VIT:
  - Nome do grupo de calculadora
  - Nome da calculadora
  - Valores de campo com sua ponderação e contribuição de pontuação de risco
  - Pontuação de risco final

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras da Calculadora de Vulnerabilidade

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

- Gravidade da vulnerabilidade
- Informações de exploração
- Criticidade
- Exposição externa do IC com a vulnerabilidade
- Pontuações de EPSS

Você pode ajustar os valores a serem usados no **Regra de risco padrão** e quanto peso dar a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a base **Pontuação de risco** .

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

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

Atribuição de uma porcentagem de ponderação

Você também pode atribuir a porcentagem de ponderação (0-100) no nível de valor do campo. Por exemplo, você pode atribuir uma porcentagem de ponderação a cada nível de gravidade (Nenhum a Crítico).

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

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

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

Configurações da regra da calculadora de vulnerabilidades

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O sistema de base **Gravidade da vulnerabilidade** A calculadora contém regras de calculadora que atribuem a cada nível de gravidade (Nenhum a Crítico) um valor (0-100) para **Pontuação de risco** com base na gravidade. **Gravidade desconhecida** é atribuída automaticamente uma pontuação de risco de 100. Esses valores podem ser ajustados e, como **Calculadora de risco padrão** novas regras de calculadora ou novas regras de risco podem ser criadas.

Pesos da pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação de risco e classificação com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *`Update Risk Rating from Risk Score`*na tabela de item vulnerável é responsável por calcular a classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis.

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

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

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

Além disso, a pontuação de risco é recalculada automaticamente quando as Vulnerabilidades e exposições comuns (CVEs) ou entradas de terceiros (TPEs) associadas nos itens de vulnerabilidade (VIS) estão vinculadas a uma Vulnerabilidade de exploração conhecida (KEV) de CVE.

Integração de vulnerabilidades do Tenable e a regra de risco do Tenable

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta regra de risco está desabilitada por padrão. Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração.

Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros

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

Visão geral

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

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

Em versões anteriores de Resposta a vulnerabilidades Detecções de item vulnerável, o relacionamento entre um IC (ativo) em seu ambiente e uma vulnerabilidade importada de um scanner de terceiros, criaram um item vulnerável exclusivo em seu ServiceNow AI Platform instância.

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

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

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões compatíveis de Resposta a vulnerabilidades

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

Integrações de terceiros compatíveis

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

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

Essas integrações de terceiros estão disponíveis com uma assinatura separada do ServiceNow Store. Para obter mais informações sobre essas integrações, consulte Integrações do Resposta a vulnerabilidades e. Operações de segurança e o ServiceNow Store para obter mais informações sobre como obter direito.

Para verificar se o scanner de terceiros está configurado para importação, consulte Instale e configure a aplicação Rapid7 Integration for Security Operations e. Instalar o Qualys Vulnerability Integration.

Principais termos para detecções de itens vulneráveis

Vulnerabilidade

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

Item vulnerável

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

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade, conforme relatada por um scanner conhecido como detecção de item vulnerável no ServiceNow AI Platform ambiente. Uma detecção inclui dados aprimorados sobre uma vulnerabilidade e todos os itens vulneráveis correspondentes. Esses dados são exibidos no registro de detecção (nº do VID) e na exibição da lista de itens vulneráveis que inclui os seguintes detalhes:

- Primeiro encontrado (dados)
- Encontrado pela última vez (data)
- Nome DNS
- BIOSname líquido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço IP
- Porta
- Protocolo
- Prova
- SSL
- Horas encontradas

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

Chave de detecção

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

Configurações de chave de detecção

Scanner	Vulnerabilid	Porta	Protocolo	ID do ativo	Prova	NIC
Qualys	Sim	Sim	Sim	Sim	Não	N/D
Tenable	Sim	Sim	Sim	Sim	Não	N/D
Rapid7	Sim	Sim	Sim	Sim	Sim (não diferencia maiúsculas de minúsculas)	Sim

Nota:

- Se a chave de detecção não for especificada, ou para versões anteriores a. Resposta a vulnerabilidades14,0, a chave de detecção é uma combinação de entrada de vulnerabilidade, porta, protocolo, ID de ativo e prova.
- A partir da v19.0 de Resposta a vulnerabilidades Uma nova NIC de chave de detecção foi adicionada para Rapid7 InsightVM, que é ativado por padrão. Detecções existentes sem NIC são atualizadas com a primeira NIC de entrada na carga de Rapid7. A chave de detecção é recalculada e preenchida novamente na detecção, incluindo NIC. Novas detecções serão criadas se detecções semelhantes forem vistas com valores de NIC diferentes. Esses dados não são acumulados na tabela Item vulnerável. O valor de NIC é armazenado em uma nova coluna nas tabelas sn_vul_detection_key_config e sn_vul_detection.

Desduplicação

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

ID externo do VI

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reabra itens vulneráveis resolvidos

Itens vulneráveis definidos como **Resolvido** em seu ServiceNow AI Platform instância, mas não fez a transição para **Encerrado/Corrigido** as execuções de integração subsequentes serão reabertas se forem detectadas durante novas verificações.

Fechado VIS com um subestado de **corrigido** ou **obsoleto** São reabertos se uma nova detecção for criada e o VIS puder ser correspondido à nova vulnerabilidade.

De acordo com a inclusão de script, `DetectionBase`método `_shouldReOpenVI()`Se o VIT foi anterior **Encerrado** com subestado **Corrigido** , **Obsoleto** ou **IC desativado** , Ele é reaberto e a detecção é mapeada para o VIT existente.

Por exemplo, digamos que a data de encerramento de um VIT seja posterior à data last_found de uma detecção. Esses registros de VIT permanecerão encerrados. No entanto, se você vir uma VIT fechada anteriormente reaberta, isso significa que a VIT foi fechada por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando uma nova detecção é encontrada que corresponde à VIT encerrada que tem a mesma vulnerabilidade no item de configuração da VIT, a VIT é reaberta.

Para Rapid7 Detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir os VIS resolvidos por idade. Vis definido como **Resolvido** então não fez a transição para **Encerrado/Corrigido** pelas verificações subsequentes, retorne para **Aberto** após o número de dias inserido.

Para Qualys Se o scanner continuar a encontrar os VIS que foram definidos como **Resolvido** então não fez a transição para **Encerrado/Corrigido** Por verificações subsequentes, esses VIS retornam para **Aberto** Quando a data da última descoberta é posterior à data de resolução.

Exibir dados de detecção

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

Solução de gestão de vulnerabilidade

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

Solução de gestão de vulnerabilidade

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos do Solução de gestão de vulnerabilidade

Solução de gestão de vulnerabilidadeé um recurso disponível no Resposta a vulnerabilidades aplicação. Solução de gestão de vulnerabilidade requer uma assinatura separada.

Para obter mais informações sobre como obter direitos para aplicações do ServiceNow Store, consulte Obtenha direito para um Operações de segurança produto ou aplicação. Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações sobre como instalar a aplicação depois de baixá-la em sua instância.

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

Nota:

Ambas as aplicações de solução podem ser configuradas no Assistente de configuração. Consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade Usando o Assistente de configuração.

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

Versões disponíveis

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

Versão de lançamento de Solução de gestão de vulnerabilidade	Versões compatíveis de Resposta a vulnerabilidades	Notas da versão
Solução de gestão de vulnerabilidade 10.3	Resposta a vulnerabilidades v18.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Sobre soluções e substituições

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

Soluções potenciais versus preferenciais

Uma possível solução pode resolver uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções potenciais. Uma solução preferencial é a solução única destinada a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

corrigir uma vulnerabilidade ou item vulnerável (VI). Comunica a intenção e permite métricas de implantação mais detalhadas.

Soluções Preferenciais

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

Solução preferencial os valores podem ser definidos no item vulnerável ou na vulnerabilidade. Quando definidos diretamente na vulnerabilidade, todos os itens vulneráveis associados à vulnerabilidade herdam essa solução. Mude **Solução preferencial** valores para vários itens vulneráveis usando o recurso de edição em massa. Quando editado em massa, somente **Solução preferencial** em, o item vulnerável é atualizado como definindo **Solução preferencial** no nível de entrada de vulnerabilidade, definiria o. **Solução preferencial** Para todos os novos VIS daqui para frente. A edição em massa se aplica somente aos itens vulneráveis atuais.

Nota: Se houver várias soluções de substituição mais alta para uma vulnerabilidade, **Solução preferencial** os valores no nível de vulnerabilidade são limpos, pois essa solução depende do ativo afetado. Quando houver várias soluções de substituição mais alta para uma vulnerabilidade, defina um **Solução preferencial** no item vulnerável. Você pode definir uma solução diferente usando **Pesquisa** lista no **Item vulnerável** formulário.

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

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

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

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

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

A partir da v24.0.6 de Resposta a vulnerabilidades, você pode ingerir soluções de scanners, além de soluções de fornecedor. Os dados de correção de scanners, como Tenable, Qualys E o Microsoft TVM é aproveitado para criar as soluções. Essas soluções de scanner são importadas usando as seguintes integrações:

- Tenable.sc Integração de plug-in
- Tenable.io Integração de plug-in
- Qualys Base de conhecimento (preenchimento)
- Microsoft TVM Machine Vulnerabilities Integration (importação completa)
- Microsoft TVM Machine Vulnerabilities Integration (importação delta)

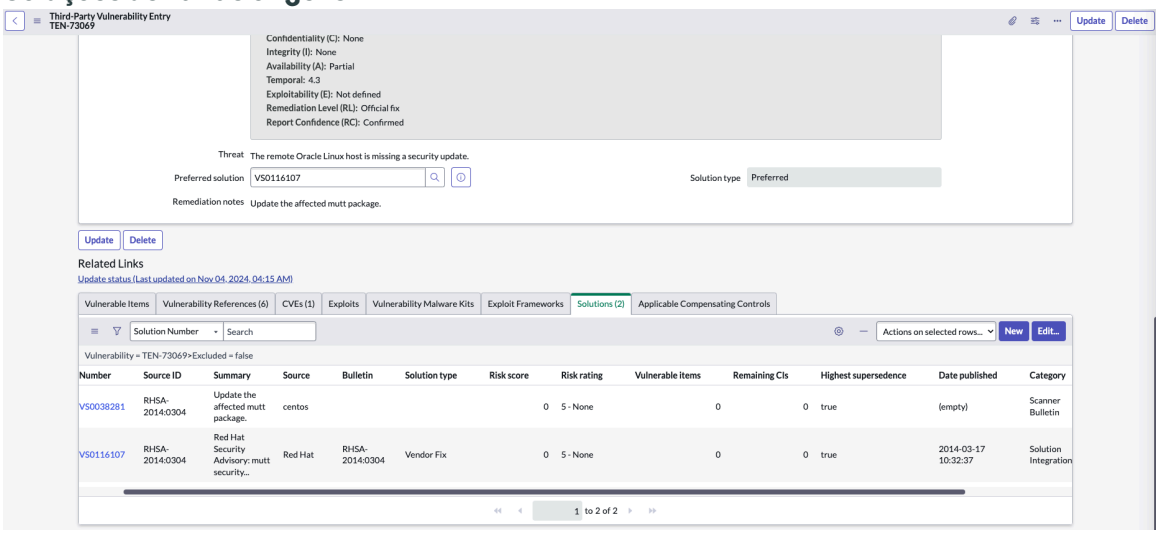
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando as integrações de vulnerabilidade são executadas, uma carga útil de informações de correção é criada antes de processar entradas de terceiros. Para Tenable e. Qualys, os dados de correção são recebidos no nível de vulnerabilidade ou de entrada de terceiros. Para o Microsoft TVM, as soluções são criadas no nível de detecção, permitindo um preenchimento direto de soluções preferenciais nos itens vulneráveis sem a necessidade de processamento adicional. Essas soluções são criadas com base nessas informações de correção e processadas conforme necessário. No processamento, a solução preferencial é preenchida nas vulnerabilidades e acumulada para os itens vulneráveis. A solução preferencial é preenchida na seguinte ordem:

- Seleção manual: Se você selecionar uma solução manualmente, ela não será substituída.
- Soluções do fornecedor (importações Microsoft, RedHat, CVRF e CSAF): Se você não selecionar uma solução manualmente, a solução do fornecedor será selecionada automaticamente.
- Soluções mais recentes (se habilitadas): Se houver várias soluções de substituição superior disponíveis para uma vulnerabilidade, então **solução preferencial** o campo permanece vazio. Nesses casos, se você habilitar a propriedade *sn_vul.latest_solutions*, a solução de fornecedor de substituição mais recente é preenchida como a solução preferencial.
- Soluções de Boletim do scanner (se habilitado): Se você não selecionar uma solução manualmente ou se as soluções do fornecedor não estiverem disponíveis, o. **Solução preferencial** o campo é preenchido com as soluções de scanner, desde que haja uma única solução de scanner. Você deve habilitar a propriedade *sn_vul.populate_scanner_solutions*para preencher as soluções do scanner.

Soluções de várias origens

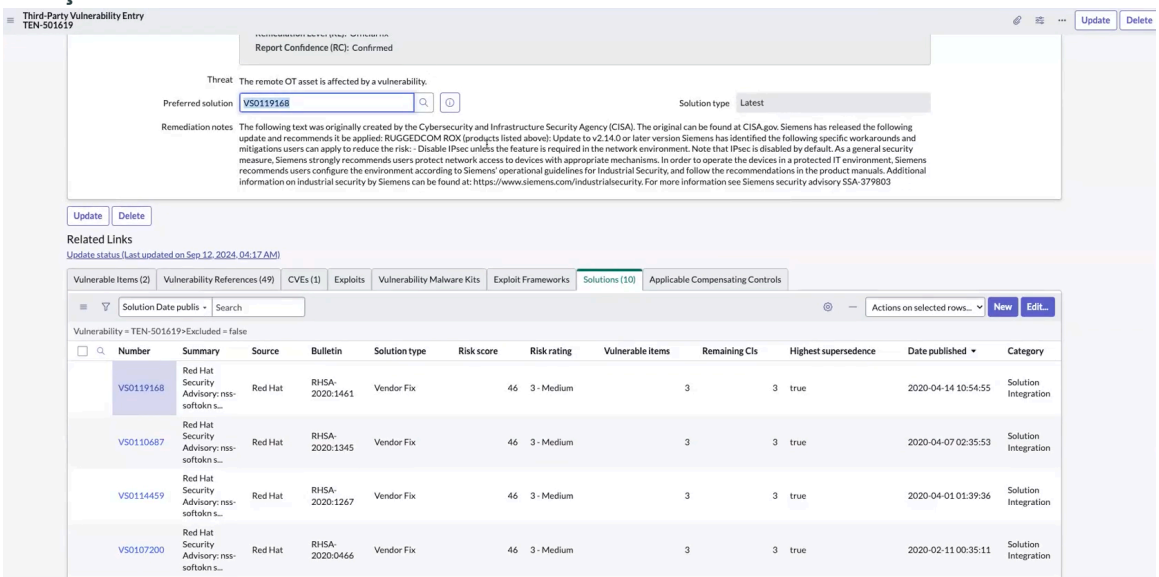


Este exemplo ilustra a seleção de uma solução se várias soluções estiverem disponíveis de fontes diferentes. Nesse caso, há duas soluções para uma vulnerabilidade - uma de um fornecedor e outra de um scanner. Como a solução VS0116107 é recebida de um fornecedor, ou seja, Redhat, que tem preferência mais alta, ela é selecionada como a solução preferencial.

Tradução automática

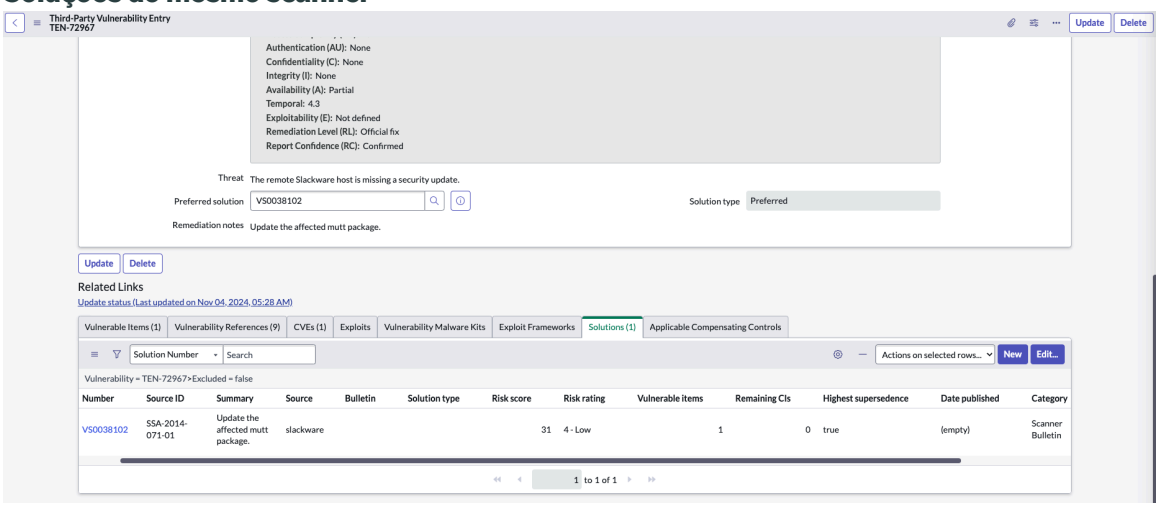
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Soluções do mesmo fornecedor



Este exemplo ilustra a seleção de uma solução se várias soluções estiverem disponíveis do mesmo fornecedor, ou seja, Redhat neste caso. . *sn_vul.latest_solutions*a propriedade está habilitada e nenhuma outra solução de fornecedor está disponível para uma vulnerabilidade específica. essas soluções são processadas, preenchendo as soluções preferenciais nas vulnerabilidades e, posteriormente, nos itens vulneráveis. Se você habilitar a propriedade *sn_vul.latest_solutions*, a solução mais recente é selecionada como a solução preferencial.

Soluções do mesmo scanner



Este exemplo ilustra a seleção de uma solução se apenas uma solução de scanner estiver disponível nos scanners. . *sn_vul.populate_scanner_solutions*a propriedade está habilitada, as soluções são processadas, preenchendo as soluções preferenciais nas vulnerabilidades e, posteriormente, nos itens vulneráveis. Se houver várias soluções de scanner, o **Solução preferencial** o campo foi deixado em branco devido à ambiguidade.

Melhorar a gestão de soluções e a otimização de desempenho

As soluções são recebidas de várias integrações, incluindo Microsoft e Redhat. O primeiro fornece atualizações mensais e estabelece uma cadeia de dependências para rastrear a solução preferencial para vulnerabilidades. No entanto, outras integrações não seguem este formato de atualização e não precisam estabelecer uma cadeia de dependências para elas. Anteriormente, era usada uma lógica de processamento que envolvia a criação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um gráfico para manter a precedência e identificar as soluções de substituição mais altas. Essas soluções foram sugeridas como a solução preferencial para as vulnerabilidades. No entanto, como a construção do gráfico é demorada, as outras integrações são excluídas desse processo. Para melhorar o desempenho, a partir da v22.0 de Resposta a vulnerabilidades, o método `utility.processNonGraphSolutions()` é chamado em `Process Vulnerability Solutions Metrics Queue`trabalho agendado. Este método lida com soluções de integrações diferentes da Microsoft.

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

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

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

Tradução automática

Métricas de status de correção

Campo	Descrição
Destinos de solução preferenciais - Status de correção para VIS para os quais esta é a solução preferencial	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas de status de correção

Campo	Descrição
Total de ICs	Número de ICs associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se ao VIS para o qual esta solução é preferencial. Esta contagem exclui itens vulneráveis adiados.
Percentual de ICs corrigidos	Percentual concluído para correção de IC. Aplica-se ao VIS para o qual esta solução é preferencial. Esta contagem exclui itens vulneráveis adiados.
Destinos de solução preferenciais (inclui adiados) - Status de correção para VIS, incluindo adiado, para o qual esta é a solução preferencial	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Total de ICs	Número de ICs associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se ao VIS para o qual esta solução é preferencial.
Percentual de ICs corrigidos	Percentual concluído para correção de IC. Aplica-se ao VIS para o qual esta solução é preferencial.
Possíveis destinos da solução - Status de correção para todos os VIS com uma vulnerabilidade relacionada a esta solução	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma solução potencial para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
Possíveis destinos da solução (inclui adiados) - Status de correção para todos os VIS, incluindo adiados, com uma vulnerabilidade relacionada a esta solução	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas de status de correção

Campo	Descrição
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção.

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

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

Em determinados cenários, a solução preferencial em um item vulnerável (VIT) pode ser diferente da solução preferencial na vulnerabilidade correspondente. Isso ocorre quando a solução preferencial é atualizada manualmente em um VIT e não na vulnerabilidade. Nesses casos, o **Tipo de solução** O campo está oculto na VIT.

O que Solução de gestão de vulnerabilidade faz

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

- MSRC Cria cadeias de substituição durante a importação que você pode exibir na lista relacionada da solução.
- Indica se uma solução é uma solução de maior substituição ou não.
- Lista a Solução **Pontuação de risco** associado a cada solução para fornecer as maiores oportunidades de redução de risco.
- Mantém **Status de correção** para soluções em **Entradas de Vulnerabilidade de terceiros** , **Tarefas de correção** e **Solução de vulnerabilidade** registros para que você possa rastrear o andamento da correção.

  Contém:

  - Contagens de itens vulneráveis por percentual corrigido, para aqueles VIS com Soluções preferenciais, com e sem esses VIS no estado Adiado.
  - Contagens de item de configuração (IC) por percentual corrigido, para aqueles VIS com soluções preferenciais, com e sem esses VIS no estado adiado.
  - Contagens de itens vulneráveis por percentual corrigido, para aqueles VIS com possíveis soluções, com e sem esses VIS no estado Adiado.
  - Contagens de item de configuração por percentual corrigido, para aqueles VIS com soluções preferenciais, com e sem esses VIS no estado adiado.

O que você pode fazer com Solução de gestão de vulnerabilidade

- Crie, atualize, exiba ou exclua soluções associadas a vulnerabilidades para que você possa rastrear soluções de vulnerabilidade que não são cobertas pelo conteúdo de soluções de terceiros. A integração da solução com o armazenamento de dados Rapid7 não é compatível.
- Associe vulnerabilidades de terceiros e entradas de NVD a um registro de solução.
- Remova e reassocie itens vulneráveis e tarefas de correção com uma solução.
- Exiba **Solução preferencial** aplicável a uma determinada vulnerabilidade nos formulários vulnerabilidade e item vulnerável.
- Exibir um **Soluções preferenciais** Lista relacionada em formulários de tarefa de correção que listam todas as soluções preferidas por pelo menos um VI ativo nesse grupo.
- Exiba **Status de correção** detalhes sobre uma solução que mostram a redução de risco associada à implantação do **Solução preferencial** em vulnerabilidade, item vulnerável, tarefas de correção e formulários de solução.
- Exiba as vulnerabilidades aplicáveis a uma determinada solução no formulário de solução.
- MSRC: Exiba as soluções de substituição de uma determinada solução em uma vulnerabilidade, para encontrar a atualização mais recente a ser implantada ou uma atualização anterior, mais focada e eficiente.
- Exiba listas de soluções classificadas para diferentes características.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Todos: Soluções classificadas por data de publicação e número.
- MSRC Maior substituição: Soluções com itens vulneráveis ativos e não adiados. Classificado por **Maior substituição** , **Data de publicação** e **Número** .
- Com itens vulneráveis: Soluções com itens vulneráveis ativos e não adiados. Classificado por **Maior substituição** ou **Preferencial** , **Pontuação de risco** e **Número** . Se implantadas, as principais entradas na lista fornecerão a maior redução de risco para os ativos em seu ambiente.

Pontuação de risco do registro da solução e classificação de risco

Nota: O registro da Solução **Pontuação de risco** e. **Classificação de risco** são diferentes dos campos usados para vulnerabilidades, itens vulneráveis e tarefas de correção.

O registro da Solução **Pontuação de risco** é um cálculo ponderado com base no item vulnerável **Pontuação de risco** e uma contagem de itens vulneráveis ativos com esta solução como **Possível solução** . A solução **Pontuação de risco** fornece uma estimativa da redução de risco que a solução deve realizar.

O registro da solução **Pontuação de risco** é calculado da seguinte forma:

- Começa tomando 85% do mais alto ou máximo **Pontuação de risco** de um item vulnerável ativo com essa possível solução.
- O registro da solução **Pontuação de risco** em seguida, tabula o número total de itens vulneráveis com essa possível solução. Para cada intervalo do número de itens vulneráveis, ele adiciona alguns pontos e chega a um total.
  - 0 a 09 itens vulneráveis não adicionam pontos
  - 10 a 99 itens vulneráveis adiciona 5 pontos
  - 100 a 999 itens vulneráveis adiciona 10 pontos
  - itens vulneráveis de 1000 e além adicionam 15 pontos

  Por exemplo, para um item vulnerável **Pontuação de risco** De 80, o registro Solução **Pontuação de risco** começaria às 68. Se houver 200 itens vulneráveis ativos com essa possível solução, a Solução final **Pontuação de risco** seria 78.

O registro da Solução **Classificação de risco** Separa o registro Solução **Pontuação de risco** Em intervalos de Crítico a Nenhum. Solução **Classificação de risco** classifica a redução de risco dos itens vulneráveis que esta solução corrige.

Até VR v16.1, as classificações de risco separaram a Solução resultante **Pontuação de risco** nos seguintes intervalos:

- 1 - Crítico (mais de 90 soluções **Pontuação de risco**)
- 2 - Alto (registro de solução 70-89 **Pontuação de risco**)
- 3 - Médio (30-69 registro de solução **Pontuação de risco**)
- 4 - Baixo (registro de solução 1-29 **Pontuação de risco**)
- 5 - Nenhum (0 registro de solução **Pontuação de risco**)

A partir do VR v16.1, as classificações de risco separam a Solução resultante **Pontuação de risco** Nos seguintes intervalos para Gestão de soluções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- 1 - Crítico (mais de 90 soluções **Pontuação de risco**)
- 2 - Alto (registro de solução 70-89 **Pontuação de risco**)
- 3 - Médio (40-69 registro de solução **Pontuação de risco**)
- 4 - Baixo (registro de solução 1-39 **Pontuação de risco**)
- 5 - Nenhum (0 registro de solução **Pontuação de risco**)

Casos de Uso

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

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

As listas de soluções comunicam os principais detalhes da solução, pontuações de risco e métricas de implantação. Usar **Pontuação de risco** E contagens de VI ativo para priorização. Veja quais soluções no ciclo de patch atual não estão em andamento, possivelmente uma indicação de um pré-requisito de implantação ausente.

Nota: Adicionar **%Vis corrigido(percent_nd_pref_vis_remediated)** em **Personalizar colunas da lista** Menu para andamento da correção no formulário Soluções de vulnerabilidade.

Integração com a solução Microsoft Security Response Center

Revisar e implementar soluções de correção propostas fornecidas pelo Integração com a solução Microsoft Security Response Center.

Integração com a solução Microsoft Security Response Center está incluído em Solução de gestão de vulnerabilidade recurso de Resposta a vulnerabilidades, disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

Microsoft Security Response Center Investiga relatórios de vulnerabilidades de segurança que afetam os produtos e serviços da Microsoft e fornece informações de solução para ajudar a gerenciar os riscos de segurança. Soluções são correções conhecidas importadas para seu Integração com a solução Microsoft Security Response Center em Microsoft Security Response Center produto.

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

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Versões disponíveis

Para a versão mais atual de Solução de gestão de vulnerabilidade e. Microsoft Security Response Center verifique se você tem a versão mais atual de Resposta a vulnerabilidades instalado.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Versão de lançamento de Resposta a vulnerabilidades	Versão de Solução de gestão de vulnerabilidade	Notas da versão
Resposta a vulnerabilidades v15.0	10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

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

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

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Integração com a solução Microsoft Security Response Center

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

A integração a seguir está incluída no sistema de base.

Integração com a solução Microsoft Security Response Center

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Soluções

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

Red Hat Solution Integration

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

Red Hat Solution Integration está incluído em Solução de gestão de vulnerabilidade recurso de Resposta a vulnerabilidades, disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

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

A partir da versão 21,0 de Resposta a vulnerabilidades, Red Hat Transmite cargas no formato Common Security Advisory Framework (CSAF) em vez do formato Common Vulnerability Reporting Framework (CVRF). CSAF, um padrão baseado em XML, difere em estrutura e formato do CVRF. Para acomodar essa mudança, um novo analisador CSAF foi desenvolvido. Este analisador interpreta o formato CSAF, extraindo os campos obrigatórios para preencher as tabelas de acordo.

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

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

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

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

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

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

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

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

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

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

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

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

Red Hat Solution Integration Contém pontos de entrada para o produto Red Hat, invocado como um trabalho agendado. O trabalho agendado simplifica o ciclo de vida de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Ele é executado automaticamente. Você também pode executar o trabalho agendado manualmente.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Versões disponíveis

Para a versão mais atual de Solução de gestão de vulnerabilidade e. Red Hat verifique se você tem a versão mais atual de Resposta a vulnerabilidades instalado.

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

Versão de lançamento de Resposta a vulnerabilidades	Versão de Solução de gestão de vulnerabilidade	Notas da versão
Resposta a vulnerabilidades v15.0	10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

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

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Red Hat Solution Integration

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

A integração a seguir está incluída no sistema de base.

Integração do Red Hat

Integração	Descrição
Red Hat Solution Integration	Recupera soluções e mapeamento do National Vulnerability Database (NVD) para associar soluções a vulnerabilidades, itens vulneráveis e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Soluções

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

Rapid7 gestão de soluções

Soluções são correções conhecidas que são importadas para seu Integração com Rapid7 Vulnerability em Rapid7 depósito de dados ou Rapid7 InsightVM. Rapid7 o data warehouse importa soluções e soluções de substituição. Com Rapid7 InsightVM, Você obtém soluções como parte da integração de item vulnerável do Rapid7 - API.

A partir da versão 21,0 de Resposta a vulnerabilidades, há uma mudança na forma como as soluções são criadas por Rapid7 InsightVM. Em vez de confiar **solution_summary** , **solution_fix** ou **solution_type** campos, Rapid7 InsightVM agora cria soluções usando solution_id fornecido pelo scanner. Mesmo se esses campos estiverem vazios, uma solução será criada, desde que um ID de solução esteja disponível.

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

. Solução de gestão de vulnerabilidade o plug-in está ativado e, em seguida, a versão mais recente de Integração com Rapid7 Vulnerability fornece os seguintes principais recursos relacionados às soluções:

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

Nota: Se você não tiver ativado o. Solução de gestão de vulnerabilidade plug-in, a aplicação funciona como está.

Gestão de soluções de vulnerabilidade

Se você ativou o. Solução de gestão de vulnerabilidade plug-in e, em seguida, o. Rapid7 soluções para ambos Rapid7 depósito de dados e. Rapid7 InsightVM Preenchido na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não tiver ativado o. Solução de gestão de vulnerabilidade plug-in e, em seguida Integração com Rapid7 Vulnerability funciona como está e importa as soluções na tabela personalizada [sn_vul_r7_solution].

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração da Gestão de soluções de pré-requisito do Rapid7

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

1. Rapid7 Integração da solução
2. Rapid7 Solução de pré-requisito
3. Rapid7 Substituição da integração da solução
4. Rapid7 Integração do mapa de soluções de vulnerabilidade
5. Rapid7 Integração da solução VI (de v19.0 de Resposta a vulnerabilidades)

Nota: Se você executar as integrações manualmente, comece com Rapid7 Integração da solução#. Não altere a cadeia Next Integration no Rapid7 Integração. A sequência é definida na coluna Próxima integração.

Lista relacionada do Rapid7 (Soluções) no TPE

Se você ativou o. Solução de gestão de vulnerabilidade plug-in, então você pode fazer o seguinte:

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

Se você não tiver ativado o. Solução de gestão de vulnerabilidade plug-in, ocorre o seguinte:

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

Solução preferencial em TPE e VIS

Rapid7 Obtém a solução do depósito de dados no nível de entrada de terceiros (TPE) e para Rapid7 InsightVM no nível de detecção.

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

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

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

Para alcançar esta população direta através Rapid7, as seguintes etapas são executadas:

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

Na execução da Integração da solução Rapid7 VI, os dados não processados obtidos de Rapid7é armazenado na tabela recém-criada. Em seguida, a transformação da Solução Rapid7 VI é acionada, processando esses dados e preenchendo a solução preferencial diretamente na tabela Item vulnerável.

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

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

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

Embora as soluções estejam enfileiradas para atualizar somente as métricas de status de correção, elas ainda tentam acumular soluções de entradas de NVD para entradas de terceiros e preencher as soluções preferenciais. Para otimizar este processo, na tabela Solução de vulnerabilidade, a coluna **Atualizar status** introduzido. Quando as métricas de status de correção nas soluções precisam ser atualizadas sem exigir o acúmulo de soluções de entradas de NVD para entradas de terceiros ou o preenchimento de soluções preferenciais, elas não são mais enfileiradas. Em vez disso, o **Atualizar status** a coluna é atualizada diretamente como verdadeira. Esta abordagem permite lidar com casos em que somente as métricas de status de correção devem ser atualizadas, resultando em economia de tempo e recursos. No trabalho agendado, depois que o processamento das soluções enfileiradas é concluído, as soluções marcadas com um status Atualizar como verdadeiras

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são identificadas. Em seguida, eles são iterados por meio dessas soluções, calculando as contagens e atualizando as métricas de status de correção de acordo. Esta etapa desempenha um papel significativo na melhoria do desempenho do trabalho agendado, pois o número de soluções que devem ser enfileiradas é reduzido.

Cadeia de substituição de solução importada do depósito de dados Rapid7 para uma vulnerabilidade

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

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

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

Atualizando o. Rapid7 aplicação

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

Se você ativa o. Solução de gestão de vulnerabilidade plug-in antes ou depois de atualizar o. Rapid7, o. **Importar desde** o campo permanece vazio para as seguintes integrações:

- #Integração da solução de substituição do Rapid7
- Integração do mapa de solução de vulnerabilidade do Rapid7
- Integração da solução Rapid7

> **Nota:** Na próxima execução de integração, os dados são preenchidos para a tabela de solução de vulnerabilidade.

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

Estrutura genérica para ingerir dados de qualquer fornecedor de solução

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

Os formatos de arquivo compatíveis são:

Common Vulnerability Reporting Framework (CVRF)

O Common Vulnerability Reporting Framework (CVRF) é uma linguagem baseada em XML. Principais fornecedores, como Oracle, Red Hat, Cisco e Microsoft Suporte ao formato CVRF.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Common Security Advisory Framework (CSAF)

O Common Security Advisory Framework (CSAF) é um padrão de código aberto que fornece avisos de segurança estruturados e legíveis por máquina baseados em JSON. Principais fornecedores, como a Siemens, Red Hat, Hitachi e Schneider são compatíveis com o formato CSAF.

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

- Configuração por meio do Assistente de configuração
- Suporte à importação de dados CVRF ou CSAF por meio da importação de arquivos
- Suporte à importação de dados CVRF ou CSAF por meio do CVRF Ou CSAF URL
- Suporte à importação de dados CVRF ou CSAF por meio de comunicados
- Mapeamento de soluções com vulnerabilidades relacionadas

O plug-in Vulnerability Response cuida da atualização dos status das métricas da solução criada.

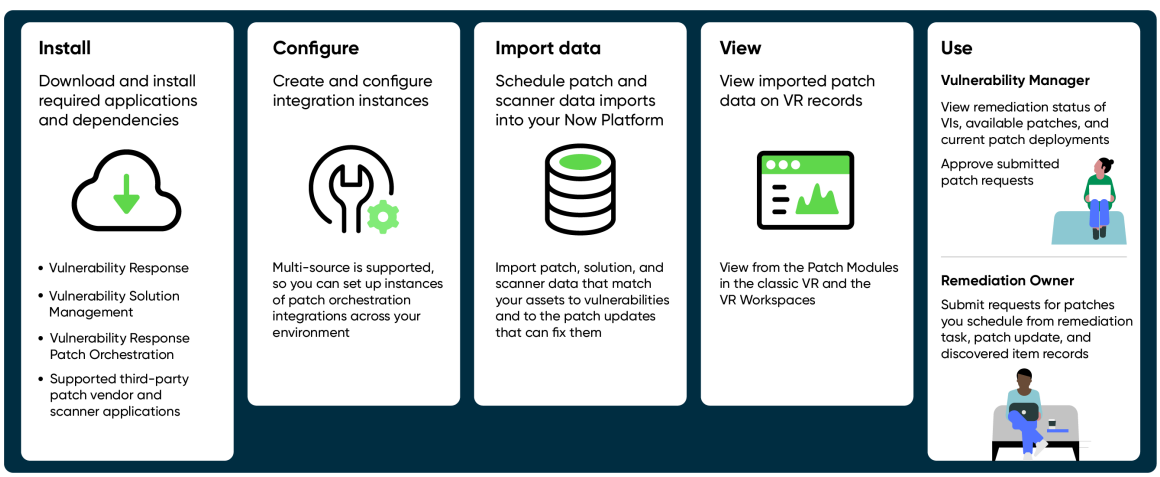
Para obter mais informações sobre como configurar os provedores de soluções, consulte Configurar provedores de solução de vulnerabilidade.

Orquestração de patches com Resposta a vulnerabilidades

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

Noções básicas sobre a orquestração de patches com Resposta a vulnerabilidades

Orquestração de patches com Resposta a vulnerabilidades usa dados de importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidades. Esses dados são correlacionados no Resposta a vulnerabilidades aplicação. Esta organização de dados permite que você conclua as etapas do ciclo de correção de vulnerabilidades. Comece identificando vulnerabilidades, aplique patches e atualizações e, por fim, feche itens vulneráveis usando dados de scanner de terceiros, tudo de dentro do ServiceNow AI Platform® instância.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração de patches com Resposta a vulnerabilidadesé compatível com o ambiente clássico e o. Resposta a vulnerabilidades espaços de trabalho.

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

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

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

Termos principais

IC (Configuration Item, item de configuração)

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

Item vulnerável (VI)

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

Instância

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

Solução

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

Patch

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

Patch preferencial

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Patches preferenciais são atualizações de software que se destinam a corrigir vulnerabilidades específicas. Depois de implantados, os patches são mapeados para os itens vulneráveis relacionados a vulnerabilidades específicas e os corrigem.

Implantação

A implantação para fins desta integração se refere a quando você aplica, inicia ou agenda um patch em uma máquina.

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

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

- A Resposta a vulnerabilidades E os plug-ins de dependência, Suporte de segurança comum e Orquestração de suporte de segurança.
- Solução de gestão de vulnerabilidade.
- Resposta a vulnerabilidades Aplicação de Orquestração de patches disponível no ServiceNow® Store.
- Uma aplicação de fornecedor de patch de terceiros compatível, como Integração da Orquestração de patch de Resposta a vulnerabilidades com o HCL BigFix ou Integração da Orquestração de patch de Resposta a vulnerabilidades com o Microsoft SCCM .
- Integrações de scanner de terceiros compatíveis com o Vulnerability Response.

Funções necessárias

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

- Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades e. Integração da Orquestração de patch de Resposta a vulnerabilidades com o Microsoft SCCM .
- Em Resposta a vulnerabilidades e o ambiente clássico, a função sn_vul_patch_orch.read_patch, que permite aos usuários exibir, mas não editar dados, é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst.

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

Há um processo de envio e aprovação para solicitações de patch incluído com as aplicações. Por padrão, uma propriedade do sistema é ativada [**sn_vul_patch_orch.patch_approval_required**] Na aplicação Orquestração de patch de resposta a vulnerabilidades em seu ServiceNow AI Platform instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta propriedade do sistema é ativada para que, quando as implantações de patch são programadas, elas sejam enviadas para revisão e aprovação aos usuários atribuídos ao grupo de aprovação de atualização de patch de nível 1. Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative [**sn_vul_patch_orch.patch_approval_required** propriedade]. Você pode preferir deixar as aprovações ativadas para que os patches agendados não entrem em conflito com o horário normal de trabalho. Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

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

- Configure o. Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix.
- Configure a Orquestração de patch de resposta a vulnerabilidades com Microsoft Integração do SCCM.

Programar patches de Resposta a vulnerabilidades registros

Os especialistas em correção podem programar atualizações de patch para resolver itens vulneráveis e monitorar o andamento da correção, tudo a partir de registros no Resposta a vulnerabilidades aplicação.

Você pode programar patches a partir dos seguintes registros:

- Atualização de patch
- Tarefa de correção
- Item descoberto

Registros que acumulam contagens de VI ativas em Resposta a vulnerabilidades

Para evitar possíveis problemas de desempenho com o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado que seleciona as mudanças modifica apenas a contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros no Resposta a vulnerabilidades aplicação:

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

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

- Dados de patch e rollup de estado para orquestração de patches em Resposta a vulnerabilidades.
- Exibição de dados de patch e programação de patches em Resposta a vulnerabilidades.
- Exibir patches sem soluções em Resposta a vulnerabilidades.

Edite itens vulneráveis em massa com patches

Você pode editar em massa itens vulneráveis no ambiente clássico que tenham patches do ambiente clássico. Para obter mais informações sobre como funciona a edição em massa, consulte Edite itens vulneráveis em massa em Resposta a vulnerabilidades. Os patches preferenciais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para todos os VIS selecionados para edição em massa. Esta opção de edição só funciona se houver patches preferenciais mapeados para todos os VIS selecionados.

Melhorias do Modelo de dados da Gestão de patches

O plug-in Patch Management Data Model, um plug-in autônomo e gratuito que encapsula o modelo de dados usado atualmente na aplicação Orquestração de patches de VR. Isso inclui tabelas-chave, como Coleção, Atualização de patch, Implantação de patch e outras.

Este plug-in pode ser usado por ferramentas de gestão de patches para ingerir os dados da Gestão de patches a serem usados por aplicações como ITSM, Resposta a vulnerabilidades e assim por diante para os fluxos de trabalho existentes.

Principais melhorias:

- Tabelas como dispositivo de coleta, atualização de patch e tabelas de implantação de patch no plug-in de orquestração de patch existente serão movidas para o novo plug-in de modelo de dados.
- Os dados da tabela antiga serão migrados para as novas tabelas para o recurso de orquestração de patch de VR existente.

Visão geral da Gestão de exceções

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

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

Ciclo de vida de uma exceção

Definição de uma exceção

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

Solicitando uma exceção

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

Aprovando uma solicitação de exceção

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- A partir de Resposta a vulnerabilidades V15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

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

  - Reabrir
  - Excluir
  - Atualize o. **Atribuição a.** ou **Grupos de atribuição** campos

- A partir da v23.0 de Resposta a vulnerabilidades. **Aprovação do estado da regra de exceção** O fluxo de trabalho foi descontinuado e substituído pela aprovação da regra de exceção de fluxo no designer de fluxo.

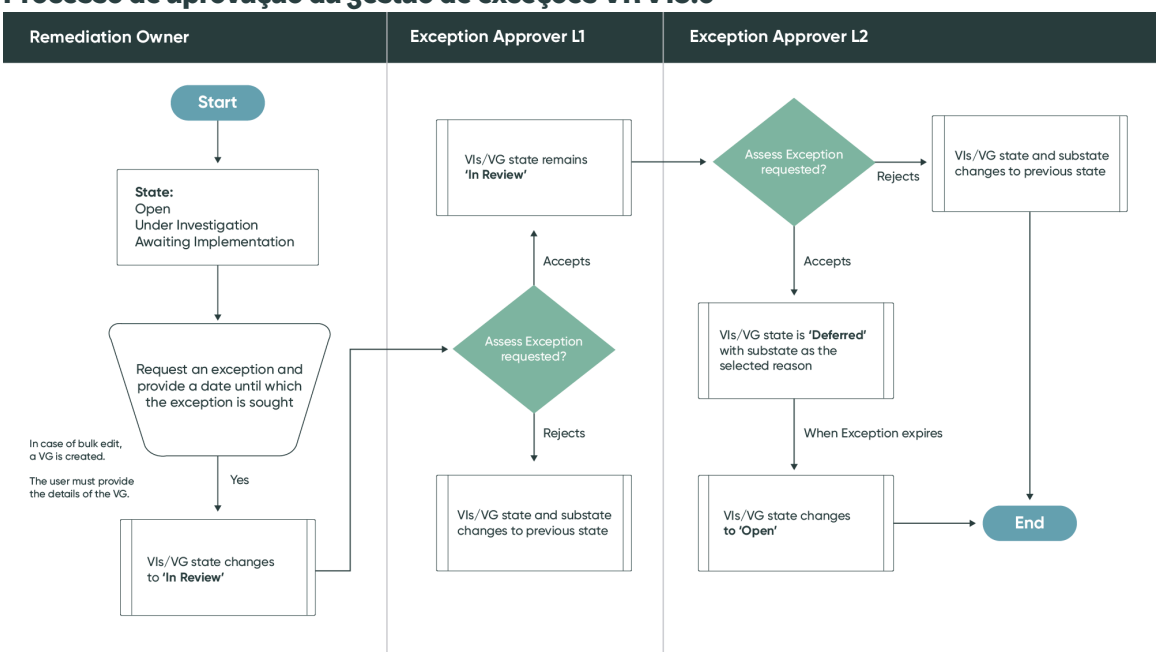
Acompanhamento de uma solicitação de exceção

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

Expiração de uma solicitação de exceção

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

Processo de aprovação da gestão de exceções VR v15.0



Se um único VI ou todos os VIS em um RT forem aprovados no próximo exame, o VIS e, quando aplicável, o RT **Estado** o campo muda para **Encerrado** com o subestado **Corrigido** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vários adiamentos

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

Tópicos relacionados

Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade

Solicite uma exceção no Espaço de correção de problemas de TI

Solicite uma exceção usando GRC: Gestão de políticas e conformidade em Espaço de correção de problemas de TI

Visão geral das regras de exceção

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

Usando regras de exceção em sua organização

Use regras de exceção para adiar automaticamente VIS novos e existentes para um período específico se corresponderem à condição de regra aprovada. A automação minimiza o risco de ausência de acordos de nível de serviço e facilita o gerenciamento de vários itens, porque você está eliminando a intervenção manual.

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

Nota:

- Você só poderá criar regras se selecionar Resposta a vulnerabilidades Na configuração Gestão de exceções. Para obter detalhes, consulte Configure a Gestão de exceções para Resposta a vulnerabilidades.
- Quando os VIS são adiados por uma regra de exceção, eles são copiados para a tarefa de correção de adiamento (RT) que é criada. Os VIS continuam a fazer parte dos RTS dos quais faziam parte anteriormente.

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

- Criando uma regra de exceção
- Aprovando uma solicitação de regra de exceção
- Ativando uma regra de exceção
- Adiar uma regra de exceção
- Expiração de uma regra de exceção

Criando uma regra de exceção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Aprovando uma solicitação de regra de exceção

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

Nota:

A partir de Resposta a vulnerabilidades V15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

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

- Cancelar
- Excluir

Ativando uma regra de exceção

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

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

Adiar uma regra de exceção

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

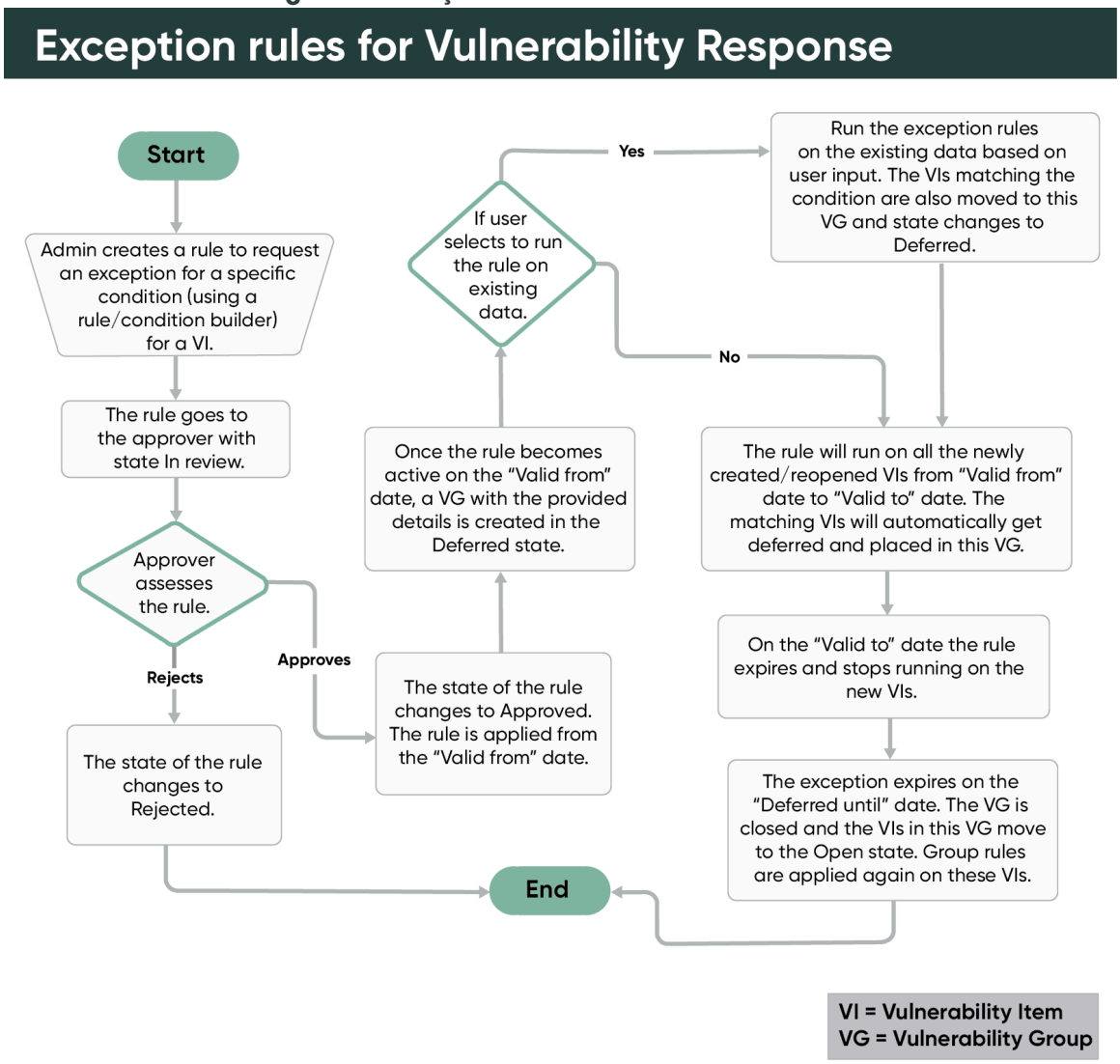
Expiração de uma regra de exceção

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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



Tradução automática

Visão geral das regras de exclusão

As regras de exclusão fornecem uma maneira de filtrar ou excluir detecções de serem convertidas em itens vulneráveis (Vits) durante o processo de ingestão em Resposta a vulnerabilidades.

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

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

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

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para novas detecções:
  - Se uma nova detecção não atender às condições de uma regra de exclusão, uma detecção será criada com os Vits.
  - Se uma nova detecção atender às condições de uma regra de exclusão, a regra será associada à detecção, mas a VIT não será criada. Preencha a referência de Regra de exclusão correspondente no registro de detecção. A coluna Regra de exclusão é preenchida com a referência de Regra de exclusão no registro de detecção de acordo.
- Para detecções existentes:
  - Se a detecção não atender às condições de nenhuma regra de exclusão, ela prosseguirá com o fluxo de trabalho normal.
  - Se uma detecção existente corresponder às condições de uma regra de exclusão, o VIT associado a essa detecção permanecerá em seu estado atual, mas a regra será associada à detecção. O estado da VIT é governado pelo valor definido em `sn_vul.close_vit_with_excluded_detections`propriedade. Por padrão, o valor nesta propriedade é definido como Falso. Se o valor for definido como Falso, as detecções em um VIT serão excluídas e o estado dos Vits permanecerão em seu estado atual. No entanto, se o valor estiver definido como verdadeiro, os seguintes cenários poderão ocorrer:
    - Se cada detecção em uma VIT for excluída, o status da VIT será atualizado para Encerrado excluído.

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

    - Se uma detecção for marcada como fechada enquanto as restantes forem excluídas, a VIT será designada como fechada fixa.
    - Se a VIT tiver detecções abertas, a VIT permanecerá aberta.

Tópicos relacionados

Crie uma regra de exclusão

Falso-positivo visão geral

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

Importante: Você pode marcar os itens vulneráveis do host como falso positivo em massa no Espaço do gerente de vulnerabilidade. Para obter mais informações sobre como marcar os itens vulneráveis do host como falso positivo em massa, consulte Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades.

Ciclo de vida de um falso positivo

Significado de falso positivo

O scanner às vezes dá um aviso, quando na realidade não há vulnerabilidade. Por exemplo, se um item de configuração tiver sido desativado, mas o scanner ainda estiver levantando um problema relacionado a ele, marque-o como falso positivo.

Marcação como falso positivo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter detalhes sobre como marcar um VI ou RT como falso positivo, consulte Marcar como falso positivo.

Trabalhar com o falso positivo

Quando um VI ou RT é marcado como falso positivo, o estado é atualizado para Encerrado e o subestado é alterado para Falso positivo. As ações a seguir podem ser realizadas:

- Reabrir
- Excluir
- Atualize a data em **Até** campo. Essa data é usada como a data de vencimento do falso positivo.

Nota: Se não for aprovado, o VI ou RT reverterá para seu estado anterior.

Aprovar um falso positivo

O aprovador pode aprovar o falso positivo do fluxo de trabalho de aprovação.

Nota:

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

Reabrindo um falso positivo

Um VI ou RT em um subestado falso positivo pode ser reaberto a qualquer momento.

Acompanhamento de um falso positivo

Use **Aprovações de mudança de estado** seção para rastrear o status do falso positivo. Uma vez aprovado, o estado do VI ou RT é atualizado para Encerrado e o motivo é Falso positivo.

Vencimento de um falso positivo

Somente o aprovador de falso positivo pode definir uma data até para o falso positivo, para que o VI ou RT expire. Além disso, somente falsos positivos para os quais o aprovador forneceu uma data Até podem expirar. Esta data pode ser fornecida após a aprovação do falso positivo.

Um falso positivo sem uma data até é um falso positivo permanente. Depois que o falso positivo expira, o estado do VI ou VR volta para Aberto.

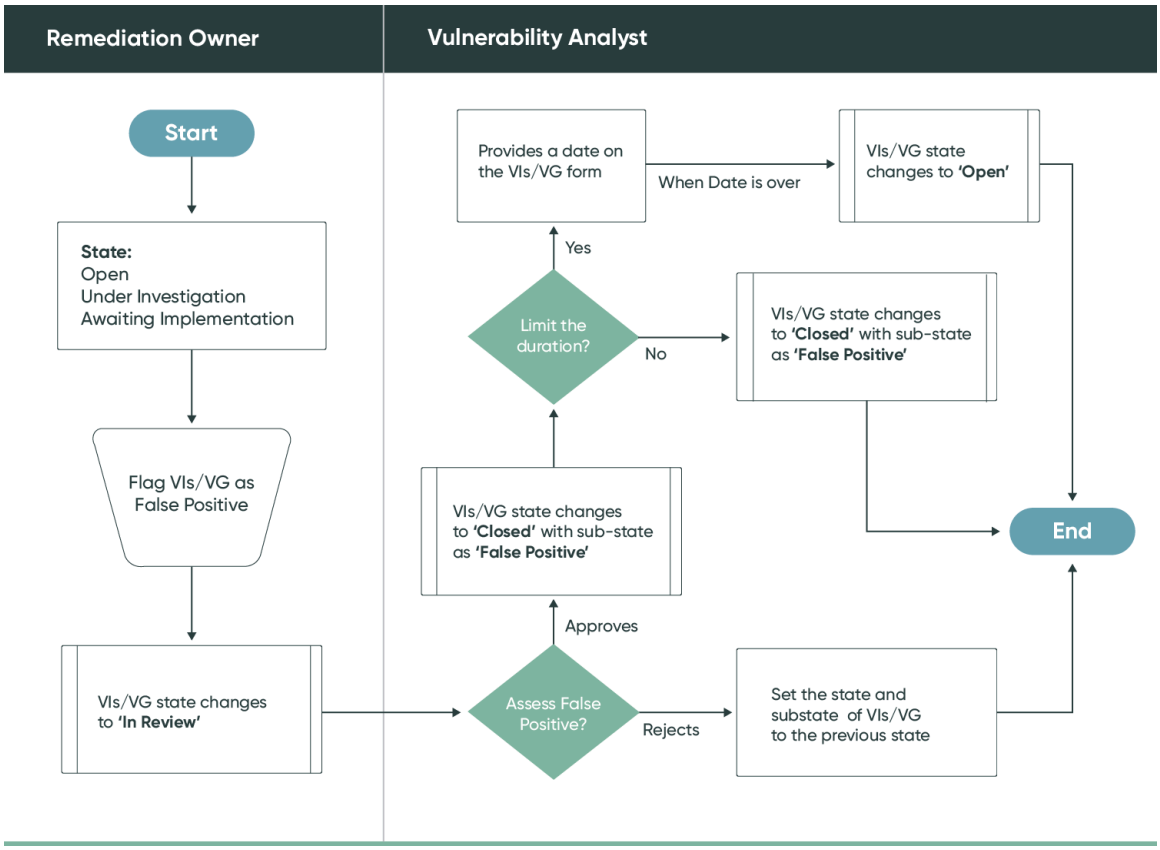
Nota:

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Processo de aprovação de falso positivo anterior à v15 .0



O processo de aprovação será automático se todos os VIS forem aprovados na próxima verificação. O VIS fecha automaticamente, independentemente do estado atual. O VIS ou, quando aplicável, o RT **Estado** os campos mudam para **Encerrado** com o subestado **Corrigido.**

Para obter mais informações, consulte Marcar e aprovar um falso positivo.

Tópicos relacionados

Solicite um falso positivo para um item vulnerável ou corrija a tarefa

Suporte a questionário no Gestão de exceções por meio da Avaliação inteligente

Configure questionários avançados como parte do processo de gestão de exceções usando a Avaliação inteligente. Isso permite que os responsáveis pela correção forneçam um contexto mais detalhado para solicitações de exceção e permite que os aprovadores configurem perguntas condicionais para coletar informações para tomada de decisão informada.

Funções necessárias

Leitor de modelo de avaliação inteligente : **sn_vul_cmn.smart_assessment_template_manager** (Administrador de vulnerabilidades e leitor de modelo) Permite que os administradores criem e editem modelos.

Agente da Avaliação inteligente : **sn_vul_cmn.smart_assessment_actor** Permite que você (responsáveis e administradores de correção) preencha os questionários/avaliações.

Leitor de Avaliação inteligente : **sn_vul_cmn.smart_assessment_reader** Permite que você (Aprovador) leia as respostas do questionário enviadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisito: Os plug-ins de avaliação inteligente devem ser instalados, pois a Avaliação inteligente é uma dependência da Resposta a vulnerabilidades.

Agora você pode configurar questionários como parte do processo de Gestão de exceções usando a Avaliação inteligente. Ele permite que os administradores/gerentes de vulnerabilidades configurem perguntas condicionais para coletar as informações corretas necessárias para a tomada de decisões informadas, permitindo que os responsáveis pela correção forneçam um contexto mais detalhado para solicitações de exceção. Isso melhora a colaboração entre as equipes de Gestão de vulnerabilidades e correção, simplificando o processo de aprovação e garantindo clareza e integridade das justificativas de exceção.

Questionários e avaliações inteligentes podem ser acessados no Workspace, bem como na Interface do usuário clássica, já que alguns fluxos de trabalho ainda exigem os questionários de estilo mais antigos, enquanto a nova avaliação é mais amigável e só é compatível com o Workspace.

Em **Configuração da Gestão de exceções** Agora você pode selecionar a Avaliação para controle de compensação, solicitar exceção e registros de falso-positivo.

Nota: Caso você opte por preencher o campo "Avaliação para solicitar exceção", o sistema permitirá que você considere o modelo de avaliação inteligente ou os questionários clássicos serão considerados.

Você pode usar as duas opções fornecidas abaixo: :

- **Avaliação inteligente** : Gerencie os questionários no Espaço de vulnerabilidades.
- **Questionário existente** : Você pode acessar o questionário existente no Espaço e na experiência clássica.

Os modelos acima podem ser acessados/editados pelo Leitor de modelos de avaliação inteligente: **sn_vul_cmn.smart_assessment_template_manager** .

Configurar o modelo de avaliação

Os modelos de avaliação contêm as perguntas que serão solicitadas durante o processo de solicitação (por exemplo, ao solicitar uma exceção). Os modelos pré-configurados mencionados acima são fornecidos com a avaliação inteligente. Você também pode criar seus próprios modelos conforme necessário.

Antes de Iniciar

Função necessária:

Função de leitor de modelo : **sn_vul_cmn.smart_assessment_reader** Permite que você (Aprovador) leia as respostas do questionário enviadas.

Função de ator do modelo : **sn_vul_cmn.smart_assessment_actor** Permite que você (responsável pela correção e administrador) preencha os questionários/avaliações.

Por Que e Quando Desempenhar Esta Tarefa

No espaço Resposta a vulnerabilidades, você pode selecionar o modelo com o destino de avaliação como VCA, a ser usado para a solicitação de exceção (como Exceção para Resposta a vulnerabilidades, Falso positivo para Resposta a vulnerabilidades). Se você selecionar o modelo padrão, ele preencherá automaticamente as perguntas. Se você optar por criar seu próprio modelo, ele poderá ser modificado.

Procedimento

1. Navegue até Espaço de avaliação.
2. Selecione um existente **Modelo de avaliação** ou selecione um **Novo modelo**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os seguintes detalhes:
   - **Nome do modelo** : Um nome exclusivo para o modelo
   - **Nome da avaliação** : O nome exibido no sistema ao exibir a avaliação.
   - **Categorias de Modelo** : Os modelos são categorizados para facilitar o gerenciamento. Algumas categorias de modelo são fornecidas prontas para uso, por exemplo, Modelos de questionário de resposta a vulnerabilidades, você pode criar modelos de sua escolha.
   - **Metas de avaliação** Especifica a tabela à qual o modelo está relacionado. Para VR, é a tabela VCA (Tabela de aprovação de mudança de vulnerabilidade).

Fluxo de trabalho de Avaliação inteligente

Os responsáveis pela correção devem preencher o questionário antes de enviar para aprovação. Os aprovadores revisam o questionário e tomam decisões de aprovação/rejeição com base nas informações fornecidas.

Antes de Iniciar

Função necessária: **sn_vul_cmn.smart_assessment_reader**

Por Que e Quando Desempenhar Esta Tarefa

A seguir está o fluxo de trabalho da adaptação de avaliação inteligente:

- **Solicitação de exceção/falso positivo** quando você solicita uma exceção ou marca algo como falso positivo, o sistema verifica se um questionário é necessário.
- **. a opção de questionário está habilitada . mensagem obrigatória** solicitará que o usuário preencha o questionário antes de prosseguir com o processo de aprovação.
- **Estado de rascunho** . **Aprovação de mudança de estado de vulnerabilidade** (VCA) permanecerá no estado de rascunho até que o questionário seja enviado e o item de vulnerabilidade (VIT) esteja no estado Aberto.
- **Exibição do aprovador** : Depois que os responsáveis pela correção preenchem o questionário e o enviam, os registros Aprovação de mudança de estado de vulnerabilidade (VCA) e Item de vulnerabilidade (VIT) são movidos para o status Em revisão. Os aprovadores podem revisar os questionários em "Todos > Minhas aprovações". O VIT será movido para o estado Adiado após a aprovação dos registros. Você pode exibir o questionário por meio de um link enviado pelos responsáveis pela correção no cabeçalho do formulário de registro.

Procedimento

1. Navegar **Tudo** > **Minhas aprovações**para exibir o questionário.
2. Quando o registro for **Aprovado** VIT é movido para o estado Adiado.
3. Você pode exibir o questionário por meio de um link enviado pelos responsáveis pela correção no cabeçalho do formulário de registro.

Questionário para falso positivo ou exceção de solicitação

Quando o questionário de falso-positivo ou exceção de solicitação é gerado, mas não preenchido integralmente.

Quando o Questionário de falso-positivo ou exceção de solicitação é gerado, mas não preenchido completamente, o registro VCA entra no estado "Rascunho". Se você quiser gerar uma exceção da mesma categoria, você será direcionado para o questionário anterior seguindo uma anotação pop-up sobre o mesmo. Caso você queira gerar um registro falso

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

positivo em vez de uma exceção de solicitação existente, o sistema substituirá a Aprovação de mudança de estado de vulnerabilidade (VCA) e criará um novo registro Aprovação de mudança de estado de vulnerabilidade falso positivo (VCA).

Caso o questionário esteja preenchido pela metade e o mesmo item de vulnerabilidade (VIT)/ ou qualquer ITEM seja aberto na exibição clássica, você será direcionado até o questionário do espaço para preencher os dados restantes se o mesmo tipo de solicitação for gerado novamente. Se o questionário na exibição clássica for preenchido seletivamente e o mesmo item for aberto no espaço, o questionário de exibição clássica será aberto no espaço.

Watchdog para Resposta a vulnerabilidades

O watchdog é usado para rastrear tabelas com base nas condições especificadas. Por exemplo, ele pode ser usado para registrar detalhes de falhas de execução de integração no Resposta a vulnerabilidades.

Você pode optar por ser notificado sobre essas falhas. Com base nesta notificação, você pode planejar a correção. Os watchdogs padrão são:

- Falha na execução da integração: Se o Estado de execução da integração estiver definido como Concluído e o subestado estiver definido como Falha, os usuários e grupos de usuários serão notificados se a condição retornar uma contagem maior que 0, ou seja, a execução da integração falhar.
- Integrações de execução longa: Script para verificar se a execução da integração está excedendo o tempo definido. Este watchdog alerta proativamente sempre que há um atraso na conclusão da execução da integração.
- Execuções periódicas sobrepostas: Script para verificar as execuções de integração recorrentes que ainda continuam sendo executadas durante a próxima ocorrência. Ele gera um link que contém a lista dessas execuções de integrações.

Log de observação

O watchdog vem com um log de observação, que fornece uma contagem do número de vezes que a condição foi atendida.

Painel Visão geral

Use o painel Visão geral para monitorar o watchdog nos últimos 30 dias. Você pode criar vários widgets para rastrear outros tópicos de watchdog que você está monitorando.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Relatório

Nome	Descrição
Falha no WatchDog nos últimos 30 dias	Todas as condições atendidas nos últimos 30 dias.

Para obter mais informações, consulte Configurar watchdog e Tratamento de erros para detecções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de mudanças para Resposta a vulnerabilidades

Como responsável pela correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente das tarefas de correção (RT) no Resposta a vulnerabilidades aplicação. As solicitações de mudança ajudam você a iniciar e rastrear atividades de mudança em seus ativos para que você possa corrigir suas tarefas de correção e seus itens vulneráveis correspondentes.

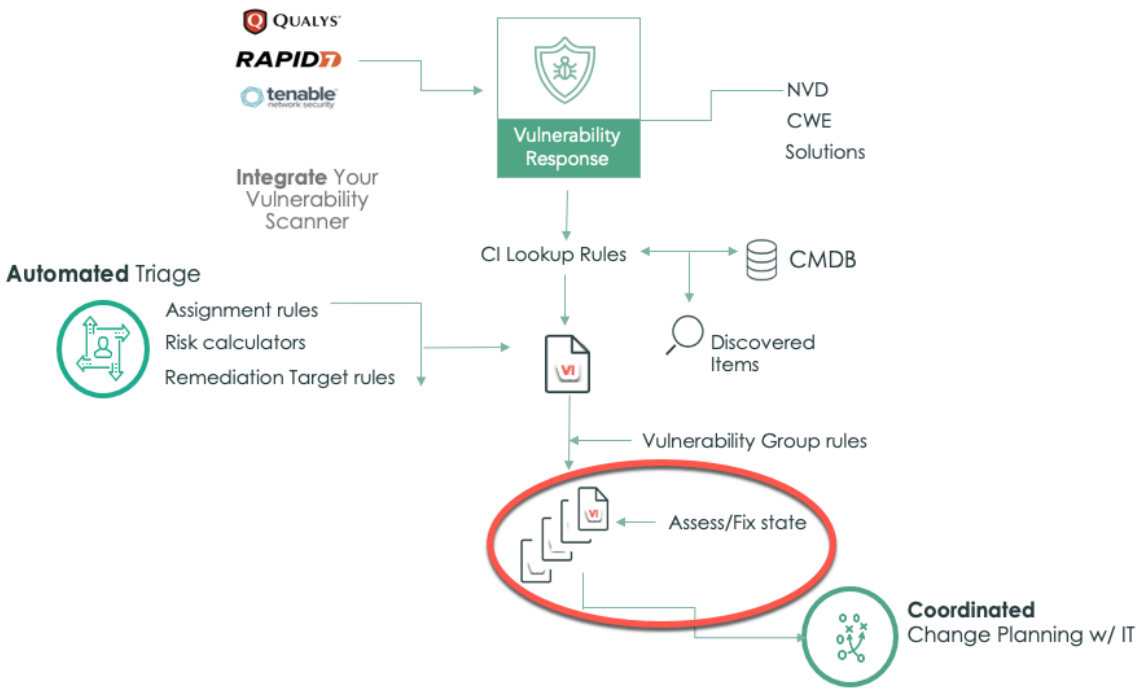
Solicitações de mudança e o fluxo de trabalho de vulnerabilidade

Se você não estiver familiarizado com a aplicação Resposta a vulnerabilidades, para obter mais informações, consulte Explorar o. Resposta a vulnerabilidades aplicação.

A imagem a seguir ilustra o fluxo de informações do Resposta a vulnerabilidades, da integração (scanner) configurada por meio de triagem automatizada e em investigação.

As solicitações de mudança e a gestão de mudanças fazem parte do processo de correção (estado Avaliar/Corrigir) no Resposta a vulnerabilidades fluxo de trabalho mostrado na figura a seguir. Durante esta fase, você pode usar solicitações de mudança para iniciar e rastrear a correção de vulnerabilidades. Você pode criar e gerenciar solicitações de mudança diretamente da tarefa de correção e listar tarefas de investigação e correção que incluem soluções para ativos afetados para os itens de configuração (IC) no CMDB.

Solicitações de mudança na Resposta a vulnerabilidades



Quando usar solicitações de mudança na resposta a vulnerabilidades

Como responsável pela correção de TI, você pode criar solicitações de mudança a partir de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro de tarefa de correção ajuda a investigar e resolver vulnerabilidades rapidamente. O VIS de tarefas de correção resolvidas pode ser verificado e verificado durante a próxima verificação programada em seu ServiceNow AI Platform e retornou à triagem automatizada do Resposta a vulnerabilidades fluxo de trabalho. As intervenções manuais que podem exigir solicitações de mudança incluem os seguintes exemplos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um patch de software, correção ou outra tarefa da TI que é necessária em itens vulneráveis antes da resolução de RT.
- Você determina que um subconjunto dos itens vulneráveis em uma tarefa de correção requer investigação adicional ou reatribuição a outro departamento.
- Você determina que um subconjunto de itens vulneráveis em um RT com um grande conjunto de itens vulneráveis pode ser movido para uma nova tarefa de correção.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar a duplicação de tarefas de correção.

Tipos de solicitações de mudança para um RT

. Resposta a vulnerabilidades a aplicação utiliza os três tipos de mudanças de serviço compatíveis com ITSM Gestão de mudanças produto em seu ServiceNow AI Platform® instância - padrão, emergência e normal. O tipo de mudança selecionado determina qual modelo de estado é invocado e o processo de mudança que deve ser seguido. As solicitações de mudança Registram as informações detalhadas sobre a mudança, como o motivo da mudança, a prioridade, o risco, o tipo de mudança e a categoria de mudança. Consulte Tipos de mudança .

. Resposta a vulnerabilidades Responsável pela correção DE TI, você tem as seguintes opções para criar solicitações de mudança normais, padrão e emergenciais diretamente de uma tarefa de correção:

- Você pode criar solicitações de mudança que contenham informações preenchidas previamente da tarefa de correção para simplificar o processo e economizar tempo.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar criar solicitações de mudança duplicadas que compartilham informações semelhantes e itens vulneráveis.
- Usando um conjunto de condições, você pode filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para um novo RT.

Você pode filtrar itens vulneráveis usando valores de qualquer campo de uma tarefa de correção e aplicar a solicitação de mudança somente aos itens que correspondem aos critérios de filtro.

Tópicos relacionados

Crie uma solicitação de mudança a partir de uma tarefa de correção

Associe uma tarefa de correção a uma solicitação de mudança existente

Divida uma tarefa de correção

Sincronização de estado entre solicitações de mudança e tarefas de correção

Avaliação de exposição de software usando Software Asset Management (SAM Foundation)

Use ServiceNow® Vulnerabilidade Aplicação de avaliação de exposição para determinar sua contagem total de software instalado para um pacote de software específico em seus ativos. Quando usado com ServiceNow® Software Asset Management (SAM) Foundation, avalie sua exposição, crie itens vulneráveis e gerencie a correção do software vulnerável descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Você pode executar a avaliação de exposição por CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e software para aproveitar os recursos adicionais no Espaço de avaliação de vulnerabilidades. Para obter mais informações, consulte Explorar o Espaço de avaliação de vulnerabilidade.

Determine sua exposição a software vulnerável fornecendo as informações de software vulnerável (fornecedor, produto, edição e versão) sem usar o banco de dados CVE (Common Vulnerabilities and Exposures). Avalie casos de vulnerabilidades de dia zero (dia atual) no software para os seguintes casos:

- Quando os produtos ainda não têm dados CVE.
- Quando há um atraso entre o momento em que uma vulnerabilidade se torna publicamente conhecida e os dados CVE com a vulnerabilidade são atualizados no NVD.
- Quando você aprende sobre a vulnerabilidade entre as verificações programadas do seu verificador de vulnerabilidades.

Com Vulnerabilidade Aplicação de avaliação de exposição, se você conhecer o fornecedor e o produto do software vulnerável, usando os registros que listam o software instalado em sua rede criada pelo SAM Foundation, você pode avaliar sua exposição a pacotes de software potencialmente mal-intencionados sob demanda.

Conhecer a escala de sua exposição a esse tipo de vulnerabilidade permite que você responda proativamente implementando um alerta vermelho e desinstalando o software ou informando seu SOC (Security Operations Center, centro de operações de segurança) para procurar um patch específico. Você pode criar itens vulneráveis e atribuir tarefas ao especialista em correção para correção adicional de investigação. Exiba uma lista de tarefas de correção (VUL) para verificar se os itens vulneráveis desejados foram criados e associados corretamente ao VUL.

Tópicos relacionados

Configure o. Vulnerabilidade Avaliação de exposição

Avalie sua exposição a software vulnerável

Gestão de crises de vulnerabilidade

Crie e rastreie eventos de vulnerabilidade crítica por meio do fluxo de trabalho de Gestão de crises de vulnerabilidade (VCM). Crie registros de avaliação de vulnerabilidade, registre os principais atributos da vulnerabilidade para calcular o risco, execute a avaliação para identificar o nível de exposição e envolva as partes interessadas para uma resposta coordenada e rápida às vulnerabilidades.

Gerenciar eventos de crise de vulnerabilidade

A Gestão de crises de vulnerabilidade é um fluxo de trabalho completo para lidar com eventos de crise de vulnerabilidade com os seguintes recursos.

- Identifique itens de configuração vulneráveis com eficiência, correlacionando vulnerabilidades críticas com o inventário de instalação de software do Software Asset Management e. Lista de materiais de software Inventário do (SBOM), vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB).
- Converta os resultados da avaliação em itens vulneráveis para correção.
- Iniciar um incidente de segurança grave para garantir uma resposta rápida e coordenada à ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Interaja e colabore com equipes em toda a organização, facilitando uma resposta unificada a vulnerabilidades.
- Forneça relatórios de status regulares para as partes interessadas interfuncionais e equipes envolvidas para manter a transparência e a comunicação durante a crise.

Gestão de crises de vulnerabilidade usando o Espaço de avaliação de vulnerabilidades

Nota: A partir da v1.0.1 da Gestão de crises de vulnerabilidade, a aplicação está disponível como uma assinatura separada na loja. Você poderá acessar a Gestão de crises de vulnerabilidade no espaço Avaliação de vulnerabilidades somente se tiver direito detalhado ou tiver instalado a aplicação da Store. Anteriormente, a Gestão de crises de vulnerabilidade era incluída com o plug-in Resposta de emergência de vulnerabilidade. A partir da v3.2.2, o plug-in Resposta de emergência de vulnerabilidade foi renomeado para Avaliação de exposição a vulnerabilidades.

Ao identificar uma vulnerabilidade de interesse, o gerenciador de eventos de vulnerabilidade cria um registro de avaliação de vulnerabilidade com informações sobre a origem de inteligência contra ameaças, as características da vulnerabilidade e os produtos afetados. Essas informações são usadas para análises adicionais de impacto e exposição.

Uma avaliação de risco é realizada depois que o registro de uma vulnerabilidade de interesse é criado. Esta avaliação compreende pontuação de risco estruturada, revisão do registro e as observações do analista que executa a tarefa. A pontuação de risco inicial para uma vulnerabilidade de interesse é calculada usando os atributos disponíveis no momento da criação do evento. A pontuação de risco da avaliação pode mudar conforme inteligência adicional se torna disponível. Use a pontuação de risco para determinar o possível impacto da exploração e estabelecer prioridades de resposta.

Depois que a avaliação de uma vulnerabilidade de interesse tiver sido criada e determinada como um risco para a infraestrutura da organização, você poderá analisar a ameaça mais detalhadamente atualizando a avaliação de risco com uma avaliação de exposição detalhada com o inventário de instalação de software de Software Asset Management, Lista de materiais de software Inventário do (SBOM), vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB). Itens de configuração e aplicações afetados são identificados automaticamente por meio de avaliação. Itens afetados adicionais podem ser adicionados manualmente.

Quando a avaliação é concluída, itens vulneráveis ou itens vulneráveis da aplicação podem ser criados para os resultados de exposição que ainda não têm um Item vulnerável associado. A calculadora de pontuação de risco de itens vulneráveis pode ser aproveitada/configurada para ajustar a pontuação de risco de itens vulneráveis vinculados a registros de avaliação de vulnerabilidade. O registro de Avaliação de vulnerabilidades pode ter nível de exposição e prioridade de evento atribuídos. Com base na prioridade do evento, o Gerenciador de eventos de vulnerabilidade pode optar por propor, promover ou vincular a avaliação de vulnerabilidade a um incidente de segurança grave.

Usar Gestão de incidentes graves de segurança para rastrear e gerenciar a atividade de correção, vincule incidentes de segurança contínuos, crie tarefas ad-hoc, envolva equipes afetadas, envie relatórios de status e colabore usando integrações de colaboração disponíveis em Gestão de incidentes graves de segurança.

ServiceNow® Software Asset Management e. Lista de materiais de software(SBOM avaliação - lógica de processamento

Usando o. Software Asset Management Os dados, os CPEs provenientes do NVD para o CVE e os modelos de descoberta são obtidos usando a lógica de correspondência de cadeia de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

caracteres. Depois de buscar os modelos de descoberta, uma verificação de instalações relacionadas é executada, os itens de configuração relacionados são obtidos e a tabela Item de configuração afetado é preenchida. Você pode fornecer mais detalhes, como Fornecedor, Produto, Versão e Edição. Todos os modelos de descoberta correspondentes e as instalações de software do registro são obtidos. Em seguida, os itens de configuração relacionados são obtidos e a tabela Item de configuração afetado é preenchida novamente.

Para SBOM O software associado ao CVE da tabela Relacionado (m2m) (entre CVE e Software) é obtido. Depois de extrair os detalhes do software, os componentes de SBOM relacionados são identificados combinando o produto e a versão do componente de SBOM com o produto e a versão do software identificados.

Depois que os componentes associados são encontrados, as entidades relacionadas aos componentes são obtidas. O modelo de produto das entidades e o IC relacionado (se encontrado) são obtidos e o item de configuração é salvo na tabela Item de configuração afetado. Se o item de configuração estiver sem itens vulneráveis, você poderá usá-lo para criar o item vulnerável. Se um item de configuração não for encontrado, o modelo de produto será salvo na tabela Modelo de software afetado e poderá ser usado para criar itens vulneráveis à aplicação.

Para obter mais informações sobre como usar o fluxo de trabalho da Gestão de crises de vulnerabilidade, consulte Usando o espaço Avaliação de vulnerabilidades .

Tópicos relacionados

Explorando a avaliação de vulnerabilidades

Explorar o Espaço de avaliação de vulnerabilidade

Guia Avaliação

Separação de domínios e Resposta a vulnerabilidades

Separação de domínios é compatível com Resposta a vulnerabilidades. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui todos os aspectos de **Básico** suporte de nível.
- As propriedades da aplicação reconhecem domínio conforme necessário.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Resposta a vulnerabilidades

Com o Domain Separation, você pode padronizar a VR (Resposta a vulnerabilidades), em toda a base de clientes que você atende, com custos operacionais reduzidos e maior qualidade de serviço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Separar espaços de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte ao Domain Separation no Vulnerability Response por versões de versão

Versão	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Roma	Padrão	
San Diego	Padrão	
Tóquio	Padrão	
Utah	Padrão	
Vancouver	Padrão	
Washingtondc	Padrão	

Separação de domínio para Resposta a vulnerabilidades a aplicação abrange as seguintes funcionalidades do produto:

- Ingere os itens vulneráveis de scanners de terceiros (por exemplo, Qualys, Rapid 7 ou Tenable) no domínio correto. Os dados ingeridos no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.
- Verifica novamente ativos específicos de Resposta a vulnerabilidades no domínio do qual foi solicitado.
- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula pontuações de risco no nível do item vulnerável de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- As regras de destino de correção são executadas em itens vulneráveis de acordo com as regras de destino de correção definidas no mesmo domínio do usuário de integração.
- As regras de tarefa de correção podem ser definidas e permanecer no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de tarefa de correção permanecem no mesmo domínio em que as regras de grupo são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados de item vulneráveis, como idade do item vulnerável, itens vulneráveis em aberto por IC, vulnerabilidades por impacto e status da data de destino de correção no domínio ao qual ele pertence.
- O conhecimento de scanners de terceiros ou do National Vulnerability Database (NVD) pode ser ingerido no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota: Em todos os casos acima, os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform se aplicam.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como criar e oferecer suporte a importações separadas por domínio, consulte Crie importações separadas por domínio para uma integração e. Crie e ofereça suporte a vários domínios na estrutura de trabalhos em segundo plano.

Casos de uso

. Resposta a vulnerabilidades a aplicação gerencia o ciclo de vida de um item de vulnerabilidade de ponta a ponta Os seguintes casos de uso reconhecem a separação de domínios:

- **Ingerir** itens vulneráveis (vulnerabilidades no ativo) da integração de terceiros.
  - Ingerir dados de várias instâncias
  - Desduplicar o item vulnerável
  - Corresponder ao IC do CMDB
- **Aprimoramento** de item vulnerável com pontuações de risco e datas de destino de correção
  - Aprimoramento de ativos (CMDB)
  - Aprimoramento da pontuação de risco e da data de destino de correção
- **Grupo** itens vulneráveis e atribua a tarefa de correção
  - Agrupar automaticamente os itens vulneráveis
  - Atribua automaticamente a tarefa de correção
- **Corrigir**
  - Tarefas de correção
  - Ciclo de vida de correção abrangente
  - Fluxo de trabalho de adiamento
- **Medida** a postura de segurança da organização e do programa de gestão de vulnerabilidades
  - Tendência de vulnerabilidade, ativo mais vulnerável, vulnerabilidade por idade
  - Status de correção pela data de destino de correção

Configuração

Configuração do Domain Separation para Resposta a vulnerabilidades não requer etapas adicionais. Todos Resposta a vulnerabilidades As tabelas adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar dados de importação de integração de vulnerabilidade para domínios específicos. Para obter mais informações, consulte Crie importações separadas por domínio para uma integração.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- O item vulnerável ingerido de scanners de terceiros permanece no mesmo domínio que o domínio do usuário de integração e não pode ser acessado de nenhum outro domínio.
- Itens vulneráveis (instâncias) ou ativos em um domínio não podem ser exibidos de outros domínios.
- O algoritmo de pontuação de risco, as regras de tarefa de correção e as regras de destino de correção não podem ser exibidas por ninguém fora do domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As informações de vulnerabilidade do NVD podem existir no domínio global e ser compartilhadas com todos os clientes.
- As tarefas de correção em um domínio não podem ser exibidas de outro domínio.
- Os fluxos de trabalho de adiamento criados em um domínio não estão visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Nota:

Os modelos de importação programada disponíveis na instância são definidos por padrão como "Domínio: Global". Portanto, para evitar conflitos quando houver vários domínios nas instâncias, adapte a seguinte prática:

- Distribua os modelos de importação disponíveis na instância entre o número de domínios envolvidos na integração.
- Atualize o domínio do registro do modelo de importação para o sys_id do domínio de destino.
- Se necessário, crie modelos de importação para cada domínio.
- Certifique-se de que cada domínio tenha 2 modelos de importação.
- sn_vul_sched_import_pool: Os registros desta tabela devem ser separados por domínio se a separação de domínio estiver presente na instância

Como os analistas de vulnerabilidade gerenciam seus próprios dados de aplicações

- Os analistas criam sua própria instalação de aplicações, gestão de aplicações de várias origens e regras de pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de gestão de adiamento e mudanças.
- Os analistas podem criar suas próprias regras de tarefa de correção, lógica de pontuação de risco para priorizar vulnerabilidades com precisão, atribuir tarefas de correção automaticamente e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam um item de vulnerabilidade manual e o encerram.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Resposta a vulnerabilidades usuários e grupos
- Integrações do Resposta a vulnerabilidades
- Configuração de configuração completa (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de tarefa de correção, calculadoras de risco, regras de meta de correção etc.)
- Ciclo de vida de correção completo, incluindo adiamento
- Programar trabalhos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Domain Separation para provedores de serviço

Mapeamento de serviços no Resposta a vulnerabilidades

O mapeamento de serviços ajuda as organizações a obter uma compreensão abrangente da sua infraestrutura DE TI e dos relacionamentos entre os vários componentes. Ele permite a descoberta automática e o mapeamento de serviços, aplicações e componentes de infraestrutura, fornecendo uma representação visual das dependências e relacionamentos.

Em Resposta a vulnerabilidades, o trabalho agendado *`Set related CI services`*Estabelece conexões entre os serviços de negócio afetados e os itens de configuração (ICs) associados aos itens vulneráveis (Vits). O processo de vinculação ocorre quando a importação da integração é concluída e em um horário designado. Para melhorar o desempenho deste trabalho agendado, várias mudanças foram implementadas a partir da v21.1.2 de Resposta a vulnerabilidades. Eles são:

- Cálculo da pontuação de risco: O processo de cálculo das pontuações de risco envolve a utilização do *`Set related CI services`*trabalho agendado. Depois que o IC é processado, este trabalho armazena os dados necessários na tabela Serviços relacionados [sn_vul_m2m_ci_services]. Anteriormente, em Conformidade de configurações cálculo de risco envolvido no acesso direto ao Configuration Management Database (CMDB) API (Application Programming Interface, interface de programação de aplicações) *`ICUtils`* para recuperar serviços para cada resultado de teste durante a importação. No entanto, o processo atual depende da saída do trabalho agendado da tabela Serviços relacionados [sn_vul_m2m_ci_services] para calcular a pontuação de risco em Conformidade de configurações. Além disso, a calculadora do sistema de base foi modificada para utilizar a tabela Serviços relacionados [sn_vul_m2m_ci_services].
- Tamanho dos serviços: O valor do serviço na propriedade do sistema *`sn_sec_cmn.services_affected_by_CI_max_size`*, que está relacionado a *`Set related CI services`*o trabalho agendado foi reduzido de 1000 para 500.
- Profundidade dos serviços: A profundidade na propriedade do sistema *`sn_sec_cmn.services_affected_by_CI_max_depth`*, que está relacionado a *`Set related CI services`*o trabalho agendado foi reduzido de 10 para 5. O valor do serviço também foi reduzido de 1000 para 500.
- Exclusão de CMDB Classes: Uma propriedade do sistema *`sn_sec_cmn.ignoreCIClassForService`*foi introduzido para habilitar a configuração de CMDB classes para as quais o cálculo de serviço deve ser ignorado. No sistema de base, esta propriedade é definida para *`cmdb_ci_unclassed_hardware`* , *`cmdb_ci_incomplete_ip`* , *`sn_sec_cmn_unmatched_ci`* como essas classes são criadas por Resposta a vulnerabilidades e podem não ter nenhum mapeamento de serviço. Anteriormente, o cálculo do serviço era baseado na VIT. No entanto, a lógica foi modificada para usar o item descoberto. O item descoberto é usado para calcular o serviço, que é associado ao IC na mesma tabela.
- Trabalho agendado para atualização completa de serviços: Um trabalho agendado sob demanda *`Full refresh-related CI services for VI`*, foi introduzido para executar uma atualização completa de serviços. Ao fazer upgrade para a v21.0 de Resposta a vulnerabilidades. *`Set related CI services`*o trabalho é executado por uma duração mais longa no início, pois a tabela base usa itens descobertos em vez de itens vulneráveis. Como resultado, o trabalho deve processar todos os itens descobertos que foram verificados nos últimos 90 dias. Se você precisar de atualizações de serviço mais frequentes, isso poderá ser acomodado programando atualizações periódicas semanais ou executando uma atualização completa. Se você realizou atividades que resultaram em mudanças nos serviços associados aos ICs e você deseja Resposta a vulnerabilidades para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

refletir essas mudanças, você pode executar o trabalho agendado sob demanda *`Full refresh related CI services for VI`*. Este trabalho usa todos os itens descobertos registrados nos últimos 90 dias e atualiza os serviços associados de acordo.

Tópicos relacionados

Mapeamento de serviços

ICUtils - Global

Implementação de Resposta a vulnerabilidades

Use as etapas ilustradas nas imagens a seguir para baixar o. Resposta a vulnerabilidades aplicação do ServiceNow Store, instale-o em seu ServiceNow AI Platform® E configure-a usando o Assistente de configuração.

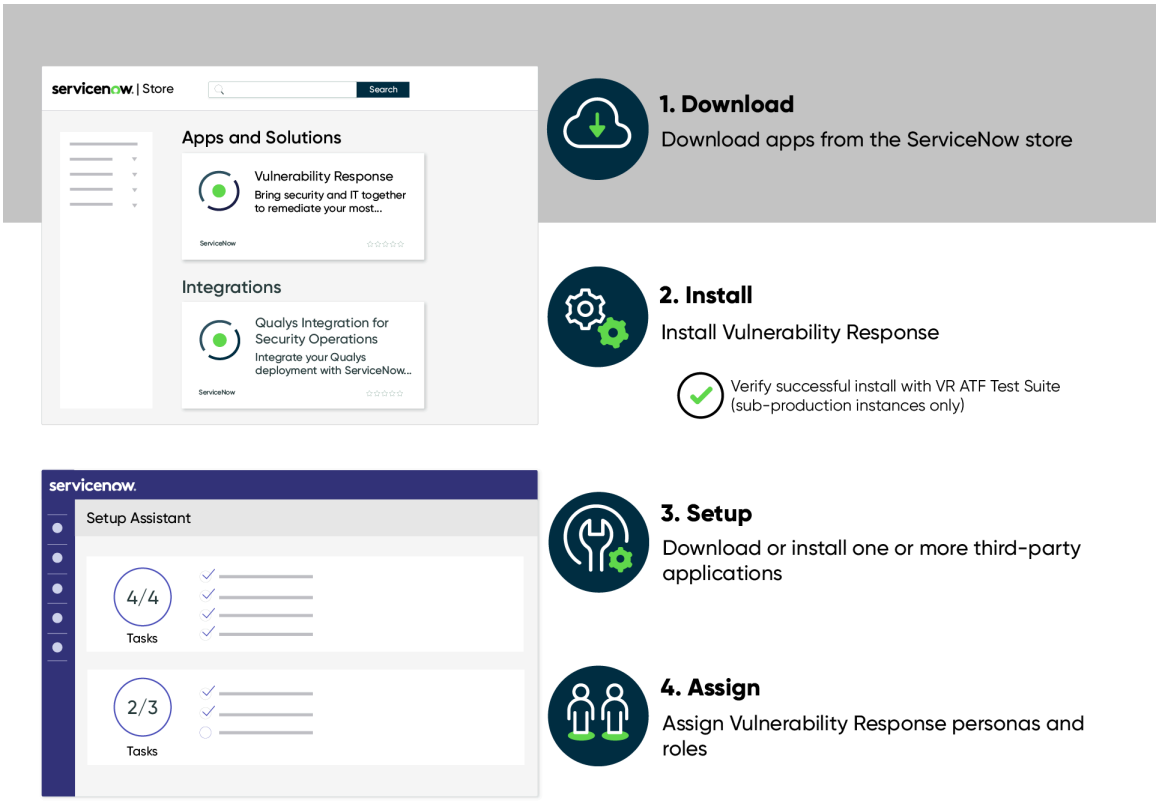
Um exemplo de instalação e configuração para instalar o sistema de base, o. Resposta a vulnerabilidades e uma aplicação de scanner de terceiros, o Qualys a aplicação, é ilustrada nas imagens a seguir. Funções obrigatórias e tarefas obrigatórias, bem como etapas opcionais, também são listadas.

- Para obter mais informações sobre cada etapa ilustrada nas imagens a seguir e uma check-list com links para a documentação de suporte, consulte Check-list de implementação do Resposta a vulnerabilidades aplicação.
- Você pode estender os conceitos e a sequência de etapas apresentados neste exemplo para instalar e configurar outros aplicativos compatíveis para Resposta a vulnerabilidades. Para obter uma lista de aplicações de suporte, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.
- A função de administrador é necessária para baixar e instalar o. Resposta a vulnerabilidades e Qualys Aplicação de vulnerabilidade usada para este exemplo.
- A função de administrador também atribui a persona Administrador de vulnerabilidades [sn_vul.vulnerability_admin] e outros Resposta a vulnerabilidades funções de persona para usuários e grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de administrador

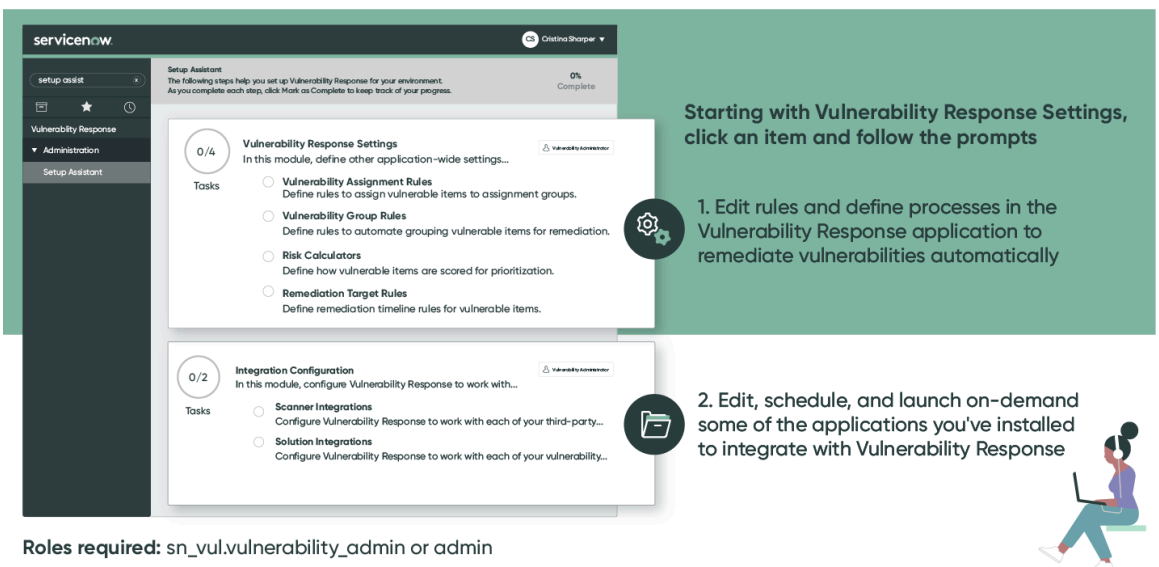


A função sn_vul.vulnerability_admin configura o. Resposta a vulnerabilidades e. Qualys No Assistente de configuração e verifica os resultados esperados.

Siga as etapas e avisos no Assistente de configuração, começando pela seção Configurações de resposta a vulnerabilidades para continuar com a instalação e a configuração. Revisar essas configurações ajuda a entender e verificar os processos de Resposta a vulnerabilidades conforme você continua a configurar seu ambiente.

Função necessária: sn_vul.vulnerability_admin ou, como alternativa, admin.

Tarefas de administrador de vulnerabilidades



Roles required: sn_vul.vulnerability_admin or admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revise as descrições, as configurações padrão e os dados de demonstração que você instalou com os aplicativos nas seguintes seções:

- Regras de atribuição de vulnerabilidade - Atribua automaticamente itens vulneráveis (VIS) ao grupo de atribuição apropriado.
- Regras da tarefa de correção - agrupe automaticamente itens vulneráveis (VIS) conforme eles são importados com base em determinadas condições.
- Calculadoras de risco - A calculadora de risco padrão está habilitada.
- Regras de destino de correção - Defina linhas de tempo de correção para VIS e tarefas de correção (RTS).
- Revise e edite as configurações dos aplicativos de terceiros e das soluções instaladas que você instalou e defina as condições para suas importações de dados. Insira suas informações de conta de terceiros e defina as configurações de importação, cronogramas, regras de pesquisa de item de configuração (IC), bem como outras configurações.

Para obter mais informações, consulte Check-list de implementação do Resposta a vulnerabilidades aplicação.

Para obter informações adicionais ao personalizar ou implementar o. Resposta a vulnerabilidades aplicação, consulte KB1000704 .

Instalar Resposta a vulnerabilidades

Antes de executar o. Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform, você deve obter direito e baixar a aplicação do ServiceNow Store, instale-o em seu ServiceNow AI Platform E conclua algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

- Verifique se você tem o necessário ServiceNow funções atribuídas à sua instância.
- A função de administrador é necessária para instalação e atribuição de funções.

Função necessária: administrador

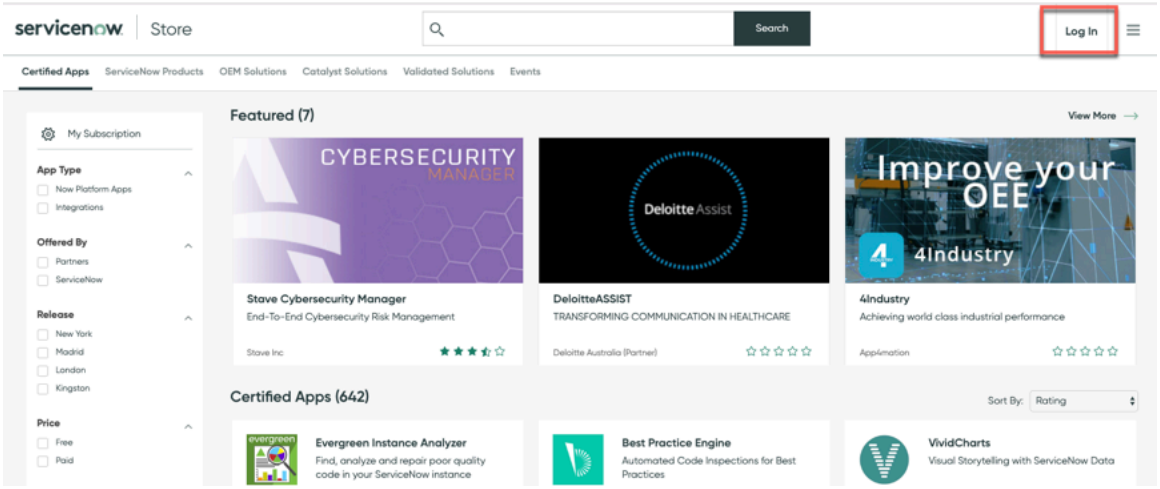
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Para obter direito e baixar o. Resposta a vulnerabilidades aplicação principal, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Faça login** .

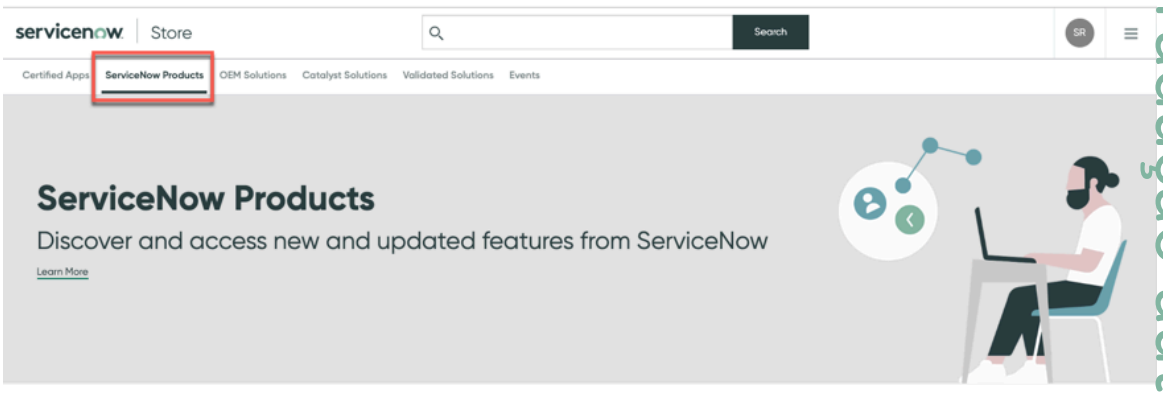
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login** .

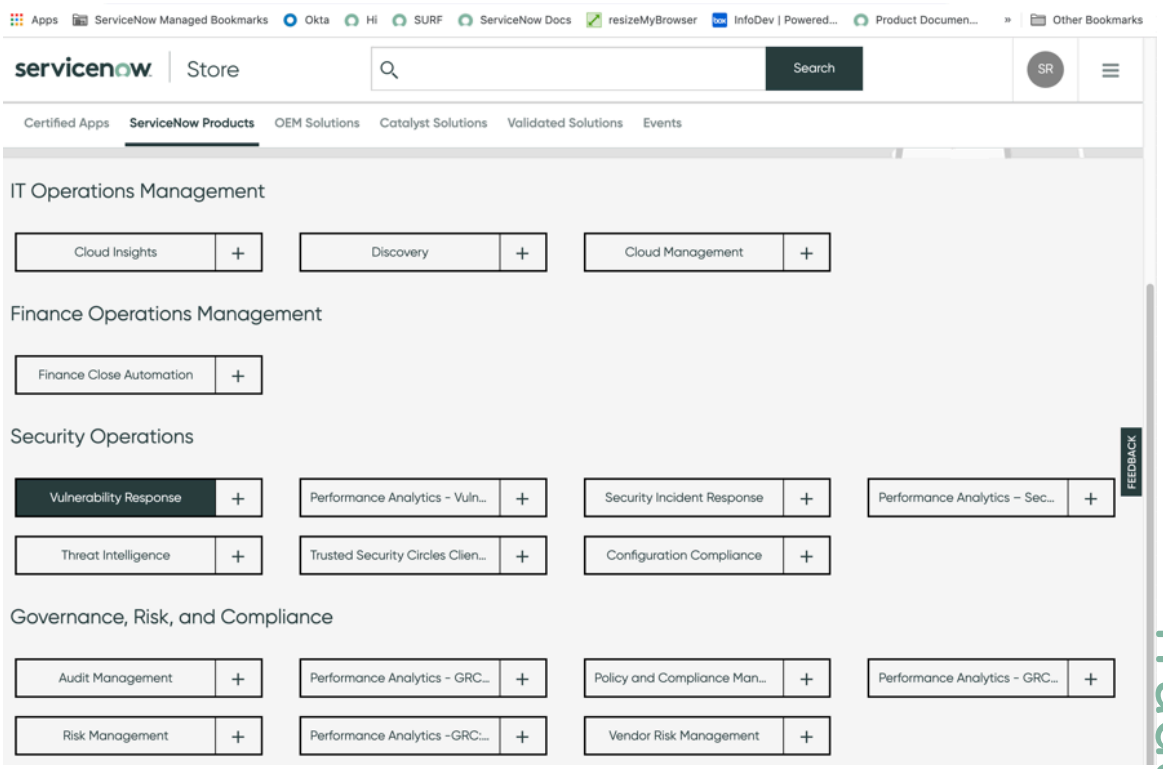
4. Na página exibida, se não estiver selecionada, clique em **Produtos da ServiceNow** guia.



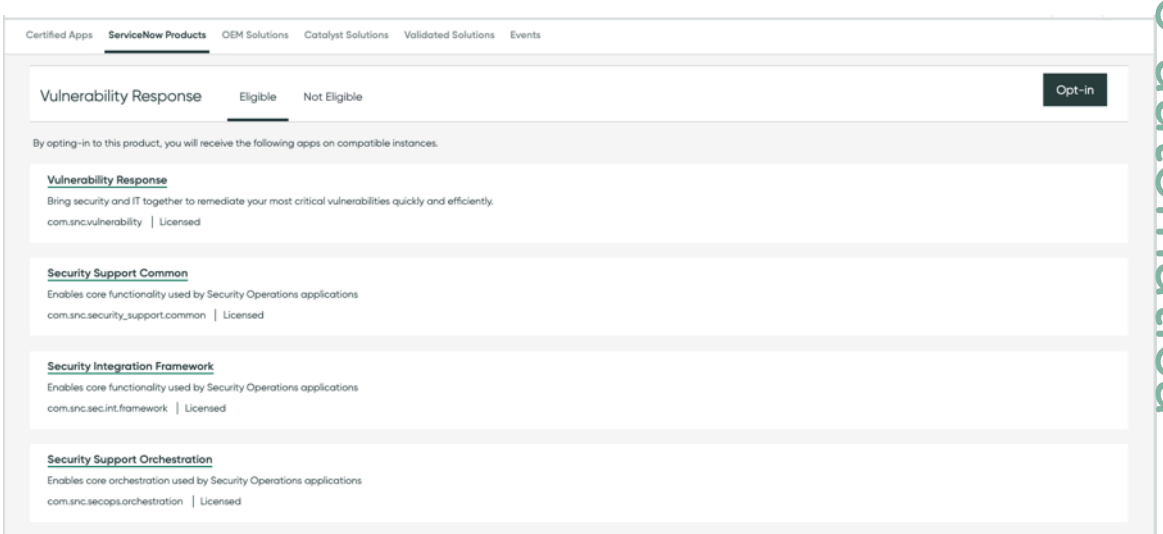
5. Para exibir as aplicações associadas para as quais você está qualificado com Resposta a vulnerabilidades na página de lista de produtos, clique em **Resposta a vulnerabilidades** produto.

Tradução automática

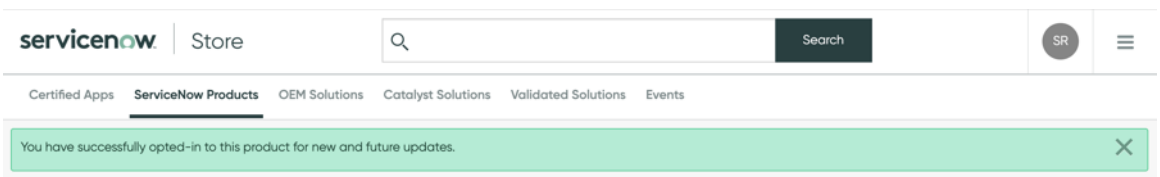
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia Qualificado lista todas as aplicações para as quais você está qualificado se você aceitar. Para obter mais informações sobre uma aplicação, clique em um link.



6. Para obter Resposta a vulnerabilidades aplicação principal, clique em **Aceite** .
7. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar** .
   É exibida uma mensagem indicando que você aceitou a aplicação com sucesso.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com ServiceNow Selecionada e exibida, uma marca de seleção verde substitui o sinal de adição à direita do Resposta a vulnerabilidades, conforme mostrado na figura a seguir.

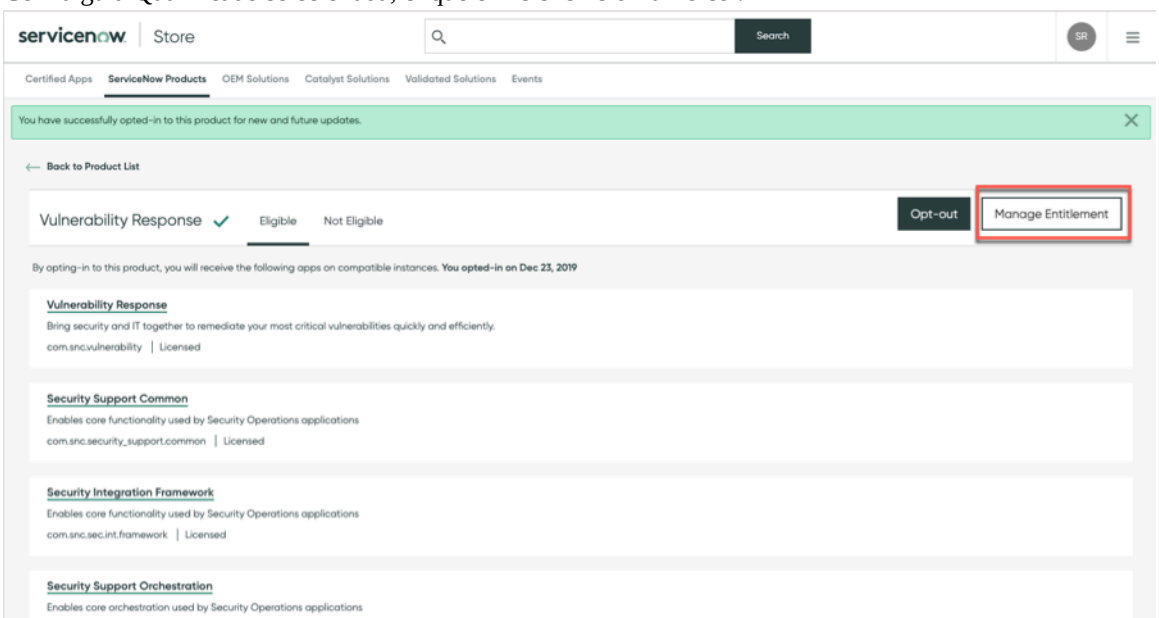


Depois de aceitar os termos e condições e os direitos gerenciados para qualquer uma das aplicações no **Produtos da ServiceNow** Na página Lista de produtos, você pode clicar no sinal de adição para obter direito e aceitação para os outros aplicativos nesta página com um único clique.

8. Passe para a etapa 10 para instalar a aplicação no seu ServiceNow AI Platform instância.
9. **Opcional:** Como alternativa, para gerenciar seu direito para Resposta a vulnerabilidades aplicação em outro ServiceNow AI Platform, siga estas etapas.

   a. Se o botão Gerenciar direito não for exibido, clique em Resposta a vulnerabilidades Na Lista de produtos para exibi-la.

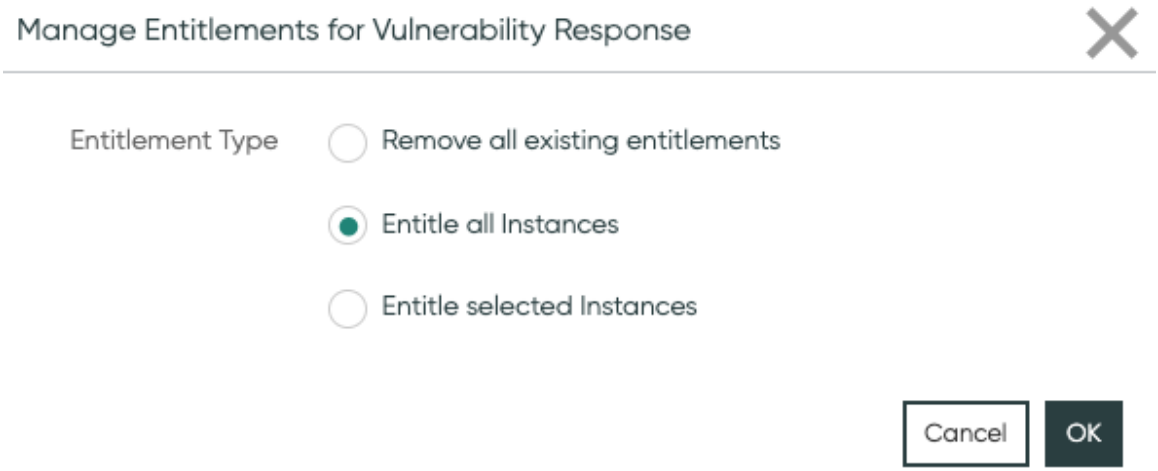
   b. Com a guia Qualificado selecionada, clique em **Gerenciar direito** .



   c. Na caixa de diálogo Gerenciar direitos para resposta a vulnerabilidades exibida, escolha uma:

Tradução automática

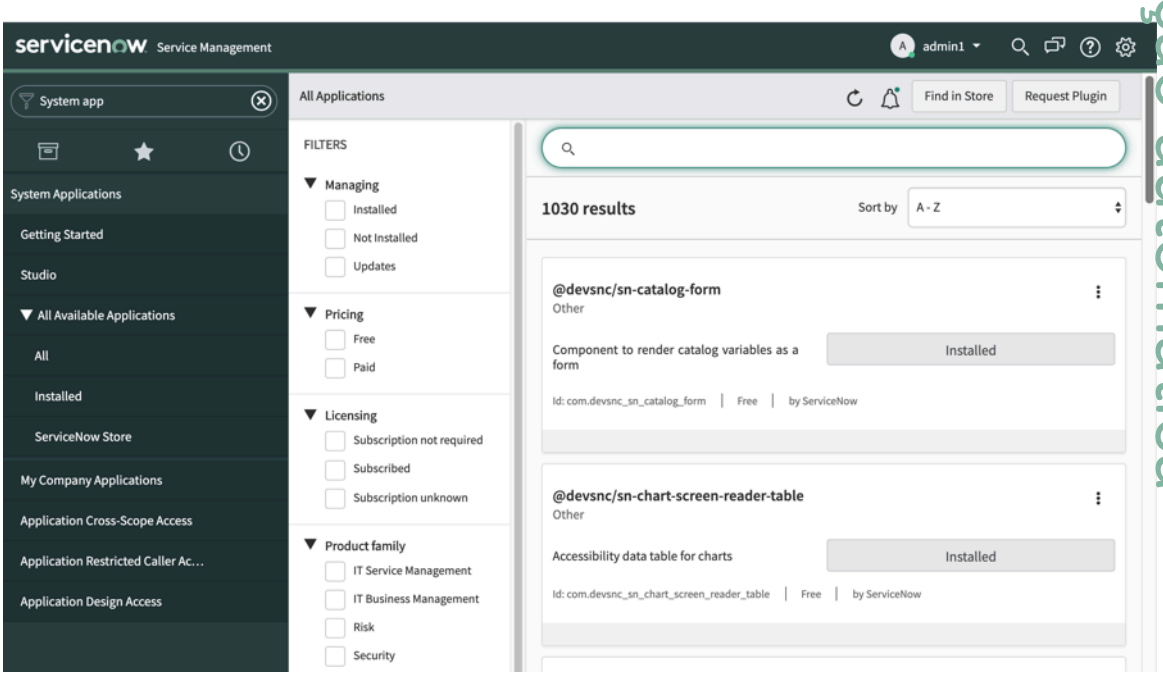
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Clique em **OK** ou **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar o aplicativo em seu ServiceNow AI Platform instâncias.

10. Faça login no ServiceNow AI Platform instância em que você deseja instalar Resposta a vulnerabilidades aplicação em.

11. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.



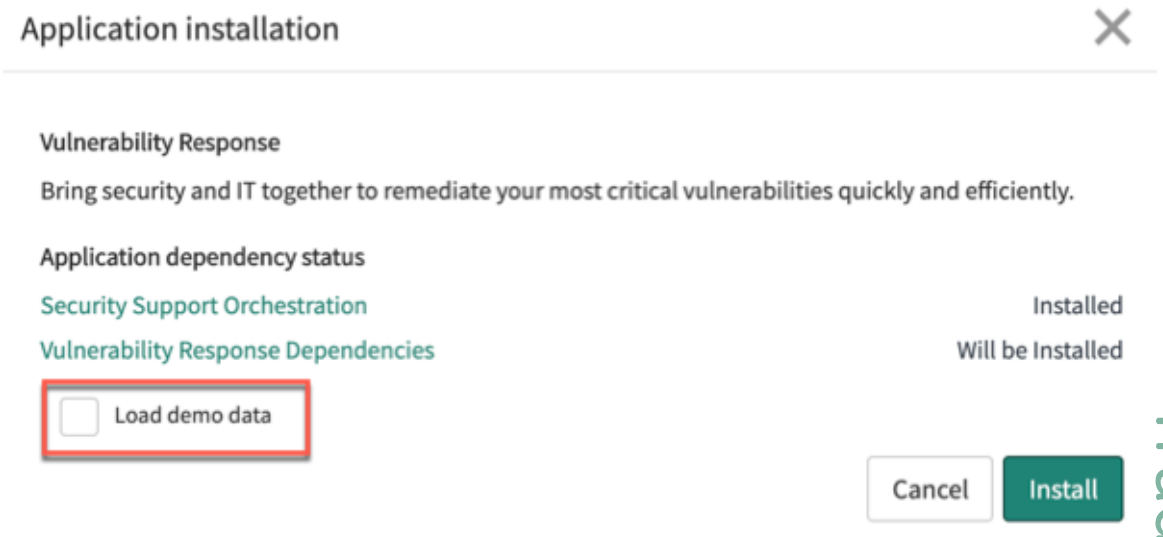
12. Nas aplicações listadas, localize a aplicação de resposta a vulnerabilidades (sn_vul), selecione uma versão na lista de seleção e clique em **Instalar** .
A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas serão exibidas.

13. **Opcional:** Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar** .

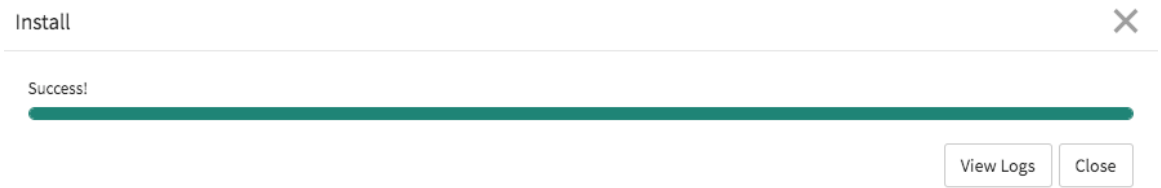
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você não selecionar **Carregar dados de demonstração** os dados de demonstração não estão disponíveis para instalação do **Gerenciador de aplicações** mais tarde. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] artigo no Now Support Base de conhecimento.



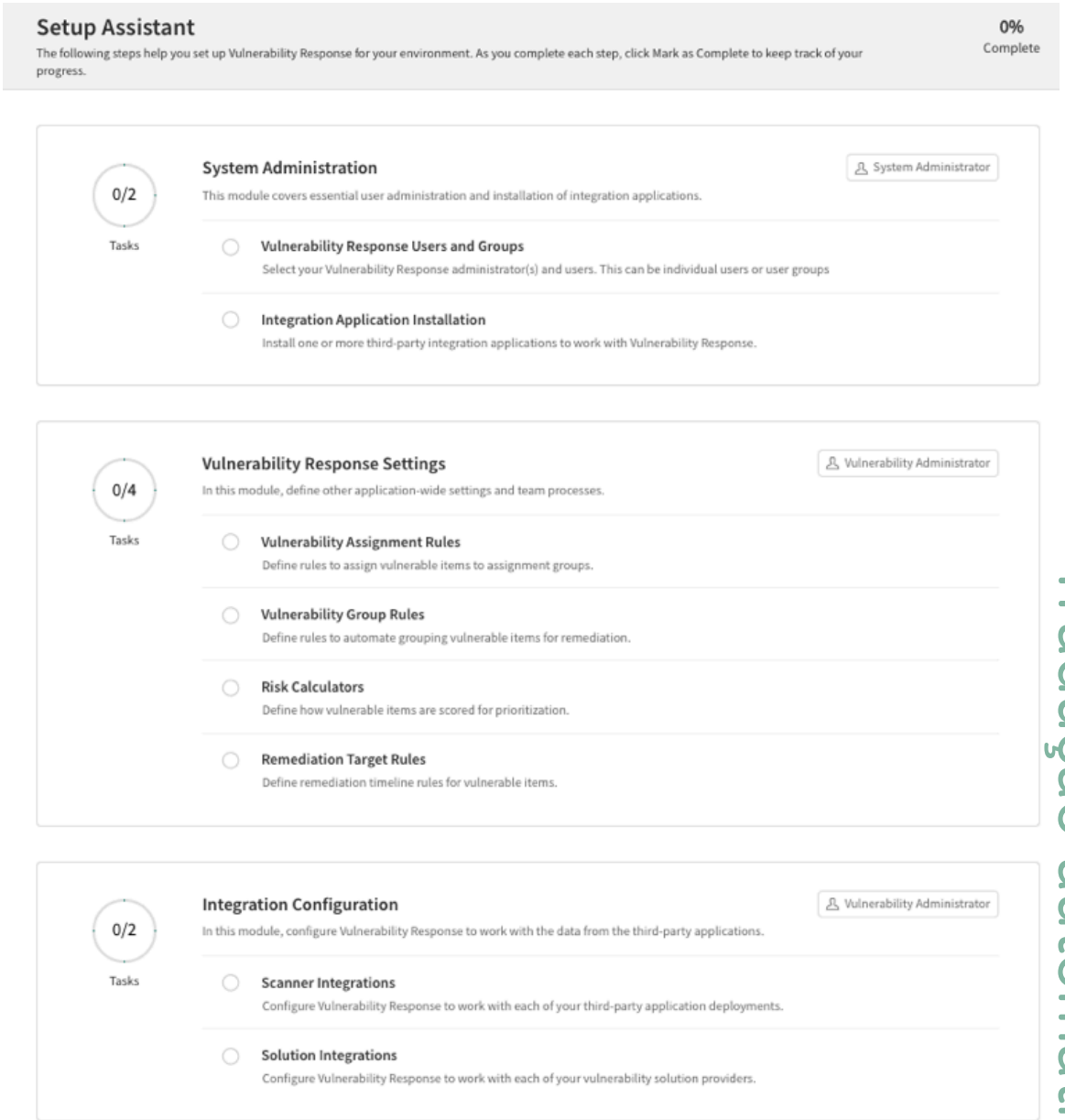
Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação é instalada com sucesso.



14. Clique em **Fechar**.
15. Após a conclusão bem-sucedida da instalação, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

16. Siga as instruções nos formulários em cada seção.

O que Fazer Depois

Para obter mais informações sobre Resposta a vulnerabilidades configurações, instalação de aplicações, configuração, integrações, regras de grupo, calculadoras de risco e regras de destino de correção, consulte Configurando Resposta a vulnerabilidades Usando o Assistente de configuração.

Componentes instalados com Resposta a vulnerabilidades

Vários tipos de componentes são instalados com a ativação do Resposta a vulnerabilidades aplicação, incluindo tabelas, funções de usuário e trabalhos agendados.

Exibir listas filtradas de componentes instalados com uma aplicação

A partir da v24.0.6 de Resposta a vulnerabilidades, as propriedades do sistema usadas com mais frequência agora estão acessíveis em Resposta a vulnerabilidades aplicação. Para exibir essas propriedades do sistema, navegue até **Tudo**Resposta a vulnerabilidades**Propriedades**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtre a tabela Arquivos de aplicações para que somente as funções, trabalhos agendados e tabelas instaladas com uma aplicação sejam exibidas. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o Construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **E.** e, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função** , **Trabalho agendado** ou **Tabela** .
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Nota: Trabalhos agendados e Tabelas para Resposta a vulnerabilidades de aplicações pode ser encontrado em Componentes instalados com Resposta a vulnerabilidades de aplicações.

Título da função [name]	Descrição	Contém as funções
sn_vul_prisma.configure_prisma_integration	Protege as operações CRUD e report_view na tabela sn_vul_prisma_hosts_import e a operação report_view na tabela sn_vul_prisma_host_attrb.	
sn_vul.view_manager_workspace	Exibições Espaço do gerente de vulnerabilidade.	
sn_vul.delete	Exclui registros de origem e itens vulneráveis. Antes da v23.0, a função de administrador tinha o privilégio de excluir os registros de origem.	• sn_vul_cmn.delete • sn_vul.delete_vulnerable_items
sn_vul_cmn.delete	Exclui registros de origem.	
sn_vulc.bulk_edit	Executa a operação de edição em massa nos resultados do teste.	
sn_vul.app_bulk_edit	Executa a operação de edição em massa em itens vulneráveis à aplicação (AVITs).	sn_vul.app_write_all
sn_vul_container.container_bulk_edit	Executa a operação de edição em massa em itens vulneráveis ao contêiner (CVITs).	sn_vul_container.write_all
sn_vul_cisa.configure_intelligence_integration	Configura integrações do Intelligence.	
Gerentes de vulnerabilidades e analistas sênior	Atualize propriedades e integrações de vulnerabilidade. A função sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)	• sn_vul.vulnerability_write • sn_vul.ciso_write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
[sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)]	é necessária para Resposta a vulnerabilidades administração, incluindo integrações de vulnerabilidades, regras de tarefa de correção, calculadoras e regras e tarefas de destino de correção, relatórios e configuração de integração de terceiros.	• sn_sec_cmn.admin • sn_vul_qualys.admin (Quando a Integração de vulnerabilidades da Qualys está instalada.) • sn_vul_r7.admin (Quando a Integração de vulnerabilidades do Rapid7 está instalada.) • sn_vul_shodan.admin (Quando a integração Shodan Exploit está instalada.) • sn_vul.configure_ntd_integration (Quando as integrações NVD estã instaladas.) • Treemap_admin (Quando a aplicaç Performance Analytics está instalada.)
Orquestração de patches	Configura integrações de fornecedores de patches de terceiros compatíveis. Exibir e aplicar dados de patch e registros de patch.	• sn_vul_patch_orch.configure_patc Configurar e aplicar patches. • sn_vul_patch_orch.read_patch Pode exibir registros e dados de patch. • sn_vul_bigfix.configure_integration Configura a aplicação BigFix Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_bigfix.read_integration e connection_admin que permitem o o usuário se conecte ao console d BigFix. • sn_vul_sccm.configure_integration Esta função contém as funções granulares sn_vul_sccm.read_integration e connection_admin que permitem o o usuário se conecte ao console d SCCM. • sn_vul_bigfix.read_integration Os usuários com esta função pode exibir (somente leitura) os#registr da aplicação Vulnerability Respons e BigFix Patch Orchestration

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
		Integration e os dados de orquestração de patches. • sn_vul_sccm.read_integration Os usuários com esta função pode exibir (somente leitura) os#registr do Vulnerability Response e o aplicativo Microsoft SCCM Patch Orchestration Integration e os dad de orquestração de patches.
Analistas de vulnerabilidades [sn_vul.vulnerability_write]	A função sn_vul.vulnerability_write é necessária para gerenciar tarefas de correção e itens vulneráveis e monitorar o andamento da correção.	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (Quando a Integração de vulnerabilidades da Qualys está instalada.) • sn_vul_shodan.write (Quando a integração Shodan Exploit está instalada.)
V19.0: Gerenciador de eventos de vulnerabilidade [sn_vul_analyst.vul_event_manager]	A função sn_vul_analyst.vul_event_manager é usada para avaliar o impacto de uma nova vulnerabilidade ou software ou adicionar uma vulnerabilidade de dia zero para identificar os ativos afetados e criar itens vulneráveis (VIS).	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emergency_respons • sn_vul.manage_exposure_assessm
Outros [sn_vul.read_all] A função sn_vul.vulnerability_read foi descontinuada.	. sn_vul.read_all a função é necessária para qualquer pessoa que precise de visibilidade sobre a gestão de vulnerabilidades. Por exemplo, executivos DE TI e segurança ou alguém que deseja detalhar os painéis de alto nível até os itens que compõem os visuais do painel. **Importante:** A partir da v24.0.6 de Resposta a vulnerabilidades, a função sn_vul.read_all tem o privilégio de acessar o. Espaço do gerente de vulnerabilidade.	• sn_sec_cmn.read • sn_vul_qualys.read (quando a Integração de vulnerabilidades da Qualys está instalada. • sn_vul_shodan.read (Quando a integração Shodan Exploit está instalada.) • pa_viewer (Quando a aplicação Performance Analytics está instalada.) • sn_vul_Tenable.read_integration (Quando a Integração de vulnerabilidades do Tenable está instalada.) • sn_vul.view_manager_workspace
sn_vul.read_assigned	Exiba itens vulneráveis atribuídos a você ou aos seus grupos de	sn_vul.view_rem_workspace

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
	atribuição na IU clássica e na Espaço de correção de problemas de TI. **Importante:** A partir da v24.0.6 de Resposta a vulnerabilidades, a função sn_vul.read_assigned tem o privilégio de acessar o. Espaço de correção de problemas de TI.	
Administrador de importação do sistema de VR [sn_vul.vr_import_admin]	Executado como usuário do sistema. Executa trabalhos agendados. **Nota:** Este usuário é o usuário de execução padrão para cada registro de integração. Não mude.	• import_admin • sn_vul.vulnerability_write
Responsável pela correção [sn_vul.remediation_owner]	Exiba e atualize permissões para itens vulneráveis, tarefas de correção atribuídas a você ou ao seu grupo. Pode exibir todas as vulnerabilidades e soluções. Tem acesso de gravação ao **Campo Anotações internas** no registro de solução.	Contido na função itil.
CISOs e executivos de vulnerabilidade [sn_vul.vulnerability_ciso]	Exiba o painel do CISO no Performance Analytics for Vulnerability Response.	• sn_vul.ciso_read • sn_vul.read_all
Aprovador de falso-positivo [sn_vul.false_positive_approver]	Aprova/rejeita solicitações de falso positivo.	sn_vul.view_manager_workspace
Aprovador de exceção [sn_vul.exception_approver]	Aprova/rejeita solicitações de exceção.	sn_vul.view_manager_workspace

Trabalhos agendados instalados

Trabalho agendado	Descrição
Preencha os filtros salvos OOTB para o módulo Host e App	Migra módulos relacionados ao módulo Host e App.
Preencha os filtros salvos OOTB para o módulo CC	Migra módulos relacionados ao módulo CC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Preencha os filtros salvos OOTB para o módulo de contêiner	Migra módulos relacionados ao módulo de contêiner.
Atualizar filtros salvos relacionados ao host	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo Host.
Atualizar filtros salvos relacionados ao CC	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo CC.
Atualizar filtros salvos relacionados ao contêiner	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo de contêiner.
Atualizar filtros salvos relacionados ao app	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo App.
Criação e execução de agregação do gatilho para filtro salvo	Cria, atualiza, executa e atualiza as agregações relacionadas ao filtro salvo.
Versão 19,0 do Vulnerability Response e v4.0 do Veracode Vulnerability Integration	A integração do Veracode CWE recupera Veracode- Dados de enumeração de pontos fracos comuns (CWE) específicos para informações de ameaças e recomendações de correção. A integração do Veracode SBOM ingere informações de versão, versão e vulnerabilidade originadas em Veracode sobre os componentes em seus projetos de software. A integração gera SBOMs no formato JSON CycloneDx e os carrega em sua instância Veracode Categories Integration recupera dados aprimorados de Categorias do Veracode. . Veracode A integração DevOps permite que os usuários do DevOps exibam detalhes resumidos de verificações de vulnerabilidade de terceiros sem uma licença SecOps. APIs baseadas em JSON para as seguintes integrações do Veracode: Item vulnerável da aplicação, Resumo da verificação, Lista de aplicações. As versões de API baseadas em XML dessas integrações foram descontinuadas.
Associe o VIS existente à regra de exceção automática	Associa automaticamente a Regra de exceção automática ao VIS existente.
Fechar detecções vulneráveis automaticamente	Fecha automaticamente as detecções vulneráveis obsoletas com base na configuração definida na tabela "sn_vul_auto_close_config".
Versão 16,1: Integrações DO HCL BigFix	Gerencie patches e implantações de patches para vulnerabilidades com patches do produto HCL BigFix.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Collection, Fixlet e Ações.	
Calcular contagens relacionadas para todas as soluções	Inativo por padrão. Processa dados de soluções uma vez à noite, em vez de continuamente. A partir da v22.0, você pode executar este trabalho somente sob demanda. Como este trabalho agendado processa todas as soluções, ele pode afetar o desempenho. Portanto, é recomendável executar este trabalho somente uma vez se os dados da solução estiverem corrompidos.
Calcular contagens de VI relacionadas para a tarefa de vulnerabilidade e correção	Captura mudanças de importação manuais e de VI do dia. Reconcilia relacionamentos de vulnerabilidade e solução e recalcula os totais. Os dados de soluções são enfileirados e processados separadamente pelo **Fila de métricas da solução de vulnerabilidade do processo** trabalho agendado.
Verifique Tempo limite do Mid-Server	Executa ping no MID Server e emite erros após 30 segundos.
V19.0: Verifique a possível exposição a vulnerabilidades	Processa os delta CVEs, o software e as instalações para obter a exposição.
Estado de execução WaitComplete	Marca uma execução de integração como concluída depois que ela é verificada como concluída.
Verifique a expiração do adiamento de itens vulneráveis e grupos	Envia notificações se itens vulneráveis ou vulnerabilidades expirarem (e se expirarem em uma semana). Verifica se alguma regra de exceção é aplicável em um VI adiado e atualiza o. **Motivo** e. **Até** campos de acordo com a regra de exceção. O estado do VI permanece adiado até a data de vencimento mais recente.
Cancelar Vits que não têm um IC associado	Fecha automaticamente itens vulneráveis que não têm um item de configuração (IC) associado e não foram atualizados por três dias. O estado é definido como Encerrado/Cancelado.
Fechar VI na exclusão de registro exp	Fecha uma VI quando ela é excluída.
Integração de resultados de conformidade	Importa resultados de teste junto com políticas, testes de configuração (controles) e citações com fontes autorizadas para processamento na aplicação Conformidade de configuração.
Integração de preenchimento de resultados de conformidade	Execução de uma integração encadeada com Tenable.io Integração de ativos, importa dados de avaliação de configuração para ativos ignorados que são descobertos (importados por meio da integração de ativos).
Sincronização do estado CR	O script atualiza todas as tarefas de correção existentes para relacionamentos CHG para que sejam sincronizados. Habilita a sincronização daqui para frente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Integração de credencial de verificação da versão 15,0	Importa e armazena com segurança temporariamente Tenable.io credenciais usadas para acessar o scanner para novas varreduras sob demanda.
Integração abrangente do CWE 2000	Integração de vulnerabilidades que extrai informações de vulnerabilidade do conjunto de dados de enumeração de pontos fracos comuns (CWE), com curadoria da MITRE Corporation.
V18.0: Excluir registros de ação de divisão obsoletos	Trabalho diário para limpar registros obsoletos em tabelas intermediárias de tarefa dividida.
Desabilite as soluções de VR quando a aplicação de soluções não estiver ativa	Desabilita e oculta o. Solução de gestão de vulnerabilidade recurso quando Solução de gestão de Resposta a vulnerabilidades a aplicação não está instalada.
Avalie os destinos de correção	Define ou atualiza datas de destino de correção em todos os itens vulneráveis. Determina o status das datas de destino de correção em relação às regras.
• Corrigindo as detecções de chave atualizada para Rapid7 • Corrigindo as detecções de chave atualizada para a Qualys • Corrigindo as detecções de chave atualizada para Tenable	Limpa os dados de detecção automaticamente por um trabalho agendado específico da integração que é acionado após o upgrade para Resposta a vulnerabilidades.
Versão 16,1: Gerar resumo de correção	Este trabalho gera automaticamente um resumo de e-mail para todos os usuários no grupo de usuários Proprietário da correção. O trabalho é ativado por padrão.
V19.0: Insira CVE explorado da CISA na configuração de exposição	Insere CVEs da CISA na tabela Configuração de exposição para calcular a exposição.
V18.0: Insira tarefas de correção clássicas na tarefa de correção unificada	Trabalho agendado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).
Integração da solução do Microsoft Security Response Center	Solução de gestão de vulnerabilidade integração que recupera soluções do Microsoft Security Response Center.
Microsoft SCCM Collection, atualização de patch e integrações de implantações 16,1	Gerencie patches e implantações de patches para vulnerabilidades com Microsoft Patches do SCCM.
Escolha o processo de integração limitada	Cria o processo de integração para Integração com Shodan Exploits.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Preencha o texto Produtos afetados	Após o upgrade, lida com soluções existentes para preencher o texto de produtos afetados. Este trabalho é executado uma vez.
Preencha a nova coluna Contagem de CR	Preenche automaticamente a nova coluna de contagem de CR para clientes com dados existentes na tabela Tarefa de correção [sn_vul_vulnerability].
Fila de métricas da solução de vulnerabilidade do processo	Processa os dados de soluções enfileiradas por: • Acúmulo de soluções de entradas de NVD para entradas de terceiros • Preenchimento de soluções preferenciais em vulnerabilidades, e. • Atualizando as métricas de status de correção nas soluções Além disso, ele também processa as soluções marcadas para status de atualização. **Nota:** Somente se você estiver usando Rapid7, você pode desabilitar este trabalho de programação para melhorar o desempenho.
Preencha registros na tabela de mapeamento de fornecedor de vulnerabilidade Preencha registros na tabela de mapeamento de fornecedor de vulnerabilidades para vulnerabilidades do Rapid7	Insere registros na tabela de mapeamento de fornecedor de vulnerabilidades para vulnerabilidades existentes.
Reabra grupos de vulnerabilidades adiados	Reabre adiado tarefas de correção quando a data de adiamento tiver passado.
Reaplique todas as regras de atribuição de vulnerabilidade	Reavalia as regras de atribuição em relação a todos **Aberto** VIS.
Versão 16,5: Contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de tarefas de VIS e correção que não estão atribuídas por este recurso para uma regra de atribuição específica.
Red Hat Solution Integration	Solução de gestão de vulnerabilidade integração que recupera soluções do Red Hat Security Advisory.
V17.1: Atualizar e resolver Vits duplicados na tarefa de correção	Encontra itens vulneráveis duplicados para os itens na tarefa de correção com "Atualizar automaticamente VIS duplicados" como ativo.
Atualizar itens vulneráveis associados para tarefa de correção	Atualiza a tarefa de correção com itens vulneráveis correspondentes aos critérios Grupo de filtros e Grupos de condições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
não baseada em regra de tarefa de correção	
Reparar itens vulneráveis incorretos abertos e encerrados pela última vez	Repara dados de IU existentes corrompidos por defeitos corrigidos anteriormente.
Executar calculadoras novamente	Reaplica as calculadoras a todos os itens vulneráveis afetados pela mudança. Aciona um recálculo das pontuações de risco cumulativas do tarefa de correção s. **Nota:** A repetição das calculadoras pode levar muito tempo, dependendo do seu ambiente.
Conjuntos de importação de integração cancelados novamente	Tenta novamente conjuntos de importação de integração cancelados. Novas tentativas 5 vezes antes de retornar um erro.
Processos de integração de novas tentativas	Tenta novamente os processos de integração. Novas tentativas 5 vezes antes de retornar um erro.
Acumule valores de item vulnerável para vulnerabilidade e grupo	Calcula a pontuação de risco, o número de itens vulneráveis e o status de destino de correção para tarefas de correção usando a calculadora de acúmulo. **Nota:** A partir da v23.0 de Resposta a vulnerabilidades, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de multithreading. Este upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.
Execute a calculadora de gravidade após a promoção de entrada de vuln	Executa a calculadora de gravidade depois que uma vulnerabilidade ausente anteriormente é atualizada com sua pontuação e outros dados de um provedor de terceiros, como Qualys Cloud Platform, Rapid7 Nexpose. **Nota:** A partir da v25.0.3 de Resposta a vulnerabilidades, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de multithreading. Este upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.
V19.0: Executar avaliação de exposição para CVEs configurados	Calcula a exposição para todos os registros CVE na tabela Configuração de exposição.
V19.0: Executar exposição de software	Calcula a exposição para todos os registros de software na tabela Configuração de exposição.
Processador da fonte de dados de vulnerabilidade programada	Verifica a fila de importação em busca de entradas a serem processadas e atribui um trabalho de importação programado com base nos recursos disponíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Limpeza programada do anexo do processo de integração de vulnerabilidades	Remove anexos XML de integração quando eles completarem 14 dias. Este tempo de retenção não é configurável.
Verificador de tempo limite programado da Integração de vulnerabilidades	Cancela execuções de integração que levam mais de 60 minutos para serem concluídas.
Definir serviços de IC relacionados para VI	Quando a importação da integração é concluída, ela vincula os serviços de negócio afetados a ICs conectados a itens vulneráveis, no horário especificado. Para obter mais informações, consulte Mapeamento de serviços no Resposta a vulnerabilidades.
Definir contagens de adiamentos	Coleta o número de vezes que um item vulnerável, um item vulnerável à aplicação, um item vulnerável ao contêiner ou uma tarefa de correção é adiada.
Acionar a próxima integração	Aciona a próxima integração em uma execução de integração encadeada.
Integração de modelo	Um único registro de modelo é enviado para Tenable.io durante uma nova verificação.
Atualizar itens vulneráveis não agrupados	Determina se um item vulnerável está em um r tarefa de ediação e adiciona ou remove do **Itens vulneráveis não agrupados** lista. **Nota:** Este trabalho é executado após o upgrade e, dependendo do seu conjunto de dados, pode levar muito tempo para ser concluído.
Atualizar vulnerabilidade no VG	Atualiza o. **Vulnerabilidade** Campo na tabela Tarefa de correção (sn_vul_vulnerabilty) após o upgrade. Este trabalho é acionado uma vez e inativo posteriormente.
Modelo de importação de vulnerabilidades	Mecanismo que processa a fila de importação. Um de 10.
Atualização encerrada da idade de resposta a vulnerabilidades	Atualiza a coluna Idade fechada na tabela VI.
Contagem de IC de resposta a vulnerabilidades	Calcula o número de ICs verificados por leitores de terceiros nos últimos 30 dias.
Upgrade de status de correção e risco de resposta a vulnerabilidades	Atualiza a classificação de risco nos dados quando você faz upgrade.
V20.0: Verificar expiração da mitigação de risco	Verifica se os controles compensatórios expiraram para um item vulnerável e tarefa de correção. Se expirarem, ele reverterá a pontuação de risco para a pontuação de risco original e enviará uma notificação por e-mail indicando que os controles compensatórios expiraram. Também envia uma notificação por e-mail se os controles compensatórios estiverem definidos para expirar em 7 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
v24.0.6 Importação de hosts Prisma [sn_vul_prisma_hosts_import]	Tabela do conjunto de importação para os hosts.
v24.0.6 Atributos do host Prisma [sn_vul_prisma_host_attrb]	Tabela de atributos de ativo para integração de hosts.
v2.0 sn_vul_cmn_auto_close_rule	Fecha detecções obsoletas automaticamente com base nas condições do filtro.
sn_vul_cmn_ws_saved_filter	Armazena os dados do filtro salvo.
sn_vul_licensing_usage	Contém o ativo duplicado, Ativo de IP incompleto, Contagens totais de ativos do scanner e Uso final.
sn_vul_m2m_entry_compensing_control	Representa a associação entre entradas de vulnerabilidade e controles de compensação.
v21.0 Mecanismo de verificação Rapid7 [sn_vul_r7_scan_engine)	Armazene os registros importados dos dados do Mecanismo de verificação responsáveis por descobrir ativos durante uma verificação e verificar se há vulnerabilidades.
v21.0 Importação do mecanismo de verificação do Rapid7 [sn_vul_r7_scan_engine_import]	Usado pela integração do Mecanismo de verificação do Rapid7 para preparar dados de importação antes do processamento.
Versão 19,0: [sn_vul_veracode_cwe_import]	Estende a tabela Categoria Veracode para recomendações de correção de CWE.
Versão 19,0: [sn_vul_veracode_category_import]	Armazena dados de categoria importados.
Versão 19,0: [sn_vul_veracode_sbom_import]	Armazena dados SBOM importados originados da Veracode.
V17.1: Adicione prova à chave VI [sn_vul_proof_key_vulnerability]	Vulnerabilidades do Rapid7 para as quais a prova deve ser incluída na chave VI. A partir da v24.0.6 de Resposta a vulnerabilidades Uma coluna "Expressão regular para dividir Vits do Tenable" é adicionada. Ele armazena a expressão regular inserida por um usuário que é usada para analisar a prova da carga.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Itens vulneráveis avaliados [sn_vul_m2m_exp_sw_vi]	Atribui uma tarefa de correção a um grupo de atribuição durante a criação da tarefa de correção.
Regra de atribuição [sn_vul_vgr_assignment_rule]	Atribui uma tarefa de correção a um grupo de atribuição durante a criação da tarefa de correção. Anterior à v15.0: Atribui um tarefa de correção para um grupo de atribuição durante tarefa de correção criação.
Associar Solicitação de Mudança [sn_vul_action_associate_cr]	Tabela de preparação usada para processar novas associações de tarefa de correção-CHG. Anterior à v15.0: Tabela de preparação usada para processar novas associações VG-CHG.
Trabalho de Item Vulnerável Assíncrono [sn_vul_async_vi_job]	Contém trabalhos em segundo plano que processam itens vulneráveis. Somente um tipo de trabalho é compatível; usado para editar vulnerabilidades em massa.
Tipo de trabalho de item vulnerável assíncrono [sn_vul_async_vi_job_type]	Contém os tipos de trabalhos em segundo plano e faz referência ao script relevante. Tem apenas um processador, o. **VulnerabilityBulkEditProcessor**
Encerrar automaticamente detecções obsoletas [sn_vul_auto_close_config]	Armazena a configuração de como as detecções obsoletas são encerradas automaticamente.
Configurar granularidade de item vulnerável [sn_vul_action_vi_granulity_config]	Armazena o formulário de IU usado para habilitar ou desabilitar Incluir porta na página de configuração no módulo Configurar granularidade do VI.
Criar solicitação de mudança [sn_vul_action_create_cr]	Usado para criar solicitações de mudança a partir da tarefa de correção.
Criar Itens vulneráveis [sn_vul_action_create_vi]	Uma tabela de preparação que é usada como um espaço reservado para informações. Esta tabela não armazena registros.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
CWE	Catálogo de vulnerabilidades de software de fraqueza comum e enumeração (CWE).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_cwe]	
Plataforma aplicável do CWE [sn_vul_cwe_m2m_cwe_platform]	Contém os dados da plataforma aplicáveis do CWE importados.
Categoria CWE [sn_vul_cwe_category]	Contém os dados da categoria CWE importados.
Consequência CWE comum [sn_vul_cwe_consquence]	Contém os dados de consequência comum do CWE importados.
Referência externa do CWE [sn_vul_cwe_reference]	Contém os dados de referência externa do CWE importados.
Exemplo observado do CWE [sn_vul_m2m_cwe_cve]	Contém os dados CVE do CWE importados.
Plataforma do CWE [sn_vul_cwe_platform]	Contém os dados importados da plataforma CWE.
Referência externa do CWE [sn_vul_cwe_reference]	Contém os dados de referência externa relacionados ao CWE importados.
Relacionamento do CWE [sn_vul_m2m_cwe_relation]	Contém os dados de relacionamento do CWE importados.
Exibição do CWE [sn_vul_cwe_view]	Contém os dados de exibição do CWE importados.
Ponto fraco do CWE [sn_vul_cwe_weakness]	Contém os dados de pontos fracos do CWE importados.
Versão 16,1: Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Versão 16,1: Atualização do dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Correspondência de software vulnerável do modelo de descoberta [sn_vul_discovery_model_software_match]	Complementa a correspondência de software vulnerável a um modelo de descoberta.
Configuração de gestão de exceções [sn_vul_exception_config]	Armazena as definições de configuração do recurso de gestão de exceções.
Regra de exceção [sn_vul_auto_exception_rule]	Contém o conjunto de regras avaliadas para a Gestão de exceções.
Explorar [sn_vul_exploit]	Contém as definições de explorações: Código publicamente disponível que aproveita uma vulnerabilidade.
Estrutura da Exploração sn_vul_exploit_framework	Contém os nomes das estruturas de exploração: Pacotes de software completos que são capazes de executar muitas explorações.
Modelos de descoberta expostos [sn_vul_m2m_exp_sw_model]	Armazena o mapeamento entre o modelo da Descoberta e Vulnerabilidade Avaliação de exposição.
Avaliação de Exposição [sn_vul_exp_by_sw]	Armazena os registros para avaliação de exposição.
V19.0: Manifesto de exposição sn_vul_analyst_exposure_manifest	Tabela de manifesto para processamento delta.
Entradas de Vulnerabilidade de Exposição [sn_vul_m2m_entry_exp]	Armazena o mapeamento entre Vulnerabilidade (sn_vul_entry) e Avaliação de exposição.
Kit de malware [sn_vul_malware_kit]	Contém os detalhes dos kits de malware: Ferramentas pré-escritas que facilitam a execução de uma exploração ou conjunto de explorações relacionadas sem fazer trabalho adicional de codificação ou configuração
Tabela de ativos ausente [sn_vul_tenable_missing_asset]	Contém IDs de ativos temporários para dados de avaliação de conformidade de configuração ignorados com ativos incompatíveis.
Atualização da Solução do Microsoft Response Center [sn_vul_msrc_update]	Contém a última vez em que os dados da solução foram atualizados pela Microsoft. Usado para comparar com a importação noturna para determinar os dados delta para download.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Microsoft Security Response Center Importação da solução [sn_vul_msrc_solution_import]	Usado pela integração da solução do Microsoft Security Response Center para preparar dados de importação antes do processamento.
Integração com a solução Microsoft Security Response Center [sn_vul_msrc_integration]	Estende a tabela Integração de vulnerabilidades [sn_vul_integration] para Integração com a solução Microsoft Security Response Center.
Entrada do Banco de Dados Nacional de Vulnerabilidades [sn_vul_nvd_entry]	Vulnerabilidade documentada do NIST National Vulnerability Database.
Importação de CVSS do NVD [sn_vul_nvd_cvss_import]	Contém dados de preparação que ainda não foram transformados para Resposta a vulnerabilidades Esquema durante a importação de NVD.
Versão 16,1 [sn_vul_patch_orch.patch_approval_required]	Quando as implantações de patch são programadas a partir de uma integração de patch, as solicitações são enviadas para revisão e aprovação aos usuários atribuídos ao grupo de aprovação de atualização de patch de nível 1. Esta propriedade é ativada por padrão.
Versão 16,1: Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre coleções e ICs.
Versão 16,1: Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Versão 16,1: Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.
V19.0: Possível exposição a vulnerabilidades sn_vul_analyst_m2m_pot_exp_sw_model	Tabela de avaliação de exposição para CVE.
Categoria do produto [sn_vul_product_category]	Contém os dados da categoria de produto importados.
Red Hat Security Advisory [sn_vul_rhsa_update]	Compara o. Red Hat soluções em relação ao trabalho noturno para determinar os dados delta para importação.
Red Hat Importações de solução [sn_vul_rh_solution_import]	Usado pelo Red Hat Solution Integration para preparar dados de importação antes do processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Red Hat Solution Integration [sn_vul_rh_integration]	Estende a tabela Integração de vulnerabilidades [sn_vul_integration] para Red Hat Solution Integration.
Serviços de negócio relacionados [sn_vul_m2m_ci_services]	Vincula ICs a Serviços de negócio para pesquisa de serviços afetados. Contém um sinalizador que indica se ele foi adicionado pelo Mapeamento de serviços.
V18.0: Contagens de esforços de correção [sn_vul_daily_count_re]	Contagem diária de esforços de correção. Esta tabela é atualizada diariamente.
V18.0: Registro de esforço de correção [sn_vul_remediation_effort_record]	Rastreia o andamento da correção dos esforços de correção (RE). Contém referências ao RES.
Regra de meta de correção [sn_vul_ttr_rule]	Define o intervalo de tempo esperado para corrigir um item vulnerável. Estende o arquivo da aplicação.
V18.0: Tarefa de correção [sn_vul_remediation_task]	Armazena todas as tarefas de correção para VR, AVR, CVR e grupos de resultados de teste. Consiste em informações relacionadas aos registros da tabela [sn_vul_vulnerability]. Os usuários que não podem exibir registros na exibição de lista da tabela [sn_vul_vulnerability] podem ver essas informações de registros na exibição de lista da tabela [sn_vul_remediation_task]. Esta tabela pode ser acessada pelos usuários no Espaço do Gerenciador de vulnerabilidades ou no Espaço de correção de TI
Integração REST [sn_vul_rest_integration]	Estende a tabela Integração de vulnerabilidades [sn_vul_integration] para as integrações baseadas EM REST.
Detecção de vulnerabilidades DO SAM NVD [sn_vul_sam_config]	Contém quais ICs e vulnerabilidades são monitorados com SAM NVD e se a detecção de vulnerabilidade SAM NVD está habilitada ou não.
Pool de importação agendada [sn_vul_sched_import_pool]	Coleção de registros de conjuntos de importação programada usados para facilitar importações simultâneas de fontes de dados.
Selecione Item vulnerável [sn_vul_action_select_vi]	Tabela de preparação de base usada para lidar com divisão de VG, criar CHGs e associar CHGs
Status de configuração	Somente interno: Usado pelo Assistente de configuração. Sempre que o Assistente de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_setup_status]	configuração é aberto, ele mostra o status das etapas concluídas e a porcentagem no canto superior direito vem desta tabela.
Mapa de Gravidade [sn_vul_severity_map]	Contém os mapeamentos da severidade de origem para a severidade normalizada.
Mapeamento do Scanner de Solução [sn_vul_solution_scanner_mapping]	Mapeia fornecedor, scanner e palavras-chave para exclusão ou inclusão.
Dividir tarefa de correção [sn_vul_action_split_vg]	Tabela de preparação usada para dividir tarefas de correção .
Entrada de vulnerabilidade de terceiros [sn_vul_third_party_entry]	Vulnerabilidade documentada de uma origem de terceiros.
[sn_vul_tenable_io_template	Um registro de modelo é enviado para Tenable.io e importados durante a nova verificação para itens que têm Tenable.io como uma origem.
Atualizar manifesto [sn_vul_update_manifest]	Lista de tarefas de correção que foram atualizados e exigem recálculo pela calculadora de acúmulo.
V17.1: Uso por classes de IC [sn_vul_licensing_usage_by_ci_classes]	Contém a contagem de uso agregada pela classe de IC.
Contagem de Itens de Configuração de VR [sn_vul_vr_configuration_item_count]	Contém a média cumulativa contínua de 90 dias de itens de configuração importados de integrações de terceiros.
Regras de Atribuição da Vulnerabilidade [sn_vul_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição no VIS.
Calculadora de Vulnerabilidade [sn_vul_calculator_group]	Contém as regras da calculadora de vulnerabilidades. A ordem da calculadora determina qual calculadora é avaliada primeiro e, em cada calculadora, uma regra de calculadora, no máximo, é usada.
Regra da Calculadora de Vulnerabilidade [sn_vul_calculator]	Contém as regras para todas as calculadoras. Para cada calculadora, as regras da calculadora são revisadas em ordem. A primeira calculadora correspondente à condição usa os valores dessa regra.
CVEs de vulnerabilidade [sn_vul_m2m_entry_cve]	Vincula dados CVE (Common Vulnerability Exposures, exposições comuns a vulnerabilidades comuns) do NVD a entradas vulneráveis.
Entrada da Fila de Importação da Fonte de dados de Vulnerabilidade	Fila para anexos antes que eles sejam processados por uma fonte de dados. Utilizado por integrações de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_ds_import_q_entry]	
Entrada de Vulnerabilidade [sn_vul_entry]	Vulnerabilidade documentada.
Verificação de entrada de vulnerabilidade [sn_vul_entry_scan]	Armazena o relacionamento entre uma verificação e uma entrada de vulnerabilidade.
Estrutura de Exploração de Vulnerabilidade [sn_vul_m2m_framework_vul]	Contém o relacionamento entre estruturas de exploração e vulnerabilidades.
V19.0: Avaliação de exposição a vulnerabilidades sn_vul_analyst_sam_config	Tabela de configuração de avaliação de exposição para CVE.
Configuração de granularidade de vulnerabilidade [sn_vul_granulity_config]	Armazena e mantém o estado de Incluir ou Excluir Porta para o módulo Configurar granularidade do VI.
Tarefas de correção [sn_vul_vulnerability]	Coleção de itens vulneráveis organizados para correção.
Solicitações de Mudança de tarefa de correção [sn_vul_m2m_vg_change_request]	Armazena a associação de tarefas de correção e solicitações de CHG.
Itens da Tarefa de correção [sn_vul_m2m_vul_group_item]	Associação de tarefas de correção e itens vulneráveis.
Regras de tarefa de correção [sn_vul_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de itens vulneráveis.
Integração de Vulnerabilidade [sn_vul_integration]	Registro programável para importar dados de vulnerabilidade de uma fonte externa. Estende a execução programada de script.
Fonte de dados de integração de vulnerabilidade [sn_vul_int_data_src]	Fonte de dados a ser usada com uma integração de vulnerabilidade.
Log de Integração de Vulnerabilidades [sn_vul_integration_log]	Registra a saída de informações de log por execuções de integração de vulnerabilidade.
Processo de Integração de Vulnerabilidades	Ocorrência de processo único para uma integração de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_integration_process]	
Fila de Integração de Vulnerabilidade [sn_vul_integration_queue]	Enfileira as solicitações de importação para uma execução de integração quando todas as fontes de dados estão em uso.
Execução de integrações de vulnerabilidade [sn_vul_integration_run]	Invocações de integração de vulnerabilidades. **Nota:** Se uma execução de integração estiver em andamento, somente uma integração poderá estar no estado pronto no backlog.
Estatísticas de execução de integração de vulnerabilidade [sn_vul_integration_stats]	Armazena o detalhamento de cada etapa: Por exemplo, hora da REST API, hora de criação de VI e assim por diante para uma execução de integração
Tarefa de Item de Vulnerabilidade [sn_vul_m2m_item_task]	Itens vulneráveis associados a problemas, mudanças e incidentes de segurança.
Kit de Malware de Vulnerabilidade [sn_vul_m2m_malware_kit_vul]	Contém os relacionamentos entre vulnerabilidades e kits de malware.
Solução de pré-requisitos de vulnerabilidade [sn_vul_m2m_solution_prerequisite]	Contém os pré-requisitos específicos da origem para aplicar uma solução, quando disponíveis.
Limite da taxa de vulnerabilidade [sn_vul_rate_limit]	Define um limite de taxa a ser usado em um scanner.
Referência de Vulnerabilidade [sn_vul_reference]	Referências externas para vulnerabilidades conhecidas.
Status de Correção de Vulnerabilidade [sn_vul_m2m_ttr_status]	Status do item vulnerável em relação à regra de destino de correção aplicada mais próxima.
Regra do Risco de Vulnerabilidade [sn_vul_calc_risk]	Regra de calculadora especializada usada com as calculadoras de Pontuação de risco. Pondera quais valores, relacionados a um VI, serão usados para calcular a Pontuação de risco.
Calculadora de Rollup de Vulnerabilidade [sn_vul_rollup]	Lista de calculadoras de acúmulo de vulnerabilidades.
Verificação de vulnerabilidades [sn_vul_scan]	Verificação de vulnerabilidades. Contém o que verificar, com que scanner e um resumo dos resultados da verificação.
Item de configuração da Verificação de vulnerabilidades	Associa ICs do CMDB que estão enfileirados para serem verificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_m2m_scan_configuration_item]	
Entrada da fila de Verificação de vulnerabilidades [sn_vul_scan_q_entry]	Registro de verificação enfileirado para verificação ou processamento. Facilita as solicitações dentro dos limites de taxa estabelecidos.
Origem da Verificação de vulnerabilidades [sn_vul_m2m_scan_source]	Associa origens a um registro de verificação e significa todos os registros enfileirados para verificação.
Tarefa da Verificação de vulnerabilidades [sn_vul_m2m_scan_vulnerability]	Associa tarefas de vulnerabilidade às origens de um registro de verificação.
Verificador de vulnerabilidades [sn_vul_scanner]	Define scanners de terceiros a serem usados em verificações.
Limite de taxa do verificador de vulnerabilidades [sn_cmn_scanner_rate_limit]	Associa um scanner a um limite de taxa.
Software de Vulnerabilidade [sn_vul_m2m_entry_software]	Contém associações entre vulnerabilidades e software vulnerável.
Solução de Vulnerabilidade [sn_vul_solution]	Contém os dados de relacionamento entre a vulnerabilidade e as possíveis soluções para ela. A partir da v24.0.6 de Resposta a vulnerabilidades Uma nova coluna intitulada Boletim do scanner foi adicionada a esta tabela.
Solução de Vulnerabilidade [sn_vul_m2m_vulnerability_solution]	Vincula a tabela Entrada de vulnerabilidade (sn_vul_entry) à tabela Solução de vulnerabilidade (sn_vul_solution).
Aprovação de Mudança do Estado de Vulnerabilidade [sn_vul_change_approval]	Rastreia o processo de aprovação de vulnerabilidades.
Solução de Substituição de Vulnerabilidade [sn_vul_m2m_solution_suplantdence]	Contém o relacionamento específico da origem entre soluções.
Manifesto de Atualização de Vulnerabilidade [sn_vul_vuln_update]	Contém uma lista de vulnerabilidades que precisam que os dados de acúmulo sejam atualizados depois que os itens vulneráveis forem atualizados, encerrados ou tiverem mudanças na pontuação de risco.
Mapeamento de Fornecedor de Vulnerabilidade	Contém uma lista de vulnerabilidades e seus fornecedores.

Tradução automática

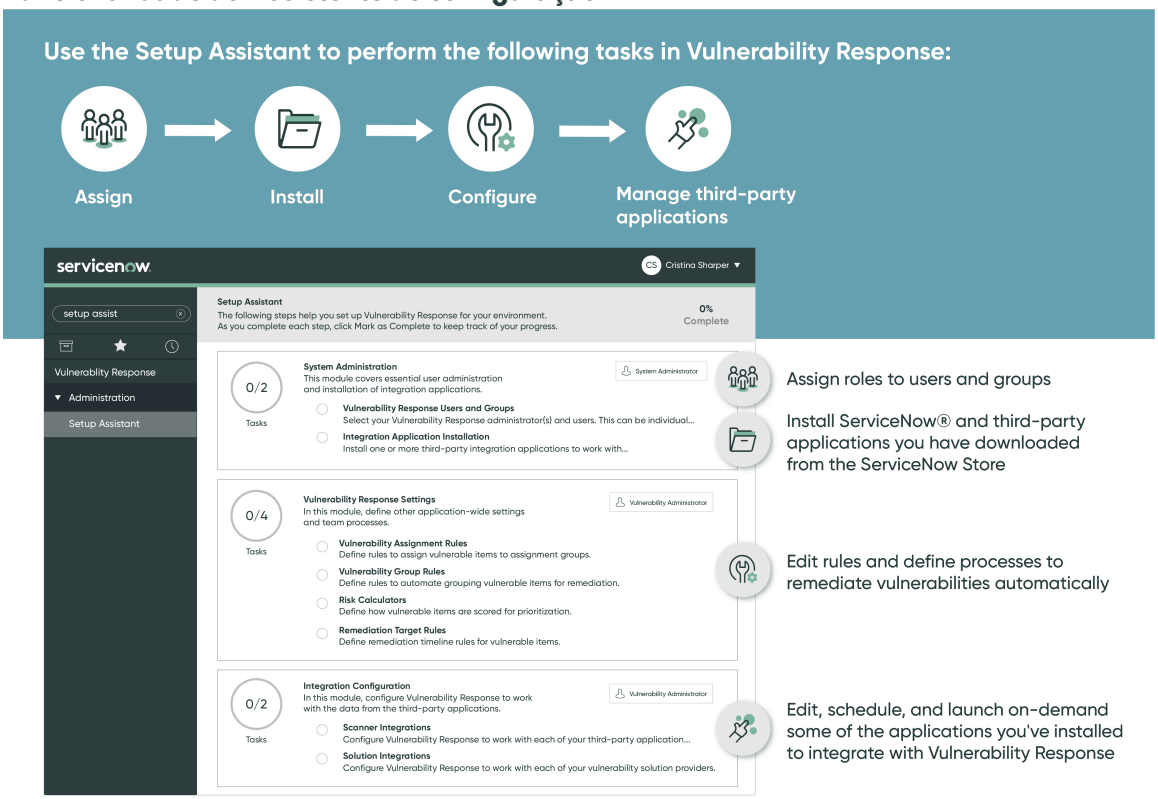
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sun_vul_vulnerability_vendor_mapping]	
Item vulnerável [sn_vul_vulnerable_item]	Contém a ocorrência de uma vulnerabilidade em um item de configuração.
Detecção de Item Vulnerável [sn_vul_detection]	Contém as detecções de item vulnerável de integrações de terceiros.
Software Vulnerável [sn_vul_software]	Software que é conhecido por ter determinadas vulnerabilidades.

Configurando Resposta a vulnerabilidades Usando o Assistente de configuração

O Assistente de configuração orienta você durante a configuração Resposta a vulnerabilidades e determinadas integrações de terceiros para seu ambiente. O Assistente de configuração fornece quase tudo o que você precisa para instalar e configurar seu ambiente para que você possa usar Resposta a vulnerabilidades.

Funcionalidade do Assistente de configuração



Now Platform® roles: admin and vulnerability admin

Usar o Assistente de configuração requer dois diferentes ServiceNow AI Platform® funções: administrador e administrador de vulnerabilidades.

Consulte as seções a seguir para complementar as instruções e avisos fornecidos no Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administração do sistema - Atribua usuários e grupos e instale aplicações de integração

Função necessária: administrador

Uma lista de usuários e integrações deve ser obtida no Gerenciador de vulnerabilidades antes de iniciar essas tarefas.

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.
2. Na primeira seção, Administração do sistema, o administrador atribui funções a usuários e grupos e instala integrações compatíveis.

   Atribuir Resposta a vulnerabilidades Personas e funções para usuários e grupos no Assistente de configuração.

   Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.
3. Atribua funções no Assistente de configuração.
   - Atribua a função de sn_vul.admin a usuários ou grupos.
   - Atribua a função sn_vul.admin para administração e configuração do Vulnerability Response, incluindo integrações de vulnerabilidades, regras de tarefa de correção, calculadoras e regras de tempo de correção.
   - Atribua a função sn_vul_vulnerability_write para a criação e atualização de tarefas de correção e itens vulneráveis.

     Nota: Todos os outros usuários recebem automaticamente acesso de gravação somente às tarefas de correção atribuídas a eles.

   - Atribua a função sn_vul_vulnerability_read para exibir tarefas de correção, itens vulneráveis e outras informações de vulnerabilidade.

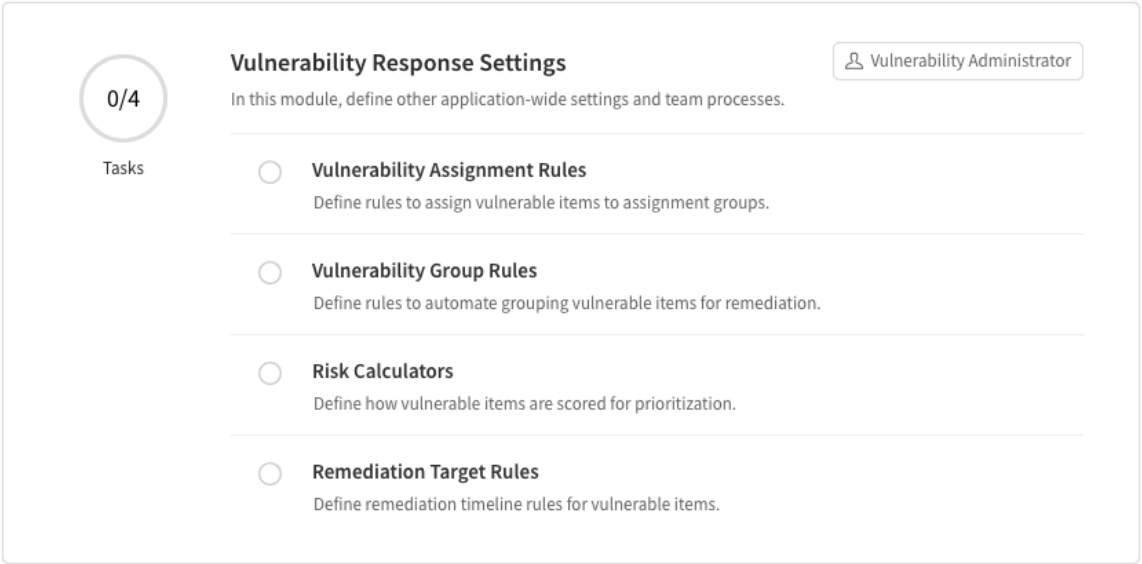
     Nota: Os usuários com a função itil recebem automaticamente a função sn_vul.remediation_owner, permitindo que eles vejam tarefas de correção e itens vulneráveis atribuídos a eles, entradas de vulnerabilidade e soluções no Resposta a vulnerabilidades em sua instância e no Mobile Agent aplicação. Nenhuma atribuição adicional é necessária.
4. Instale aplicações de integração de terceiros.
   - Consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis e. Integrações do Resposta a vulnerabilidades para obter mais informações sobre aplicações compatíveis com Resposta a vulnerabilidades.
   - Para obter mais informações sobre como usar o assistente de configuração para instalar aplicativos compatíveis, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

Resposta a vulnerabilidades Configurações

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Em Configurações de resposta a vulnerabilidades, o administrador de vulnerabilidades define as configurações de toda a aplicação e define regras para Resposta a vulnerabilidades. Como alternativa, o administrador pode executar essas tarefas.

1. Criar regras de atribuição de vulnerabilidade.

Crie regras que definem a atribuição automática de tarefas de correção para resolução. Pelo menos uma regra é enviada com o sistema de base. Para obter mais informações, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Nota:

O recurso Reaplicar requer uma aplicação de linha de base das regras. Depois que suas regras forem criadas, ative *`Reapply all vulnerability assignment rules`*trabalho programado para ser executado, conforme sua conveniência. Caso contrário, você será solicitado a reaplicar todas as regras a todos os VIS em aberto antes de alterá-las.

Quando o trabalho estiver concluído, defina **Executar** campo no trabalho agendado para se adequar ao seu ambiente. Dependendo do número de VIS ativos que você tem, avaliá-los e atualizá-los diariamente pode ter um impacto no desempenho não trivial. Para ambientes maiores, considere atualizar uma vez por semana ou até mesmo uma vez por mês.

Reaplicar regras de atribuição não reagrupa os itens vulneráveis.

2. Criar regras de tarefa de correção.

Crie regras que definem a criação automática de tarefas de correção para resolução. Pelo menos uma regra, **Vulnerabilidade,** é fornecido com o sistema de base. Você pode reaplicar as regras na exibição de formulário ou de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando uma regra de grupo é excluída, na exibição de formulário ou de lista, você tem a opção de excluir tudo **Aberto** grupos criados por essa regra. Grupos que não estão em **Aberto** os estados são excluídos.
- Consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros para obter mais informações sobre como criar regras para seu ambiente.
- Consulte Explorar o. Resposta a vulnerabilidades aplicação para obter mais informações sobre como usar Resposta a vulnerabilidades para corrigir vulnerabilidades.

3. Crie e habilite Calculadoras de risco.

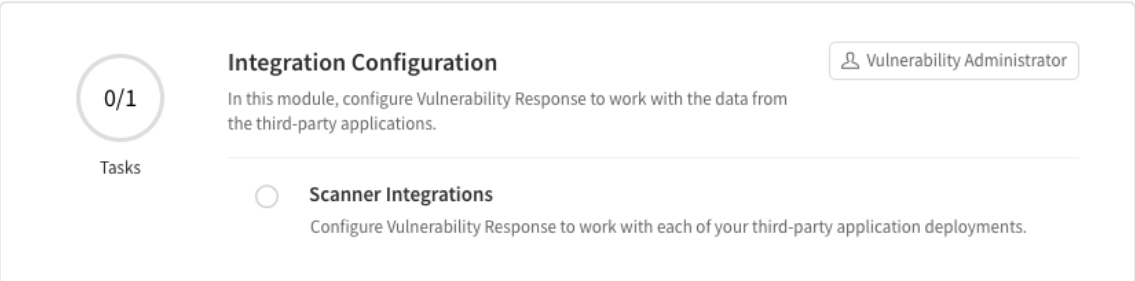
   Habilite calculadoras de risco que definem como os itens vulneráveis são pontuados para priorização. Várias calculadoras de risco são enviadas com o sistema de base. Consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade informações sobre como criar ou editar calculadoras de risco para seu ambiente.

4. Criar regras de destino de correção.

   Crie regras de destino de correção para categorias de correção. Pelo menos uma regra é enviada com o sistema de base. Consulte Resposta a vulnerabilidades regras de destino de correção para obter mais informações sobre como criar regras para seu ambiente.

Configuração de Integração

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin.



Na seção Configuração de integração, configure, programe, edite e inicie sob demanda as seguintes integrações de scanner de vulnerabilidades de terceiros e, se o Solução de gestão de Resposta a vulnerabilidades a aplicação está instalada, provedores de soluções.

- Consulte Configure o. Qualys Vulnerability Integration Usando o Assistente de configuração para obter mais informações sobre como configurar o. Qualys Vulnerability Integration.
- Configuração do Integração de Resposta a vulnerabilidades com Tenable a aplicação é compatível. Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração.
- Depois de instalar o. Solução de gestão de vulnerabilidade, o. **Integrações de soluções** a opção é exibida abaixo **Integrações do scanner** . Clique em **Integrações de soluções** Para configurar os provedores de solução de vulnerabilidade instalados nesta seção do Assistente de configuração. . Red Hat Solution Integration e. Integração com a solução Microsoft Security Response Center são compatíveis.

  Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre soluções instaladas. Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações sobre a instalação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade Usando o Assistente de configuração para obter mais informações sobre como configurar suas soluções instaladas.

- Se uma integração for de várias origens, você poderá ter várias implantações da mesma integração de terceiros.
- As configurações da integração de terceiros original são usadas como um modelo para as configurações de cada nova integração.

Nota: Se você excluir a integração de vulnerabilidade original, será necessário selecionar outra integração para usar como modelo. Desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância do Resposta a vulnerabilidades.

Nota: Integrações de várias vulnerabilidades para Rapid7 InsightVM Não estão disponíveis no Assistente de configuração. Consulte Crie importações separadas por domínio para uma integração para obter informações sobre como configurar e criar vários Rapid7 InsightVM integrações.

Tarefas adicionais

Consulte Adicional Resposta a vulnerabilidades tarefas de instalação e configuração Para obter mais informações sobre tarefas de configuração não incluídas no Assistente de configuração.

Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração

Atribua o. Resposta a vulnerabilidades Funções de persona para grupos ou usuários com o Assistente de configuração.

Antes de Iniciar

Se você já atribuiu funções de persona em Resposta a vulnerabilidades Usando o Assistente de configuração e quiser mais informações sobre como editar e gerenciar suas funções granulares e atribuições de função no módulo Administração de usuários, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para a aplicação Resposta a vulnerabilidades. Acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e as funções de responsável pela correção disponíveis nas versões anteriores de Resposta a vulnerabilidades não mudou.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver no Resposta a vulnerabilidades aplicação no nível da tarefa, você pode preferir usar funções de persona e granulares.

Se você ainda não atribuiu a função de persona sn_vul.vulnerability_admin usando o Assistente de configuração, siga as etapas abaixo para atribuí-la. Uma vez atribuído, o administrador de vulnerabilidades com esta função de persona tem permissão para concluir as tarefas do Assistente de configuração após a primeira seção e gerenciar regras e integrações de terceiros no Resposta a vulnerabilidades aplicação.

Para obter uma visão geral sobre funções de persona e funções granulares, consulte Resposta a vulnerabilidades personas e funções granulares.

Se você for um cliente de upgrade, use a tabela a seguir como referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição anterior	Atribuição recomendada [persona do usuário]	Descrição
sn_vul.admin	sn_vul.vulnerability_admin [Administrador de vulnerabilidades]	Fornece acesso completo à aplicação Resposta a vulnerabilidades (VR). Usuários com esta função configuram aplicações e regras de VR e instalam integrações de terceiros.
sn_vulnerability_write	sn_vul.vulnerability_analyst [Analista de vulnerabilidades]	Permite exibir e atualizar todos os registros para correção de VIT.
sn_vul.remediation_owner	sn_vul.remediation_owner [responsável pela correção]	Permite que usuários e grupos corrijam vulnerabilidades atribuídas a eles ou a seus grupos e atualizem os registros relacionados.
sn_vul.admin	sn_vul.ci [Gerenciador de IC]	Permite o gerenciamento de itens de configuração incompatíveis não encontrados no CMDB, incluindo a atualização de itens descobertos.
sn_vul.admin	sn_vul.exception_approver [aprovador de exceção]	Permite a aprovação de exceções, adiamentos e fechamentos de tarefas de correção e itens vulneráveis.
sn_vul.vulnerability_read	sn_vul.read_all ou sn_vul.read_group_rules	Concede acesso somente leitura a áreas específicas na aplicação. Use sn_vul.read_all para exibir todos os registros de VR ou sn_vul.read_group_rules para exibir as regras da tarefa de correção. Usuários com essas funções não podem atualizar registros. **Nota:** Várias outras funções de leitura estão disponíveis no Resposta a vulnerabilidades escopo para acesso mais granular.

Para exibir as funções granulares que um usuário ou grupos com uma função de persona herdam por padrão, navegue até **Tudo** > **Administração de Usuários** > **Funções**. Localize a função desejada e clique nela para abrir o registro. A guia Contém funções lista todas as funções granulares da função de persona, bem como todas as funções herdadas.

Você pode preferir verificar se todos os usuários e grupos necessários foram criados antes de atribuir funções no Assistente de configuração. Como alternativa, para adicionar novos usuários e grupos de dentro do Assistente de configuração, clique em **Módulo Administração de usuários** link no formulário mostrado na figura a seguir.

Para o exemplo a seguir, para limitar o acesso ao Resposta a vulnerabilidades este exemplo mostra como atribuir um usuário com a persona de administrador de

Tradução automática

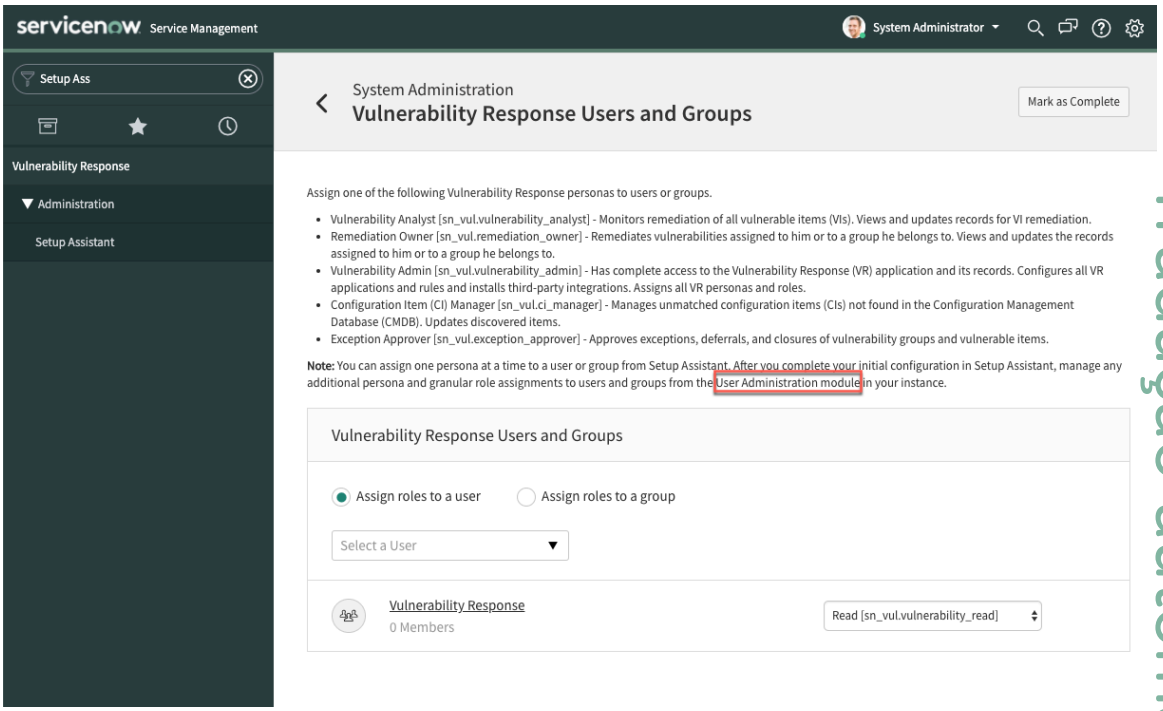
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidade. Normalmente, você pode preferir atribuir funções de persona diferentes de sn_vul.vulnerability_admin aos grupos.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração Assistente de configuração** .
   A página Assistente de configuração é exibida.
2. Clique em Usuários e grupos de resposta a vulnerabilidades.
   A página Usuários e grupos de resposta a vulnerabilidades da Administração do sistema é exibida.



3. Atribuir funções a um usuário selecionado, escolha um usuário existente na lista.

   Você só pode atribuir um usuário ou um grupo com uma função de persona.

   À direita do formulário, depois de selecionar um usuário ou grupo, a persona padrão, responsável pela correção [sn_vul.remediation_owner] é atribuída por padrão e permanece exibida na lista até que você a altere.

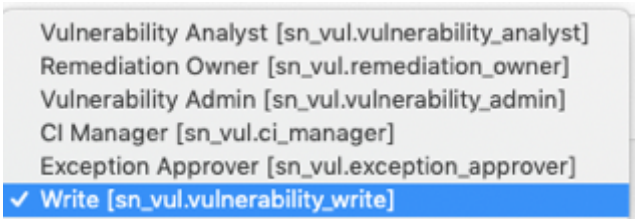
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você estiver atualizando para uma versão mais recente de Resposta a vulnerabilidades e você atribuiu anteriormente a função sn_vul.vulnerability_read ou sn_vul.vulnerability_write a um usuário ou grupo antes do upgrade, ela é exibida junto com as novas funções de persona, conforme mostrado na figura a seguir.

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para a aplicação Resposta a vulnerabilidades. O acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário da correção anteriores à 10.3 não foi alterado.

Observe que, para usuários existentes ou grupos atualmente atribuídos com as funções sn_vul.vulnerability_read ou sn_vul.vulnerability_write, essas funções são exibidas junto com as funções de persona na lista. Depois de atribuir uma função de persona, a função antiga não estará mais disponível no futuro. Por exemplo, como mostrado na figura a seguir, a função Write [sn_vul.vulnerability_write] não é mais exibida como uma opção para este usuário ou grupo depois que ele é atribuído a uma das funções de persona.

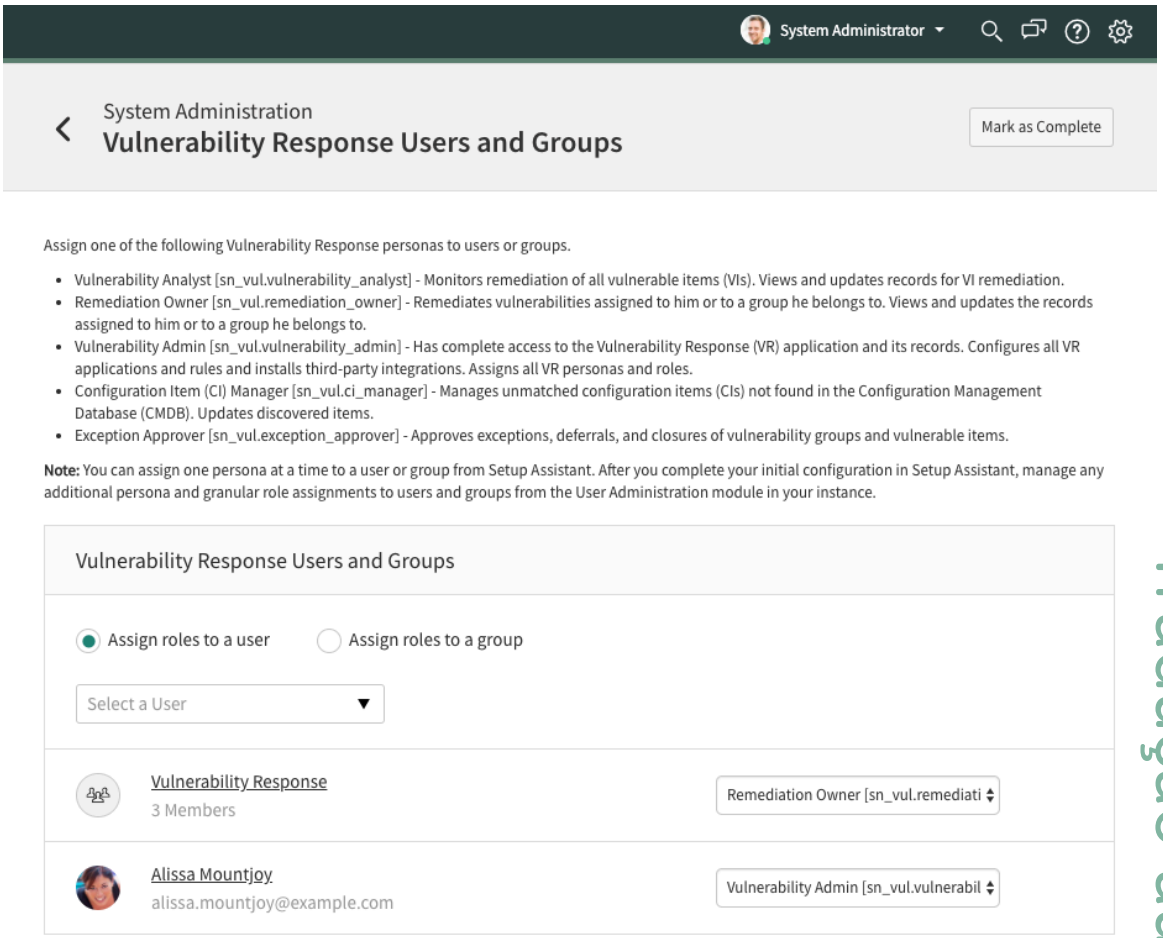


4. Na lista à direita do formulário, selecione **Administrador de vulnerabilidades [sn_vul.vulnerability_admin]** .
   É exibida uma mensagem indicando que o usuário ou grupo foi atribuído com sucesso à persona.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona do responsável de correção atribuída a um grupo e persona de administrador de vulnerabilidade atribuída a um usuário



5. Usando as descrições das funções de persona listadas acima, continue atribuindo todos os usuários e grupos às funções de persona restantes: Responsável pela correção, analista de vulnerabilidades, gerente de IC e aprovador de exceção.
   Você concluiu com sucesso a atribuição de funções de persona a usuários e grupos usando o Assistente de configuração.
6. **Opcional:** Para editar os usuários em um grupo do Assistente de configuração, siga estas etapas.

   a. Com o grupo exibido no formulário, clique no nome do grupo que você deseja editar.
   O registro do Grupo é exibido.

   b. Com a guia Membros do grupo selecionada, clique em **Editar** .
   O formulário Editar membros é exibido

   c. Use o slushbucket para selecionar ou remover usuários.

   d. Clique em **Salvar** Para salvar suas mudanças e retornar ao registro do grupo.

   e. Clique em **Atualização** Para retornar ao Assistente de configuração.

   f. Na página Assistente de configuração, clique em **Usuários e grupos de Resposta a vulnerabilidades** Para continuar com a configuração no Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Como administrador do sistema, continue com a configuração de Resposta a vulnerabilidades No Assistente de configuração. Depois que a primeira seção for concluída, você poderá fazer com que um usuário atribuído a você com a função de persona de administrador de vulnerabilidades conclua as tarefas no Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares e exemplos, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Gerencie funções granulares e de persona para Resposta a vulnerabilidades

Depois de concluir a atribuição inicial de funções de persona usando o Assistente de configuração, gerencie atribuições de função granulares adicionais para usuários ou grupos no módulo Administração de usuários em sua instância.

Antes de Iniciar

Se você ainda não concluiu a configuração e a configuração iniciais de Resposta a vulnerabilidades Usando o Assistente de configuração ou funções de persona atribuídas a usuários e grupos, navegue até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**. Consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

Para obter termos principais e uma visão geral das funções de persona, consulte Resposta a vulnerabilidades personas e funções granulares.

Uma função de persona é uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidades, Analista de vulnerabilidades, Proprietário da correção, Gerenciador de item de configuração, e o Exception Manager são projetados para corresponder a cargos comuns para gerentes, analistas e responsáveis pelo serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Se você quiser que seus usuários e grupos tenham mais acesso do que uma das funções permite, adicione funções mais granulares a usuários e grupos. Por outro lado, se você quiser limitar o acesso de usuários e grupos específicos no nível da tarefa, poderá remover funções granulares. Além disso, você pode criar funções personalizadas para atender às suas necessidades.

Função necessária: administrador

Procedimento

1. Para gerenciar funções granulares para usuários e grupos, escolha uma para continuar.

Opção	Descrição
Edite as funções granulares de um usuário ou grupo	Atribua ou remova funções granulares para usuários ou grupos ou edite funções granulares para que somente usuários selecionados em um grupo tenham permissões expandidas ou limitadas. Um exemplo segue a tabela.
Crie uma nova função	Crie uma nova função usando uma ou mais funções granulares da biblioteca para um cargo específico ou para atender a um requisito específico. Um exemplo segue a tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os nomes das funções granulares em Resposta a vulnerabilidades geralmente descreva o que os usuários podem fazer e ver. Para exibir descrições de funções granulares específicas, navegue até **Tudo** > **Administração de Usuários** > **Funções** e localize a função desejada. A descrição da função, as funções que são herdadas automaticamente quando uma função é atribuída e todas as funções que dependem de outras funções também são listadas.

2. Para atribuir ou remover uma função granular para um usuário ou grupo, siga estas etapas.
   Por exemplo, suponha que você queira atribuir um gerente DE TI com uma função que permita que esse gerente exiba registros, mas não os atualize ou edite. Para exibir registros em Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidades e para todas as integrações de terceiros, você atribui a este usuário a função granular sn_vul.read_all.

   a. Navegar até **Tudo** > **Administração de Usuários** > **Usuários**.

   b. Localize o usuário e, na coluna Nome, clique no registro para abri-lo.
      O registro do usuário é exibido.

   c. Se não estiver selecionado, selecione a guia Funções.
      As funções atribuídas ao usuário no momento são exibidas.

   d. Clique em **Editar**.
      O formulário Editar membros é exibido.

   e. No campo Coleção da slushbucket, insira o nome da função, se você souber, ou insira `*sn_vul` Para exibir somente as funções granulares disponíveis para Resposta a vulnerabilidades.

   f. Localize e mova sn_vul.read_all para a Lista de funções.

      Nota: Use o mesmo processo para remover funções granulares específicas dos usuários na caixa de listagem movendo a função da lista Funções para a lista Coleção.

   g. Clique em **Salvar**.
      O registro do usuário é exibido com a nova função granular.

   h. Clique em **Atualização** Para salvar suas mudanças e retornar à lista de usuários.
      Você forneceu a um usuário permissão para ler, mas não atualizar registros em Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidades e para integrações de terceiros.

3. Para editar um grupo para que somente membros específicos tenham acesso expandido com funções mais granulares, siga estas etapas.
   Por exemplo, suponha que você queira permitir que determinados usuários no grupo Proprietário da correção (sn_vul.remediation_owner) criem itens vulneráveis manualmente, mas você não queira expandir essa permissão para todos os usuários do grupo. A permissão para criar itens vulneráveis manualmente é concedida pela função granular sn_vul.create_vulnerable_items. Para conceder essa permissão para selecionar somente usuários deste grupo, siga estas etapas.

   a. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.

   b. Localize o grupo responsável pela correção e, na coluna Nome, clique no grupo para abrir o registro.
      O registro do grupo é exibido.

   c. Se não estiver selecionado, selecione a guia Membros do grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os membros atuais do grupo são exibidos.

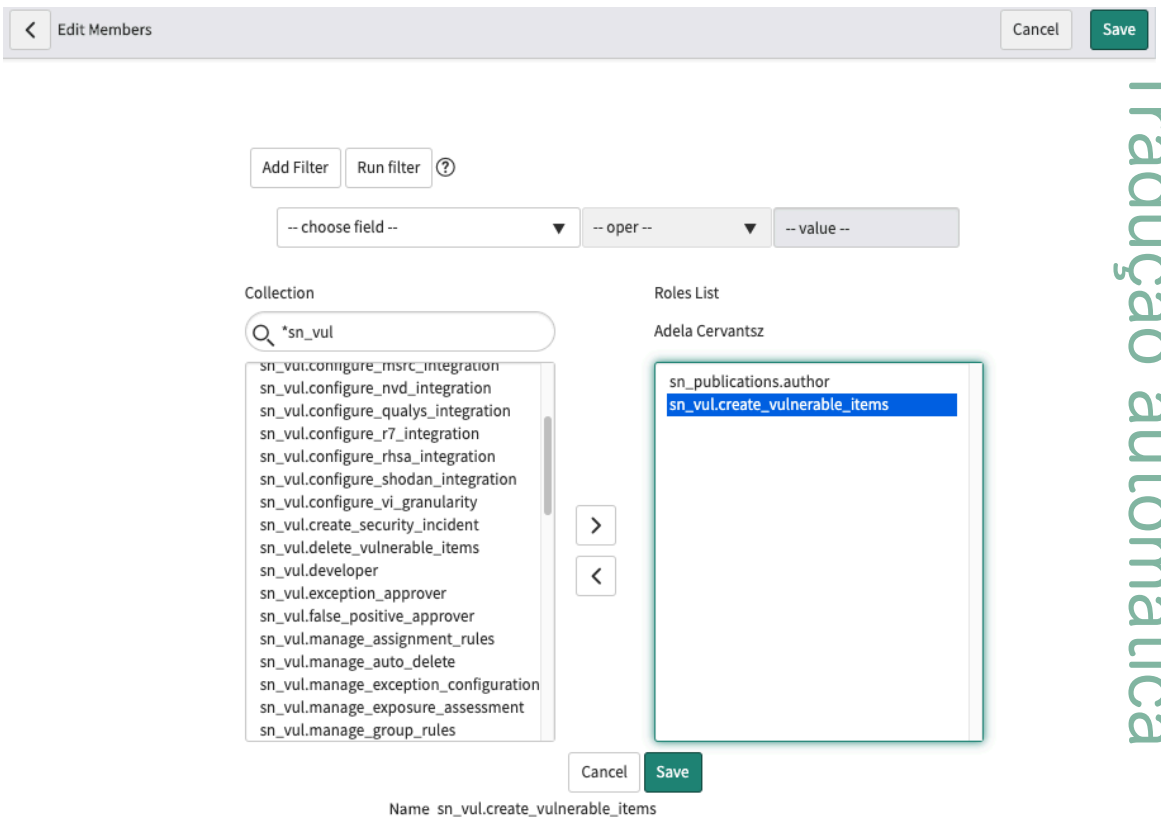
d. Clique em um nome na lista à qual você deseja atribuir a função granular e abra o registro.

e. No registro, role até a guia Funções e selecione-a.
As funções atribuídas ao usuário são exibidas.

f. Clique em **Editar**.
O formulário Editar membros é exibido.

g. No campo Coleção, insira o nome da função, se você souber, ou insira `*sn_vul` Para exibir todas as funções granulares disponíveis para Resposta a vulnerabilidades.

h. Localize e mova sn_vul.create_vulnerable_items para a Lista de funções.



i. Clique em **Salvar**.
O registro do usuário é exibido com a nova função granular.

j. Clique na seta Voltar para retornar e exibir os usuários no registro do grupo Responsável pela correção

k. Clique nos nomes na lista à qual você deseja atribuir esta função granular, abra os registros e use a caixa de listagem para atribuir a função.

l. Depois de concluir suas edições, clique em **Atualização** para salvar suas mudanças e retornar à lista de grupos.
Alguns usuários do grupo responsável pela correção (sn_vul.remediation_owner) forneceram permissão para criar itens vulneráveis manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para criar uma nova função usando somente as funções granulares selecionadas, siga estas etapas.
   Para este exemplo, suponha que você deseja criar uma função para um auditor de conformidade. Esta função funciona em estreita colaboração com Governance, Risk, and Compliance (GRC), e o trabalho requer as seguintes permissões e tarefas em Resposta a vulnerabilidades:
   - Gerencia os prazos de correção para itens vulneráveis e grupos de vulnerabilidades
   - Aprova solicitações de exceção para estender prazos ou adiar correção
   - Gerencia a limpeza de itens vulneráveis mais antigos com exclusão automática
   - Definir pontuações de risco
   - Lê todos os registros em Resposta a vulnerabilidades mas não tem permissão para editá-los.

   a. Navegar até **Tudo** > **Administração de Usuários** > **Funções**.

   b. Na lista Funções, clique em **Novo** .

   c. No registro de função, preencha os campos.

      Crie um nome, selecione a aplicação que contém este registro e insira uma descrição resumida para sua nova função. Para obter mais informações sobre os outros campos no formulário, consulte Crie uma função

      Nota: Ao criar um nome para sua nova função, você pode preferir usar um nome que seja facilmente reconhecido na lista Funções e descreva a funcionalidade da função. Para este exemplo, você pode preferir um título como Auditor de conformidade - GRC-VR.

   d. Clique em **Enviar**.
      A lista Funções é exibida.

   e. Localize sua nova função e clique nela para abrir o registro.

   f. Clique em **Editar**.
      O formulário Editar membros é exibido.

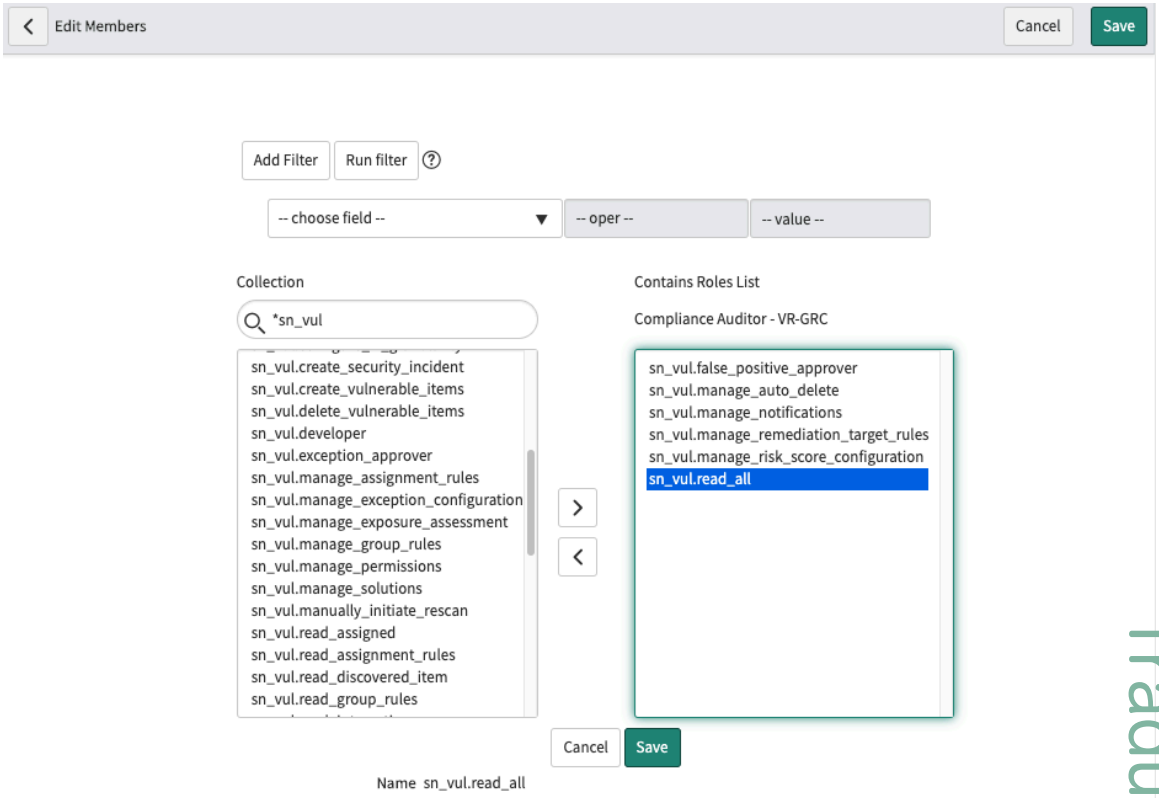
   g. Use o slushbucket para adicionar funções granulares à sua nova função.

      Para este exemplo, as funções necessárias para esta nova função são exibidas na coluna à direita na figura a seguir.

      Para exibir somente as funções granulares da Resposta a vulnerabilidades, no campo Coleção, insira `*sn_vul` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



h. Clique em **Salvar**.
O registro da sua nova função é exibido. Começando com a guia Contém funções, continue editando a função conforme necessário.

i. Clique em **Atualizar** para salvar suas mudanças.
Sua nova função é exibida na lista Funções.

Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração

Instale os aplicativos de integração de terceiros para os quais você tem direito em Resposta a vulnerabilidades Usando o Assistente de configuração.

Antes de Iniciar

O Assistente de configuração oferece suporte à instalação da maioria das aplicações de integração de terceiros com Resposta a vulnerabilidades, mas você continua com a configuração de alguns aplicativos que instala a partir dos módulos de configuração em sua instância. Consulte Integrações do Resposta a vulnerabilidades para obter uma lista de aplicações compatíveis com Resposta a vulnerabilidades.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

- Depois de instalado, o Solução de gestão de vulnerabilidade recurso de Resposta a vulnerabilidades fornece acesso ao Integração com a solução Microsoft Security Response Center e o. Red Hat Solution Integration No Assistente de configuração.
- Solução de gestão de vulnerabilidade está disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de instalar e ativar aplicações de terceiros a partir do Assistente de configuração, execute as seguintes tarefas para garantir uma instalação tranquila:

Tarefas de configuração	Descrição
Verifique se você tem válido ServiceNow direitos para as aplicações de integração que você deseja instalar.	Navegar até **Gestão de assinaturas** > **Assinaturas** em sua instância para verificar direitos. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para um Operações de segurança aplicação do ServiceNow Store, consulte Obtenha direito para um Operações de segurança produto ou aplicação.
(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instale e configure o Vulnerability Response .
Se ainda não estiver instalado e ativado, você deverá ativar e importar dados de vulnerabilidade com o trabalho agendado de Integração de NVD e CWE antes de executar um aplicativo de scanner de terceiros para importar dados.	Execute as integrações de NVD e CWE como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Para obter mais informações, consulte Noções básicas sobre as integrações de NVD.
Verifique se você concluiu todas as tarefas de configuração necessárias para as integrações de terceiros para Resposta a vulnerabilidades.	Revise todas as tarefas de configuração necessárias para cada integração que você deseja instalar em Integrações do Resposta a vulnerabilidades.

Função necessária: administrador

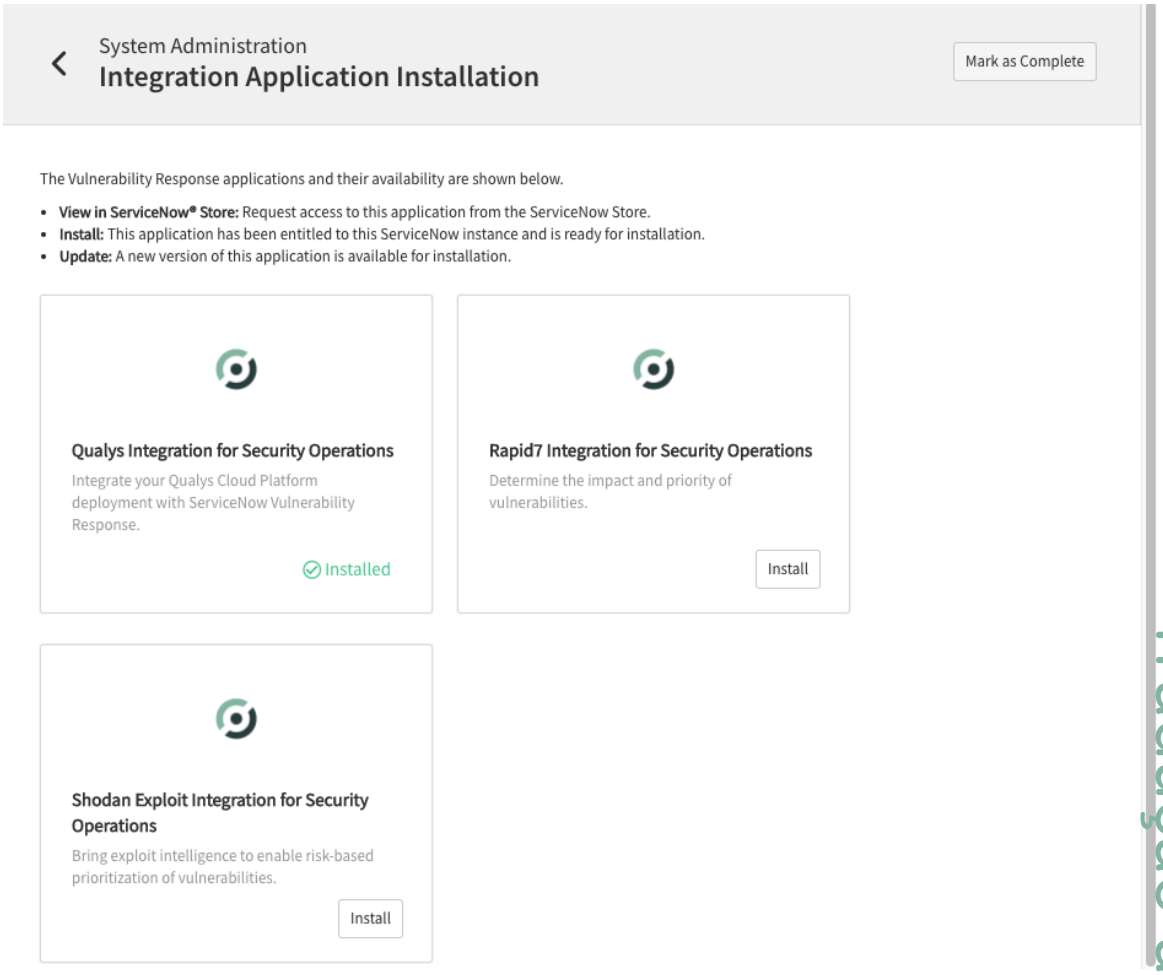
Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Administração do Sistema** > **Instalação de aplicação de integração**.

   Após alguns momentos, as aplicações para as quais você tem direito e que estão disponíveis para instalação em sua instância são exibidas.

Tradução automática

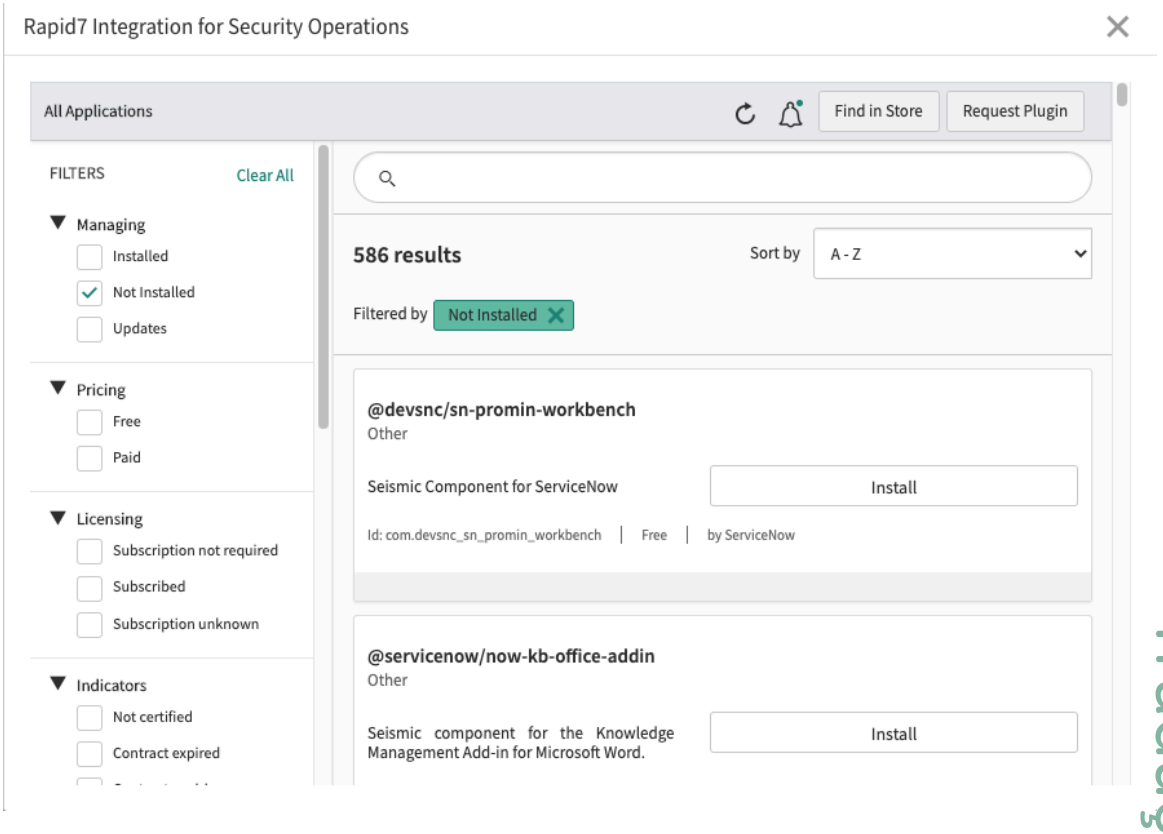
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Localize a aplicação que deseja instalar e clique em **Instalar** no bloco aplicação.
A caixa de diálogo Todas as aplicações é exibida com o nome do bloco da aplicação em que você clicou, por exemplo, Rapid7 Integration for Security Operations, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

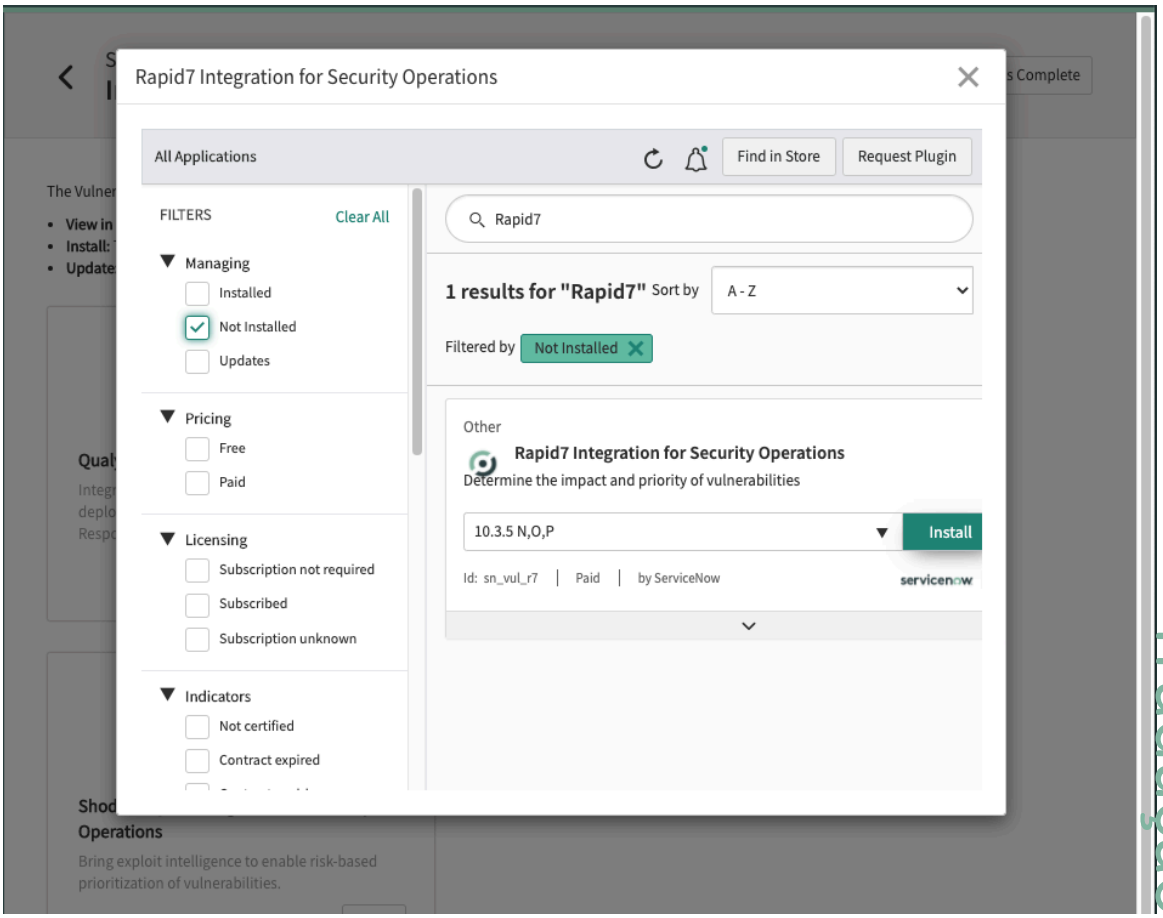


3. Localize a aplicação, selecione uma versão na lista de seleção e clique em **Instalar** .

Se uma atualização estiver disponível para a aplicação, o **Atualização** o botão é exibido.

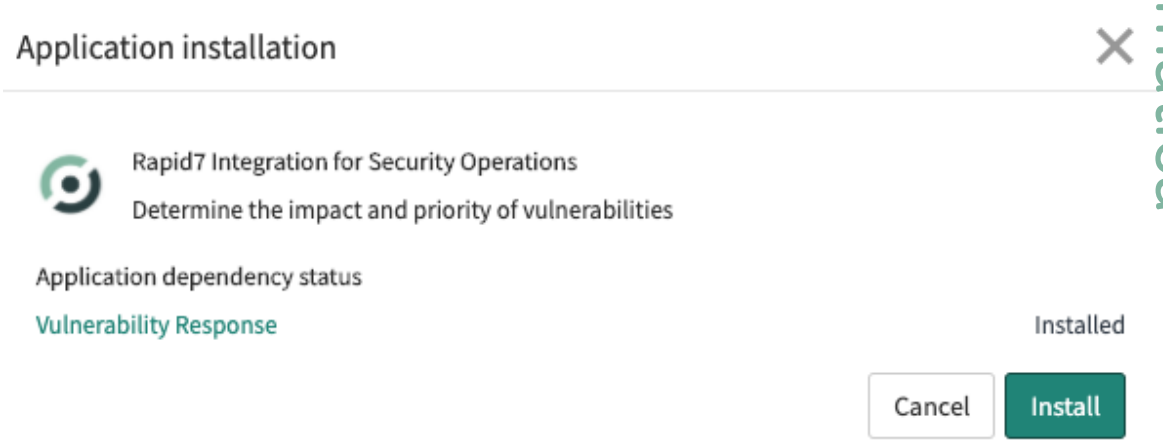
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo de instalação da aplicação, clique em **Instalar** .



A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo.
É exibida a página Todas as aplicações que mostra que sua aplicação foi instalada com sucesso.

Após a instalação e a ativação, você pode configurar, programar e iniciar os seguintes aplicativos e soluções instaladas diretamente na seção Configuração de integração do Assistente de configuração :

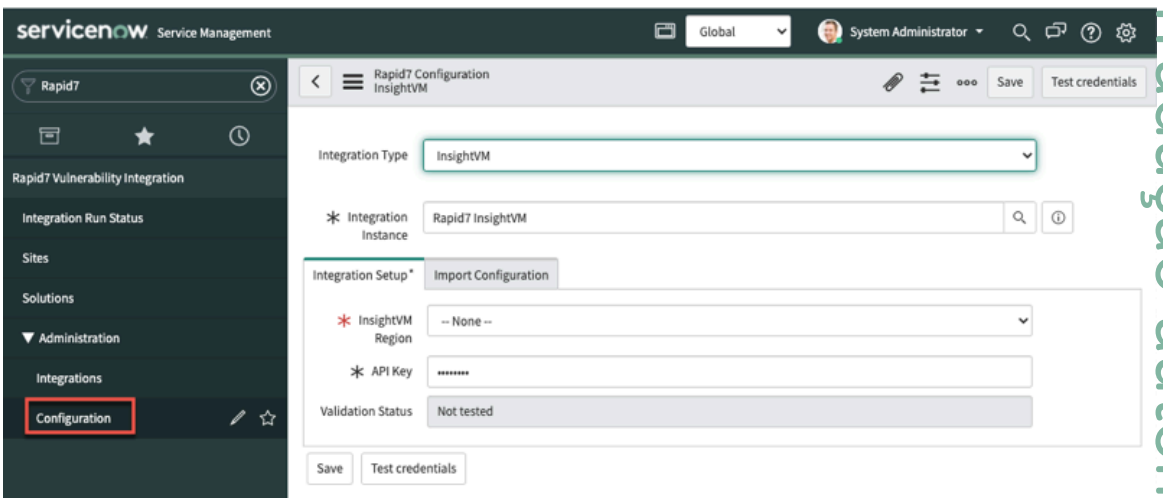
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O Qualys Vulnerability Integration
- . Integração de Resposta a vulnerabilidades com Tenable.
- O Integração com a solução Microsoft Security Response Center
- O Red Hat Solution Integration
- Integração com a solução Microsoft Security Response Center
- . Gestão de vulnerabilidades do Microsoft Defender Integração

Para outras aplicações não listadas acima, navegue diretamente até o módulo de configuração da aplicação para continuar com a configuração e inserir as credenciais de terceiros necessárias. Por exemplo, a imagem a seguir mostra o local da Configuração e do módulo do Rapid7 aplicação.

Para obter mais informações sobre como configurar aplicações específicas, consulte a documentação do produto de instalação e configuração por nome de produto fornecida para cada aplicação.



Tradução automática

O que Fazer Depois

Continue com a configuração da sua aplicação no Assistente de configuração se a sua aplicação for compatível.

Se sua aplicação não for compatível com configuração no Assistente de configuração, navegue diretamente até o módulo de configuração da aplicação para continuar com a configuração. Para exibir aplicações compatíveis no Assistente de configuração, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros

Se ainda não estiver instalado, baixe e execute a integração NVD e execute o trabalho agendado do CWE como parte da configuração inicial do Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. A Integração de Resposta a vulnerabilidades com NVD está disponível no ServiceNow Store.

Ingestão de dados de CWE e NVD

Os dados importados das integrações NVD e CWE são usados para enriquecer os dados de vulnerabilidade em sua instância e ajudar você a decidir se escalar a correção de uma vulnerabilidade, item vulnerável ou tarefa de correção. Após uma importação inicial, você

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pode atualizar registros da biblioteca sob demanda ou configurar um trabalho agendado para atualizar registros regularmente. Resposta a vulnerabilidades armazena-os em **Bibliotecas** .

O CVSS (Common Vulnerability Score System, sistema comum de pontuação de vulnerabilidade), incluído nas entradas NVD e de terceiros, captura as principais características de uma vulnerabilidade. Resposta a vulnerabilidades Usa dados CVSS para produzir um valor normalizado que reflete a gravidade da vulnerabilidade. Quando a gravidade é calculada, a vulnerabilidade fornece uma melhor compreensão do risco representado por essa vulnerabilidade para sua organização. A gravidade ajuda a avaliar e priorizar a correção de vulnerabilidades.

Se esta for sua primeira instalação de Resposta a vulnerabilidades ou antes de ingerir dados pela primeira vez com um produto de scanner de terceiros:

1. Execute uma importação inicial de dados do CWE com a Integração abrangente do CWE 2000.

   Para obter mais informações, consulte Configure e execute o trabalho agendado para atualizar registros CWE. Você executa atualizações de CWE **Sob demanda** no registro de integração por padrão, e você deve configurá-lo se quiser que ele seja executado como um trabalho agendado.

   Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados NVD. O dia padrão para a atualização do NVD é **Semanalmente** ativado **Segunda-feira** .

2. Verifique Resposta a vulnerabilidades A integração com a aplicação NVD está instalada e os dados da API do NIST National Vulnerability Database Integration - API (CVE somente) ou da API do NIST National Vulnerability Database Integration - API (CVE e CPE) são importados com sucesso.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois que ele é instalado, a integração NIST National Vulnerability Database Integration - API (CVE somente) é ativada por padrão. Ele é executado diariamente. Consulte Noções básicas sobre as integrações de NVD e. Instale o. Resposta a vulnerabilidades Integração com o NIST National Vulnerability Database para obter mais informações.

3. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Exibindo dados de vulnerabilidade importados e itens vulneráveis

As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, isso é apenas para referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

Tópicos relacionados

Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades

Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades

Antes de poder usar Solução de gestão de Resposta a vulnerabilidades recurso de Resposta a vulnerabilidades em sua instância, você deve concluir a instalação do Solução de gestão de vulnerabilidade aplicação. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Execute essas tarefas de configuração para uma instalação tranquila.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

. Integração com a solução Microsoft Security Response Center e. Red Hat Solution Integration as aplicações de solução estão disponíveis em Solução de gestão de Resposta a vulnerabilidades depois de instalar Solução de gestão de vulnerabilidade.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Solução de gestão de Resposta a vulnerabilidades requer Resposta a vulnerabilidades aplicação. Para a versão mais atual de Solução de gestão de vulnerabilidade verifique se você tem a versão mais atual de Resposta a vulnerabilidades instalado. Consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão . Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem direito à aplicação.	Para verificar se você tem direito ao Solução de gestão de vulnerabilidade aplicação, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter direito para Solução de gestão de vulnerabilidade aplicação do ServiceNow Store e baixe-o no seu ServiceNow AI Platform instância, consulte Obtenha direito para um Operações de segurança produto ou aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Certifique-se de que seus registros de NVD estejam atualizados nos últimos 10 anos.	Consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.
Certifique-se de que suas vulnerabilidades de terceiros estejam atualizadas.	Consulte Integrações do Resposta a vulnerabilidades para obter informações sobre integrações de vulnerabilidades de terceiros.
Verifique se você tem o necessário ServiceNow AI Platform funções atribuídas à sua instância.	As seguintes funções são necessárias para a instalação e verificação dos resultados esperados: Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades. • O administrador do sistema [admin] instala a aplicação. Se ainda não estiver atribuído, o administrador atribuirá a função administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Funções necessárias: administrador para instalar o. Solução de gestão de vulnerabilidade o administrador de aplicações e vulnerabilidades deve configurá-lo.

Procedimento

1. Navegue até ServiceNow Store.
2. Clique em **Faça login** E insira suas credenciais HI.
3. Clique em **Produtos da ServiceNow** para exibir os disponíveis ServiceNow produtos.
4. Clique em mais (**.** sinal de) ao lado de **Gestão de soluções de vulnerabilidade** para exibir todos os aplicativos associados para os quais você está qualificado.
5. Clique em **Aceite** para verificar se você tem direito a. Solução de gestão de vulnerabilidade para a aplicação.
6. Se você já tiver direito, pule para a etapa 10 para instalar a aplicação em seu ServiceNow AI Platform instância.
7. Marque a caixa de seleção e clique em **Aceitar** para concordar com os termos e condições no prompt.
   É exibida uma mensagem indicando que você aceitou a aplicação com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. **Opcional:** Clique em Gerenciar direito se quiser gerenciar seu direito para Solução de gestão de vulnerabilidade em outro ServiceNow AI Platform instâncias.

   Nota: . **Gerenciar direito** não for exibido, clique em **Gestão de soluções de vulnerabilidade** Na Lista de produtos para exibi-la.

   a. Escolha uma opção

   b. Clique em **OK** ou **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em suas instâncias.

9. Faça login no ServiceNow AI Platform instância em que você deseja instalar Solução de gestão de vulnerabilidade aplicação em.
10. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
11. Localize Solução de gestão de vulnerabilidade(sn_vul_solution) e clique em **Instalar** .
    A caixa de diálogo de instalação da aplicação exibe o status do plug-in de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.
12. Clique em **Instalar**.
    Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

    Agora, o administrador de vulnerabilidades pode configurar a aplicação no Assistente de configuração.
13. Clique em **Fechar**.

    . Integração com a solução Microsoft Security Response Center e. Red Hat Solution Integration as aplicações de solução estão disponíveis em Solução de gestão de Resposta a vulnerabilidades depois de instalar Solução de gestão de vulnerabilidade.

    Exiba as Soluções de vulnerabilidade navegando até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**. Para obter mais informações, consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade Usando o Assistente de configuração.

O que Fazer Depois

Depois de configurar a aplicação e as soluções disponíveis, verifique se os CVEs e as Soluções concordam usando a tabela Solução de vulnerabilidade [sn_vul_m2m_vulnerability_solution].

Instale e configure o. Performance Analytics para Resposta a vulnerabilidades Aplicação [PA]

Antes de poder usar Performance Analytics para Resposta a vulnerabilidades, você deve obter direito e baixar a aplicação do ServiceNow Store, instale-o em seu ServiceNow AI Platform® e conclua algumas etapas de instalação e configuração. A aplicação PA não está instalada como parte do Resposta a vulnerabilidades aplicação. Ele está disponível com uma assinatura separada.

Antes de Iniciar

Se você já tiver a aplicação em sua instância e estiver atualizando para uma versão mais recente da aplicação, prossiga para a etapa 8 nas etapas a seguir para continuar com a atualização e a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para uma nova instalação, conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Para verificar se os plug-ins e as aplicações estão instalados e ativados, navegue até **Tudo** > **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o plug-in Dependências de resposta a vulnerabilidades (com.snc.vul_dep) está instalado e ativado.	**Dependências de resposta a vulnerabilidades** Este plug-in contém todos os plug-ins de dependência necessários para oferecer suporte à aplicação . Para verificar se o plug-in está instalado e ativado, em sua instância, você deseja que a aplicação navegue **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**. Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links nas caixas de diálogo e siga as instruções para continuar.
Verifique se o ServiceNow Resposta a vulnerabilidades a aplicação (sn_vul) está instalada e ativada.	**Resposta a vulnerabilidades** Para verificar se o plug-in está instalado e ativado, em sua instância, você deseja que a aplicação navegue **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**. Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links nas caixas de diálogo e siga as instruções para continuar. A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Entre em contato com a ServiceNow para obter mais detalhes.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

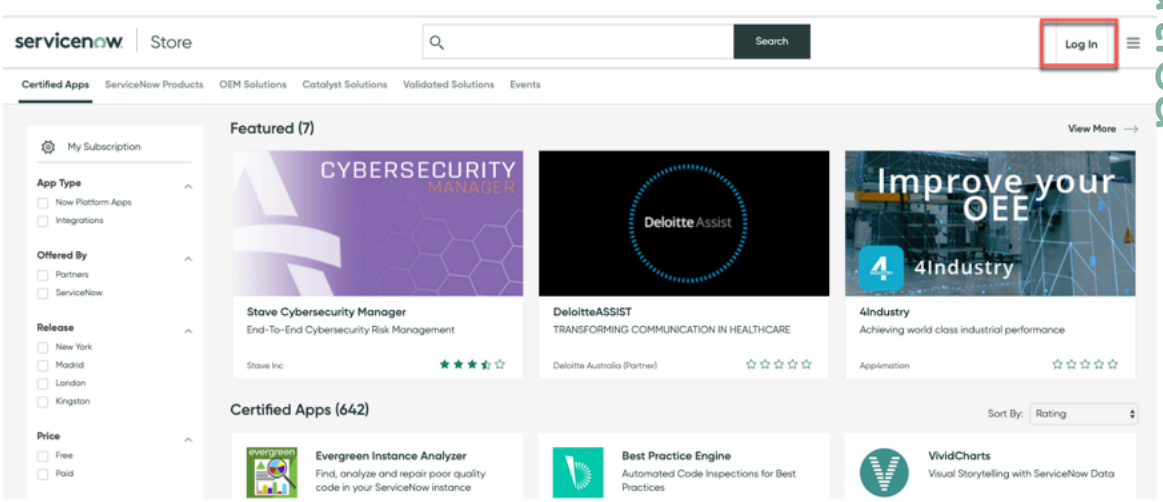
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.	• O administrador do Performance Analytics [pa_admin] ou o sistema [admin] instala a aplicação e verifica os resultados esperados. • O administrador de vulnerabilidades [sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)] supervisiona a configuração e verifica os resultados esperados com os painéis de PA. • O responsável pela correção [sn_vul.remediation_owner] supervisiona as tarefas de gestão de mudanças e lê e atualiza os registros atribuídos. A função sn_vul.remediation_owner também é atribuída automaticamente quando qualquer usuário recebe a função itil.
Verifique o Performance Analytics e Resposta a vulnerabilidades as aplicações são compatíveis.	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Função necessária: administrador ou pa_admin

Procedimento

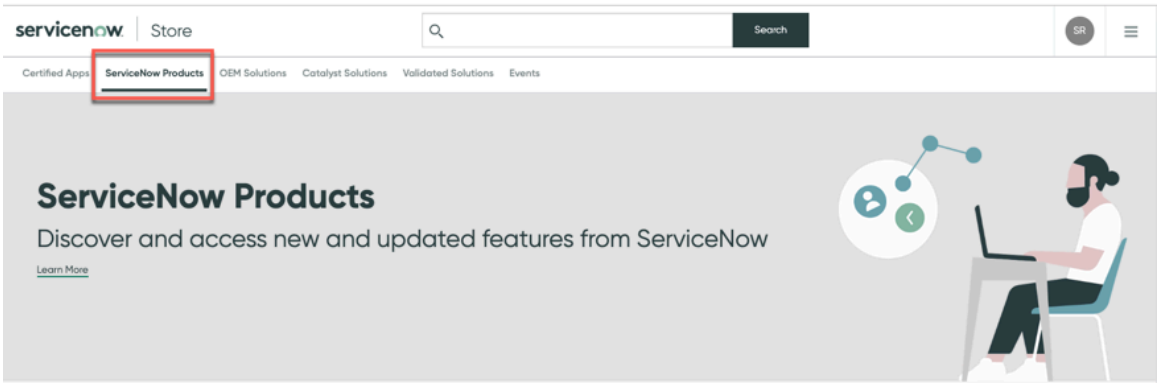
1. Para obter direito e baixar a aplicação em seu ServiceNow AI Platform, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Faça login** .



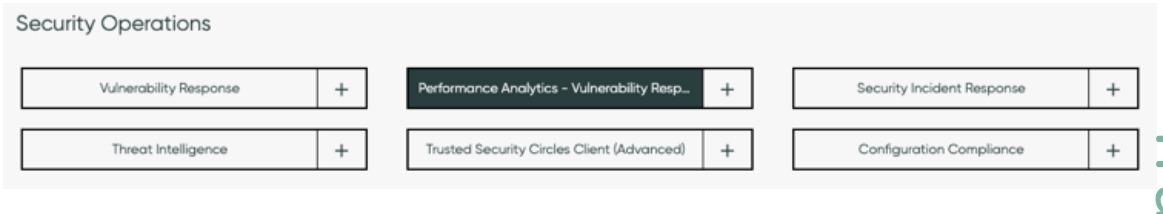
3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login** .
4. Na página exibida, se não estiver selecionada, clique em **Produtos da ServiceNow** guia.

Tradução automática

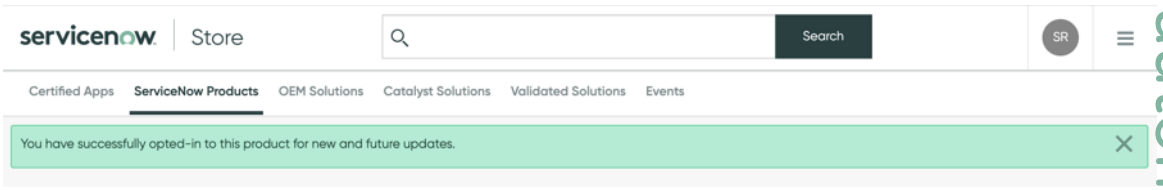
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na página de lista de produtos, clique em **Performance Analytics - Resposta a vulnerabilidades** .



6. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
   Uma página com o botão Aceitar é exibida.
7. Para obter Performance Analytics para Resposta a vulnerabilidades aplicação, clique em **Aceite** .
8. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar** .



9. **Opcional:** Como alternativa, para gerenciar seu direito para a aplicação em outro ServiceNow AI Platform, siga estas etapas.

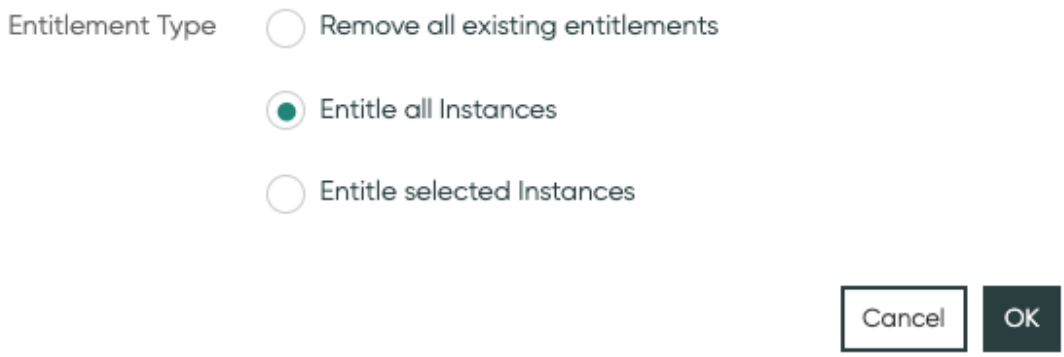
   a. Se o botão Gerenciar direito não for exibido, clique em Performance Analytics para Resposta a vulnerabilidades Na Lista de produtos para exibi-la.

   b. Com a guia Qualificado selecionada, clique em **Gerenciar direito** .

   c. Na caixa de diálogo Gerenciar direitos para resposta a vulnerabilidades exibida, escolha uma:

Tradução automática

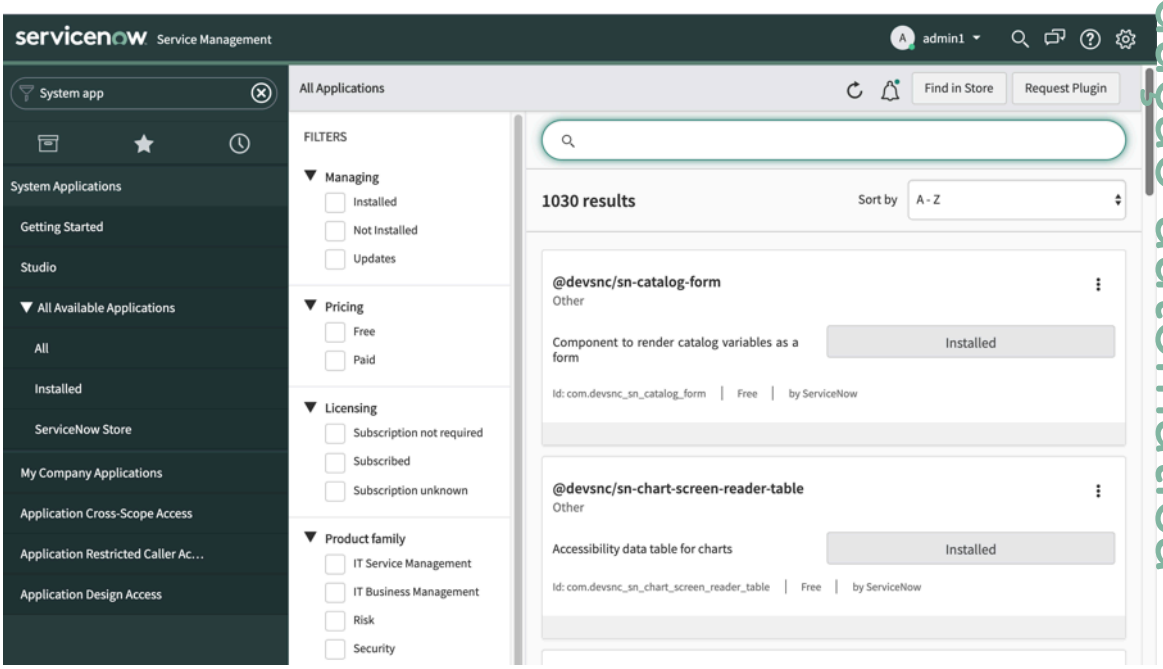
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Clique em **OK** ou **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar o aplicativo em seu ServiceNow AI Platform instâncias.

10. Faça login no ServiceNow AI Platform instância em que você deseja instalar Resposta a vulnerabilidades aplicação em.

11. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.



12. Nas aplicações listadas, localize a aplicação Performance Analytics - Pacote de conteúdo - Resposta a vulnerabilidades (sn_vul_analytics) e clique em **Instalar** .

Nota: Se você estiver atualizando para uma nova versão, selecione a versão desejada na lista de seleção.

e clique em **Atualização** .
A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas automaticamente com a aplicação também serão exibidas.

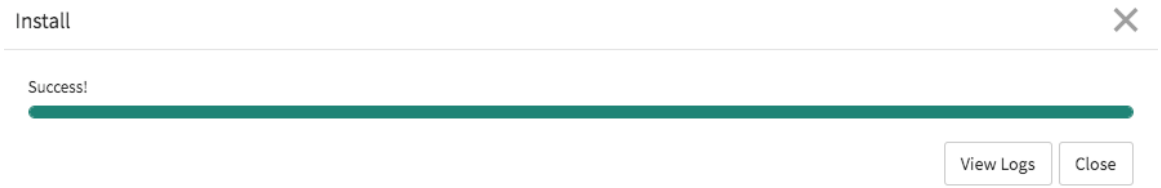
13. **Opcional:** Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você não selecionar **Carregar dados de demonstração** os dados de demonstração não estão disponíveis para instalação do **Gerenciador de aplicações** mais tarde. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] artigo no Now Support Base de conhecimento.

Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação é instalada com sucesso.

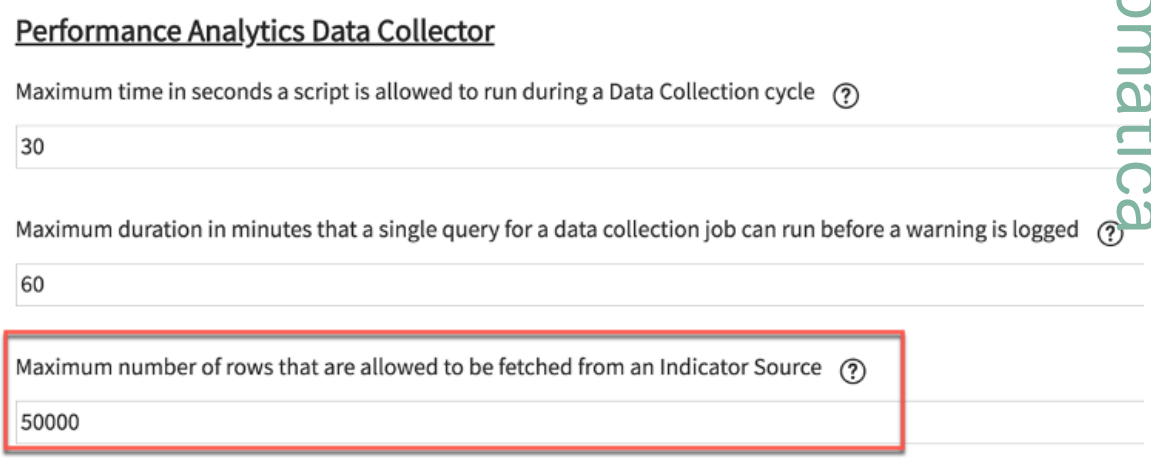


14. Clique em **Fechar**.
15. **Opcional:** Se você prevê um grande número de itens vulneráveis ativos em seu ambiente, pode preferir mudar a configuração padrão para o número máximo de registros coletados, habilitar trabalhos agendados e definir horários de coleta fora do horário comercial.
Para alterar essas e outras configurações da aplicação após sua instalação, siga estas etapas.

    a. Navegar até **Tudo** > **Performance Analytics** > **Console do administrador**.

    b. No bloco Configuração avançada, clique em **Propriedades do Performance Analytics** link.

    c. Na página Console do administrador [Performance Analytics], role até a seção Coletor de dados do Performance Analytics.
    A configuração padrão (50 000 registros) é exibida para o número máximo de linhas que podem ser obtidas de uma Origem de indicador.



    d. Você pode preferir aumentar esse número para um valor aproximadamente 20% maior do que o número total de itens vulneráveis ativos (VIS) que você prevê em seu ambiente.

    e. Clique em **Salvar**.

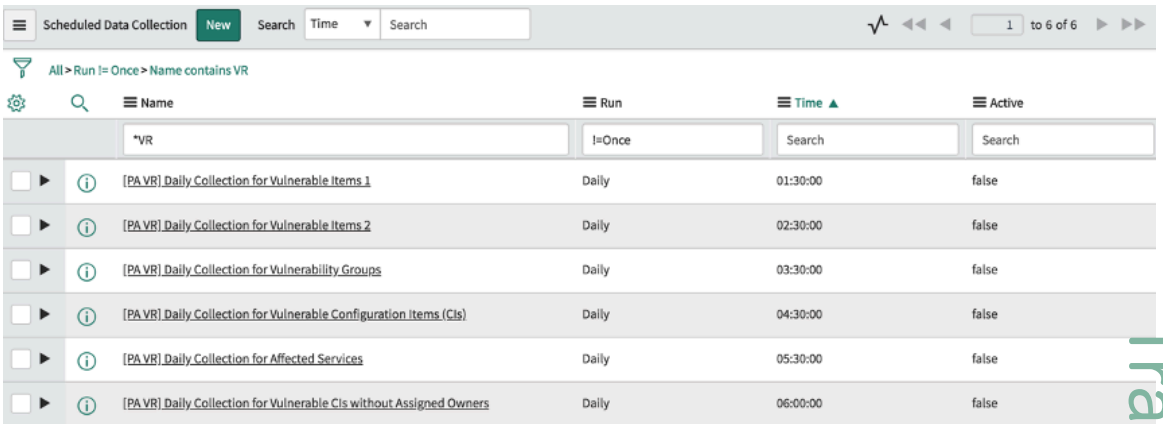
    f. Para ativar trabalhos agendados, navegue até **Análise de desempenho** > **Coletor de Dados** > **Trabalhos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A lista Coleta de dados programada é exibida. Na coluna Ativo, os trabalhos agendados listados na coluna Aplicação para Performance Analytics - Pacote de conteúdo - Resposta a vulnerabilidades por padrão estão desabilitados (`falso`).

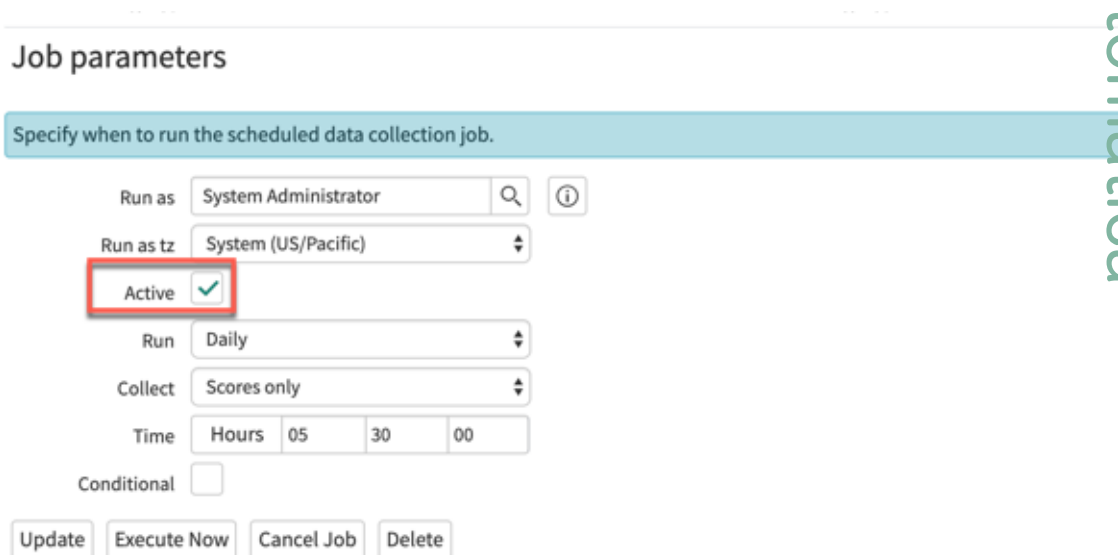
Nota: um trabalho agendado para coleta de dados históricos não é exibido na lista de trabalhos. Para grandes conjuntos de dados, você pode preferir começar a coletar dados e tendências ao longo do tempo habilitando seus trabalhos diários ao configurar o Performance Analytics para Resposta a vulnerabilidades aplicação.



g. Na coluna Nome, clique em um link para abrir um registro de trabalho de PA_VR.

h. Se os campos não forem editáveis, clique em **aqui** link para editá-los.

i. Na seção Parâmetros do trabalho, clique na caixa de seleção Ativo para programar um trabalho. Os campos de tempo são exibidos.



j. Insira a hora de início do trabalho.
Se você prevê um grande volume, pode preferir definir horários de coleta fora do horário de expediente. Se você prevê 10 milhões de VIS ativos ou mais em seu ambiente, entre em contato com ServiceNow® parceiro de implementação para obter mais informações sobre como configurar seu ambiente de coleta de dados.

Para obter mais informações sobre os indicadores usados para coleta de dados, consulte Exiba Performance Analytics indicadores para Resposta a vulnerabilidades[PA].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

k. Depois de habilitar todos os trabalhos desejados, clique em **Atualização** .
A lista Coleta de dados programada é exibida. Para obter mais informações, consulte Propriedades do Performance Analytics .

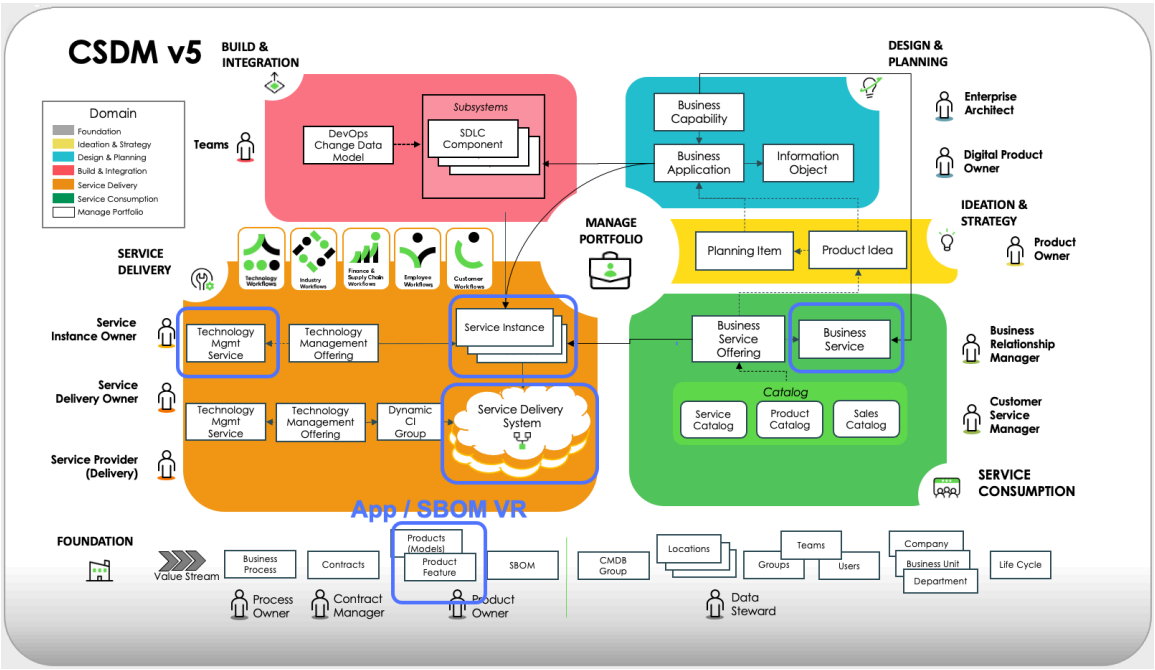
O que Fazer Depois

Navegar até **Resposta a vulnerabilidades** > **Visão geral** para exibir o painel.

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações.

. CSDM estrutura de dados e. Resposta a vulnerabilidades aplicações



CSDM tabelas referenciadas por Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software aplicações

À medida que os ativos são importados de scanners de vulnerabilidade de terceiros (integrações), eles são trazidos para Resposta a vulnerabilidades e representados em tabelas específicas:

- Host Resposta a vulnerabilidades Itens descobertos.
- Nuvem e. Contêiner de Resposta a vulnerabilidades imagens descobertas
- Resposta a vulnerabilidades de aplicações Aplicações descobertas (modelo de produto)

Como parte do Operações de segurança Pesquisa de item de configuração (IC) do CMDB, uma pesquisa é realizada para corresponder a um registro (IC) de dados importados com registros existentes no CMDB.

Tradução automática

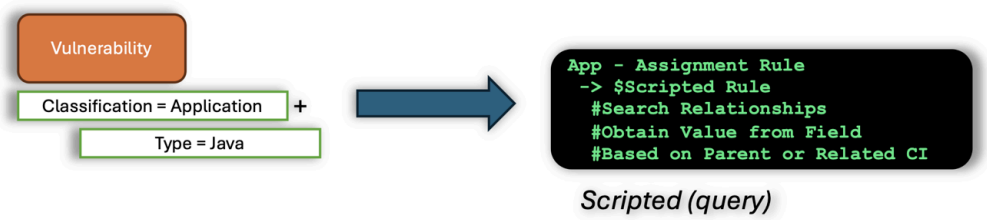
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada registro de IC específico pode conter atributos não detectáveis, por exemplo, Grupo de suporte ou Classificação, que são preenchidos no IC que podem ser usados como entrada para Regras de atribuição de item vulnerável. Esses atributos podem ser preenchidos a partir das sincronizações do Common Service Data Model (CSDM) com base nas ofertas de serviço técnico ascendentes.

Se você quiser aproveitar objetos do CSDM relacionados para Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software aplicações, você precisa usar regras com script.

Por exemplo, para atribuir automaticamente itens vulneráveis para correção usando regras de atribuição de item vulnerável, você pode criar uma regra que aproveita os valores de classificação de item de configuração conforme eles são atualizados nas entradas de vulnerabilidade importadas. Para este caso, você precisa de uma regra com script para consultar o valor de destino desejado do objeto CSDM relacionado.

Abaixo está um exemplo de uma consulta com script que você pode usar para ver se um IC tem Java e está vinculado a uma entrada de vulnerabilidade.



Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software as aplicações fazem referência às tabelas a seguir. Consulte CSDM estrutura de dados e. Resposta a vulnerabilidades imagem de aplicações para obter mais informações.

- A tabela Modelo de produto [cmdb_model] (referenciada por Resposta a vulnerabilidades de aplicações e. Lista de materiais de software).
- A tabela Modelo de aplicação [cmdb_application_product_model] (referenciada por Resposta a vulnerabilidades de aplicações e. Lista de materiais de software).
- A tabela Item de configuração [cmdb_ci].
- A tabela Serviço de negócio [cmdb_ci_service_business].
- A tabela Serviço [cmdb_ci_service].
- Tabela Grupo do CMDB [cmdb_group].
- Tabela Grupo de IC dinâmico [cmdb_ci_query_based_service].

CSDM tabelas usadas por Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software aplicações

1. Tabela Modelo de produto [cmdb_model] (usada por Resposta a vulnerabilidades de aplicações e. Lista de materiais de software).
2. Tabela Modelo de aplicação [cmdb_application_product_model] (usada por Resposta a vulnerabilidades de aplicações e. Lista de materiais de software).
3. A tabela Item de configuração [cmdb_ci].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Aplicação de negócios [cmdb_ci_business_app] (usada por Resposta a vulnerabilidades de aplicações e. Lista de materiais de software).
5. Serviço de negócio [cmdb_ci_service_business].
6. Tabela Serviço de gestão de tecnologia [cmdb_ci_service_technical] (anteriormente Serviço técnico).

Nota:

Ao carregar Lista de materiais de software, as aplicações SBOM tentam corresponder qualquer Modelo de produto e Aplicações de negócios que você carrega aos que já existem no CMDB. Você pode vincular instâncias de serviço (anteriormente chamadas de serviços de aplicações) ou aplicações de negócios para um modelo de produto.

Produtos que agregam valor a. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software aplicações

Usando o. Resposta a vulnerabilidades aplicações com o seguinte ServiceNow os produtos podem beneficiar sua organização.

Scanners de vulnerabilidade de terceiros e integrações

Vulnerabilidades importadas do National Vulnerability Database (NVD) e dados de detecção de scanners de terceiros são reconciliados com os ativos no CMDB. Quando uma vulnerabilidade importada corresponde a um ativo existente, um item vulnerável é criado. Os itens vulneráveis são agrupados automaticamente em tarefas para correção, risco pontuado com contexto de negócios, priorizados e atribuídos às equipes apropriadas para correção. Para obter mais informações e uma lista de integrações, consulte Integrações do Resposta a vulnerabilidades.

As Integrações abrangentes do CWE 2000 e NVD

Os dados importados das integrações NIST National Vulnerability Database (NVD) e Common Weakness Enumeration (CWE) são usados para enriquecer os dados de vulnerabilidade em sua instância e ajudá-lo a decidir se escalar a correção de uma vulnerabilidade, item vulnerável ou tarefa de correção. Para obter mais informações, consulte Noções básicas sobre as integrações de NVD e Configure e execute o trabalho agendado para atualizar registros CWE.

Produtos que se beneficiam da integração com Lista de materiais de software

Controle de posturas de segurança

Controle de posturas de segurança permite que as equipes de segurança cibernética tenham visibilidade de todo o inventário de ativos empresariais e determinem sua postura geral de segurança. Políticas em SPC o pode ajudar você a detectar ativos com vulnerabilidade importados com Resposta a vulnerabilidades aplicações para ajudá-lo a localizar lacunas de cobertura da ferramenta de segurança.

Governança, risco e conformidade

Conecte a segurança e A TI com um programa de risco integrado que oferece monitoramento contínuo, priorização e automação.

DevOps

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proteja seus ambientes contra componentes potencialmente prejudiciais durante os ciclos de desenvolvimento de software com ações do GitHub que você inicia no seu ambiente do GitHub. Carregar arquivos SBOM para ServiceNow AI Platform Dos repositórios do GitHub.

Criar ou editar Resposta a vulnerabilidades regras de atribuição

Depois de concluir a avaliação inicial das regras de atribuição usando o Assistente de configuração, você pode criar regras para atribuir automaticamente itens vulneráveis com base nas condições do filtro. Essas regras atribuem itens vulneráveis conforme eles são importados ou criados manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

O sistema de base é fornecido com uma regra de atribuição de vulnerabilidade, **Atribuir ao grupo de suporte de IC** , Que atribui itens vulneráveis ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra pode ser modificada usando condições de filtro ou você pode criar uma nova regra. Com as regras de atribuição, você define as condições de atribuição e a ordem de execução. Quando um VI corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Abra o. **Atribuir ao grupo de suporte de IC** ou clique **Novo** .
3. Se **Novo** preencha os campos no formulário, conforme apropriado.

Regras de Atribuição da Vulnerabilidade

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, onde o risco é crítico ou um VI deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde não há manipulação especial r e você sabe quem deve ser responsável por eles. Por fim, crie uma regra padrão para atribuir VIS ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Descrição	Descrição da regra de atribuição.
Condição	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visualização	Mostra quantos resultados esta consulta retornará.
Campos de condição	Condições que devem ser atendidas. **Nota:** Para fazer Rapid7 InsightVM Etiquetas de ativo disponíveis para uso no filtro de condição para Regras de atribuição, você deve executar o. Rapid7 InsightVM Integração da lista de ativos antes da outra Rapid7 InsightVM integrações. A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: Selecione um grupo de usuários na tabela de pesquisa. ◦ Campo de grupo de usuários: Selecione um campo de grupo de usuários no menu suspenso. ◦ Script: Crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow experiência.

4. Clique em **Enviar**.
Regras novas ou atualizadas são avaliadas na próxima importação.

Nota:

O recurso Reaplicar requer uma aplicação de linha de base das regras. Depois que suas regras forem criadas, se você ainda não tiver feito isso, ative *`Reapply all vulnerability assignment rules`*trabalho programado para ser executado, conforme sua conveniência. Aplica todas as regras a todos os VIS abertos, exceto aqueles atribuídos manualmente. Dependendo de quantos VIS ativos você tem em seu ambiente, lembre-se de definir **Executar** campo apropriado após a execução inicial para evitar impactos no desempenho.

Se você não tiver executado este trabalho agendado, ao tentar usar o. **Aplicar mudanças** No formulário Regras de atribuição, você terá que fazer isso. Reaplicar regras de atribuição não reagrupa os itens vulneráveis.

Crie um Resposta a vulnerabilidades Regra de atribuição usando ML

Use o script a seguir para criar uma regra de atribuição abrangente para itens vulneráveis que usa recomendações DE ML da Inteligência preditiva para atribuí-los automaticamente para correção.

Antes de Iniciar

Recomendações de atribuição de vulnerabilidades para Resposta a vulnerabilidades a aplicação deve ser instalada e ativada. Esta aplicação está disponível no ServiceNow Store.

Uma solução de classificação deve ser definida, ativa e treinada. Você usa este modelo para ajudar a prever o grupo de atribuição apropriado para itens vulneráveis (VI) nos casos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em que suas regras de atribuição não encontraram uma correspondência correta para os destinatários pretendidos.

Esta regra pode ajudá-lo a reduzir o número de VIS não atribuídos depois que outras regras de atribuição já tiverem sido concluídas.

Para obter mais informações, consulte Instalar Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades e Criar e treinar uma definição de solução para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode preferir executar esta tarefa somente se tiver experiência avançada de codificação ou se tiver conhecimento profundo sobre ServiceNow AI Platform, Seus recursos de Inteligência preditiva e como funcionam as regras de atribuição.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Consulte Criar ou editar Resposta a vulnerabilidades regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script** .
5. No editor, copie e cole o script a seguir.

```
/*
* Catch-all assignment rule using ML recommendation
* NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
* Classification Solution must be active and trained
*/
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
  var ARU = new sn_vul.AssignmentRecommendationUtils();
  ARU.initialize();

  var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
  /*
  *returns object containing array of predictions
  *payload structure:
  *
  {
    "predictions": [
      {
        "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
        "name": "Windows Server support ",
        "confidence_score": "57.54"
      },
      ...
    ],
    "exception": ""
  }
  */
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    var viPredictionArray = viPredictionObj['predictions'];
    var topPredictionObj = viPredictionArray.shift();

    return topPredictionObj['sys_id'];
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revisão Resposta a vulnerabilidades visão geral das regras de atribuição para obter mais informações gerais sobre regras de atribuição e *`Reapply all vulnerability assignment rules`*trabalho agendado.

Crie um Resposta a vulnerabilidades regra de atribuição para suporte de serviço

Use o script a seguir para criar uma regra que atribua itens vulneráveis para correção com base nos serviços de negócios que afetam.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode preferir executar esta tarefa somente se tiver experiência avançada de codificação ou se tiver conhecimento profundo sobre ServiceNow AI Platform e como funcionam as regras de atribuição.

Com esta regra, os VIS são atribuídos de acordo com o quão próximos eles correspondem aos serviços de negócio listados no seu CMDB. Se nenhum serviço, departamento ou grupo de suporte relacionado for correspondido, os VIS serão atribuídos ao grupo Analista de vulnerabilidades.

Esta regra pode ajudá-lo a reduzir o número de VIS atribuídos incorretamente ou que permanecem sem atribuição após a conclusão de outras regras de atribuição.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Consulte Criar ou editar Resposta a vulnerabilidades regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script** .
5. No editor, copie e cole o script a seguir.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
    var ci = vitGR.getValue('cmdb_ci');
    var defaultAssignmentGroup = 'Vulnerability Analyst';
    var defaultGR = new GlideRecord('sys_user_group');
    defaultGR.get('name', defaultAssignmentGroup);
    var defaultAssignmentGroupID = defaultGR.sys_id;
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
  var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
  var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
  var customValues = {
     "maxDepth": maxDepthValue,
     "maxSize": maxSizeValue
  };
  var ciu = new global.CIUtils();
  var services = ciu.servicesAffectedByCI(ci, customValues);
  var svc = new GlideRecord("cmdb_ci_service");
  var hasSvc = false;
  if (services && services.length > 0) {
     svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
     svc.addNotNullQuery("busines_criticality"); // typo intended
     svc.orderBy("busines_criticality");
     svc.setLimit(1);
     svc.query();
     hasSvc = svc.next();
  }
  if (!hasSvc) {
     // If there are no services it should be assigned to a default assignent group
     return defaultAssignmentGroupID;
  } else {
     var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
     return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
  }
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revisão Resposta a vulnerabilidades visão geral das regras de atribuição para obter mais informações gerais sobre regras de atribuição e *`Reapply all vulnerability assignment rules`*trabalho agendado.

Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção

Depois de concluir a avaliação inicial das regras de tarefa de correção usando o Assistente de configuração, você pode criar regras para agrupar automaticamente itens vulneráveis com base nas condições do filtro. Essas regras agrupam automaticamente itens vulneráveis conforme eles são importados ou criados manualmente. Use o filtro para limitar os itens vulneráveis agrupados por esta regra, como selecionar todos os itens vulneráveis com explorações.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

O sistema de base é fornecido com uma regra de tarefa de correção, **Vulnerabilidade** , que agrupa itens vulneráveis por vulnerabilidade e grupo de atribuição (de **Regras de**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atribuição). Você pode reaplicar as regras na exibição de formulário ou de lista. Para algumas entradas de amostra, Resposta a vulnerabilidades exemplos de regra de tarefa de correção.

Esta regra pode ser modificada da seguinte forma:

Usando condições de filtro e Agrupar por opções.

Por padrão, as tarefas de correção usam **Regras de atribuição** , quando disponível, como parte de seus critérios de filtro.

Nota: Se não houver regras de atribuição, você poderá selecionar um grupo usando **Grupo de usuários** campo.

A partir da versão 18,0 de Resposta a vulnerabilidades. **Vulnerabilidade** a regra da tarefa de correção está desativada em Resposta a vulnerabilidades para novas implementações.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou clique em **Novo** .
3. Se **Novo** preencha os campos no formulário, conforme apropriado.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra da tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição diferencia maiúsculas de minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. **Nota:** Para fazer Rapid7 InsightVM Etiquetas de ativo disponíveis para uso no filtro de condição para Regras de tarefa de correção, você deve executar o. Rapid7 InsightVM Integração da lista de ativos antes da outra Rapid7 InsightVM integrações. Por padrão, (**Distinção entre maiúsculas e minúsculas** caixa de seleção desabilitada), o texto de pesquisa inserido no construtor de condições nos registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefa.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis de	A tabela que a regra usa para agrupar VIS. Você pode ter até seis filtros. As opções são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Item vulnerável [sn_vul_vulnerable_item] ○ Item vulnerável → Item de configuração [cmdb_ci] ○ Item vulnerável → Vulnerabilidade [sn_vul_third_party_entry] **Nota:** Se você escolher uma tabela estendida, o **Usando o campo** é aplicado somente a itens vulneráveis que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar VIS.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir tarefas de correção automaticamente, a opção Atribuição é usada além de **Agrupar por** opções para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para garantir que cada item vulnerável seja colocado em uma tarefa com um conjunto de grupos de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ○ Agrupar por campo: Se você selecionou qualquer campo de grupo de usuários no **Usando o campo** valores em **Agrupar por** , eles aparecem no menu suspenso. ○ Grupo de usuários: Use a lista de pesquisa para selecionar um grupo de usuários estático.

Nota: Se você mudar de ideia sobre qualquer um dos **Agrupar por** . **Limpar agrupar por campos** o link relacionado redefine o. **Agrupar por** campos no formulário.

Quando uma regra de grupo é excluída, na exibição de formulário ou de lista, você tem a opção de excluir tudo **Aberto** grupos criados por essa regra. Grupos que não estão em **Aberto** os estados são excluídos.

Para obter algumas entradas de amostra, consulte Resposta a vulnerabilidades exemplos de regra de tarefa de correção.

Defina campos e pesos para a regra de risco para Calculadoras de risco de resposta a vulnerabilidades

Personalize os parâmetros e os pesos da regra de risco para que você possa gerar pontuações de risco que usam a vulnerabilidade e os dados de ativos exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Além disso, você pode usar atributos em configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco de resposta a vulnerabilidades. Se, por exemplo, você determinar que os ICs voltados para o exterior em sua organização são mais vulneráveis e podem exigir correção imediata, poderá atribuir atributos como `Internet Facing`Para esses ICs. E outros atributos estão listados nas notas de versão do Modelo de dados de serviço comum da versão da família Orlando. Para obter informações e orientações atuais sobre CMDB, consulte os seguintes tópicos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Modelo conceitual do Modelo de dados de serviço comum
- Modelo de esquema do CMDB

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de Vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidades, selecione **Calculadora de risco padrão** .
3. Navegar até **Página Calculadora de vulnerabilidades** > **Guia Regras da calculadora de vulnerabilidades** > **Regra de Risco Padrão**.
4. **Opcional:** Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo da pontuação de risco geral.
5. Para desativar a regra, você deve limpar **Ativo** caixa de seleção.
6. Para adicionar campos de regra de risco aos critérios da Calculadora de risco, selecione **Adicionar critérios** .
7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir a ponderação da pontuação de risco. Você pode selecionar uma destas opções: ○ **Item vulnerável** : Adicione campos que são diretamente passíveis de observação com pontos do item vulnerável (VI). ○ **Item vulnerável - Item de configuração** : Adicione campos caminháveis com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci). ○ **Item vulnerável - Vulnerabilidade** : Adicione campos passíveis de observação com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, entrada de terceiros. Esses campos não fazem parte da tabela base de Entrada de vulnerabilidades. ○ **Tabela de referência de item vulnerável** : Adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Tabela de referência do item de configuração** : Adicione campos que

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Tabela de referência de vulnerabilidade** : Adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Condições personalizadas** : Use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ○ **Item vulnerável -> Item de configuração** ○ **Item vulnerável -> Vulnerabilidade** ○ **Tabela de referência do item vulnerável** ○ **Tabela de referência do item de configuração** ○ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada na tabela Escolher referência. Selecione o valor mínimo ou máximo a ser considerado para cálculos quando Campo for selecionado nas tabelas relacionadas (m2m).
Peso	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Defina Valor ponderado	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1 a 5). Os pesos devem ser inteiros entre 0 e 100. **Nota:** Este campo não aparecerá se a opção Condições personalizadas estiver selecionada na tabela Escolher referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela de condição	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Insira um nome para os critérios de risco.
Condição	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Selecione **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

Nota: A partir da versão 23,0 de Resposta a vulnerabilidades, no caso de:

- **Calculadora de risco padrão** Regra: Sempre que a pontuação de risco em um item vulnerável (VIT) muda, os seguintes detalhes são documentados na seção Anotações da VIT:
  - Nome do grupo de calculadora
  - Nome da calculadora
  - Valores de campo que têm uma ponderação maior que 1 e sua contribuição de pontuação de risco.
  - Pontuação de risco final
- **Gravidade da vulnerabilidade** Regra de risco: Sempre que a pontuação de risco é atualizada em um VIT, o. **Anotações** a seção é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadora
  - Nome da calculadora: Dependendo se a regra da calculadora é baseada em um modelo ou script, o nome é anexado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e selecione **Exibição avançada** caixa de seleção. Em **Tipo de valor** caixa suspensa, selecione a opção necessária. Se **Modelo** selecionado, a pontuação de risco é atualizada de acordo com a condição especificada na regra. Se **Script** selecionado, você pode adicionar ou atualizar o script existente.

Example:
Exemplo 1: Adicione uma gravidade de origem como critério para uma regra de risco.

Caso de uso: Fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas em **Gravidade da origem** campo na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, faça o seguinte:

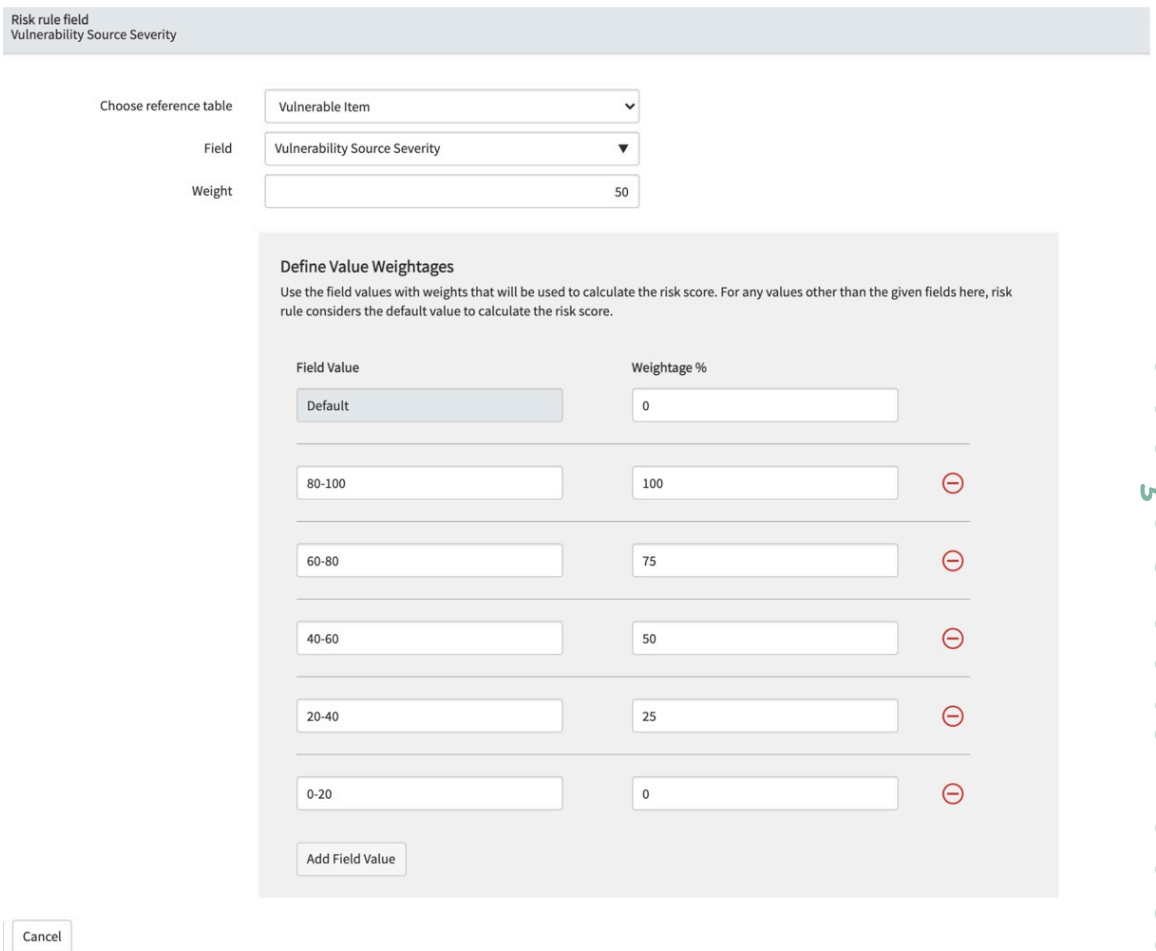
1. Navegue até a página Regra de risco.
2. Para desativar a regra, limpe **Ativo** caixa de seleção.
3. Para adicionar campos de regra de risco aos critérios da Calculadora de risco, selecione **Adicionar critérios** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na lista Escolher tabela de referência, selecione **Item vulnerável** .
5. Na lista Campo, selecione **Severidade Vulnerability.Source** .
6. Em **Peso** insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
7. Na seção Definir ponderação de valor, adicione valores de campo e atribua um peso a eles.

Tabela de Item Vulnerável



8. Selecione **Enviar**.

Exemplo 2: Adicione uma criticalidade comercial como critério para uma regra de risco.

Caso de uso: Vamos presumir que sua organização tenha muitos serviços de negócios. O item de configuração (IC) LINUX-SF-6381 está sendo usado pelos seguintes serviços:

Criticidade dos serviços de negócio

Serviço de negócios	Criticidade
Gestão de nuvem	1 - Mais crítico
E-Commerce	2 - Um pouco crítico
Serviços ao cliente	3 - Menos crítico
Viagem e despesa	4 - Não crítico

Tradução automática

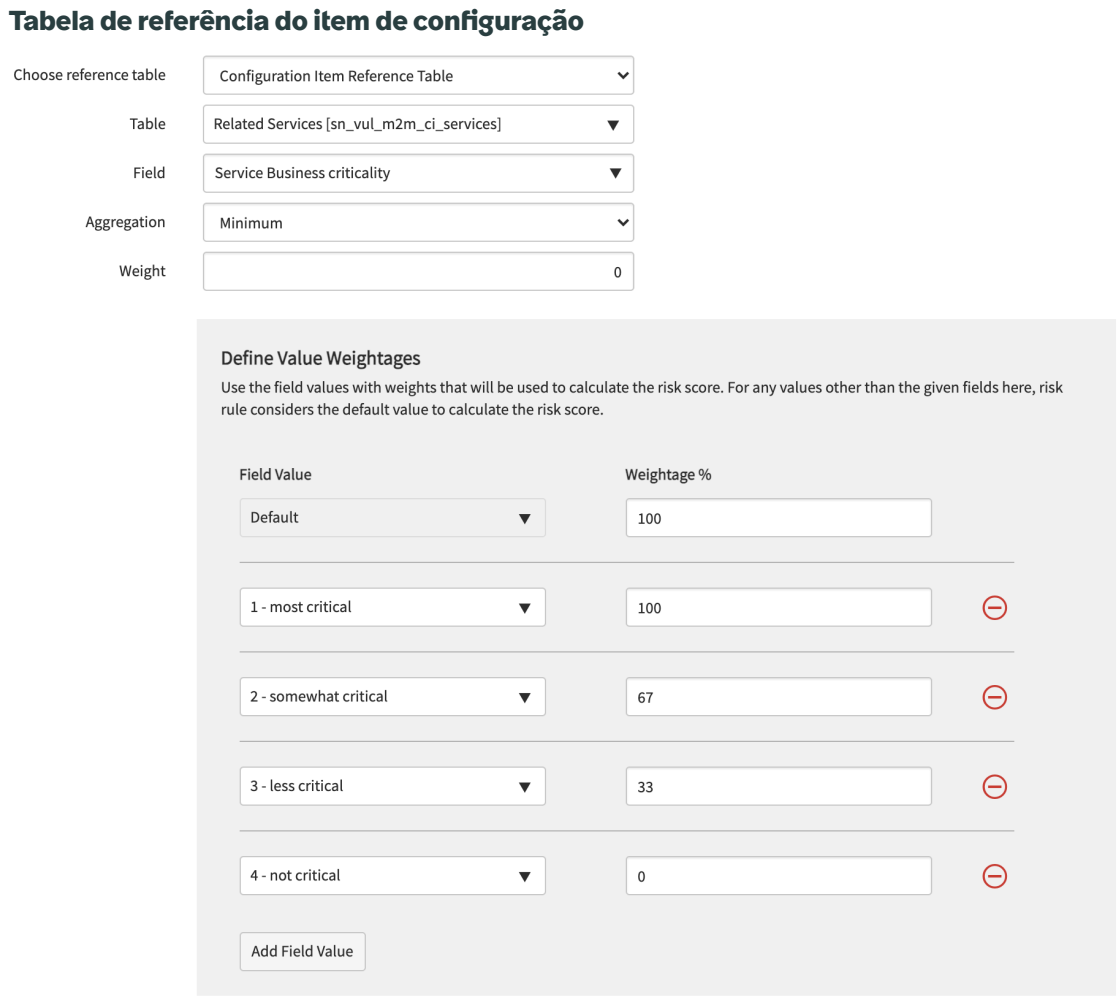
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O mapeamento entre o IC e os serviços é armazenado na tabela Serviços relacionados [sn_vul_m2m_ci_services]. Quando uma vulnerabilidade é encontrada no ativo LINUX-SF-6381, um item vulnerável (VI) é criado. Você pode usar o valor da criticidade comercial dos serviços afetados para calcular a pontuação de risco para este VI Para usar o valor de criticidade desses serviços para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, limpe **Ativo** caixa de seleção.
3. Para adicionar campos de regra de risco aos critérios da Calculadora de risco, selecione **Adicionar critérios** .
4. Na lista Escolher tabela de referência, selecione **Tabela de referência do item de configuração** .
5. Na lista Tabela, selecione **Serviços relacionados [sn_vul_m2m_ci_services]** .
6. Na lista Campo, selecione **Criticalidade do negócio** .
7. Em **Agregação** campo, selecione **Mínimo** para recuperar o serviço mais crítico para este caso de uso (**1- Mais crítico** Valor) ou máximo para recuperar o serviço menos crítico para este caso de uso (**4 – Não crítico** para este caso de uso.
8. Em **Peso** insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
9. Na seção Definir pesos do valor, adicione valores de campo e atribua um peso a eles.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Selecione **Enviar**.

Exemplo 3: Adicione um critério condicional à calculadora de risco.

Vamos supor que uma organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar pesos de pontuação de risco para esses ICs externos.

Nota: Você pode identificar esses ICs pelo nome deles. Os nomes começam com "external".

Para adicionar um critério condicional à regra de risco, faça o seguinte:

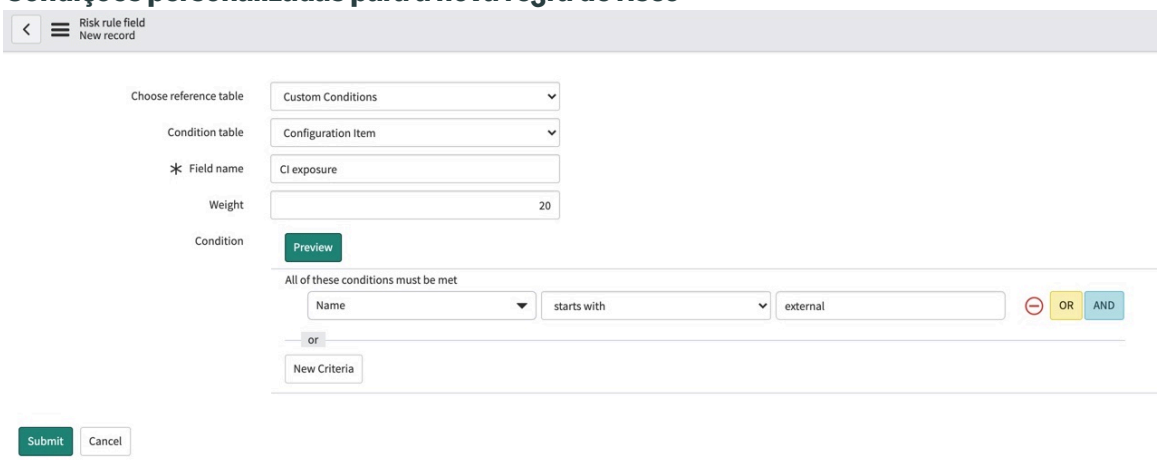
1. Navegue até a página Regra de risco.
2. Para desativar a regra, limpe **Ativo** caixa de seleção.
3. Para adicionar campos de regra de risco aos critérios da Calculadora de risco, selecione **Adicionar critérios** .
4. Na lista Escolher tabela de referência, selecione **Condições personalizadas** .
5. Na lista Tabela de condições, selecione **Item de configuração** .
6. Em **Nome do campo** , insira o nome **Exposição de IC** .
7. Em **Peso** insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Em **Condição** campo, selecione **Nome** > **começa com** e insira o valor **externo** .

Condições personalizadas para a nova regra de risco



9. Selecione **Enviar**.

Nota: Adicionar critérios condicionais à regra de risco pode prejudicar o desempenho.

Tópicos relacionados

Calculadoras de resposta a vulnerabilidades e regras da calculadora de vulnerabilidades

Crie uma calculadora de Resposta a vulnerabilidades

Filtrando na Resposta a vulnerabilidades

Resposta a vulnerabilidades Calculadoras de acúmulo

Após a avaliação inicial das calculadoras de risco no Assistente de configuração, use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativa é calculada para tarefas de correção e vulnerabilidades importadas.

Use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativo é calculada para tarefas de correção e vulnerabilidades importadas. As seguintes calculadoras de rollup são enviadas com o sistema de base:

- *`Remediation Task Rollup`*: Acumula as pontuações de risco de todos os itens vulneráveis em tarefas de correção para fornecer uma pontuação de risco geral para todo o grupo de itens vulneráveis.
- *`Patch Update Rollup`*: Acumula as pontuações de risco de todos os itens vulneráveis com a mesma atualização de patch para fornecer uma pontuação de risco geral para a atualização de patch.
- *`Organization Risk Score Rollup`*: Acumula as pontuações de risco de todos os itens vulneráveis do host, itens vulneráveis à aplicação, itens vulneráveis ao contêiner e problemas de configuração em uma organização, para fornecer uma pontuação de risco geral para toda a organização no painel unificado.

  Nota: A partir da v22.0 de Resposta a vulnerabilidades, você pode configurar pesos de acúmulo para pontuação organizacional. Calculadoras de roll-up individuais foram removidas.

- *`Vulnerable Item Rollup`*: Acumula as pontuações de risco de todos os itens vulneráveis do host em uma organização para contribuir com a pontuação de risco geral de toda a organização para o painel unificado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- *Vulnerability Entry Rollup*: Acumula as pontuações de risco de todos os itens vulneráveis com a mesma entrada de vulnerabilidade para fornecer uma pontuação de risco geral para a entrada de vulnerabilidade.
- *Rollup EPSS Scores from NVD to TPEs*: Acumula as pontuações de EPSS para todos os itens vulneráveis/CVEs listados no NVD tabela Para TPEs existentes, para fornecer uma probabilidade geral da vulnerabilidade ser explorada.
- *Remediation Effort Rollup*: Acumula as pontuações de risco de todos os registros em um esforço de correção para fornecer uma pontuação de risco geral para o esforço de correção.

Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Calculadora de Rollup de Vulnerabilidade**.

Configure a calculadora de acúmulo para especificar quanto peso atribuir a cada um desses valores calculados na definição da pontuação de risco cumulativa. Quanto maior o peso, mais esse valor será usado para determinar a pontuação de risco acumulada nas tarefas de vulnerabilidade ou correção.

Nota: Quando **Incluir adiado** estiver selecionado, todos os itens vulneráveis adiados serão incluídos no cálculo de acúmulo das tarefas de correção. Certifique-se de entender o impacto no cálculo total antes de selecionar esta opção.

Calculadoras de acúmulo executam o trabalho agendado, *Rollup vulnerable item values to vulnerability and groups*a cada 15 minutos para selecionar mudanças e acumular os detalhes e pontuações de risco para tarefas de correção e vulnerabilidades. Esses trabalhos agendados também calculam valores cumulativos para o número de VIS, pontuação máxima de risco, data de destino de correção e status das tarefas de correção.

Nota: Os valores calculados para entradas de vulnerabilidade não incluem dados de destino de correção.

A pontuação de risco é calculada quando:

- A pontuação de risco, o destino de correção, o status de correção ou as mudanças de vulnerabilidade nos itens vulneráveis.
- O estado do item vulnerável muda para Aberto, Adiado, Encerrado ou muda de Encerrado ou Adiado.
- Itens vulneráveis são excluídos.
- Itens vulneráveis são adicionados ou removidos da tarefa de correção.

Exemplo de calculadora de acúmulo de vulnerabilidades: Considere uma tarefa de correção VUL324533, que tem os seguintes itens vulneráveis:

- VIT1001 com pontuação de risco de 30
- VIT1002 com pontuação de risco de 40
- VIT1003 com pontuação de risco de 50

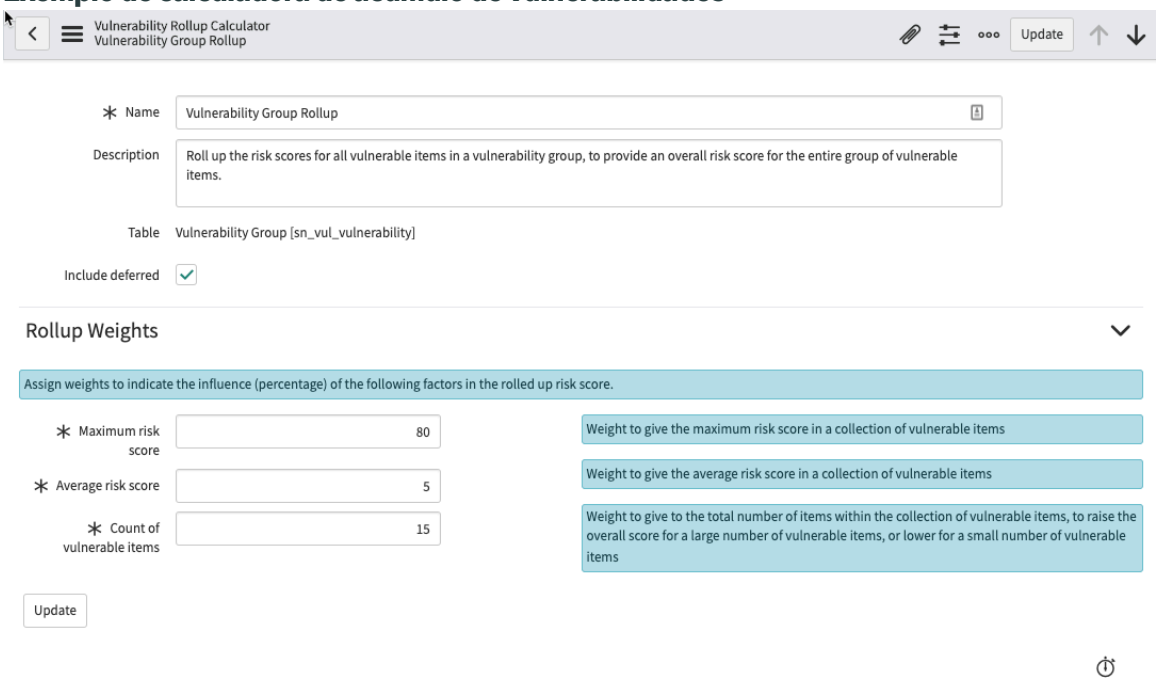
Considere também os seguintes pesos na calculadora de acúmulo de vulnerabilidades:

- Pontuação máxima de risco: 80
- Pontuação média de risco: 5
- Contagem de itens vulneráveis: 15

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de calculadora de acúmulo de vulnerabilidades



No exemplo da calculadora de acúmulo de vulnerabilidades, a fórmula para determinar a tarefa de correção **Pontuação de risco** :

(**Pontuação de risco máxima** * 100) * 80 (**Pontuação média de risco** * 100) * 5 ou mais (fator * 15)

O fator é determinado da seguinte forma:

Contagem de IV	Fator
Menos de 10	0,2
10-100	0,4
101-1000	0,6
1001-10000	0,8
> 10000	1

Para a tarefa de correção, VUL324533:

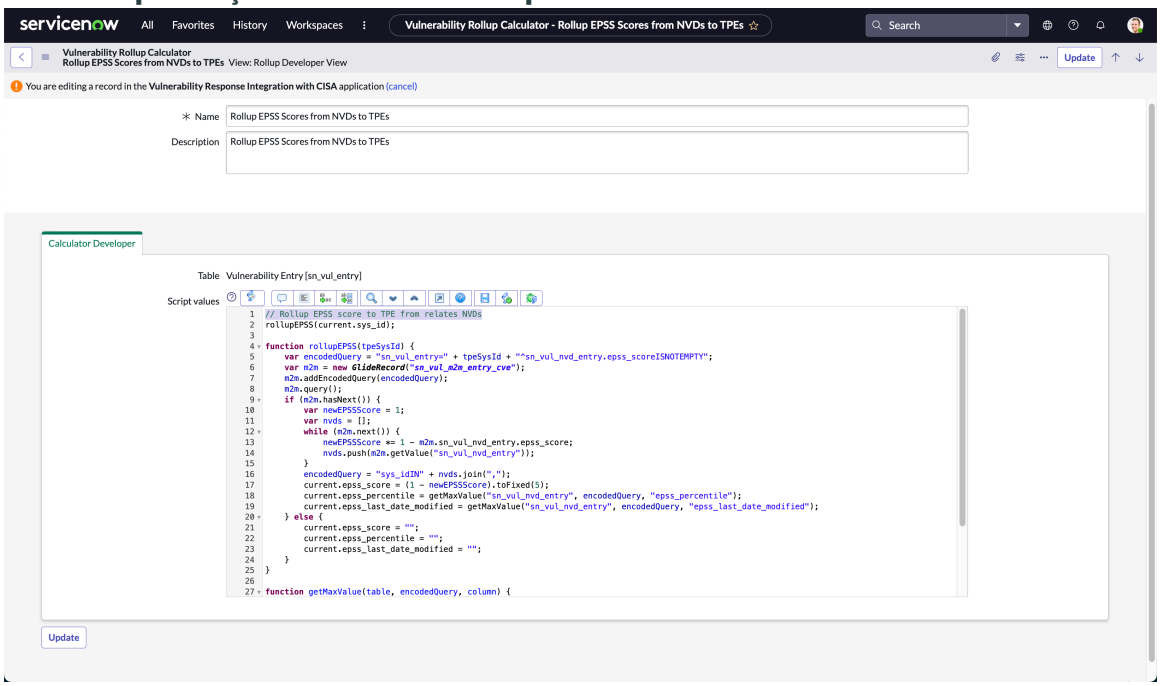
- A pontuação média de risco é 40
- A pontuação máxima de risco é 50
- 50 (pontuação de risco máxima)
- O fator é 0,2

. **Pontuação de risco** 45 [(50/100) * 80 (40/100) * 5 * 0,2 * 15: 40 e 2: 3: 45]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acumular pontuações de EPSS de NVDs para TPEs



Calculadora de acúmulo de EPSS - Exemplo

Por exemplo, considere uma organização com 100 vulnerabilidades, cada uma com 5% de chance de ser explorada. A questão de grande interesse para um defensor de rede pode ser: Qual é a probabilidade de que pelo menos uma dessas vulnerabilidades seja explorada e, portanto, qual é a minha ameaça geral? Pelo menos um evento ocorre é simplesmente o complemento (oposto) de nenhum evento ocorrendo, ou seja:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Em que, a probabilidade de nenhuma vulnerabilidade é o produto linear de cada vulnerabilidade não sendo explorada. Cada vulnerabilidade tem 5% de chance de ser explorada, cada uma delas tem 95% de chance de não ser explorada. E como há 100 deles, podemos escrever isso como:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

Que diz que a probabilidade de pelo menos uma das vulnerabilidades ser explorada é de 99,4%.

Importante: Para modificar *`Rollup EPSS Scores from NVD to TPEs`*, Você precisa alternar a exibição do menu de contexto do formulário para **Rollup do Desenvolvedor** em **Exibição padrão** .

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Após a avaliação inicial das regras de destino de correção no Assistente de configuração, os gerentes de vulnerabilidades podem configurar uma regra de destino de correção no nível do item vulnerável para orientar a correção de vulnerabilidades de alto risco em tempo hábil. Quando a data de correção de um item vulnerável se aproxima, uma notificação é enviada para os usuários ou grupos especificados na regra.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de meta da correção**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os itens vulneráveis devem ser corrigidos, desde a última abertura.
V17.1: Meta de (data)	Data a partir da qual os ANS de destino são calculados. Você pode especificar somente os campos de data ou de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1642413 .
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra de destino de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes do tempo de correção de destino para que uma notificação seja enviada. A data de notificação calculada usando este valor é usada para mostrar o status de correção e a codificação por cores. Se a data for anterior à data da notificação, o status da correção será "Em andamento". Se a data de notificação for anterior à data de destino de correção, o status será mostrado como Meta de aproximação. **Nota:** Se este campo estiver definido como 0, somente um **Meta perdida** a notificação foi enviada.
Descrição	Texto que descreve a regra de destino de correção.
Condição	Usando o filtro de condição, selecione os critérios para aplicar a regra aos itens vulneráveis. Para evitar impacto no desempenho, teste suas condições em escala de produção total. O teste permite que você determine por quanto tempo **Avalie os destinos de correção** o trabalho leva para ser executado, dadas as condições e o tamanho do seu Configuration Management Database (CMDB). A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Notificações **Nota:** A contagem mostrada no e-mail de notificação não inclui itens vulneráveis em **Adiado** , **Resolvido** ou **Encerrado** estado.	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usuários	As pessoas a serem notificadas quando o item vulnerável selecionado estiver se aproximando ou passar no tempo de meta de correção direcionado.
Grupo	O grupo a ser notificado quando o item vulnerável selecionado estiver se aproximando ou passar pelo tempo de destino de correção.
Atualizar histórico	
	Não usado para a criação inicial de uma regra. Em seguida, as anotações de trabalho do sistema são registradas aqui.

4. Clique em **Enviar**.
   Esta regra entra em vigor durante a próxima execução do trabalho agendado, *`Evaluate remediation targets`*ou ao usar **Aplicar mudanças** Botão na exibição de lista Regras de destino de correção. O mesmo acontece quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho agendado e. **Aplicar mudanças** , consulte Resposta a vulnerabilidades regras de destino de correção.

Configure integrações de terceiros instaladas usando o Assistente de configuração

Configure o Vulnerability Response para funcionar com cada uma das implantações de aplicações de terceiros instaladas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração**.
2. Selecione **Integrações do scanner** para configurar implantações de aplicações de terceiros instaladas.
3. Se Solução de gestão de Resposta a vulnerabilidades instalado, você pode selecionar **Integrações de soluções** para configurar seus provedores de solução de vulnerabilidade.

Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade Usando o Assistente de configuração

Depois de instalar a aplicação Gestão de soluções de vulnerabilidade, você pode configurar seus provedores de solução de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Use as seções a seguir para complementar as instruções e prompts fornecidos no Assistente de configuração para integrações de soluções instaladas para Solução de gestão de Resposta a vulnerabilidades.

- Verifique se você já instalou Solução de gestão de vulnerabilidade e as integrações de solução que você deseja antes de começar. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
- Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações antes de configurar as soluções instaladas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**.

   . Integração com a solução Microsoft Security Response Center Requer uma chave de API e URL do Microsoft Security Response Center para configurá-lo.

   Nota: Inserir a chave de API é opcional para MSRC. Para obter o. MSRC, você deve ter um ID da Microsoft de uma conta de e-mail live.com, outlook.com ou Microsoft.com, um número de telefone registrado na Microsoft ou um login do Skype.

2. Insira o URL.
   O URL no Assistente de configuração para MSRC é https://api.msrc.microsoft.com .
3. Clique em **Concluir**.
4. **Opcional:** Você pode executar importações sob demanda clicando em **Executar agora** na página de configuração depois de inserir suas credenciais.
5. . Red Hat Solution Integration também está disponível.
   Não requer uma chave de API.
6. No Assistente de configuração, à direita de Red Hat Solution Integration clique em **Editar** .
7. Verifique o URL no Assistente de configuração para RHSI. https://access.redhat.com/hydra/rest
8. **Opcional:** Você pode executar importações sob demanda clicando em **Executar agora** na página de configuração.
9. Clique em **Concluir** seguido por **Marcar como concluído** para concluir a configuração.
   Uma marca de seleção será exibida no Assistente de configuração para integrações de soluções quando você concluir a configuração.

Configure a Integração de vulnerabilidades do MS TVM usando o Assistente de configuração

Configure o. Resposta a vulnerabilidades Integração com a aplicação Microsoft Threat and Vulnerability Management (MS TVM), depois de instalá-lo usando o Assistente de configuração.

Antes de Iniciar

Além das instruções e avisos fornecidos no Assistente de configuração do Resposta a vulnerabilidades Integração com a integração do Microsoft Threat and Vulnerability Management, execute as seguintes ações:

- Antes de começar, verifique se você já instalou a aplicação. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.
- Consulte Preparando-se para a Integração de vulnerabilidades do Microsoft Threat and Vulnerability Management Para obter mais informações antes de configurar a integração do Microsoft Threat and Vulnerability Management para Resposta a vulnerabilidades.
- Verifique se você tem credenciais de conta MS TVM disponíveis. Para obter essas credenciais, consulte Configurar Microsoft Integração do Azure para MS TVM.

Funções necessárias: Administrador do sistema (admin) para instalação, Administrador de vulnerabilidades (sn_vul.vulnerability_admin) ou sn_vul.admin (descontinuado) e Configurar integração (sn_vul_msft_tvm.configure_integration) para configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   O bloco Gestão de ameaças e vulnerabilidades da Microsoft é exibido.

   O MS TVM é uma integração de várias origens, o que significa que você pode ter várias implantações da mesma integração de terceiros. As configurações da integração de terceiros original são usadas como um modelo para as configurações de cada nova integração.

   Nota: Se você excluir a integração de vulnerabilidade original, será necessário selecionar outra integração para usar como modelo. Desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

   Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância do Resposta a vulnerabilidades.

2. Para configurar a integração do Microsoft Threat and Vulnerability Management, clique em **Editar** .

3. No formulário, preencha os campos.

Formulário Credenciais da conta

Campo	Descrição
Nome	Nome da instância.
Região de TVM	Região próxima do local do servidor. Use o servidor mais próximo do seu local para obter o desempenho ideal da API.
Tipo de autenticação	Método para verificar a identidade. A autenticação do usuário controla a visibilidade de ativos específicos para usuários específicos. O MS TVM exporta os grupos de dispositivos atribuídos a este usuário. O valor padrão é Aplicação.
ID de locatário	Identidade do locatário da sua organização.
ID de cliente	Identidade do cliente gerada após o registro do MS TVM no Microsoft Azure.
Nome do usuário	Usuário que tem acesso ao grupo de dispositivos completo. Este campo aparece somente quando Usuário é selecionado no tipo Autenticação.
Senha	Senha do nome de usuário que tem acesso ao grupo de dispositivos completo. Este campo aparece somente quando Usuário é selecionado no tipo Autenticação.
Segredo do cliente	Segredo do cliente gerado após o registro da aplicação MS TVM. Este campo aparece somente quando a aplicação é selecionada no tipo Autenticação.

4. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Próximo** .
   O formulário Configuração de importação de vulnerabilidades é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Habilite ou desabilite a importação de vulnerabilidades, determine a data de início inicial das vulnerabilidades que você deseja importar e programe quando a importação de vulnerabilidades do MS TVM deve ser executada.
   Se você quiser importar todas as vulnerabilidades, deixe a data de início inicial em branco.
   a. Para importar dados sob demanda, clique em **Importar vulnerabilidades agora** .
   b. Para ver o registro de integração, clique em **Configurações avançadas** .
6. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Próximo** .
   O formulário Configuração de importação de recomendações é exibido.
7. Habilite ou desabilite a importação de recomendações e determine a programação em que a importação de vulnerabilidades do MS TVM deve ser executada.
   a. Para importar dados sob demanda, clique em **Importar recomendações agora** .
   b. Para ver o registro de integração, clique em **Configurações avançadas** .
8. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Próximo** .
   O formulário Configuração de importação de máquinas é exibido.
9. Habilite ou desabilite a importação de máquinas, determine a data de início inicial das máquinas que você deseja importar e programe quando a importação de máquinas MS TVM deve ser executada.
   Se você quiser importar todas as máquinas, deixe a data de início inicial em branco.

   Nota: Os marcadores de máquina são importados por padrão e usados para organizar e rastrear as máquinas listadas no ambiente MS TVM.

   a. Para exibir as regras de pesquisa de item de configuração (IC) padrão, clique em **Regras de pesquisa de IC** . As regras de pesquisa de IC definem como os dados de máquina de fontes de terceiros são usados para identificar itens de configuração (ICs) no ServiceNow AI Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.
   b. Para importar dados sob demanda, clique em **Importe máquinas agora** .

      Nota: As máquinas que têm o status como integrado no MS TVM são recuperadas pela aplicação ServiceNow.

   c. Para ver o registro de integração, clique em **Configurações avançadas** .
10. Para salvar suas mudanças e ir para o primeiro formulário de integração, clique em **Próximo** .
    O formulário Configuração de importação de vulnerabilidades da máquina é exibido.
11. Habilite as integrações a seguir e determine a data de início inicial das vulnerabilidades que você deseja importar.

Formulário Configuração de importação de vulnerabilidades da máquina

Integração	Descrição
Importação delta de vulnerabilidades da máquina com Microsoft TVM	Recupera vulnerabilidades que foram atualizadas durante a importação completa de vulnerabilidades, incluindo vulnerabilidades novas, corrigidas e atualizadas. Você só pode importar dados delta dos últimos 14 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Importação completa de vulnerabilidades da máquina com Microsoft TVM	Recupera todas as vulnerabilidades em aberto. Devido ao alto volume de importação de dados, você pode programá-lo para execução semanal.

Nota:

Execute a importação de máquinas antes da integração de vulnerabilidades da máquina. Os VIS não são criados para as máquinas ausentes.

12. Para salvar suas mudanças e concluir a configuração no Assistente de configuração, clique em **Concluir** .

O que Fazer Depois

Se você quiser ativar um agrupamento de itens vulneráveis no ambiente clássico, navegue até > **Resposta a vulnerabilidades** > **Administração** > **Regras de tarefa de correção** > **Recomendação do Microsoft TVM**.

No formulário exibido, selecione **Ativo** opção para ativá-lo. Como alternativa, selecione **Novo** para criar uma nova regra.

Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção.

Configure o. Qualys Vulnerability Integration Usando o Assistente de configuração

Depois de instalar o. Qualys, configure-o usando o Assistente de configuração.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e prompts fornecidos no Assistente de configuração para configurar o. Qualys Vulnerability Integration.

- Antes de começar, verifique se você já instalou a aplicação. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.
- Consulte Preparando para Qualys Vulnerability Integration para obter mais informações antes de configurar o. Qualys Vulnerability Integration.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar alguns aplicativos de terceiros.

Funções necessárias: Administrador do sistema (admin) para instalação, Administrador de vulnerabilidades (sn_vul.vulnerability_admin) ou sn_vul.admin (descontinuado) para configuração.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
   As integrações instaladas são exibidas.
2. Clique em **Editar** à direita do Qualys Vulnerability Integration que você deseja configurar.
3. No formulário Credenciais da conta, insira seu Qualys Cloud Platform credenciais.
   Suas credenciais são necessárias para configurá-lo.
4. Use as anotações a seguir como um guia ao continuar com a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- . **Configurações avançadas** o link direciona você para Qualys Registro de integração. Você pode adicionar parâmetros compatíveis com Qualys produto para suas consultas programadas para ajudar você a filtrar os dados de vulnerabilidade importados. Consulte Defina parâmetros de filtro adicionais para Qualys importações para obter mais informações.
- Se você fez upgrade de uma versão anterior de Resposta a vulnerabilidades com uma versão do Qualys Vulnerability Integration essa versão, com suas definições de configuração preservadas, ainda está disponível.

  Em Configurações de importação em Configuração de detecção de host para Qualys Vulnerability Integration há uma opção para exibir fixo Qualys registros de detecção de vulnerabilidades. Se habilitado, isso permitirá que você crie itens vulneráveis a partir de registros de detecção em um status fixo (estado **Corrigido**). Para obter mais informações sobre detecções de itens vulneráveis, consulte Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros.

  Você pode ativar o. **Pesquisa por partição de rede** Caixa de seleção na página Configuração de detecção de host para incluir o identificador da partição de rede na pesquisa de endereço IP. Para obter mais informações, consulte Atualize itens de configuração com o identificador de partição de rede para Qualys Vulnerability Integration.

  Todos os marcadores de host são importados como parte do Qualys Integração da lista de hosts. Marcadores de host são usados principalmente para filtragem no Resposta a vulnerabilidades Regras de tarefa de atribuição e correção. Eles são exibidos no formulário Item descoberto.

  Nota: . Qualys A integração da Lista de hosts deve ser executada antes de criar regras de tarefa de atribuição ou correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

  Qualys **Etiquetas do ativo** São armazenados no módulo de marcadores de host em Qualys Vulnerability Integration.

- . Qualys Vulnerability Integration compatível com várias origens. Você pode ter várias implantações da mesma integração de terceiros. Para adicionar outra integração, na página Integrações do scanner, clique em **Adicionar integração** .

  As configurações da integração de terceiros original são usadas como um modelo para as configurações de cada nova integração.

  Nota: Se você excluir a integração de vulnerabilidade original, será necessário selecionar outra integração para usar como modelo. Desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

  Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância do Resposta a vulnerabilidades.

- Você pode executar importações sob demanda clicando em **Executar agora** em uma página de configuração.

5. Clique em **Concluir** Para concluir a configuração no Assistente de configuração.

Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração

Depois de instalar o. Integração de Resposta a vulnerabilidades com Tenable, configure-o usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e prompts fornecidos no Assistente de configuração do Integração de Resposta a vulnerabilidades com Tenable integração.

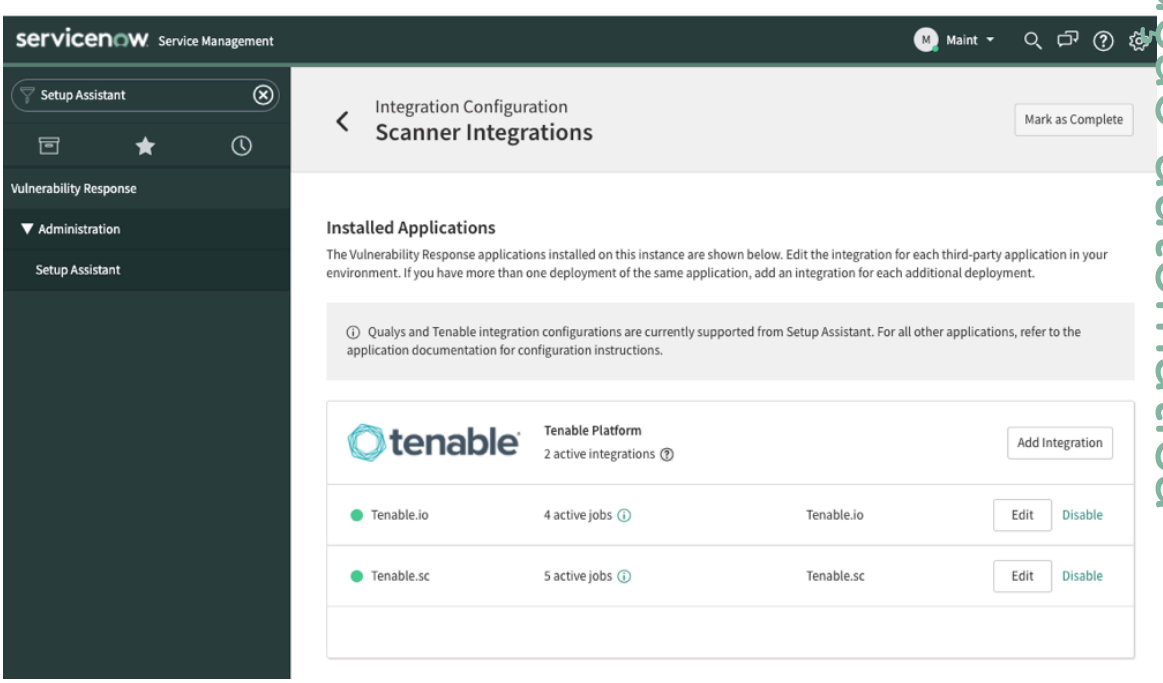
- Antes de começar, verifique se você já instalou a aplicação. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.
- Consulte Preparando para a Integração de vulnerabilidades do Tenable para obter mais informações antes de configurar o. Tenable para Resposta a vulnerabilidades.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar alguns aplicativos de terceiros.

Funções necessárias: Administrador do sistema (admin) para instalação, Administrador de vulnerabilidades (sn_vul.vulnerability_admin) ou sn_vul.admin (descontinuado) e Configurar integração (sn_vul_tenable.configure_integrations) para configuração.

Procedimento

1. Se não for exibido, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   . Tenable.io, Tenable.sc e Tenable.csas integrações são exibidas.



   O Tenable é uma integração de várias origens e você pode ter várias implantações da mesma integração de terceiros. As configurações da integração de terceiros original são usadas como um modelo para as configurações de cada nova integração.

   Nota: Se você excluir a integração de vulnerabilidade original, será necessário selecionar outra integração para usar como modelo. Desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

   Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância do Resposta a vulnerabilidades.

2. À direita da integração do Tenable que você deseja configurar, selecione **Editar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário Credenciais da conta, preencha os campos.

- Tenable.io Requer acesso de administrador com um atributo de permissão maior ou igual a 64.

  Nota: A partir da v3.8 de Integração de Resposta a vulnerabilidades com Tenable acessando Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

- Tenable.sc Requer acesso de analista de segurança ou gerente.
- Tenable.cs Requer um token com acesso ao token Gerar da plataforma Tenable CS.

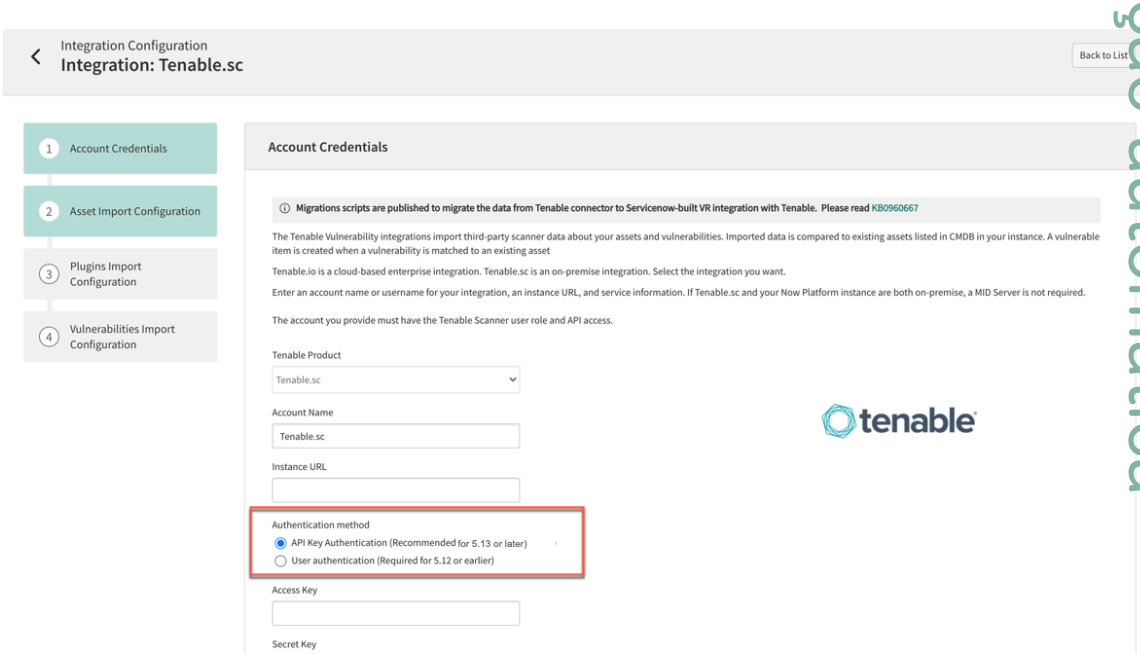
a. Selecione seu produto Tenable.

b. Insira o nome da sua conta Tenable.

c. No campo URL da instância, insira o URL da sua plataforma Tenable.

d. Selecione um método de autenticação (em caso de Tenable.cs, prossiga para a etapa f) .

Com base em sua versão de Tenable.sc, você tem duas opções de autenticação:



i. A partir da v5.13 de Tenable.sc, selecione **Autenticação de chave de API** . Insira suas Chaves de acesso e segredo do Tenable.

ii. A autenticação de usuário anterior à versão 5.13 é compatível com ServiceNow AI Platform® a instância e é necessária. Insira seu ServiceNow AI Platform nome de usuário e senha.

Somente a autenticação de chave de API é compatível com Tenable.sc. Insira suas Chaves de acesso e segredo do Tenable.

e. Opcional: Selecione um MID Server.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) . ServiceNow AI Platform e seu Tenable.sc A aplicação não está no mesmo local, escolha um MID Server configurado na lista. Para obter mais informações, consulte MID Server .

- A partir da v15.0 de Resposta a vulnerabilidades e v3.0 do Integrações de vulnerabilidade da Tenable, você tem a opção de habilitar `Async_request`parâmetro conforme descrito em Configurações de recuperação de dados para a Integração de vulnerabilidades do Tenable. Se você quiser fazer chamadas síncronas, será necessária alguma configuração com o Tenable. Entre em contato com o produto Tenable para obter ajuda. Uma vez ativado, este parâmetro é aplicável a todas as integrações de Tenable.sc e há um tempo limite de 30 segundos. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

- (Optional) Para os clientes existentes, um script de correção estará disponível se você estiver usando chamadas assíncronas.

. ServiceNow AI Platform e seu Tenable.sc Ambas as aplicações são no local, embora não sejam obrigatórias, você tem a opção de selecionar um MID Server configurado na lista.

Nota: Se você optar por empregar um MID Server ou não, as integrações expiram após cinco minutos e uma mensagem é exibida quando não há resposta do servidor.

Se você receber um erro de tempo limite, no Assistente de configuração, verifique se você inseriu as credenciais e o URL corretos.

f. Insira o token da API.

Nota: Se você receber um erro para credenciais inválidas no Assistente de configuração, verifique se inseriu as credenciais e o URL corretos.

4. Selecione **Próximo** para salvar suas mudanças e prosseguir para o primeiro formulário de integração. Em caso de Tenable.io e. Tenable.sc, O formulário Configuração de importação de ativos é exibido. Em caso de Tenable.cs, O formulário Configuração de importação de ativos de contêiner é exibido.

Nota: O formulário Configuração de importação de ativos de contêiner ficará visível somente se Contêiner de Resposta a vulnerabilidades instalado.

5. Neste formulário, ative ou desative a Integração de importação de ativos, determine a data de início inicial dos ativos que você deseja importar e programe quando a importação de ativos do Tenable deve ser executada.

Para Tenable.io

- A integração de ativos pode ser usada com Tenable.io Resultados de conformidade e Integração de preenchimento de resultados de conformidade para importar dados de avaliação de configuração seguros sobre seus ativos para o. Conformidade de configurações aplicação.
- Versão 12,2 do Conformidade de configurações a aplicação será necessária em sua instância se você quiser importar e exibir esses dados de avaliação de configuração segura.

Consulte Conformidade de configurações dados importados para obter mais informações sobre quais dados são importados com essas integrações e onde eles são publicados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- . Tenable.io Integrações de preenchimento de resultados de conformidade e resultados de conformidade não são ativadas por padrão. Se você ativá-los, talvez prefira usar as configurações de programação padrão fornecidas. Consulte as etapas listadas abaixo para saber como localizar e ativar integrações para Integrações de vulnerabilidade da Tenable.
- Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Tenable.io produto da sua instância. . Tenable.io Integração de modelo e Tenable.io A integração de credenciais de verificação deve ser ativada antes de iniciar novas verificações.

Por padrão, essas integrações estão desativadas. Quando você insere suas credenciais para Tenable.io. todos Tenable.io as integrações são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

a. Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.

b. Na lista exibida, localize Tenable.io registros de integração desejados.

c. Abra cada registro e selecione **Ativo** caixa de seleção para ativar a integração.

d. Selecione **Atualizar** para salvar suas mudanças.

e. Retorne ao Assistente de configuração para continuar com a configuração do Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

- Para Tenable.io integração, você também tem a opção de ativar e desativar a importação de etiquetas de ativos. As etiquetas de ativo são importadas por padrão e usadas para organizar e rastrear os ativos listados em seu CMDB no Tenable.io ambiente.
- Para ambos Tenable.io e. Tenable.sc produtos, se você selecionar **Habilitar Pesquisa por partição de rede** Em Pesquisa por partição de rede, você pode criar ICs individuais usando o mecanismo de identificação e reconciliação (IRE) para seus ativos que têm o mesmo endereço IP. Para obter mais informações, consulte Atualize itens de configuração com o identificador de partição de rede para Integrações de vulnerabilidade da Tenable e Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação.
- Para Tenable.io e Tenable.sc na parte superior da tela ao lado do link Importação de ativo, selecione **Regras de pesquisa de IC** Link para exibir as regras de pesquisa de item de configuração (IC) padrão. As regras de pesquisa de IC definem como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) no ServiceNow AI Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.
- Selecione **Importe ativos agora** para importar dados sob demanda.
- . **Configurações avançadas** O link direciona você para o registro de Integração de ativos. A partir da v3.3, você pode adicionar parâmetros compatíveis com Tenable.io produto para suas consultas programadas para ajudar você a filtrar os dados de vulnerabilidade importados com Tenable.io E as Integrações de vulnerabilidades fixas e abertas. Consulte Defina parâmetros de filtro adicionais para Tenable.io importações para obter mais informações.

6. Selecione **Próximo** para salvar suas mudanças e prosseguir para o próximo formulário.

Nota: Em caso de Tenable.io e. Tenable.sc. Para Tenable.cs O formulário Configuração de importação de vulnerabilidades do host é exibido, continue a partir da etapa 9 para obter mais configurações do Tenable CS.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O formulário Configuração de importação de plug-ins é exibido.

7. Em Configuração de importação do plug-in Habilitar ou desabilitar a importação de plug-ins (entradas de vulnerabilidade de terceiros) Determine a data de início inicial dos plug-ins que você deseja importar e programe quando a importação de plug-ins Tenable deve ser executada.

   Se você quiser importar todos os plug-ins, vulnerabilidades e ativos, deixe a data de início inicial em branco.

   - Selecione **Importar plug-ins agora** para importar dados sob demanda.
   - . **Configurações avançadas** O link direciona você para o registro de integração de plug-ins.
   - Para a importação de vulnerabilidades, você pode programar e definir níveis de gravidade para Tenable.io para as vulnerabilidades que você deseja ingeridas. Determine uma data para que somente as vulnerabilidades criadas ou atualizadas começando com uma data específica sejam importadas.
   - Para Tenable.sc, você pode determinar um filtro de consulta e uma data para que somente as vulnerabilidades criadas ou atualizadas começando com uma data específica sejam importadas.

8. Selecione **Próximo** para salvar suas mudanças e prosseguir para o próximo formulário.
   O formulário Configuração de importação de vulnerabilidades é exibido. Habilite ou desabilite a integração e determine a data de início inicial das vulnerabilidades que você deseja importar.

   Para Tenable.io produto:

   - Importe somente as vulnerabilidades e os VIS associados que correspondam às condições escolhidas com o filtro de gravidade.
   - Para Tenable.io integração de ativos, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
   - Habilite o. **Vulnerabilidades corrigidas** Opção para exibir VIS para registros de detecção fixos. Se este sinalizador estiver habilitado no Assistente de configuração, novos VIS serão criados para detecções no **Corrigido** estado que não existe em sua instância. Quando habilitado, este recurso pode afetar negativamente o desempenho de ingestão.
   - . **Configurações avançadas** O link ao lado de Importar filtros direciona você para o registro Integração de vulnerabilidades.
   - Selecione **Cronogramas de importação** link na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.

   Para Tenable.sc produto:

   - Importe somente as vulnerabilidades e os VIS associados que correspondem aos filtros de condição definidos por uma consulta do Tenable na plataforma Tenable. Consulte a documentação do Tenable para obter mais informações sobre consultas do Tenable.

     O filtro de consulta do Tenable selecionado no Assistente de configuração também se aplica ao Tenable.sc Integração de ativos. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.

   - Habilite o. **Vulnerabilidades corrigidas** Opção para exibir VIS para registros de detecção fixos. Se este sinalizador estiver ativo no Assistente de configuração, novos VIS serão criados para detecções no **Corrigido** estado que não existe em sua instância. Quando ativo, este recurso pode afetar negativamente o desempenho de ingestão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para incluir o identificador da partição de rede na pesquisa de endereços IP, selecione **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede** seção. Para obter mais informações, consulte Atualize itens de configuração com o identificador de partição de rede para Integrações de vulnerabilidade da Tenable.
- Selecione **Cronogramas de importação** na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.
- . **Configurações avançadas** O link ao lado de Importar filtros direciona você para o registro Integração de vulnerabilidades.
- . ServiceNow® Tenable.sc A integração de credenciais de verificação está habilitada (Ativo Automaticamente de dentro do Assistente de configuração na sua instância quando você configura o. Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades em aberto e corrigido).

  Esta integração importa e atualiza as credenciais do scanner do Tenable.sc produto em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais do Tenable. Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Integrações** > **Integração de credenciais de verificação do Tenable.sc** Para exibir mais informações sobre a Integração de credenciais de verificação.

9. Selecione **Próximo** Na etapa Configuração de importação de ativos de contêiner.
   O formulário Configuração de importação de vulnerabilidades do host é exibido. Habilite ou desabilite a integração.
   - Importe somente as vulnerabilidades e os VIS associados que correspondam às condições escolhidas com o filtro de gravidade.
   - O link Configurações avançadas ao lado de Importar filtros direciona você para o registro Integração de vulnerabilidades.
   - Selecione o link Cronogramas de importação na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.
   - Na parte superior da tela ao lado do link Cronogramas de importação, selecione o link Regras de pesquisa de IC para exibir as regras de pesquisa de item de configuração padrão (IC). As regras de pesquisa de IC definem como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) no ServiceNow AI Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de integrações de vulnerabilidades de terceiros do Resposta a vulnerabilidades.

10. **Nota:** Esta etapa é somente para Tenable.cs Produto.

    Selecione Avançar para salvar suas mudanças e prosseguir para o próximo formulário.
    - Importe somente as vulnerabilidades do contêiner e o CVIS associado que correspondam às condições escolhidas com o filtro de gravidade.
    - O link Configurações avançadas ao lado de Importar filtros direciona você para o registro Integração de vulnerabilidades.
    - Selecione o link Cronogramas de importação na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.
    - A Configuração de importação de vulnerabilidades do contêiner será vista somente se o Resposta de vulnerabilidade do contêiner estiver instalado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O formulário Configuração de importação de vulnerabilidades de contêiner é exibido. Habilite ou desabilite a integração.

11. Selecione **Concluir** Para salvar suas mudanças e concluir a configuração no Assistente de configuração.

O que Fazer Depois

(Opcional) Navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de Vulnerabilidade** > **Calculadora de Risco Padrão** > **Regra de risco da Tenable** Para habilitar a Regra de Risco da Tenable.

No formulário Regra da calculadora de vulnerabilidades exibido, marque a caixa de seleção Ativo para habilitá-lo.

A Regra de Risco do Tenable é instalada com Integração de Resposta a vulnerabilidades com Tenable Aplicação como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidades de Resposta a vulnerabilidades. A Classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable importado e usado com a nova calculadora de risco padrão. Esta regra de risco está desativada por padrão. Ao habilitar a regra da calculadora de risco do Tenable, os valores de VPR importados são usados para calcular a Pontuação de risco para itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR é 70%, Ativo é 15% e Criticalidade dos negócios é 15%. Habilitar esta regra da Calculadora de risco do Tenable pode afetar o desempenho de ingestão de dados.

Veja Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade

Configurar provedores de solução de vulnerabilidade

Configure provedores de solução de vulnerabilidade seguindo a check-list e configurando os provedores no Assistente de configuração.

Preparar check-list de integração da solução

Use o Assistente de configuração para se preparar para implementar uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados CVRF (Common Vulnerability Reporting Framework) ou CSAF (Common Security Advisory Framework).

Preparando a integração da solução Common Vulnerability Reporting Framework (CVRF)

Use o Assistente de configuração para se preparar para implementar uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados CVRF (Common Vulnerability Reporting Framework).

Antes de começar

Para integrar com os fornecedores que fornecem as soluções, certifique-se de executar as tarefas na check-list a seguir. Você pode imprimir a check-list e verificar se os itens listados estão concluídos antes de instalar a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Aplicações dependentes ☐	Verifique se os seguintes aplicativos estão instalados a partir do ServiceNow Store: • Vulnerability Solution Management: Para obter mais informações sobre como instalar Solução de gestão de vulnerabilidade, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração e. Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. • Resposta a vulnerabilidades: Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,1 de Resposta a vulnerabilidades ou posterior.
Credenciais de conta de terceiros ☐	Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
Autenticação do fornecedor ☐	Verifique se você autenticou os fornecedores para importação de soluções usando as APIs. Para obter mais informações sobre como autenticar fornecedores, consulte Configure aliases de conexão e credencial. Se você não quiser configurar um fornecedor baseado em API, poderá ignorar esta etapa.
Personalização do fluxo e da ação do fluxo ☐	Se você quiser configurar um fornecedor baseado em API diferente da Cisco, personalize o fluxo e a ação de fluxo para extrair uma chave exclusiva e uma URL CVRF da resposta de um comunicado. **Nota:** Publicar URL do CVRF não é padrão entre os fornecedores. Para personalizar o fluxo para fornecedores diferentes da Cisco, consulte Configure um fornecedor do Common Vulnerability Reporting Framework diferente da Cisco. Você pode ignorar esta etapa se eles não quiserem configurar outros fornecedores além da Cisco. Por padrão, o fluxo da Cisco foi enviado com a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Funções ☐	Verifique se você tem um grupo de administradores ou usuário que pode gerenciar a integração. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções.

Preparando a integração da solução Common Security Advisory Framework (CSAF)

Use o Assistente de configuração para se preparar para implementar uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados Common Security Advisory Framework (CSAF).

Antes de começar

Para integrar com os fornecedores que fornecem as soluções, certifique-se de executar as tarefas na check-list a seguir. Você pode imprimir a check-list e verificar se os itens listados estão concluídos antes de instalar a aplicação.

Check-list de preparação da integração

Tarefa	Descrição
Aplicações dependentes ☐	Verifique se os seguintes aplicativos estão instalados a partir do ServiceNow Store: • Vulnerability Solution Management: Para obter mais informações sobre como instalar Solução de gestão de vulnerabilidade, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração e. Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. • Resposta a vulnerabilidades: Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,1 de Resposta a vulnerabilidades ou posterior.
Credenciais de conta de terceiros ☐	Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Autenticação do fornecedor ☐	Verifique se você autenticou os fornecedores para importação de soluções usando as APIs. Para obter mais informações sobre como autenticar fornecedores, consulte Configurar aliases de conexão e credencial para o Common Security Advisory Framework (CSAF). Se você não quiser configurar um fornecedor baseado em API, poderá ignorar esta etapa.
Personalização do fluxo e da ação do fluxo ☐	Se você quiser configurar um fornecedor baseado em API diferente de Red Hat, Em seguida, você deve personalizar o fluxo e a ação de fluxo para extrair uma chave exclusiva e a URL do CSAF da resposta de um comunicado. **Nota:** Publicar URL do CSAF não é padrão entre os fornecedores. Para personalizar o fluxo para outros fornecedores que não Red Hat, consulte Configure um fornecedor do Common Security Advisory Framework diferente de Red Hat. Você pode ignorar esta etapa se eles não quiserem configurar fornecedores diferentes de Red Hat. Por padrão, o fluxo para Red Hat foi enviado com a aplicação.
Funções ☐	Verifique se você tem um grupo de administradores ou usuário que pode gerenciar a integração. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções.

Configurar provedores de solução de vulnerabilidade

Depois de instalar a aplicação Gestão de soluções de vulnerabilidade, configure os provedores de solução de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração**.
2. Clique em **Integrações de soluções** .
3. Em Soluções instaladas Busque dados usando uma URL, uma API ou uma importação.
   - Para buscar dados usando uma URL ou API, clique em **Adicionar integração** .
   - Para buscar dados carregando um Common Vulnerability Response Framework (CVRF) Ou arquivo Common Security Advisory Framework (CSAF) clique em **Arquivo de importação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Dependendo de qual formato você deseja importar o. dados em , você pode executar uma das seguintes tarefas:

- Para CVRF:
  - Se você quiser importar um arquivo CVRF, consulte Importe dados do Common Vulnerability Reporting Framework por meio da importação de arquivos.
  - Se você quiser importar dados de CVRF usando as APIs, consulte Importe dados do Common Vulnerability Reporting Framework (CVRF) por meio da URL do CVRF.
  - Se você quiser importar dados de CVRF por meio de avisos, consulte Importe dados do Common Vulnerability Reporting Framework de comunicados.
- Para CSAF:
  - Se você quiser importar um arquivo CSAF, consulte Importe dados do Common Security Advisory Framework por meio da importação de arquivos.
  - Para importar dados do CSAF usando as APIs, consulte Importe dados do Common Security Advisory Framework (CSAF) por meio da URL do CSAF.
  - Se você quiser importar dados do CSAF por meio de avisos, consulte Importe dados da Estrutura de consultoria de segurança comum dos comunicados.
-

Common Vulnerability Reporting Framework (CVRF)

O Common Vulnerability Reporting Framework (CVRF) oferece uma estrutura padronizada para a criação de documentação de relatório de vulnerabilidade. É uma linguagem baseada em XML que simplifica o compartilhamento de informações cruciais relacionadas à segurança entre diversas partes interessadas em várias organizações. Ao utilizar o formato CVRF, a troca e o processamento de informações podem ser acelerados.

Importe dados do Common Vulnerability Reporting Framework por meio da importação de arquivos

Importe um arquivo CVRF para exibir dados no formato CVRF. A importação é uma atividade única.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin.

Por Que e Quando Desempenhar Esta Tarefa

Uma vez importada, uma entrada de fila é criada com um anexo, que é analisado quando a entrada é processada. Os dados são preenchidos nas respectivas tabelas. Antes de analisar os dados de CVRF, um registro de mapeamento de scanner é criado com base na configuração. Em seguida, os dados de mapeamento do scanner são transformados em dados de mapeamento do fornecedor.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique em **Arquivo de importação** .

> **Nota:** Você pode carregar apenas um arquivo XML por vez com um tamanho máximo de arquivo de 1 GB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Nome** , insira um nome exclusivo para a integração.
   O programador é criado com este nome.
4. Em **Fornecedor** , insira o nome do fornecedor.
   . **Origem** o campo das soluções é preenchido com o nome do fornecedor.
5. Clique em **Concluir**.

Resultado

Uma fila de importação é criada. Clique no link na barra de informações para exibir as entradas da fila do fornecedor junto com a lista relacionada. Você também pode exibir o status do trabalho.

Depois que os dados são importados para o formato CVRF, os dados são processados da seguinte maneira:

1. Quando a fila é processada, o arquivo é analisado com uma fonte de dados dedicada.
2. Quando o processamento é concluído, o log da aplicação é atualizado.
3. Depois que o arquivo XML CVRF é analisado, ele preenche as tabelas a seguir no ServiceNow® Resposta a vulnerabilidades aplicação.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Você pode ver as informações detalhadas relacionadas a erros ou exceções nos logs da aplicação.

Configure aliases de conexão e credencial

Configure aliases de conexão e credencial para autenticar fornecedores. Na análise de consultoria, os fornecedores de terceiros são autenticados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Procedimento

1. Criar autenticação OAuth.
   Consulte Crie um endpoint para os clientes acessarem a instância .
2. Crie um alias de conexão e credencial.
   Consulte Crie um alias de conexão e credencial .
3. Criar uma conexão.
   a. Clique no nome do alias de conexão e credencial recém-criado.
   b. Em **Conexões** clique em **Novo** .
   c. Se o tipo de autenticação for OAuth, selecione o Perfil de registro da aplicação criado na etapa 1 como **Perfil de entidade OAuth** .
   d. Crie um registro em Conexões na lista relacionada do registro.
   e. Em **Credencial** , selecione o registro de credencial criado na etapa 3d.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Em **URL de conexão** , insira o URL do fornecedor.

g. Clique em **Enviar**.

Configure um fornecedor do Common Vulnerability Reporting Framework diferente da Cisco

Configure um fornecedor CVRF (Common Vulnerability Reporting Framework) diferente da Cisco com suporte a API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Conexão e Credencial** > **Aliases de conexão e credenciais**.
2. Crie um registro com o tipo de autenticação compatível com o fornecedor.
   Para obter mais informações sobre como autenticar um fornecedor, consulte Configure aliases de conexão e credencial.
3. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Flow Designer**.
4. Duplique o fluxo chamado "Análise de consultoria".

   Nota:
   - Se alguma das ações precisar ser alterada, copie a ação e use-a no novo fluxo.
   - Atualize a lógica relacionada à paginação de acordo com o fornecedor

5. Se a lógica do parâmetro de intervalo de datas não for igual à Cisco, copie a ação **Atualizar parâmetros de paginação** e fazer mudanças conforme necessário para o fornecedor.
6. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Mapeamento de dados de aprimoramento**.
7. Crie um registro de acordo com a Cisco alterando **Chave de propriedade** valor de acordo com o fornecedor.
   Esta lógica serve para mapear campos obrigatórios de uma carga de consultoria para um ServiceNow tabela.
8. Mapeie os seguintes marcadores de API da Carga de API.
   Esses marcadores precisam ser mapeados com detalhes a serem preenchidos na tabela Mapeamento de dados de aprimoramento. Por padrão, o mapeamento específico da Cisco é enviado.

   Nota: Você precisa criar um registro se precisar configurar vários fornecedores que publicam comunicados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration	Descrição
URL do CVRF	cvrf_url	Nome do marcador que contém o URL do CVRF.
ID de aviso (chave exclusiva para resposta)	Id	Nome do marcador que contém um identificador exclusivo.
Data da última modificação	last_modified_date	Nome do marcador que contém a data em que o registro foi atualizado pela última vez.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration	Descrição
SecurityAdvisoryIntegrationSysId	integração	Refere-se ao SYSID do trabalho agendado de integração, que cria os registros de solução de vulnerabilidade.

9. Com base no formato de resposta, mude a lógica de análise copiando a ação **Recuperar lista** Do fluxo de Análise de consultoria.

Importe dados do Common Vulnerability Reporting Framework de comunicados

Importe dados de CVRF de comunicados configurando o URL do fornecedor com o tipo de importação como API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os avisos são obtidos. A URL CVRF e o ID dos avisos são extraídos da carga. As chamadas da REST API são feitas para cada URL CVRF e os dados são analisados e armazenados na tabela sn_vul_solution.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique em **Adicionar integração** .
3. No formulário, preencha os campos.

Importar formulário de avisos de solução

Campo	Descrição
Tipo de importação	Opção para selecionar o tipo de importação. Selecione **API** .
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** . **Origem** O campo das soluções é preenchido com o nome do fornecedor.
Alias de conexão	Opção para selecionar uma credencial autenticada. **Nota:** A tabela sys_alias armazena credenciais e o URL base para avisos.
Agendamento	Frequência na qual os dados devem ser atualizados.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Configuração de APIs	
Fluxo	Opção para selecionar o fluxo. O fluxo é acionado quando o programador é executado. O fluxo cuida da análise de avisos e extrai o URL do CVRF e armazena esses detalhes nas tabelas de atualização. Você pode copiar o fluxo existente e editar conforme necessário. Por exemplo, você pode fazer mudanças relacionadas à paginação.
Ação de fluxo	Opção para selecionar a ação de fluxo. As ações de fluxo tratam da capacidade da janela deslizante. Você pode atualizar as ações de fluxo e adicionar o parâmetro de consulta diretamente à ação arrastando.
Tabela de mapeamento	Opção para selecionar a tabela de mapeamento. O registro da Tabela de mapeamento de dados de aprimoramento é usado para extrair o URL CVRF e o ID de aviso da carga útil dos avisos.
Consultas de resposta	Opção para inserir o nome do marcador da carga útil de avisos de onde a lista de avisos pode ser extraída.
Critérios de filtro	
Parâmetros de intervalo de tempo	Opção para selecionar o intervalo de tempo da solicitação e o formato de data para chamadas de API. O parâmetro de solicitação Data de início/ Data de término é o nome do parâmetro usado para data de início e data de término durante chamadas de API. Por exemplo, StartDate , Start_date, endDate, end_date.
Formato de data	Opção para inserir o formato de data, como, dd/mm/aaaa. . O formato de data é o formato que a API precisa para filtragem. Formatos que não são compatíveis com GlideDate não funcionam.
Intervalo inicial em dias	E ner os dias para os quais os dados devem ser obtidos quando o programador é executado pela primeira vez.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para execuções subsequentes, o mecanismo da janela deslizante é seguido. **Nota:** Se você não quiser selecionar um intervalo de tempo, selecione **Nenhum parâmetro** .
Mapeamentos do scanner	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Clique em **Concluir**.

Importe dados do Common Vulnerability Reporting Framework (CVRF) por meio da URL do CVRF

Importe dados de CVRF configurando o URL do fornecedor no Assistente de configuração.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa
Quando a integração é executada, os dados são obtidos do URL que é analisado. Os dados são armazenados na tabela sn_vul_solution com origem como o nome do fornecedor.

Nota: A Oracle publica diretamente o URL do CVRF para fornecer soluções. Portanto, se você quiser configurar a integração para importar dados do Oracle, certifique-se de ter o URL do CVRF para Oracle e siga as etapas a seguir.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique em **Adicionar integração** .
3. No formulário, preencha os campos.

Importar formulário CVRF

Campo	Descrição
Tipo de importação	Tipo de importação. Selecione **URL** .
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** . **Origem** O campo das soluções é preenchido com o nome do fornecedor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL	URL da qual você deseja buscar os dados da solução no formato CVRF.
Agendamento	Frequência na qual os dados devem ser atualizados. **Nota:** Se o marcador de status do CVRF mostrar "FINAL", o campo será definido automaticamente como **Sob demanda** para evitar execuções desnecessárias.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.

4. Clique em **Concluir**.

Solução de problemas de importação de dados do Common Vulnerability Reporting Framework

As ações de solução de problemas podem ajudar a resolver problemas comuns ao importar dados de CVRF na aplicação Vulnerability Response.

Ocorrência	Ação
A duração da execução da integração é longa	Se a integração for executada por um período maior do que o esperado, faça o seguinte: 1. Navegue até a tabela sn_vul_ds_import_q_entry. 2. Agrupar por **Status** campo. Você pode ver as entradas, que estão nos estados Concluído, Em andamento ou Em fila.
Falha na integração na importação baseada em API	Se a integração falhar na importação baseada em API, faça o seguinte: 1. Navegue até **Flow Designer** . 2. Abra o fluxo selecionado na configuração. **Nota:** No caso da Cisco, abra o fluxo Análise de consultoria. 3. Clique em **Execuções** . 4. Abra a execução mais recente ou a execução que deve ser depurada. 5. Verifique o fluxo em cada fase.
Falha na integração na importação baseada em API com um erro de tempo limite	Se a integração falhar em uma importação baseada em API devido ao tempo limite no fluxo de análise de consultoria, faça o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ocorrência	Ação
	1. Aumente o tempo limite abrindo Sys_properties.LIST . 2. Na coluna Nome, pesquise sn_vul.CVRFFlowTimeout (inMiliSeconds) . **Nota:** O tempo é mostrado em milissegundos. 3. Abra o registro e atualize o valor com um número grande. 4. Salve o registro e execute novamente a integração.
Falha na integração com o erro "Mapeamento do scanner para transformação de dados de mapeamento de fornecedor em andamento"	Verifique se a integração falha durante a importação baseada em URL ou API, com o seguinte erro: O mapeamento do scanner para a transformação de dados de mapeamento de fornecedor está em andamento. Os dados serão preenchidos somente após a conclusão da transformação. Tente executar depois de algum tempo. Se você tiver esse erro, aguarde algum tempo e execute a integração novamente.
A fila de importação não é criada durante a importação de arquivos	Às vezes, durante uma importação de arquivo, a fila de importação não é criada. Esta falha significa que a transformação que mapeia os dados de mapeamento do scanner para os dados de mapeamento do fornecedor está em andamento. A entrada da fila é criada quando o processo é concluído.

Common Security Advisory Framework (CSAF)

Quando usado com Solução de gestão de vulnerabilidade, O Common Security Advisory Framework (CSAF) permite notificações de segurança de automação por meio de um formato JSON legível por máquina.

O CSAF permite integrar com qualquer fornecedor de inteligência de soluções usando a estrutura de gestão de soluções para importar os dados de inteligência. As notificações de segurança do CSAF podem ser um dos seguintes tipos.

- Consultorias de segurança
- Troca de exploração de vulnerabilidades (VEX)
- Resposta a incidentes de segurança
- Comunicado Informativo

O CSAF oferece suporte somente às importações de arquivos, importações de URL e importações de API de avisos de segurança de fornecedores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importe dados do Common Security Advisory Framework por meio da importação de arquivos

Importe um arquivo CSAF para exibir dados no formato CSAF. A importação é uma atividade única.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa
Uma vez importada, uma entrada de fila é criada com um anexo, que é analisado quando a entrada é processada. Os dados são preenchidos nas respectivas tabelas. Antes de analisar os dados do CSAF, um registro de mapeamento de scanner é criado com base na configuração. Em seguida, os dados de mapeamento do scanner são transformados em dados de mapeamento do fornecedor.

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no National Vulnerability Database (NVD), que são vulnerabilidades com uma CVE (Common Vulnerability Entry) no banco de dados NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for revertida para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada de NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar manualmente uma solução. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Arquivo de importação** .

   Nota: Você pode carregar apenas um arquivo JSON por vez com um tamanho máximo de arquivo de 15 MB.

3. Em **Nome** , insira um nome exclusivo para a integração.
   O programador é criado com este nome.
4. Em **Fornecedor** , insira o nome do fornecedor.
   . **Origem** o campo das soluções é preenchido com o nome do fornecedor.
5. Selecione **Concluir**.

Resultado
Uma fila de importação é criada. Selecione o link na barra de informações para exibir as entradas da fila do fornecedor junto com a lista relacionada. Você também pode exibir o status do trabalho.

Depois que os dados são importados para o formato CSAF, os dados são processados da seguinte maneira:

1. Quando a fila é processada, o arquivo é analisado com uma fonte de dados dedicada.
2. Quando o processamento é concluído, o log da aplicação é atualizado.
3. Depois que o arquivo JSON CSAF é analisado, ele preenche as tabelas a seguir no ServiceNow® Resposta a vulnerabilidades aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_solution
- sn_vul_m2m_vulnerability_solution
- sn_vul_nvd_entry
- sn_vul_software
- sn_vul_product_category

Você pode ver as informações detalhadas relacionadas a erros ou exceções nos logs da aplicação.

Configurar aliases de conexão e credencial para o Common Security Advisory Framework (CSAF)

Configure aliases de conexão e credencial para autenticar fornecedores. Na análise de consultoria, os fornecedores de terceiros são autenticados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Procedimento

1. Criar autenticação OAuth.
   Consulte Crie um endpoint para os clientes acessarem a instância .
2. Crie um alias de conexão e credencial.
   Consulte Crie um alias de conexão e credencial .
3. Criar uma conexão.
   a. Selecione o nome do alias de conexão e credencial recém-criado.
   b. Em **Conexões** , selecione **Novo** .
   c. Se o tipo de autenticação for OAuth, selecione o Perfil de registro da aplicação criado na etapa 1 como **Perfil de entidade OAuth** .
   d. Crie um registro em Conexões na lista relacionada do registro.
   e. Em **Credencial** , selecione o registro de credencial criado na etapa 3d.
   f. Em **URL de conexão** , insira o URL do fornecedor.
   g. Selecione **Enviar**.

Configure um fornecedor do Common Security Advisory Framework diferente de Red Hat

Configure um fornecedor do Common Security Advisory Framework (CSAF) diferente de Red Hat Com suporte a API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Conexão e Credencial** > **Aliases de conexão e credenciais**.
2. Crie um registro com o tipo de autenticação compatível com o fornecedor.
   Para obter mais informações sobre como autenticar um fornecedor, consulte Configurar aliases de conexão e credencial para o Common Security Advisory Framework (CSAF).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Flow Designer**.
4. Duplique o fluxo chamado "Análise de consultoria".

   Nota:
   - Se alguma das ações precisar ser alterada, copie a ação e use-a no novo fluxo.
   - Revise os parâmetros page_index_key e page_size_key de acordo com a API do fornecedor.
   - Atualize a lógica relacionada à paginação de acordo com o fornecedor

5. Se a lógica do parâmetro de intervalo de datas não for igual a. Red Hat, copie a ação **Atualizar parâmetros de paginação** e fazer mudanças conforme necessário para o fornecedor.
6. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Mapeamento de dados de aprimoramento**.
7. Crie um registro de acordo com Red Hat alterando **Chave de propriedade** valor de acordo com o fornecedor.
   Esta lógica serve para mapear campos obrigatórios de uma carga de consultoria para um ServiceNow tabela.
8. Mapeie os seguintes marcadores de API da Carga de API.
   Esses marcadores precisam ser mapeados com detalhes a serem preenchidos na tabela Mapeamento de dados de aprimoramento. Por padrão, o Red Hat o mapeamento específico foi enviado.

   Nota: Você precisa criar um registro se precisar configurar vários fornecedores que publicam comunicados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration	Descrição
URL do CSAF (URL do recurso que aponta para a carga do CSAF)	cvrf_url	Nome do marcador que contém o URL do CSAF.
ID de aviso (chave exclusiva para resposta)	Id	Nome do marcador que contém um identificador exclusivo.
Data da última modificação	last_modified_date	Nome do marcador que contém a data em que o registro foi atualizado pela última vez.
CSAF (valor estático)	advisory_format	Valor do formato de consultoria para cargas do CSAF. Observe que este é um valor estático aplicável a todas as integrações do CSAF.
SecurityAdvisoryIntegrationSysId	integração	Refere-se ao SYSID do trabalho agendado de integração, que cria os registros de solução de vulnerabilidade.

9. Com base no formato de resposta, mude a lógica de análise copiando a ação **Recuperar lista** Do fluxo de Análise de consultoria.

Importe dados da Estrutura de consultoria de segurança comum dos comunicados

Importe dados do CSAF de comunicados configurando o URL do fornecedor com o tipo de importação como API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa
Quando a integração é executada, os avisos são obtidos. O URL do CSAF e o ID dos avisos são extraídos da carga. As chamadas da REST API são feitas para cada URL do CSAF e os dados são analisados e armazenados na tabela sn_vul_solution.

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no National Vulnerability Database (NVD), que são vulnerabilidades com uma CVE (Common Vulnerability Entry) no banco de dados NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for revertida para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada de NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar manualmente uma solução. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Procedimento
1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Adicionar Integração**.
3. No formulário, preencha os campos.

Importar formulário de avisos de solução

Campo	Descrição
Tipo de importação	Opção para selecionar o tipo de importação. Selecione **API** .
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** . **Origem** O campo das soluções é preenchido com o nome do fornecedor.
Alias de conexão	Opção para selecionar uma credencial autenticada. **Nota:** A tabela sys_alias armazena credenciais e o URL base para avisos.
Agendamento	Frequência na qual os dados devem ser atualizados.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Configuração de APIs	
Fluxo	Opção para selecionar o fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O fluxo é acionado quando o programador é executado. O fluxo cuida da análise de avisos e extrai o URL do CSAF e armazena esses detalhes nas tabelas de atualização. Você pode copiar o fluxo existente e editar conforme necessário. Por exemplo, você pode fazer mudanças relacionadas à paginação.
Ação de fluxo	Opção para selecionar a ação de fluxo. As ações de fluxo tratam da capacidade da janela deslizante. Você pode atualizar as ações de fluxo e adicionar o parâmetro de consulta diretamente à ação arrastando.
Tabela de mapeamento	Opção para selecionar a tabela de mapeamento. O registro da Tabela de mapeamento de dados de aprimoramento é usado para extrair o URL do CSAF e o ID de aviso da carga útil dos comunicados.
Consultas de resposta	Opção para inserir o nome do marcador da carga útil de avisos de onde a lista de avisos pode ser extraída.
Critérios de filtro	
Parâmetros de intervalo de tempo	Opção para selecionar o intervalo de tempo da solicitação e o formato de data para chamadas de API. O parâmetro de solicitação Data de início/ Data de término é o nome do parâmetro usado para data de início e data de término durante chamadas de API. Por exemplo, StartDate , Start_date, endDate, end_date.
Formato de data	Opção para inserir o formato de data, como, `dd/mm/aaaa.` . O formato de data é o formato que a API precisa para filtragem. Formatos que não são compatíveis com GlideDate não funcionam.
Intervalo inicial em dias	E ner os dias para os quais os dados devem ser obtidos quando o programador é executado pela primeira vez. Para execuções subsequentes, o mecanismo da janela deslizante é seguido. **Nota:** Se você não quiser selecionar um intervalo de tempo, selecione **Nenhum parâmetro** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Mapeamentos do scanner	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Selecione **Concluir**.

Importe dados do Common Security Advisory Framework (CSAF) por meio da URL do CSAF

Importe dados do CSAF configurando o URL do fornecedor no Assistente de configuração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os dados são obtidos do URL que é analisado. Os dados são armazenados na tabela sn_vul_solution com origem como o nome do fornecedor.

Nota: O URL pode ser uma carga CSAF direta, que contém os detalhes do comunicado, ou uma URL do Feed do ROLIE (Resource-Oriented Lightweight Information Exchange, troca de informações leve orientada a recursos). Em ambos os casos, a carga é analisada de acordo e os registros da solução são criados. Conclua as etapas a seguir para importação de URL do CSAF.

Você também pode importar soluções de vulnerabilidade de agregadores CSAF ou Provedores confiáveis por meio de uma importação de URL compatível com o Feed ROLIE. Essas soluções de vulnerabilidade são mapeadas automaticamente para o fornecedor correto e Itens vulneráveis (Vits) com base nas Vulnerabilidades e exposições comuns (CVEs).

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no National Vulnerability Database (NVD), que são vulnerabilidades com uma CVE (Common Vulnerability Entry) no banco de dados NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for revertida para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada de NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar manualmente uma solução. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Adicionar Integração**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar formulário CSAF

Campo	Descrição
Tipo de importação	Tipo de importação. Selecione **URL** .
Nome	Nome exclusivo da integração.
Único fornecedor	Selecione esta opção se você estiver importando CSAF de um fornecedor.
Fornecedor	Nome do fornecedor Este campo só estará disponível se você selecionar **Fornecedor único** . **Nota:** . **Origem** O campo das soluções é preenchido com o nome do fornecedor.
Multifornecedor	Selecione esta opção se você estiver importando CSAF de vários fornecedores.
Agregador	Um provedor confiável cuja solução você pode importar.
URL	URL da qual você deseja buscar os dados da solução no formato CSAF.
Agendamento	Frequência na qual os dados devem ser atualizados. **Nota:** Se o marcador de status do CSAF mostrar "FINAL", o campo será definido automaticamente como **Sob demanda** para evitar execuções desnecessárias.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Mapeamentos do escâner **Nota:** A seção Mapeamentos do scanner é opcional para o CSAF.	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Selecione **Concluir**.

Importação de dados do Common Security Advisory Framework

As ações de solução de problemas podem ajudar a resolver problemas comuns ao importar dados do CSAF na aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ocorrência	Ação
A duração da execução da integração é longa	Se a integração for executada por um período maior do que o esperado, faça o seguinte: 1. Navegue até a tabela sn_vul_ds_import_q_entry. 2. Agrupar por **Status** campo. Você pode ver as entradas, que estão nos estados Concluído, Em andamento ou Em fila.
Falha na integração na importação baseada em API	Se a integração falhar na importação baseada em API, faça o seguinte: 1. Navegue até **Flow Designer** . 2. Abra o fluxo selecionado na configuração. **Nota:** No caso de Red Hat Abra o fluxo de Análise de consultoria. 3. Selecione **Execuções** . 4. Abra a execução mais recente ou a execução que deve ser depurada. 5. Verifique o fluxo em cada fase.
Falha na integração na importação baseada em API com um erro de tempo limite	Se a integração falhar em uma importação baseada em API devido ao tempo limite no fluxo de análise de consultoria, faça o seguinte: 1. Aumente o tempo limite abrindo Sys_properties.LIST . 2. Na coluna Nome, pesquise `sn_vul.CVRFFlowTimeout (inMiliSeconds)` . **Nota:** O tempo é mostrado em milissegundos. 3. Abra o registro e atualize o valor com um número grande. 4. Salve o registro e execute novamente a integração.
Falha na integração com o erro "Mapeamento do scanner para transformação de dados de mapeamento de fornecedor em andamento"	Verifique se a integração falha durante a importação baseada em URL ou API, com o seguinte erro: O mapeamento do scanner para a transformação de dados de mapeamento de fornecedor está em andamento. Os dados serão preenchidos somente após a conclusão da transformação. Tente executar depois de algum tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ocorrência	Ação
	Se você tiver esse erro, aguarde algum tempo e execute a integração novamente.
A fila de importação não é criada durante a importação de arquivos	Às vezes, durante uma importação de arquivo, a fila de importação não é criada. Esta falha significa que a transformação que mapeia os dados de mapeamento do scanner para os dados de mapeamento do fornecedor está em andamento. A entrada da fila é criada quando o processo é concluído.

Adicional Resposta a vulnerabilidades tarefas de instalação e configuração

Para ajudá-lo com a correção, você pode executar essas tarefas adicionais de configuração administrativa como parte da configuração fora da configuração básica. Você executa essas tarefas fora do Assistente de configuração.

Você pode usar o relatório padrão fornecido com Resposta a vulnerabilidades para supervisionar sua postura de segurança. Você pode editar esses relatórios se eles não se adequarem ao seu ambiente ou usá-los como modelos para criar o seu próprio.

. Performance Analytics para Resposta a vulnerabilidades instalado, você pode criar relatórios, painéis dinâmicos e muito mais. Consulte Introdução aos relatórios para obter mais informações.

As notificações por e-mail aumentam a produtividade e o fluxo de trabalho suave.

Com a Avaliação de exposição de software, pesquise o fornecedor, o nome do produto e o número da versão no Software Asset Management (SAM Foundation para determinar sua exposição a software vulnerável.

A visibilidade das bibliotecas de vulnerabilidades pode fornecer flexibilidade com tarefas de agrupamento e correção.

Configure a Gestão de exceções para ajudá-lo Quando sua organização não puder cumprir um gerenciamento de vulnerabilidades ou uma política de segurança publicada, padrão ou diretriz, você poderá solicitar uma exceção.

Para obter mais tarefas de configuração adicionais, consulte os tópicos que seguem esta visão geral.

Testes de início rápido para Resposta a vulnerabilidades

Valide se Resposta a vulnerabilidades ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em não produção ou produção. Consulte Execute o pacote de testes ATF (Automated Test Framework) para Resposta a vulnerabilidades para obter mais informações sobre como configurar e executar o pacote de testes para Resposta a vulnerabilidades.

Os testes de início rápido Resposta a vulnerabilidades exigem a ativação da aplicação Resposta a vulnerabilidades (sn_vul) e o carregamento dos dados de demonstração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
VR: criar regras de destino de correção	Crie regras de destino de correção.	Madrid
VR: criar regras do grupo de vulnerabilidades	Crie regras do grupo de vulnerabilidades.	Madrid
VR: criar item vulnerável por meio de formulário	Determine se um usuário pode criar com êxito um item vulnerável a partir do formulário de Item vulnerável.	Madrid
VR: ciclo de vida do grupo de vulnerabilidades	Determine se um usuário pode resolver com êxito um grupo de vulnerabilidades.	Madrid
VR: ciclo de vida do item vulnerável	Determine se um usuário pode mover com sucesso um item vulnerável durante o ciclo de vida e também se um item vulnerável encerrado pode ser reaberto.	Madrid
VR: calculadora de acúmulo	Determine se a calculadora de risco de acúmulo pode fornecer uma pontuação de risco geral para um grupo inteiro de itens vulneráveis usando as pontuações de todos os itens vulneráveis em um grupo de vulnerabilidade.	New York
VR: regras de atribuição de Resposta a vulnerabilidades	Determine se um conjunto de exemplo de regras de atribuição pode atribuir automaticamente itens vulneráveis a um grupo de atribuição para correção.	New York
VR: calculadoras de vulnerabilidade	Teste as calculadoras de vulnerabilidade.	New York
VR: Pesquisa de IC - Qualys	Crie uma nova regra de pesquisa com o método "field_matching" chamada "Pesquisa por adaptador de rede" para Qualys. Determine se um item de configuração foi correspondido com êxito na tabela Item descoberto por adaptador de rede e endereço IP com a nova regra de pesquisa.	Orlando
VR: criar solicitação de mudança normal e de emergência	Determine se o usuário pode criar com êxito solicitações de mudança normais e de emergência a partir de um grupo de vulnerabilidades.	Orlando
VR: dividir grupo de vulnerabilidade	Determine se um usuário pode dividir com êxito um grupo de vulnerabilidades.	Orlando

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
VR: atualize o estado do VG quando um CHG é cancelado.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada ao grupo de vulnerabilidades é cancelada.	Orlando
VR: atualize o estado do VG quando um CHG muda para revisão.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada a ele é movida para o estado revisão.	Orlando
VR: Pesquisa de IC - Rapid7	Teste a pesquisa de IC usando a regra de pesquisa Integração com Rapid7 Vulnerability existente **IP Address**.	Orlando
VR: Pesquisa de IC - Qualys	Teste a pesquisa de IC criando uma nova regra de pesquisa para o Qualys Vulnerability Integration	Orlando
VR: fluxo de trabalho de aprovação de exceção para VI	Crie uma solicitação de exceção e verifique se o processo de aprovação está funcionando.	Orlando
VR: fluxo de trabalho de aprovação falso-positivo para VI	Crie uma solicitação de exceção de falso-positivo e verifique se o processo de aprovação está funcionando.	Orlando
VR: AVR (Resposta a vulnerabilidades de aplicações)	Determine se suas regras e calculadoras estão funcionando corretamente. Verifique se as atualizações estão funcionando.	Orlando
Regras de destino de correção: teste de importação de VI	Teste as regras de destino de correção de VR durante a importação.	Paris
VR: regra de classificação	Um exemplo de regra de classificação que classifica uma vulnerabilidade automaticamente.	Tokyo

Tópicos relacionados

Testes de início rápido

Execute o pacote de testes ATF (Automated Test Framework) para Resposta a vulnerabilidades

Execute o pacote de testes ATF (Automated Test Framework) depois de instalar ou fazer upgrade do Resposta a vulnerabilidades aplicação.

Antes de Iniciar

Confirme uma instalação bem-sucedida e se sua instância funciona conforme projetado.

Tradução automática

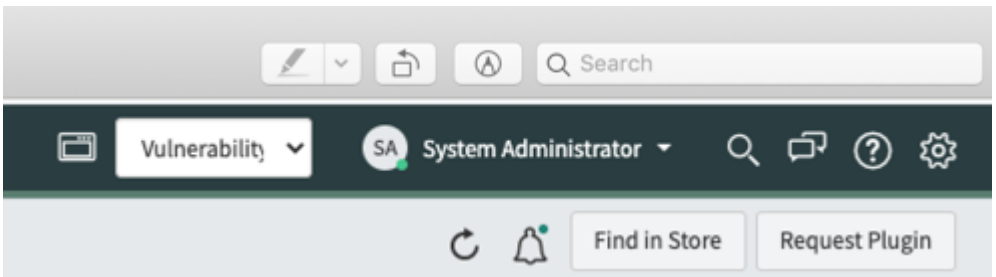
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em não produção ou produção.

- Verifique se você instalou os dados de demonstração ao instalar Resposta a vulnerabilidades. Os dados de demonstração são necessários para executar o. Resposta a vulnerabilidades pacote de testes.
- Para habilitar o teste, siga estas etapas:

1. Navegar até **Tudo** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
2. Se não estiver selecionado, selecione **Habilitar execução de pacote de testes/testes** caixa de seleção.
3. Clique em **Salvar**.
4. Se o escopo não estiver definido como **Resposta a vulnerabilidades** ou o escopo não for exibido no cabeçalho, clique no ícone de configurações na parte superior da página na janela do navegador .
5. Na janela Configurações do sistema, clique em **Desenvolvedor** .
6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
7. Na lista exibida ao lado de Administrador do sistema clique em **Resposta a vulnerabilidades** para o campo.

   O campo é exibido conforme mostrado na imagem a seguir.



Função necessária: admin ou atf_test_admin

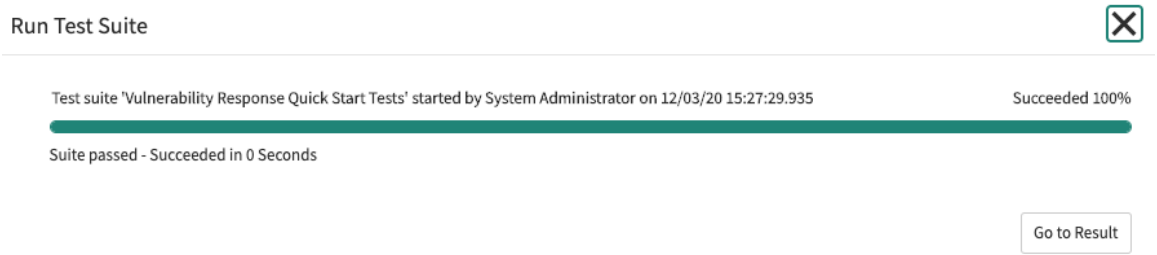
Procedimento

1. Navegar até **Tudo** > **Automated Test Framework (ATF)** > **Pacotes**.
2. Na lista Pacotes de testes, localize **Testes de início rápido de resposta a vulnerabilidades** .
3. Selecione-o para abrir o registro.
4. No registro Aberto, selecione **Ativo** caixa de seleção.
5. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. . **Executar Pacote de testes** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar Pacote de testes** para iniciar o teste.
   Após alguns momentos, a caixa de diálogo Executar pacote de testes indica um teste bem-sucedido. Clique em **Ir para Resultado**para obter mais



informações.

O que Fazer Depois

Parabéns! Você pode continuar com sua configuração de Resposta a vulnerabilidades.

Para obter mais informações sobre testes automatizados para Resposta a vulnerabilidades e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Instalar Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades

Instalar Recomendações de atribuição de vulnerabilidade para que você possa reduzir o tempo gasto na identificação de responsáveis por descobertas de vulnerabilidade que não estão atribuídas ou atribuídas incorretamente. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Antes de Iniciar

Antes de executar o. Recomendações de atribuição de vulnerabilidade recurso de Resposta a vulnerabilidades em seu ServiceNow AI Platform® primeiro, você deve baixar e instalar o. Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades aplicação. Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Para obter mais informações, consulte Ativar uma aplicação da ServiceNow Store .

Função necessária: administrador

Tarefas de configuração	Ação
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**. Resposta a vulnerabilidades será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Instalar Resposta a vulnerabilidades.
Verifique se o Inteligência preditiva a aplicação está instalada e ativada.	Navegar até **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**.

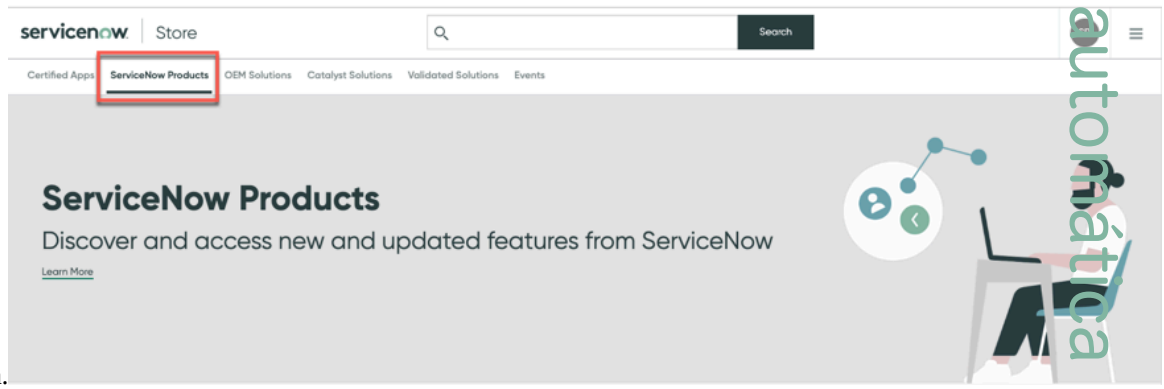
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Ação
	Inteligência preditiva será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Instalar Inteligência preditiva .
Verifique se você tem o necessário ServiceNow funções para sua instância.	Verifique se você tem estas funções necessárias para instalação e verificação dos resultados esperados: • Vulnerability_admin: Necessário para habilitar e configurar Recomendações de atribuição de vulnerabilidade. Você também pode usá-lo para exibir e selecionar recomendações de atribuição para itens vulneráveis e tarefas de correção. • ServiceNow administrador: Necessário para instalar aplicações.

Procedimento

1. Navegue até ServiceNow Store.
2. Clique em **Faça login** E insira suas credenciais HI.
3. Para exibir o disponível ServiceNow produtos, clique em ServiceNow **Produtos**guia.



4. Para exibir todas as aplicações associadas às quais você está concedendo direito Recomendações de atribuição de vulnerabilidade, clique em Resposta a vulnerabilidades produto.

   A página lista todas as aplicações para as quais você está qualificado se aceitar. Para obter informações sobre uma aplicação, clique no link da aplicação.

5. Para verificar se você tem direito ao Recomendações de atribuição de vulnerabilidade clique em **Aceite** .
6. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar** .
   É exibida uma mensagem indicando que você aceitou a aplicação com sucesso.
7. Passe para a etapa 10 para instalar a aplicação no seu ServiceNow AI Platform instância.
8. **Opcional:** Se você quiser gerenciar seu direito para Recomendações de atribuição de vulnerabilidade aplicação em outro ServiceNow AI Platform instâncias, clique em **Gerenciar direito** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

. **Gerenciar direito** não for exibido, clique em Recomendações de atribuição de vulnerabilidade Na Lista de produtos para exibi-la.

a. Escolha uma opção.

b. Clique em **OK** ou **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar o aplicativo em seu ServiceNow AI Platform instâncias.

9. Faça login no ServiceNow AI Platform instância em que você deseja instalar Recomendações de atribuição de vulnerabilidade aplicação em.
10. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
11. Nas aplicações listadas, localize Recomendações de atribuição de vulnerabilidade(sn_vul_recom) e clique em **Instalar** .
A caixa de diálogo de instalação da aplicação é exibida e todas as dependências instaladas são exibidas.
12. **Opcional:** Se você quiser dados de demonstração, selecione **Carregar dados de demonstração** marque a caixa e clique em **Instalar** .

Nota: Se você não selecionar **Carregar dados de demonstração** Os dados de demonstração não estão disponíveis para instalação do Gerenciador de aplicações posteriormente. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] artigo no Now Support Base de conhecimento.

Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

13. Clique em **Fechar**.
14. Para configurar Recomendações de atribuição de vulnerabilidade, consulte Configurar recomendações de atribuição de vulnerabilidades para Resposta a vulnerabilidades.

Configurar recomendações de atribuição de vulnerabilidades para Resposta a vulnerabilidades

Habilitar Recomendações de atribuição de vulnerabilidade para reduzir o tempo gasto na identificação dos responsáveis pelas descobertas de vulnerabilidade que não estão atribuídas ou atribuídas incorretamente.

Antes de Iniciar
Função necessária: sn_vul.manage_assignment_recom_config

Por Que e Quando Desempenhar Esta Tarefa
Esta aplicação não está habilitada por padrão.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Recomendações de atribuição**.
2. Selecione **Habilitar Recomendações de atribuição** .
. **Campo de definição da solução de Inteligência preditiva** aparece. O valor padrão é **Atribuição de item vulnerável** .
3. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar e treinar uma definição de solução para Resposta a vulnerabilidades

Criar e treinar um modelo de definição de solução para Resposta a vulnerabilidades usando Inteligência preditiva. Você pode usar este modelo para prever o grupo de atribuição de um item vulnerável (VI) ou tarefa de correção (RT) com base nos dados existentes.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Inteligência preditiva** > **Classificação** > **Definições de solução**.
2. No formulário Definições de classificação, clique em **Atribuição de item vulnerável** .
   Esta é a definição da solução padrão.

   Nota:

   - A Frequência de treinamento padrão é de 30 dias. Isso significa que a cada 30 dias, o modelo é retreinado automaticamente usando o conjunto de dados de VI que corresponde à condição de filtro configurada.
   - Os campos da tabela Item vulnerável podem ser usados para treinamento. A definição de solução padrão é treinada em dois campos de VI: **Vulnerabilidade.Resumo** e. **Item de configuração.Nome** . Você pode personalizar os campos usados para treinamento, dependendo de quais campos você achar úteis para prever a propriedade da vulnerabilidade em sua organização.

3. Para criar e treinar a solução de classificação, consulte Criar e treinar uma solução de classificação .

   Nota: Você também pode criar e treinar uma semelhança ou uma solução de cluster. Para obter mais informações, consulte:

   - Crie e treine uma solução de semelhança .
   - Criar e treinar uma solução de cluster .

4. Clique em **Atualizar e treinar novamente**.

   Nota: Para definir configurações avançadas para soluções DE ML, consulte Definir configurações avançadas para suas soluções DE ML .

Crie um Resposta a vulnerabilidades calculadora

Uma calculadora de vulnerabilidade é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. Calculadoras, que calculam o item vulnerável **Pontuação de risco** , pode conter **Regras de risco** .

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode notar degradação no desempenho ao executar calculadoras de vulnerabilidade que contêm scripts.

Ordene que suas regras executem as regras mais simples primeiro e executem scripts somente nos itens que não podem ser manipulados com um valor de condição e modelo ou uma regra de risco.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Calculadoras de Vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Formulário da calculadora de vulnerabilidades

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidades.
Tabela	Preenchido automaticamente com o nome da tabela de item vulnerável.
Aplicação	Preenchido automaticamente com Resposta a vulnerabilidades.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Ligar ou desligar a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar** .
. **Regras da Calculadora de vulnerabilidades** a seção é exibida.
5. Clique em para criar uma regra para a calculadora **Novo** .

Nota: Para **Novas Regras de Risco** (disponível somente quando **Campo de destino** . **Pontuação de risco** consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da calculadora de vulnerabilidades

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual executar a calculadora de vulnerabilidades. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionado, as condições de script e os valores de script podem ser selecionados **Tipo de condição** e. **Tipo de valor** .

7. Preencha os campos em **Quando esta condição é atendida** , conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando esta condição é atendida

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual executar a calculadora de vulnerabilidades. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará a itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionado, selecione Condições com script e Valores com script de **Tipo de condição** e. **Tipo de valor** .
Tipo de condição	Disponível quando você seleciona **Exibição avançada** . As opções incluem: ◦ Filtro: Usa condições de filtro. ◦ Grupo de filtros: Consulte crie um novo grupo de filtros para definir os critérios da calculadora. ◦ Script: Condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne ao **Calculadoras de vulnerabilidades** lista. Explore os registros da calculadora de vulnerabilidades enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. Selecionando **Grupo de filtros** ou **Script** tipos de condição, oculta este campo. A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

8. Clique em **Defina esses valores** e preencha os campos no formulário, conforme apropriado.

Defina a guia estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona **Exibição avançada** . As opções incluem: ◦ Modelo: Defina os valores a serem definidos em cada campo. ◦ Script: Usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou **Script** tipo de valor. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Selecionando **Script** tipo de valor, oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar** .

Nota: Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar **Reaplicar Calculadora** botão. Ele é executado em todos os itens vulneráveis (VIS) ativos e, se essa calculadora for usada para definir seu valor, recalcula o valor desses VIS. Reaplicar uma calculadora pode levar muito tempo, um trabalho agendado lida com isso.

10. Para **Novas Regras de Risco** preencha os campos conforme apropriado.

Defina cada ponderação de acordo com a porcentagem do resultado que deve vir desse valor. Para quaisquer dados que o scanner não forneça ou dados que não devem fazer parte da pontuação de risco, defina o peso como zero.

Você pode adicionar, excluir ou atualizar os campos. Você também pode configurar a porcentagem de ponderação para os valores de campo. Para obter mais informações, consulte Defina campos e pesos para a regra de risco para Calculadoras de risco de resposta a vulnerabilidades.

Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os previstos **Pontuação de risco** resultados.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual executar a calculadora de vulnerabilidades. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. Selecionando **Grupo de filtros** ou **Script** tipos de condição, oculta este campo.
Pesos	
Severidade da Vulnerabilidade	Percentual do resultado que vem da gravidade.
Pontuação de EPSS de vulnerabilidade	Probabilidade da vulnerabilidade ser explorada. Por padrão, o peso desses critérios é zero. Se você quiser usar isso para o cálculo de pontuação de risco, defina um peso apropriado em relação a esses critérios.
Exploração presente	Porcentagem do resultado que vem da existência de uma exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.

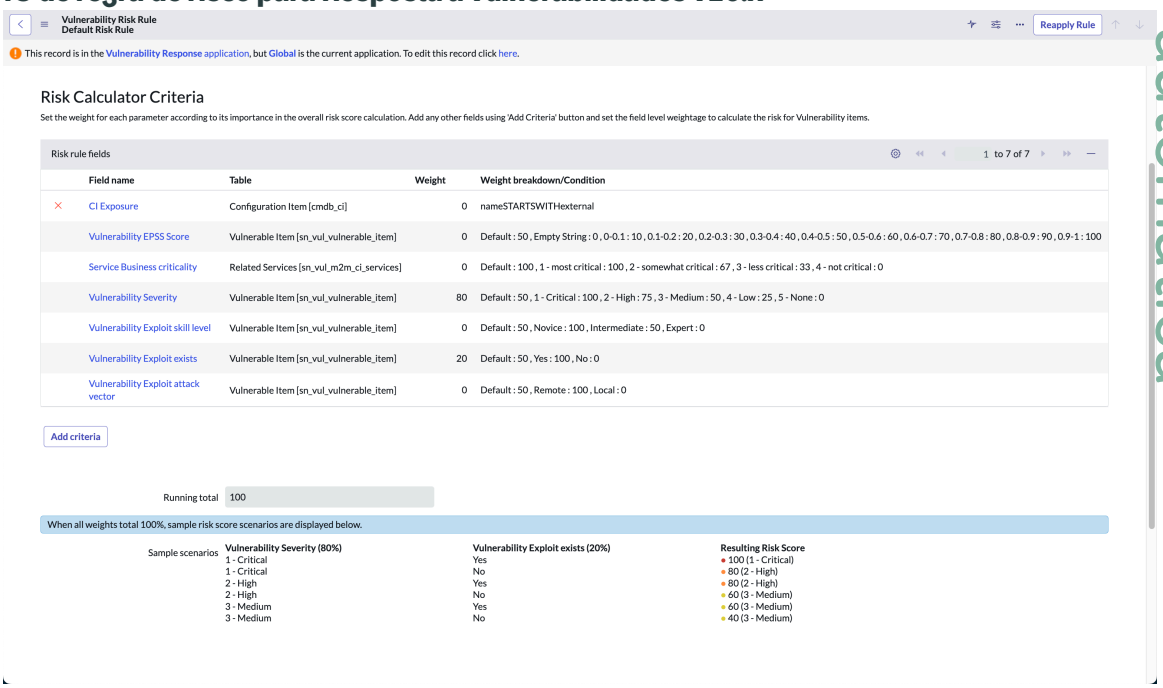
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nível de habilidade da exploração	Percentual do resultado que vem do nível de habilidade exigido pela exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Vetor de ataque da exploração	Percentual do resultado que vem de onde o ataque é direcionado. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Criticidade do negócio do serviço	Percentual do resultado que vem da criticidade dos negócios. Se você não vinculou seus ICs aos serviços de negócio, defina o peso como zero.
Exposição de IC	Percentual do resultado que vem de se o IC é voltado para a Internet. Se o peso for diferente de zero, um filtro de condição aparecerá para definir quais ICs são voltados para a internet. Defina o filtro para selecionar os itens de configuração voltados para a Internet. Você pode visualizar quais registros correspondem à condição.
Total da execução	Totais percentuais calculados automaticamente. Quando esse valor atinge 100, a visualização do cenário mostra pontuações de risco de amostra em diferentes cenários.
Cenários de pontuação de risco	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Você pode adicionar ou remover critérios e ajustar o peso de cada critério usando a lista Incorporado.

IC de regra de risco para Resposta a vulnerabilidades v20.x



11. Clique em **Enviar**.

Desabilite a calculadora de vulnerabilidades padrão se não for usada

Se você não usar calculadoras de vulnerabilidade, desabilite a calculadora padrão, além de todas as outras que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de Vulnerabilidade**.
2. Abra a calculadora relevante.
3. Limpe **Ativo** caixa de seleção para desativar a calculadora.
4. Clique em **Atualizar**.

Criar, habilitar ou modificar Resposta a vulnerabilidades regras de exclusão automática

Você pode criar, habilitar ou modificar as regras de exclusão de item de vulnerabilidade (VI) e tarefa de correção (RT). Use a exclusão automática para remover registros mais antigos das tabelas VI e RT.

Antes de Iniciar
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Funções necessárias:

- administrador: modifique as regras de exclusão automática
- sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado): exiba o módulo de exclusão automática

Por Que e Quando Desempenhar Esta Tarefa
Ao longo do tempo, uma grande quantidade de registros encerrados provavelmente se acumulará nas tabelas vi e VUL em sua instância. Muitos desses registros podem ter sido encerrados por mais de 365 dias, mas não foram removidos. Use regras de exclusão automática para remover muitos desses registros encerrados mais antigos. Remover esses registros não apenas reduz significativamente o número de registros nas tabelas vi e VUL, mas excluí-los também ajuda a manter o alto desempenho.

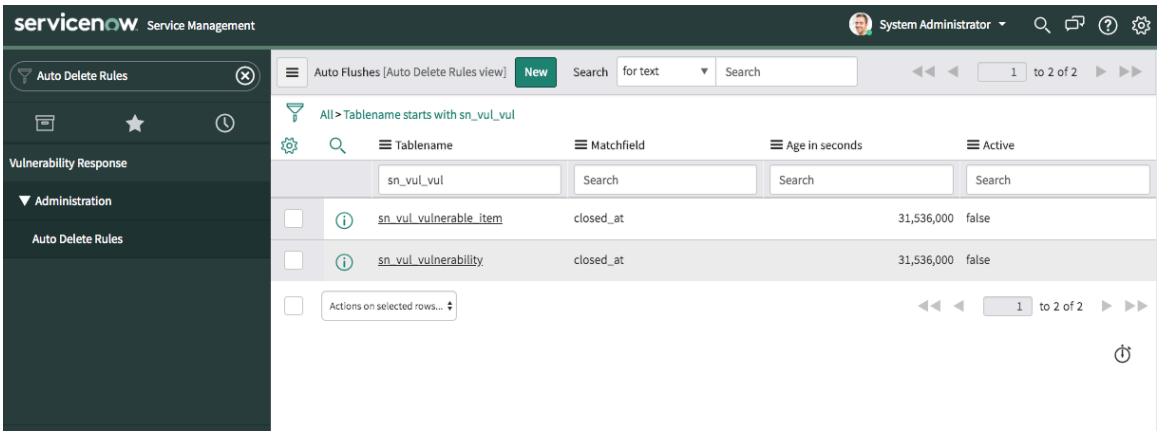
Por padrão, a exclusão automática visa registros que foram encerrados por 365 dias, mas a primeira execução pode tentar limpar muitos registros em uma única transação. Dependendo do tamanho do seu ambiente, você pode preferir escalonar o processo de exclusão para limitar o escopo da consulta. Por exemplo, você pode iniciar sua primeira execução para registros encerrados com mais de 450 dias. Após a conclusão dessa execução, você pode reduzir o número de registros com mais de dias (425, 400, 375) até reduzir o número de registros com mais de 365 dias.

Há duas regras fornecidas com seu ServiceNow AI Platform® que excluem automaticamente registros encerrados que atendem às condições especificadas junto com todos os registros que se referem a eles. Uma regra exclui itens vulneráveis e a outra exclui tarefas de correção. Por padrão, essas regras de exclusão automática estão desabilitadas para que você precise ativá-las manualmente antes de excluir qualquer registro. Você pode escolher as duas regras pré-configuradas que são fornecidas com sua instância ou criar suas próprias regras.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exclusão automática**.
   A exibição de lista é exibida.

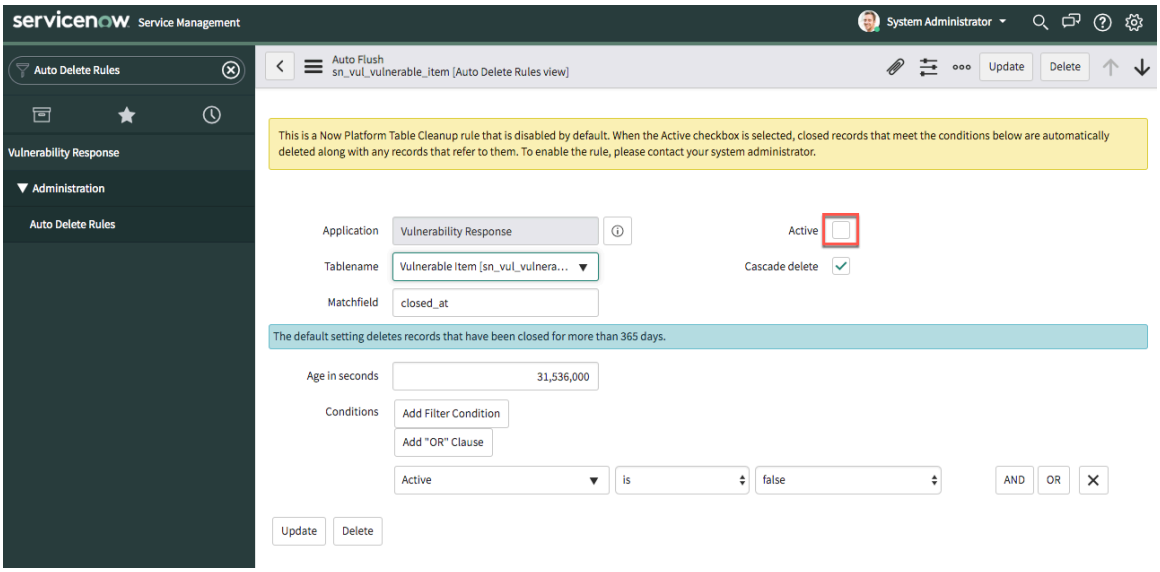


2. Para editar, selecione a regra de exclusão para itens vulneráveis (sn_vul_vulnerable_item) ou a regra para tarefas de correção (sn_vul_vulnerability).
3. Para criar uma nova regra, clique em **Novo**.
4. Preencha ou edite os campos no formulário, conforme apropriado.

Campo	Descrição
Aplicação	Nome da aplicação na qual os registros estão sendo excluídos. O valor padrão é Resposta a vulnerabilidades.
Nome da tabela	Nome da tabela à qual a regra está sendo aplicada.
Campo de correspondência	Campo para o qual o sistema monitora a duração.
Ativo	Opção para ativar a regra. Uma vez ativado, o registro pode ser excluído.
Exclusão em cascata	Opção para excluir todos os registros correspondentes, além de todos os registros que se referem a eles. Se esta opção não estiver selecionada, somente os registros correspondentes serão excluídos, mas não os registros que se referem a eles.
Idade em segundos	Idade do registro de vulnerabilidade a ser excluído. Para as regras VI e RT, a idade é de 365 dias. Esta idade é exibida em segundos.
Condições	Condições de filtro que definem os registros nas tabelas VI e RT (VUL) às quais as regras se aplicam.

5. Selecione **Ativo** caixa de seleção para ativar uma regra.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando a regra é ativada, a função da plataforma por hora, **Lavagem automática** exclui esses registros da tabela para a qual a regra está ativada.

Se o seu ambiente tiver milhões, ou dezenas de milhões, de registros que correspondem aos critérios de exclusão, convém consultar ServiceNow suporte ao cliente antes de habilitar as regras de exclusão automática para ajudá-lo a excluir registros usando um processo em fases.

Adicione gráficos de significância de vulnerabilidade à página inicial de Resposta a vulnerabilidades

Você pode adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar

- Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.
- O plug-in Análise de vulnerabilidades deve ser ativado.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Visão geral**.
   Por padrão, alguns relatórios são adicionados ao painel. Para obter mais informações sobre esses relatórios, consulte Usando o padrão Resposta a vulnerabilidades painéis.
2. Perto do cabeçalho do painel, clique no ícone de exibição de cartão + **Adicionar conteúdo** para abrir a caixa de diálogo e adicionar mais widgets.
3. Nas listas em **Adicionar Widgets** caixa de diálogo, selecione **Relatórios** para exibir mais Resposta a vulnerabilidades relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conteúdo	Opções
Detalhes da tarefa de correção	**Mapa de Árvore** > **Importância da vulnerabilidade** > **Importância da vulnerabilidade**
Relatório de pontuação de significância da vulnerabilidade	**Performance Analytics** > **Pontuação** > **Serviços com significância de vulnerabilidade**
Entrada vulnerável	**Relatórios** > **Entrada vulnerável** > **Vulnerabilidades por impacto, pontuação, semana**
Tarefa de correção	**Relatórios** > **Tarefa de correção** > **Tarefa de correção por tempo para corrigir o status**
Item da Tarefa de correção	**Relatórios** > **Item da Tarefa de correção** > **Novos itens vulneráveis**
Execução de integrações de vulnerabilidade	**Relatórios** > **Execução de integrações de vulnerabilidade** > **Duplicatas da Qualys, Novas VIS, Resultados, Visualizações atualizadas, Execuções de integração da Qualys 30**
Item vulnerável	**Relatórios** > **Item vulnerável** > **Uma lista extensa de filtros de itens vulneráveis, incluindo Open Qualys VIS.**.

4. Clique no local na tela em que você deseja adicionar o medidor.
5. Feche o. **Adicionar conteúdo** caixa.

Definir Resposta a vulnerabilidadesnotificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações falso-positivas. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas sobre como criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultado

Quando um destinatário clica nos links em uma notificação por e-mail, os links são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para os usuários com as funções, sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com a função, sn_vul.remediation_owner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Definir Resposta a vulnerabilidades modelos de e-mail

Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

Para obter instruções detalhadas sobre como criar modelos de e-mail, consulte Crie uma mensagem de e-mail com um modelo .

Criar ou editar notificações de destino de correção

Os administradores de vulnerabilidades podem editar a notificação de destino de correção ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo** .
3. Preencha os campos no formulário, conforme apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultado

A partir de v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para os usuários com as funções, sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul.remediation_owner.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configure o. Vulnerabilidade Avaliação de exposição

Avalie a exposição de dia zero (dia atual) de seus ativos a software vulnerável com Vulnerabilidade Aplicação de avaliação de exposição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Você pode executar a avaliação de exposição por CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e software para aproveitar os recursos adicionais no Espaço de avaliação de vulnerabilidades. Para obter mais informações, consulte Explorar o Espaço de avaliação de vulnerabilidade.

Função necessária: administrador

Compatibilidade e requisitos do sistema

. Resposta a vulnerabilidades a aplicação está disponível no ServiceNow Store. . Software Asset Management A aplicação Foundation (SAM) [com.snc.asset_management] é instalada como parte do Resposta a vulnerabilidades aplicação. Para verificar se o SAM Foundation a aplicação está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e pesquise com.snc.asset_management . Se a aplicação não estiver instalada, selecione **Instalar** . Para obter mais informações, SAM Foundation consulte Plug-in Software Asset Management Foundation .

. Vulnerabilidade A aplicação Avaliação de exposição requer acesso aos dados do ativo no seu ServiceNow AI Platform® as aplicações de gestão de ativos devem ter dados para referência. A tabela Modelos da Descoberta de software [cmdb_sam_sw_discovery_model] e as Instalações de software [cmdb_sam_sw_install] exigem dados.

. Vulnerabilidade Aplicação de avaliação de exposição e também funciona com o SAM Foundation Ou o SAM Pro ServiceNow AI Platform® aplicações. A aplicação SAM Pro não faz parte do núcleo Resposta a vulnerabilidades produto do ServiceNow Store e requer uma assinatura separada.

Nota: A aplicação SAM Pro é necessária somente para a Biblioteca de conteúdo, o que pode produzir melhores resultados.

A partir da v23.0 de Resposta a vulnerabilidades Se você tiver a assinatura Pro ou Enterprise, será redirecionado para **Avaliação de exposição** Nos Espaços de trabalho com base em sua função ao clicar em **Avaliação de exposição** link no **Todos** menu:

Acessar a página de avaliação de exposição nos espaços de trabalho

Função	Espaço
Gerenciador de vulnerabilidades	Espaço para gerentes de vulnerabilidades
Gerenciador de eventos [sn_vul_analyst.vul_event_manager] ou Resposta de emergência [sn_vul_analyst.emergency_response]	Espaço de avaliação de vulnerabilidade

Para evitar ser redirecionado para os espaços de trabalho e permanecer na página Avaliação de exposição clássica, defina **Tipo de link** . *Lista de registros* Na guia Tipo de link na página Módulo - Avaliação de exposição. Você pode acessar a página Módulo - Avaliação de exposição selecionando **Editar módulo** ícone ao lado de **Avaliação de exposição** link no **Todos** menu.

Com a função de gravação de vulnerabilidade [sn_vulnerability_write], você pode exibir o módulo Avaliação de exposição e criar e editar registros de avaliação de exposição sob demanda para software vulnerável em sua instância com Resposta a vulnerabilidades aplicação.

Tópicos relacionados

Avalie sua exposição a software vulnerável

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a Gestão de exceções para Resposta a vulnerabilidades

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

Antes de Iniciar

Limitar a duração de uma exceção solicitada e adicionar um questionário à solicitação de exceção ou falso positivo usando o. Resposta a vulnerabilidades módulo. Por padrão, uma exceção é solicitada usando ServiceNow® Resposta a vulnerabilidades módulo. Você também pode solicitar uma exceção usando GRC: Gestão de políticas e conformidade integração.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Resposta a vulnerabilidades habilitado, você pode limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o GRC: Gestão de políticas e conformidade o módulo está instalado, você pode selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite que você solicite uma exceção que especifica o objetivo de Política e controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que levantou a solicitação de exceção ou falso positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador da exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção em **Gerencie exceções usando** lista.
   Você pode selecionar qualquer um Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade. Você deve ativar o. GRC plug-in a ser usado GRC: Gestão de políticas e conformidade para solicitar uma exceção. Mudar a configuração não afeta os dados existentes.
3. Se você selecionou Resposta a vulnerabilidades insira as seguintes informações:

Formulário de Configurações do Gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. . **Questionário de exceção** é exibido por padrão. **Nota:** Este campo aparece somente quando você seleciona **Habilite o questionário para solicitar exceção** caixa de seleção.
Questionário para controle de compensação	Exibe o questionário que um responsável pela correção deve responder para solicitações de redução de risco. A partir de v20.0 de Resposta a vulnerabilidades, você pode definir o questionário para solicitações de redução de risco. . **Questionário de controle de compensação** selecionado por padrão. **Nota:** Este campo aparece somente quando você seleciona **Habilite o questionário para solicitar exceção** caixa de seleção.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação falso-positivo é exibido por padrão. **Nota:** Este campo aparece somente quando **Habilite o questionário para marcar falso-positivo** a caixa de seleção está marcada.

Se você personalizou o questionário existente e fez upgrade para v20.0, esse questionário personalizado aparecerá para solicitação de redução de risco em vez do padrão **Questionário de controle de compensação** .

4. Se você selecionou GRC: Gestão de políticas e conformidade insira as seguintes informações:

Formulário de Configurações do Gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação falso-positivo é exibido por padrão.

5. Para configurar questionários com base em condições para solicitações de exceção e falso-positivo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na seção Configuração do questionário de VR, selecione **Novo** .

b. No formulário Configuração do questionário - Novo registro, preencha os campos e selecione **Enviar** .
Para obter mais informações sobre os campos do formulário Configuração do questionário, consulte Campos do formulário Configuração do questionário.
O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para Gestão de exceções de VR.

Por exemplo, se você quiser configurar o questionário para solicitações falso-positivas para itens vulneráveis críticos, selecione **Falso-positivo para itens vulneráveis** regra de aprovação, forneça a condição como A classificação de risco é 1 - Crítica e selecione o questionário desejado em Configuração do Questionário formulário.

6. Selecione **Save** (Salvar).

Adicione um aprovador de exceção

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribuo. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Até Resposta a vulnerabilidades v14.0, um e a solicitação de xception para um item vulnerável ou tarefa de correção é aprovada usando o fluxo de trabalho de aprovação de dois níveis padrão. A solicitação deve ser aprovada por dois níveis de aprovadores.

Nota: Até Resposta a vulnerabilidades v14.0, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir de Resposta a vulnerabilidades V15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho.Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.
2. Na coluna Nome, pesquise **Exceção** e clique em **Aprovador de exceção - Nível 1** .

Nota: A partir de Resposta a vulnerabilidades V12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio de fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção ou falso positivo é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Tudo** > **Propriedades do sistema** e selecione `sn_vul.exception_approver_L1`, `sn_vul.exception_approver_L2`ou `sn_vul.false_positive_approver_group`para mudar o valor da propriedade.

3. No formulário Aprovador de exceção de grupo - Nível 1, clique na lista relacionada Membros do grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário de usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário da instância e encerrar todas as sessões ativas do usuário. O sistema impede que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ○ Listas de usuários ○ Lista de seleção em campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário do local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
7. Repita as etapas 1 a 5 para criar um Aprovador de exceção - Nível 2.
   O aprovador deve navegar até **Resposta a vulnerabilidades** > **Minhas aprovações** e aprovar solicitações.

Nota: Para aprovar uma exceção para GRC: Gestão de políticas e conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Configure regras de aprovação para Gestão de exceções

Começando com Resposta a vulnerabilidades v15.0, use o designer de fluxo para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades(VR) Pela primeira vez, o Flow Designer é habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Se você for um usuário de VR existente, a opção padrão será Fluxo de trabalho.
Se você implantou Resposta a vulnerabilidades v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation*definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Resposta a vulnerabilidades antes da v15.0, o valor desta propriedade do sistema era definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota: Você não pode reverter para usar o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso positivo para itens vulneráveis

Nota: Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação . (dias) A partir de v21.0 de Resposta a vulnerabilidades	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir de v21.0 de Resposta a vulnerabilidades	Data após a qual o aprovador é notificado para executar uma ação.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Crie configurações para uma regra de aprovação.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Crie configurações para uma regra de aprovação

Defina as condições para filtrar itens vulneráveis correspondentes, tarefas de correção ou regras de exceção para um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Nota: Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Configure regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até **Configurações de aprovação** guia.
3. Selecione uma configuração.
4. No formulário, preencha os campos.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.

5. Defina uma condição para os itens vulneráveis ou tarefas de correção de uma das seguintes maneiras:

Campo	Descrição
Condição	Identifica os itens vulneráveis ou as tarefas de correção correspondentes.
Condição avançada	Script que define a condição dos itens vulneráveis ou tarefas de correção. **Nota:** Este campo aparece quando você seleciona **Avançado** caixa de seleção.

6. Selecione **Atualizar**.
   Você pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Você pode definir diferentes caminhos de aprovação para:

- Exemplo 1: Diferentes tipos de vulnerabilidades ou itens de configuração (voltados para a internet ou internos).
- Exemplo 2: Solicitações de adiamento e redução de risco quando um responsável pela correção gera essas solicitações simultaneamente para itens vulneráveis (Vits) do host ou tarefas de correção (VUL).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A coluna Aprovação de mudança contém os registros de aprovação de mudança do estado de adiamento. Quando você define uma condição na coluna Aprovação de mudança usando o construtor de condições, o registro de aprovação de adiamento é considerado, mas não o registro de aprovação de redução de risco. Portanto, para definir a condição no registro de aprovação de mudança do estado de redução de risco, use **Condição avançada** campo.

Para **Solicitação de exceção para itens vulneráveis** regra de aprovação, o. **Solicitação de classificação de risco de Médio a Baixo** a configuração de aprovação é enviada com o sistema de base. Por padrão, esta configuração é definida como falsa. Você pode usar esta configuração para definir um caminho de aprovação para as solicitações de redução de risco de Médio para Baixo. Você também pode atualizar o script nesta configuração para que ele seja aplicável a várias mudanças de classificação de risco nas solicitações de redução de risco.

Configuração de solicitação de classificação de risco de média a baixa:

```
function evaluate() {
   var gr = new GlideRecord("sn_vul_change_approval");
   gr.addQuery("sys_id", approval);
   gr.addQuery("current_value", "3 - Medium");
   gr.addQuery("desired_value", "4 - Low");
   gr.query();
   if (gr.next()) {
      return true;
   }
   return false;
}
evaluate();
```

Defina a configuração anterior como verdadeira com a ordem mais baixa e defina **Solicitação de exceção para VI** configuração como verdadeira.

Resultado: Quando um responsável pela correção gera solicitações de adiamento e redução de risco simultaneamente do Espaço de correção de TI, as solicitações de aprovação de adiamento são redirecionadas para os aprovadores definidos em **Solicitação de exceção para VI** e as solicitações de aprovação de redução de risco são redirecionadas para os aprovadores definidos em **Solicitação de classificação de risco de Médio a Baixo** configuração.

Criar níveis de aprovação para Gestão de exceções

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até **Configurações de aprovação** guia.
3. Selecione uma configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na seção Níveis de aprovador, selecione um nível de aprovador.
5. No formulário, preencha os campos.

Formulário de nível de aprovador

Campo	Descrição
Nome	Nome do nível de aprovação.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ○ Um aprovador necessário ○ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção de: ○ Usuário e grupo de usuários ○ Campo da tabela de aprovação ○ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções: ○ sn_vul.exception_approver: Para gestão de exceções e regras de exceção ○ sn_vul.false_positive_approver: Para falso positivo
Usuários	Edite os usuários listados nos grupos.

6. Para salvar as mudanças, selecione **Atualização** .

Nota: Antes da v15.0, o processo de fluxo de trabalho é funcional se houver usuários somente no nível de exceção 1. No entanto, a partir da v15.0, deve haver pelo menos um usuário em cada nível.

Antes da v15.0, no fluxo de trabalho, se não houvesse nenhum usuário no segundo nível, o item de vulnerabilidade ou o grupo vulnerável era adiado. No entanto, a versão 15.0 em diante, se não houver nenhum usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para vulnerabilidades para servidores Linux e Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de gestão de exceções versus Flow Designer

Começando com Resposta a vulnerabilidades v15.0, se você estiver implantando Resposta a vulnerabilidades(VR) Pela primeira vez, o designer de fluxo para aprovar solicitações de exceção no gerenciamento de exceções está habilitado por padrão. Se você for um usuário de VR existente, a opção padrão será Fluxo de trabalho.

Nota: Começando com Resposta a vulnerabilidades v19.0, somente o flow designer é compatível com novos clientes. Se você for um usuário existente e fizer upgrade para Resposta a vulnerabilidades v19.0, o flow designer e o fluxo de trabalho de gestão de exceções são compatíveis.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
Versão	V15.0 de Resposta a vulnerabilidades.	A partir da v15.0 de Resposta a vulnerabilidades.
Opção padrão	Opção padrão se você for um usuário de VR existente.	Opção padrão para novos usuários de VR a partir da v15.0.
Definindo o processo de aprovação	A gestão de exceções inclui solicitações de exceção e falso positivo junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. A gestão de exceções inclui solicitações de exceção e falso positivo junto com regras de exceção.
Atualizando para o Flow Designer	Você pode fazer upgrade para o Flow Designer a partir do fluxo de trabalho. No entanto, as solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	O Flow Designer está habilitado por padrão.
Propriedade do sistema `sn_vul.flow_designer_activation`	Se você estiver usando o fluxo de trabalho para gestão de exceções antes da v15.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usar o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando VR pela primeira vez para a v15.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o. **Habilitar regras de aprovação do módulo** o trabalho agendado é executado em 24 horas. Este trabalho agendado habilita **Regras de aprovação** módulo. Para ativar este módulo	Se você implantou o VR pela primeira vez do VR v15.0, este módulo estará disponível por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
	instantaneamente, execute este trabalho manualmente.	
Níveis de aprovação	Fornece a opção de definir somente dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de aprovador e adicionar aprovadores dinamicamente para cada regra.

Adicione um aprovador falso positivo

Somente usuários adicionados ao grupo Aprovador de falso positivo podem aprovar falsos positivos para itens vulneráveis (VIS) e tarefas de correção (VULs). Conceder um falso positivo é um processo de aprovação de nível único.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Nota:

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

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > > **Administração de Usuários** > **Grupos**.
2. Em **Nome** coluna, pesquise **Falso-positivo** e clique na opção.
3. No formulário Grupo, navegue até **Membros do grupo** > **Novo** (ou **Editar**).
4. No formulário Usuário, crie um registro inserindo os detalhes do usuário e clique em **Enviar** .
   Todas as funções são concedidas ao usuário. Os usuários selecionados são adicionados à lista Membros do grupo. Esses membros podem aprovar solicitações para marcar tarefas de VIS ou correção como falso positivo. Uma vez aprovado, o estado do registro é atualizado para Encerrado e é reaberto somente na data especificada.

Configurar questionário para redução de risco

Começando com Resposta a vulnerabilidades v20.0, você pode personalizar o questionário da solicitação de redução de risco para um conjunto de itens vulneráveis filtrados ou tarefas de correção.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

. **Questionário para compensar controles de itens vulneráveis** e. **Questionário para compensar controles de grupo vulnerável** as regras de aprovação são enviadas com o sistema de base.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção**.
2. No formulário Configurações para Gestão de exceções de VR, marque a caixa de seleção Habilitar questionário para solicitar exceção.
3. Para configurar questionários com base nas condições para solicitações de redução de risco:
   a. Na seção Configuração do questionário de VR, selecione **Novo** .
   b. No formulário Configuração do questionário - Novo registro, selecione **Questionário para compensar controles de grupos vulneráveis** ou **Questionário para compensar controles de itens vulneráveis** regra de aprovação e forneça a condição.
   c. Selecione o questionário desejado e selecione **Enviar** .
   Para obter mais informações sobre os campos do formulário Configuração do questionário, consulte Campos do formulário Configuração do questionário.
   O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para Gestão de exceções de VR.
4. Selecione **Salvar** No formulário Configurações para Gestão de exceções de VR.

Exiba ANS de resposta a vulnerabilidades para tarefas de correção

Para garantir que os itens vulneráveis sejam processados corretamente, você pode definir um Acordo de nível de serviço (ANS) para Resposta a vulnerabilidades tarefas de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

As definições de ANS nesta lista são um subconjunto da lista de ANS da plataforma, específica para Resposta a vulnerabilidades.

Para obter instruções detalhadas, consulte Criação de uma definição do ANS .

Se você estiver rastreando o tempo necessário para corrigir o VIS, talvez prefira usar Resposta a vulnerabilidades regras de destino de correção. As regras de destino de correção definem os intervalos de tempo esperados para corrigir itens vulneráveis (VI) especificamente no contexto da Resposta a vulnerabilidades, enquanto os SLAs podem fornecer um intervalo de tempo para corrigir a vulnerabilidade em si.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Definições do ANS**.
2. Clique em uma definição.
   ANS de tarefa são mostrados nas listas relacionadas de **Tarefas de correção** .

Configurar watchdog

Use a página de configuração do watchdog para criar novos watchdogs ou atualizar os watchdogs existentes com as condições que você deseja especificar. Você pode habilitar a notificação para cada watchdog e ser notificado quando as condições forem atendidas.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **WatchDog** > **Configuração**.
2. Selecione o watchdog que você deseja implementar.
3. No formulário, preencha os campos.

Formulário de integração do Watchdog

Campo	Descrição
Nome	Nome do watchdog.
Ativo	Defina a caixa de seleção como `true`para habilitar o watchdog.
Tipo de condição	Escolha Filtro ou Script.
Condição avançada	Este campo aparece somente quando Script é selecionado no tipo de condição.
Tabela	Selecione a tabela para executar a condição de watchdog.
Condição	Condição para avaliar o watchdog.
Notificar	Caixa de seleção para notificar os grupos ou usuários se a condição de watchdog for atendida.
Usuários	Lista de usuários a serem informados se a condição de watchdog for atendida.
Grupos	Grupo a ser informado se a condição de watchdog for atendida.
Log de observação	
Watchdog	Referência à tabela watchdog.
Contagem	Número de registros que atendem aos critérios de watchdog.
Anotações	Anotações adicionais para os logs do watchdog.

4. Selecione **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o máximo de linhas na lista relacionada

Controle o número de linhas que aparecem nas listas relacionadas para reduzir o tempo de carregamento e melhorar a legibilidade e o desempenho na Resposta a vulnerabilidades (VR), Conformidade de configuração (CC), Resposta a vulnerabilidades na nuvem (CVR) e Resposta a vulnerabilidades da aplicação (AVR). As listas relacionadas exibem registros associados, como ICs afetados, descobertas ou tarefas de correção, para que você possa acessar rapidamente detalhes relevantes sem sair do formulário.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Sys_properties.LIST**.
2. PESQUISE e abra a propriedade: *sn_vul_cmn.related_list.set_max_row*
3. No campo Valor, insira um dos seguintes:
   - Inteiro positivo: Exibe o número de linhas em cada lista relacionada.
   - Inteiro negativo: Entrada inválida ou valor ignorado.
   - Vazio (sem valor): Exibe todas as linhas.

   Nota: Exibir mais de 100 linhas afeta o desempenho.
4. Selecione **Atualização** para aplicar as mudanças.

Resultado

Depois de atualizar a propriedade do sistema, as seguintes listas relacionadas refletirão o limite de linhas configurado:

Na IU clássica

- ICs afetados
- Descobertas de imagem
- Possíveis itens duplicados
- Soluções potenciais
- Soluções Preferenciais
- Tarefas de correção
- Itens vulneráveis

Na IU do espaço

- Soluções potenciais
- ICs afetados
- Aplicações afetadas
- Imagens do Docker afetadas

Avançado Resposta a vulnerabilidades tarefas de configuração

As tarefas de configuração a seguir exigem codificação ou avançado ServiceNow e não são considerados parte da configuração básica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode preferir executar essas tarefas somente se tiver experiência avançada em codificação ou se tiver um conhecimento especializado do ServiceNow AI Platform.

Crie importações separadas por domínio para uma integração

Se você exigir que os dados importados estejam em um domínio específico, o usuário atribuído para executar as integrações deverá pertencer a esse domínio.

Antes de Iniciar

Função necessária:

import_admin e a função de integração de configuração para sua integração específica, por exemplo, sn_vul.configure_r7_integration ou sn_vul_tenable.configure_integration.

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação ou avançado ServiceNow experiência.

As filas de importação contêm anexos de dados que os trabalhos agendados (integrações) processam. Em um ambiente separado por domínio, você deve corresponder o trabalho agendado à fila de importação correta.

Procedimento

1. Crie um domínio.
2. Para cada domínio que você criar, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um **run_as** espaço reservado para o domínio em sua integração de vulnerabilidades. É o equivalente a **VR.System** usuário no domínio global. Este usuário precisa de acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Não use este usuário para nenhuma outra finalidade.

3. Criar um trabalho agendado em cada domínio.
   Para obter mais informações sobre precauções e configurações adicionais, consulte Configurações adicionais para Domain Separation.

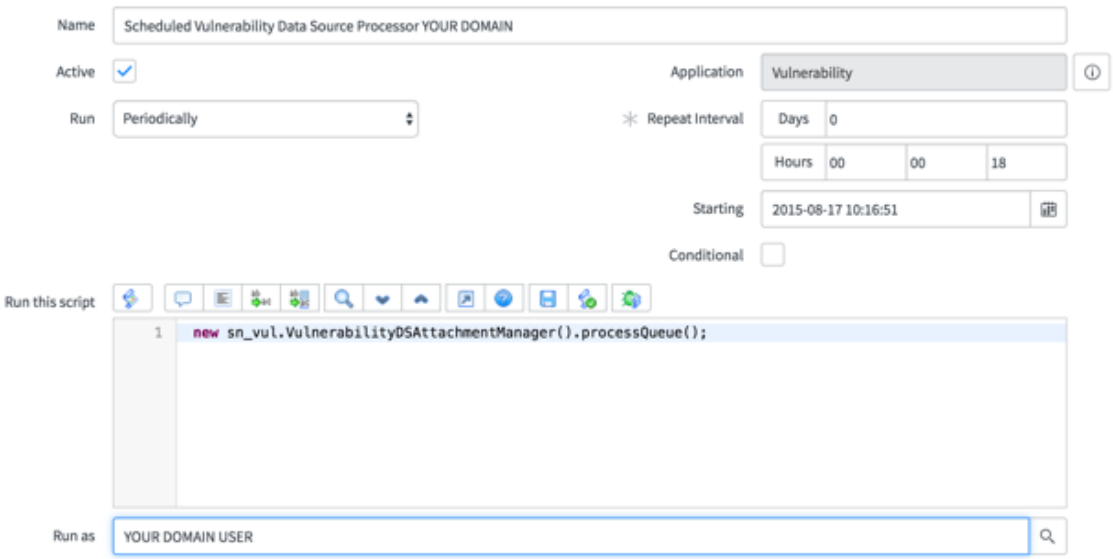
   a. Navegar até **Tudo** > **Definição do Sistema** > **Trabalhos agendados**.

   b. Cópia **Processador da fonte de dados de vulnerabilidade programada** no domínio.

   c. Para identificar o trabalho agendado, anexe o domínio ao nome.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Em **Executar como** , altere **run_as** Usuário para o usuário que você criou na Etapa 2.

A partir da v20.1 de Resposta a vulnerabilidades, as seguintes mudanças de script são enviadas com o sistema de base.

4. **Nota:** Edite a ação de IU a seguir para que a integração seja executada no **run_as** domínio do usuário.

   Edite o. **Executar agora** Ação de IU no **Integração do Qualys Host Detection** trabalho de integração para adicionar este bloco de código à parte superior do arquivo.

   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. **Nota:** Edite as inclusões de script a seguir para que a integração seja executada no **run_as** domínio do usuário.

   Edite o. **VulnerabilityIntegrationUtils** método de inclusão de script **AddaIntegrationExecutar** para adicionar o código realçado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Edite o. **VulnerabilityIntegrationUtils** método de inclusão de script, **AddProcessExecutar** para adicionar o código realçado na imagem a seguir .
   Código addProcessRun

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Edite o. **VulnerabilityIntegrationUtils** método de inclusão de script, **CopyProcess** para adicionar o código realçado na imagem a seguir.
   CopyProcess code

Script

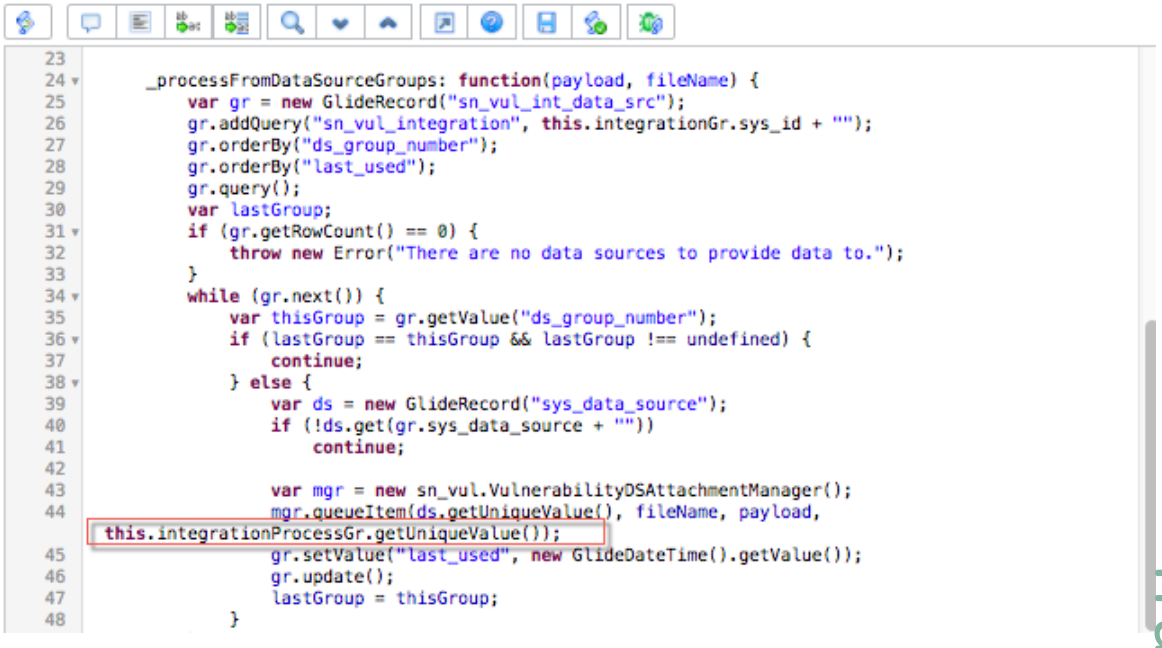
```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```

8. Edite o. **DataSourceVulnReportRefreshProcessor** método de inclusão de script **_ProcessFromDataSourceGroups** para mudar este código original:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

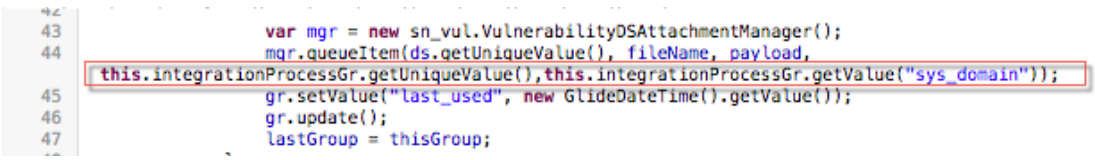
Código _processFromDataSourcesGroups original



```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

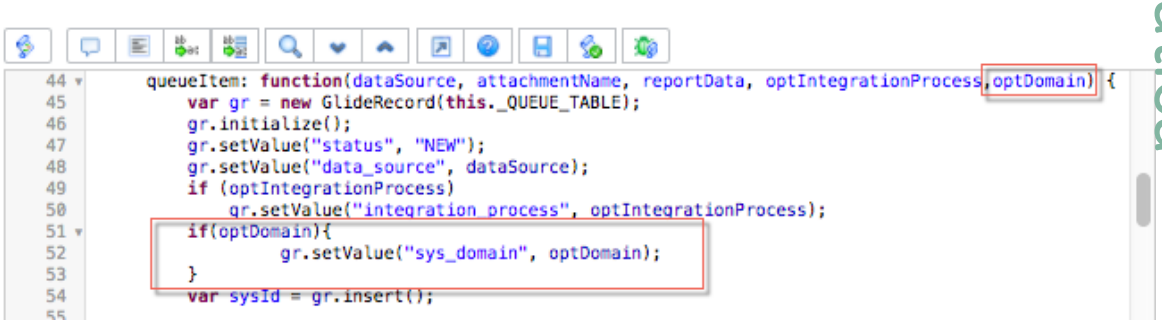
Para:

Código _processFromDataSourcesGroups editado



```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

9. Edite o. **VulnerabilityDSAttachmentManager** método de inclusão de script, **QueueItem** para adicionar os seguintes blocos de código realçados
QueueItem



```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_GetNext

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

Função _processQueueEntry

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

Neste ponto, você está pronto para importações separadas por domínio.

Nota: Se você tiver várias implantações de um Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações repita este processo para cada implantação.

Crie e ofereça suporte a vários domínios na estrutura de trabalhos em segundo plano

Os trabalhos em segundo plano em produtos de resposta a vulnerabilidades são projetados para serem executados por longos períodos para executar vários processos em seus registros. Os processadores de trabalho em segundo plano são enviados com o sistema de base que é executado por meio do usuário do sistema e criam registros no domínio global.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Administrador de Domínio** > **Domínios**.
2. Crie um domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como criar um domínio, consulte Criação de um domínio .

Para cada domínio criado, crie um usuário e atribua o usuário ao domínio. Suponha que este usuário seja um espaço reservado run_as para o domínio. É o equivalente ao usuário VR.System no domínio global. Este usuário precisa de acesso aos dados de vulnerabilidade.

3. Mude run_as dos trabalhos agendados `Scheduled Background Job Manager` e `Close the parent background job`.

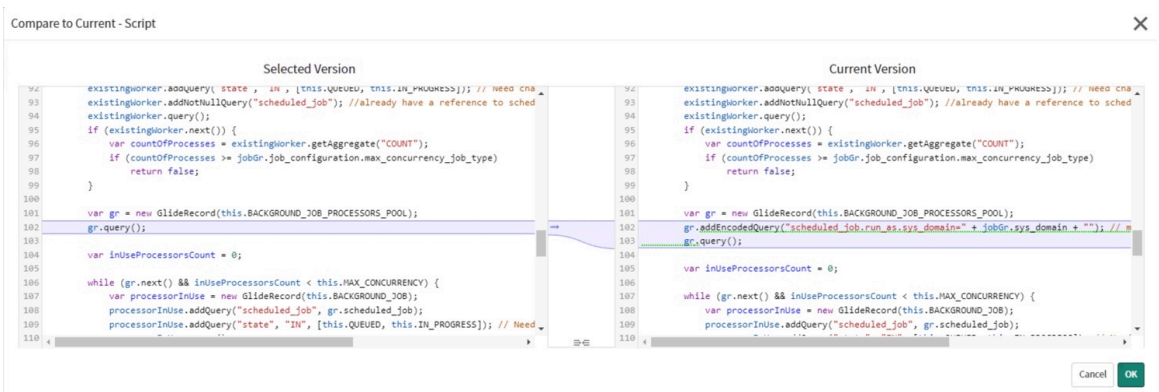
   Se você tiver vários domínios criados, duplique este trabalho e mude o usuário run_as de acordo. Você também pode manter uma cópia dos trabalhos anteriores com o usuário run_as do domínio global em um modo inativo.

   Dez trabalhos de processador (por exemplo, `Background job processor 10`) são enviados com o sistema de base. A execução a desses trabalhos para o usuário separado por domínio. Se vários domínios estiverem presentes, dois trabalhos por domínio serão suficientes, mas esses trabalhos também poderão ser duplicados, se necessário. Mantenha dois trabalhos de processador com usuário run_as no domínio global.

   A partir de v20.0 de Resposta a vulnerabilidades, as seguintes mudanças de script são enviadas com o sistema de base.

4. Modifique a inclusão de script `BackgroundJobManager` e adicione a seguinte linha, conforme mostrado na imagem a seguir.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



Nota: Acionar a reaplicação sob demanda de todas as regras do domínio correto.

Crie uma regra de pesquisa de IC de resposta a vulnerabilidades

. **Regras de pesquisa de IC** o módulo contém regras que são usadas para encontrar o registro correspondente das informações do host recebidas durante as importações de integração de vulnerabilidades de terceiros. As informações do host são correspondidas aos itens descobertos, classes de item de configuração incompatíveis e Configuration Management Database (CMDB).

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribuição. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Criar regras de pesquisa de IC requer avançado ServiceNow e. Resposta a vulnerabilidades experiência. Em vez de modificar um dos existentes pesquisa considere copiá-lo e modificar a cópia. Quando você estiver satisfeito com que a nova regra faz o que você deseja, desative o original.

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

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Regras de pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ○ **Script** Script pré-criado (endereço IP, nome DNS e assim por diante) ou script personalizado. ○ **Correspondência de campo** : Pesquisa na tabela ou campo no CMDB.
Tipo	Tipo usado com o Script **Método de pesquisa** .
Ordem	Ordem de precedência da regra. Regras com a ordem mais baixa são avaliados primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Origem	Origem usada como entrada para esta regra.
Campo de origem	Campo de origem usado como entrada para esta regra. Selecione qualquer campo, mas ele será tratado como um valor da cadeia de caracteres.
Condição	Condição baseada na qual a regra de pesquisa de IC é aplicada. Esta condição depende do atributo do scanner de terceiros. **Nota:** O atributo do ativo faz parte da carga. Ele é recebido do scanner de terceiros. Consulte a tabela Itens descobertos para obter exemplos de carga útil.
Script	Script de amostra editável, com base em **Tipo** é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão. **Nota:** A função de processo tem três parâmetros: `rule`, `sourceValue`e `sourcePayload`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisar na tabela	Tabela para pesquisar no CMDB. Usado com correspondência de campo **Método de pesquisa** .
Pesquisar no campo	Campo que contém informações que podem ser usadas para localizar um IC. Usado com a correspondência de campo **Método de pesquisa** . Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.

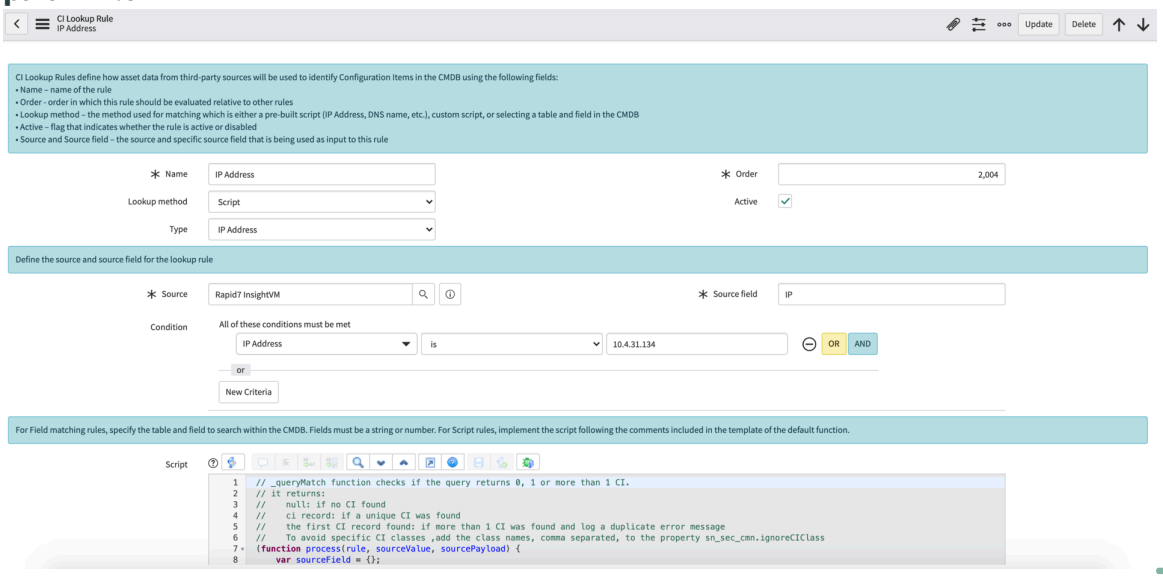
4. Clique em **Enviar**.

Para obter mais informações Informações de implementação para regras de pesquisa de IC, consulte, Etapas para ajudar a evitar registros duplicados ou órfãos após a execução Resposta a vulnerabilidades Regras de pesquisa de IC.

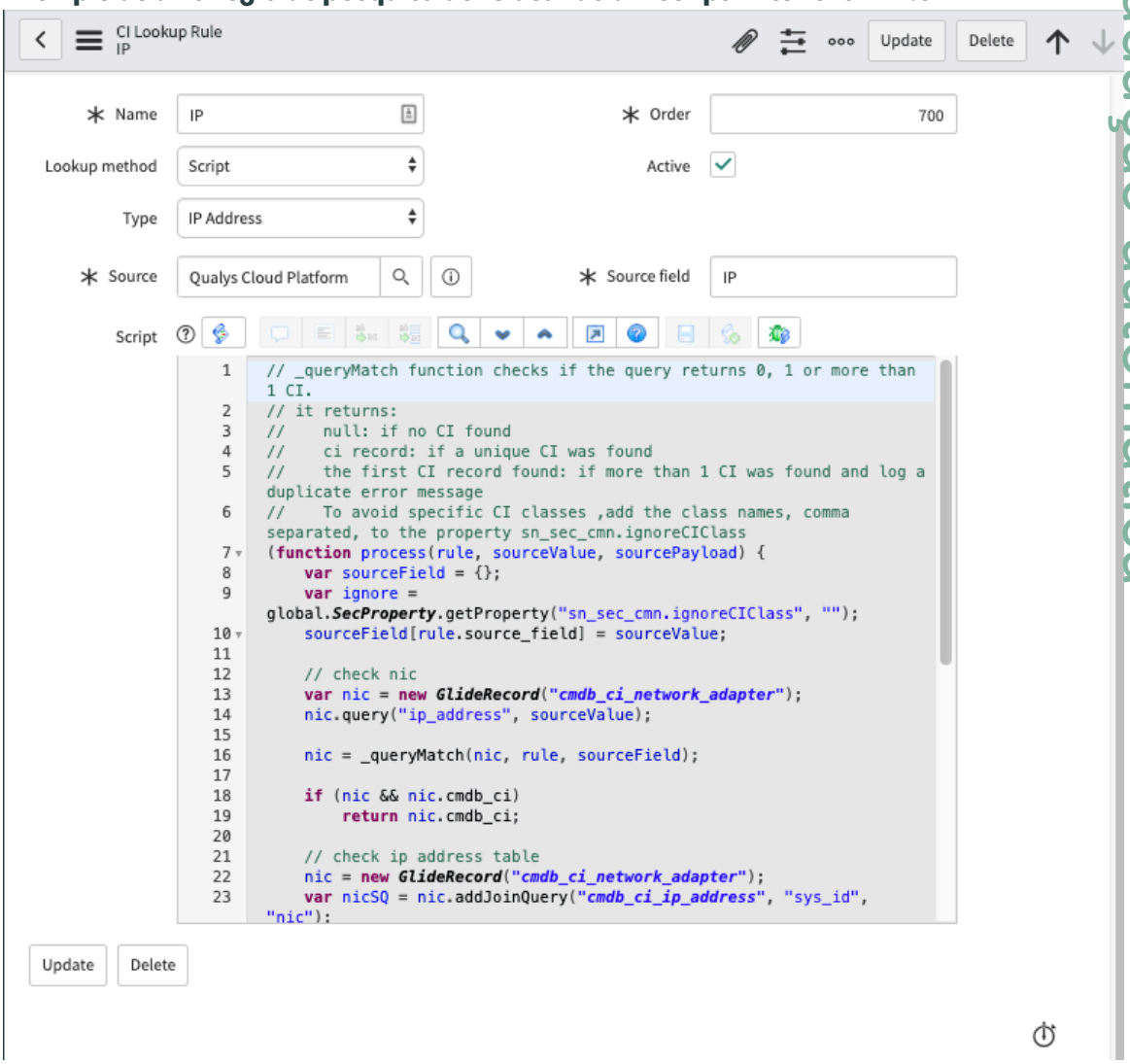
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de uma regra de pesquisa de IC usando um construtor de condições para V12.0



Exemplo de uma regra de pesquisa de IC usando um script Anterior à V12.0



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Resposta a vulnerabilidades campos de formulário de item vulnerável

Ignorar classes de IC

Para ignorar algumas classes de item de configuração (IC), por exemplo Balanceador de carga [cmdb_ci_lb], ao executar Regras de pesquisa de IC, defina **IgnoreCIClass** [*sn_sec_cmn.ignoreCIClass*propriedade do sistema].

Antes de Iniciar

Função necessária: administrador

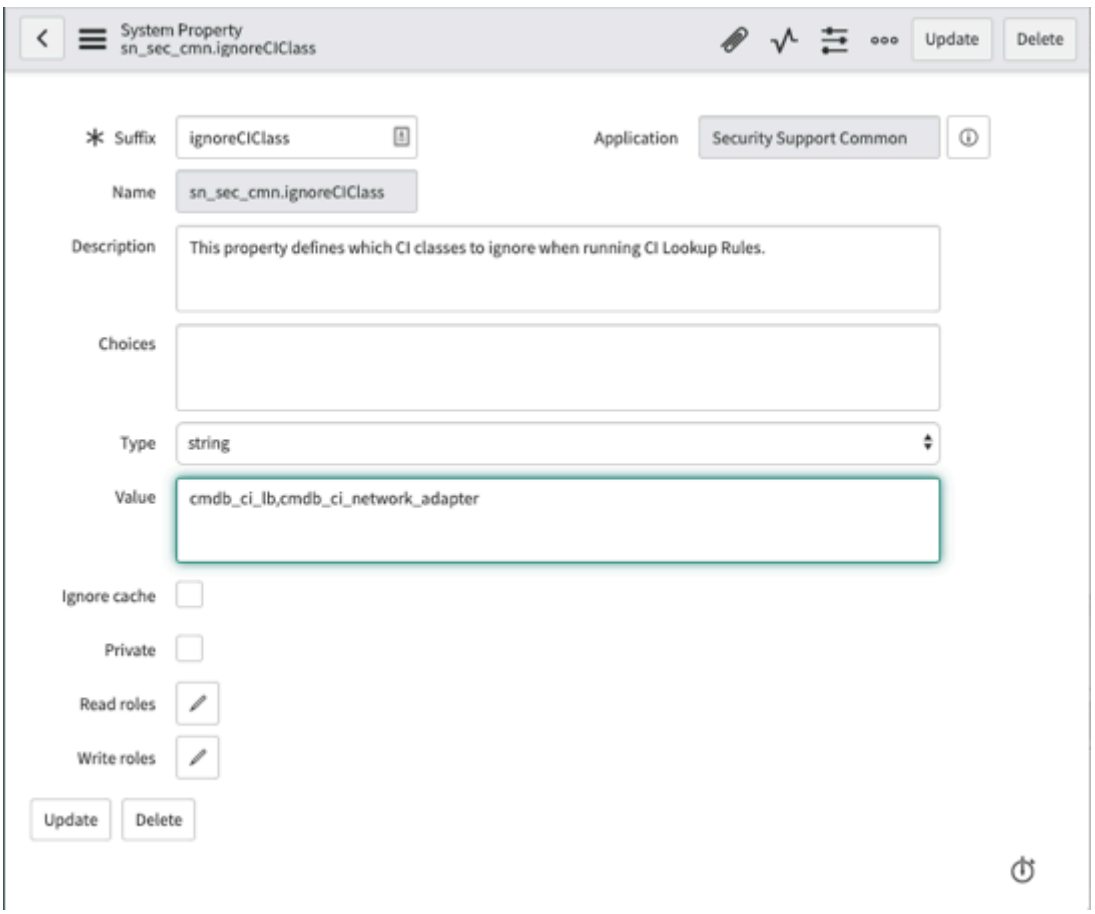
Nota:

. **IgnoreCIClass** a propriedade do sistema está disponível a partir de Resposta a vulnerabilidades v9.0, no entanto, a funcionalidade da propriedade não está disponível após o upgrade de qualquer versão anterior.

Se você fez upgrade de qualquer Operações de segurança aplicação, anterior à versão 9,0, consulte KB0788209 para obter instruções sobre como habilitar esta funcionalidade.

Procedimento

1. Insira sys_properties.list na barra de navegação esquerda.
2. Clique em **Insira** .
3. Em **Pesquisa** menu, em **Nome** insira sn_sec_cmn.ignoreCIClass .
4. Em **Valor** Caixa de texto, insira as classes de IC a serem excluídas em uma lista separada por vírgulas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
   Esta lista é usada pelas Regras de pesquisa de IC durante a próxima importação. Itens vulneráveis criados durante a importação não são associados a um IC de nenhum tipo listado em **Valor** . `sn_sec_cmn.ignoreCIClass` propriedade do sistema.

Filtrar ICs desativados

Filtre itens de configuração (ICs) desativados ao executar as regras de pesquisa de IC. Para filtrar ICs desativados ao executar as regras de pesquisa de IC do CMDB de operações de segurança, defina **FilterOutDeCommissionedIC** [**sn_sec_cmn.filterOutDeCommissionedIC**] propriedade do sistema como verdadeira.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O valor padrão da propriedade do sistema é Verdadeiro. Esta propriedade só se aplica a regras de pesquisa de IC em Resposta a vulnerabilidades E isso não afeta a lógica de pesquisa de IRE.

Procedimento

1. Insira `sys_properties.list` na barra de navegação esquerda.
2. Selecione **Insira** .
3. Em **Pesquisa** menu, em **Nome** insira `sn_sec_cmn.filterOutDeCommissionedIC` Para filtrar os ICs desativados.
4. Em **Valor** caixa de texto, insira o valor verdadeiro ou falso.
   O valor padrão é verdadeiro.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação. . `sn_sec_cmn.filterOutDeCommissionedIC` A propriedade do sistema filtra ICs que atendem às condições mostradas abaixo ao executar as regras de pesquisa.

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
      var install_status = false;
      var life_cycle_stage_status = false;
      // check for property
      if (filterDecommissionCi == "true") {
         if (gr.isValidField("install_status"))
            install_status = gr.install_status == 7;
         if (gr.isValidField("life_cycle_stage_status"))
            life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
      }
      return install_status || life_cycle_stage_status;
```

Promover ICs automaticamente

Edite a cadeia de caracteres JSON no **AutoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] Propriedade do sistema para que suas regras de pesquisa de item de configuração (IC) promovam automaticamente todos os ICs do CMDB de operações de segurança para entradas correspondentes na tabela [cmdb_ci].

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O tipo de propriedade do sistema é "String" e requer que você insira uma cadeia de caracteres JSON. Esta propriedade é ativada por padrão e promove ICs correspondentes ao executar as regras de pesquisa de IC.

Scripts de pesquisa personalizados podem retornar registros de tabela secundária do script. Para esta propriedade, `_autoPromoteCI.CIIdentify Script Include`Usa o IC retornado pelo script de pesquisa e atravessa automaticamente os relacionamentos para chegar ao `cmdb_cie` devolva-o.

Para substituir a lógica de promoção automática, ou seja, para adicionar ou atualizar novas classes de IC, adicione o objeto JSON no campo Valor em [**sn_sec_cmn.autoPromoteFields**] propriedade do sistema.

Procedimento

1. Insira sys_properties.list na barra de navegação esquerda.
2. Selecione **Insira** .
3. Localize [**sn_sec_cmn.autoPromoteFields**] propriedade do sistema e selecione o registro para abri-lo.

   Cadeia de caracteres padrão:

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. Em **Valor** caixa de texto, edite a cadeia de caracteres usando o formato de emparelhamento padrão.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação.

Configure a chave do item vulnerável

Configurar a granularidade do item vulnerável (vi (T) digite Resposta a vulnerabilidades Aplicação para definir o que torna um item vulnerável (vi T) em sua organização.

Antes de Iniciar

Função necessária: administrador

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Principais termos:

IC (Configuration Item, item de configuração)

Um ativo existente listado no seu CMDB.

Vulnerabilidade

Um registro de uma vulnerabilidade conhecida importada do National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE) ou integrações de terceiros com Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item vulnerável

Um item vulnerável é criado quando uma vulnerabilidade importada corresponde a um item de configuração no CMDB.

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade conforme relatada pelos scanners de suas integrações de terceiros. As detecções são importadas e exibidas nos registros de detecção e de item vulnerável em sua instância. Também conhecida como detecção de item vulnerável.

Por padrão, um item vulnerável é uma combinação exclusiva de um item de configuração (IC), uma vulnerabilidade e uma instância de integração. Para criar itens vulneráveis com mais granularidade, adicione portas exclusivas Ou recomendações (somente para vulnerabilidades do Microsoft TVM) de detecções de item vulnerável. Isso ajuda a gerenciar a correção de vulnerabilidades no nível que você considera mais eficaz para sua organização.

Se você quiser criar itens vulneráveis com mais granularidade, configure a chave do item vulnerável para que ela inclua a porta ou recomendação.

- Quando **Incluir porta** itens vulneráveis são criados por portas exclusivas a partir de detecções de itens vulneráveis.
- Quando **Incluir recomendação** habilitado, um item vulnerável separado é criado para cada recomendação associada a uma vulnerabilidade.

Nota: . **Incluir recomendação** A opção aparecerá na IU somente se a integração do Microsoft TVM estiver habilitada em seu ambiente.

A partir do Vulnerability Response V17.1, você pode identificar e corrigir vulnerabilidades do Rapid7 adicionando prova como a chave VI. Para obter mais informações, consulte Adição de prova às chaves de item vulnerável do Rapid7.

Escolha uma opção na tabela a seguir para habilitar a opção Incluir porta.

Três cenários para habilitar a opção Incluir porta com a chave VI pela primeira vez

Se...	Descrição
Uma ou mais das seguintes condições é verdadeira: • Você está atualizando de uma versão de Resposta a vulnerabilidades anterior à 10.0 que não era compatível com detecções de itens vulneráveis. • Você é um novo cliente e não tem dados de Resposta a vulnerabilidades (itens vulneráveis ou detecções de itens vulneráveis) em seu ServiceNow AI Platform® instância. • Você já tem todos os seus registros de itens vulneráveis e dados relacionados excluídos Em sua instância e você está pronto para criar todos os seus dados de Resposta a vulnerabilidades, começando com uma nova importação para incluir VIS diferenciados por porta exclusiva.	Habilitar Incluir Porta. Depois que Incluir porta é habilitada, as detecções importadas criam itens vulneráveis que incluem VIS diferenciados por porta exclusiva, começando com a próxima importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Três cenários para habilitar a opção Incluir porta com a chave VI pela primeira vez

Se...	Descrição
Ambas as condições são verdadeiras: • Você tem a versão 10.0 ou posterior de Resposta a vulnerabilidades E você tem dados de Resposta a vulnerabilidades existentes (itens vulneráveis ou detecções de itens vulneráveis) em sua instância que você deseja preservar. • Você deseja começar a criar novos itens vulneráveis para incluir VIS diferenciados por porta exclusiva.	Habilitar Incluir porta. Suas detecções existentes e os itens vulneráveis associados são preservados. Depois que Include port é habilitada, novas detecções criam novos itens vulneráveis que incluem VIS diferenciados por porta exclusiva, começando com a próxima importação.
Ambas as condições são verdadeiras: • Você tem a versão 10.0 ou posterior de Resposta a vulnerabilidades. • Você tem dados de Resposta a vulnerabilidades existentes (itens vulneráveis ou detecções de itens vulneráveis), mas não deseja preservar seus dados existentes, porque prefere criar seus dados de vulnerabilidade a partir de uma importação nova e deseja incluir o VIS diferenciado por porta exclusiva.	1. Exclua todos os registros de itens vulneráveis e dados relacionados da sua instância. 2. Habilitar Incluir porta. Depois que Include port é habilitada, novas detecções criam novos itens vulneráveis que incluem VIS diferenciados por porta exclusiva, começando com a próxima importação.

Nota:

Se a opção Incluir porta estiver habilitada, mais de um item vulnerável poderá ser criado para um item de configuração. Por exemplo, se houver uma vulnerabilidade para duas portas em um item de configuração, portas 80 e 443, dois VIS exclusivos serão criados, um para cada porta que começa com a próxima importação.

Nota: Certifique-se de que você deseja criar o VIS para incluir o VIS por portas exclusivas antes de habilitar este recurso. Depois de habilitar a chave VI para incluir a porta, você deve primeiro excluir os dados de Resposta a vulnerabilidades antes de desabilitar Incluir porta e retornar à importação de dados de vulnerabilidade usando a granularidade de chave VI padrão, ou seja, em que os VIS são criados para a porta, mas não diferenciados por uma porta exclusiva. Para obter mais informações sobre como excluir seus dados de vulnerabilidade, consulte Exclua todos os seus registros de itens vulneráveis e dados relacionados em Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configurar Item vulnerável G. ranularidade**.

   O campo Atualizado pela última vez exibe a data em que a chave VI foi configurada pela última vez.

2. Selecione . **Incluir Porta** marque a caixa para habilitá-la.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você configurou a integração do Microsoft TVM, o. **Incluir recomendação** a opção também está disponível. Isso permite dividir itens vulneráveis por recomendação exclusiva de dados do Microsoft TVM.

3. Selecione **Save** (Salvar).
   A caixa de diálogo Confirmação é exibida.

   Se você não tiver registros de detecção de item vulnerável em sua instância, as detecções de item vulnerável e os itens vulneráveis serão criados por porta exclusiva, começando com sua próxima importação.

   Se você tiver detecções de itens vulneráveis e itens vulneráveis em sua instância, as detecções existentes e os itens vulneráveis associados serão preservados. Novas detecções criam novas vulnerabilidades que incluem VIS diferenciados por porta exclusiva, começando com a próxima importação.

O que Fazer Depois

Verifique se os itens vulneráveis por porta são exibidos nos registros de detecção de item vulnerável e de item vulnerável. Para obter mais informações, consulte Exibir Resposta a vulnerabilidades dados de detecção de item vulnerável.

Adição de prova às chaves de item vulnerável do Rapid7

Adicione prova como uma chave de item vulnerável (VI) para Rapid7 VIS. Incluir a prova de vulnerabilidades específicas habilita o. Rapid7 Integração do scanner para criar VIS para cada prova recebida de Rapid7.

Uma chave VI é a combinação de vulnerabilidade, item de configuração (IC) e instância de integração. Dividir detecções em diferentes VIS com base na prova cria vários VIS. Você pode atribuir as vulnerabilidades aos responsáveis pela correção apropriados.

Por exemplo, pode haver duas detecções com a mesma vulnerabilidade e IC, mas com provas diferentes, levando à criação de um VI A partir de Resposta a vulnerabilidades V17.1, você pode identificar e corrigir vulnerabilidades adicionando prova como a chave VI.

Você pode adicionar a prova como uma chave VI da seguinte maneira:

Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV** e selecione a opção para incluir prova.

Caso de uso: Incluindo prova na chave vi para VIS existente ou dividir VIS existente com base na prova de detecção

Para criar VIS com base em prova, você pode usar as vulnerabilidades r7 log4j. Por exemplo, você pode usar uma das várias vulnerabilidades r7 log4j, como `R7-apache-log4j-core-cve-2021-44228` , `amazon_linux-cve-2021-44228` ou `amazon-linux-ami-2-cve-2021-44228` .

Se todas as detecções em uma VI tiverem a mesma prova, a VI existente será atualizada para incluir "Proof in the VI Key (external_id)". Se houver várias detecções com provas diferentes, o VI existente será encerrado. As detecções são divididas entre o novo VIS com "Proof in the VI Key (external_id)".

Nota:

Se você fornecer o ID da vulnerabilidade, os VIS existentes serão divididos com base na prova. As novas vulnerabilidades para este ID de vulnerabilidade também têm prova como uma das chaves de VI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exclua todos os seus registros de itens vulneráveis e dados relacionados em Resposta a vulnerabilidades

Remova permanentemente todos os dados de Resposta a vulnerabilidades (itens vulneráveis ou detecções de itens vulneráveis) e dados e registros relacionados do do Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform® instância.

Antes de Iniciar

Exclua registros de detecção de item vulnerável, itens vulneráveis, grupos de vulnerabilidade e quaisquer registros relacionados no Resposta a vulnerabilidades da sua instância. Use este processo para limpar sua instância para importar dados com um novo começo de suas integrações de terceiros ou como um pré-requisito para retornar a configuração de chave de item vulnerável (VI) à configuração padrão. Para obter mais informações sobre como configurar a chave vi, consulte Configure a chave do item vulnerável.

Nota: Esta ação exclui todos os registros de item vulnerável e todos os dados relacionados da sua instância. Depois de excluídos, esses dados não podem ser recuperados. Também requer que você suspenda a importação de dados e desabilite suas integrações de terceiros ativas com Resposta a vulnerabilidades.

É necessário excluir os dados do item vulnerável com este processo antes de alterar a configuração da chave VI. Remover todos os dados garante que todos os itens vulneráveis e as detecções de itens vulneráveis sejam mapeados e atualizados com os dados mais atuais, começando com a próxima importação.

Antes de excluir seus dados, verifique se as seguintes condições se aplicam:

- Você tem a versão 10.0 ou posterior de Resposta a vulnerabilidades instalado. Para obter mais informações, consulte Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros.
- Você deseja desabilitar Incluir porta e retornar a configuração da chave VI para sua configuração padrão.
- Você tem itens vulneráveis e detecções de itens vulneráveis existentes, mas não deseja ou precisa atualizá-los e mantê-los.
- Você determinou que deseja remover todos os dados de Resposta a vulnerabilidades existentes e registros relacionados para limpar sua instância.

Função necessária: sn_vul.vulnerability_admin

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Integrações de Vulnerabilidade**.
2. Registre todas as integrações ativas exibidas.

   Todas as integrações ativas listadas com trabalhos agendados são desabilitadas antes da exclusão de todos os itens vulneráveis e dados relacionados para que nenhum novo dado seja importado durante a remoção de dados. Gravar esta lista ajuda você a ativar suas integrações após a conclusão da exclusão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Revise Como excluir dados de resposta a vulnerabilidades existentes para reimportação artigo na Base de conhecimento HI.
4. Se uma mensagem de aviso for exibida impedindo que você grave na coluna Ativo, para desabilitar as integrações ativas, siga estas etapas.
   a. Na coluna Nome, clique em um item para abrir o registro.
   b. Se você não puder editar a caixa de seleção Ativo, clique em **aqui** link para editar o registro.
   c. Clique em **Ativo** caixa de seleção para desabilitar a integração e cancelar o próximo trabalho agendado.
   d. Clique em **Atualização** para salvar suas mudanças e retornar à lista.
   e. Verifique se você desabilitou todas as integrações ativas da lista Integrações.
      Depois que você desabilita uma integração, ela não é mais exibida na lista de integrações ativas. Para exibir uma lista de integrações inativas e localizar todas as integrações desabilitadas após excluir todos os dados de vulnerabilidade, na coluna Ativo na parte superior, insira `falso` .
5. Continue com as etapas no artigo da base de conhecimento para excluir os dados de vulnerabilidade existentes.
6. Depois de confirmar que todos os dados foram excluídos com sucesso, navegue até **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.
7. No formulário:
   - Se você excluiu dados porque prefere criar seus dados de vulnerabilidade para incluir a porta de uma nova importação, habilite Incluir porta e clique em **Salvar** .
   - Se você excluiu dados porque deseja retornar a chave VI à configuração padrão, desabilite Incluir porta e clique em **Salvar** .

   Para obter mais informações, consulte Configure a chave do item vulnerável.

Filtrando em Resposta a vulnerabilidades

Regras de tarefa de correção, calculadoras e regras de atribuição usam condições durante a importação, criadas usando o. **Construtor de condições** . As mudanças em seus critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

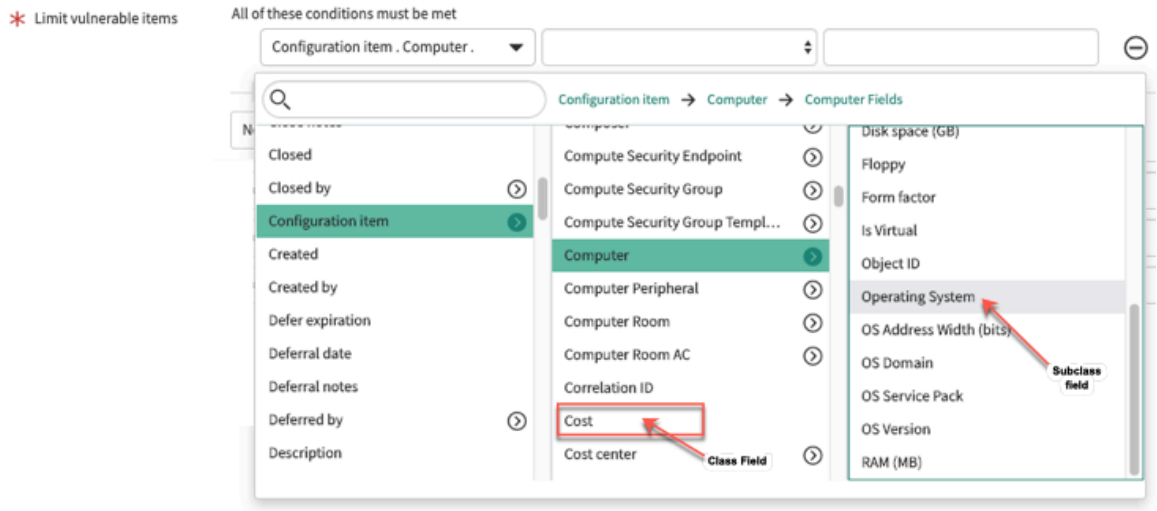
As regras e calculadoras fornecidas com o sistema de base são otimizadas para desempenho. Editar ou criar regras ou calculadoras toma cuidado e pode exigir ambos ServiceNow e. Resposta a vulnerabilidades experiência.

Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão . Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro poderá ser caro para construir e avaliar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por exemplo, filtrando em **Item de configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de classe e não um campo de subclasse de **Item de configuração**.



Item de configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Esse processo pode levar muitos milissegundos, o que se soma rapidamente, quando milhões de itens vulneráveis estão sendo importados e afeta o desempenho.



Nota: Usar a condição [Contém] é como uma pesquisa curinga e pode causar impacto no desempenho. Usar [IS], sempre que possível, é mais eficiente.

Mapeamento de gravidade para Resposta a vulnerabilidades

O Vulnerability Response é enviado com o National Vulnerability Database (NVD) para o mapeamento de gravidade da ServiceNow normalizado. As integrações de terceiros da ServiceNow fornecem mapeamentos de gravidade após a instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Mapeamento de gravidade da integração de vulnerabilidades do Rapid7

Normalized_severity

Calcule normalized_severity na entrada de terceira parte usando a severidade proveniente de **sn_vul_nvd_entry** tabela. Isso é definido usando regras de negócio para severidade normalizada de pesquisa em **sn_vul_entry** tabela.

Source_severity

Dados do **severity_score** a tabela está mapeada para **source_severity** enquanto **Integração de vulnerabilidades do Rapid7- API** está em execução.

Prioridade

Este campo está vazio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de gravidade da Integração de vulnerabilidades da Qualys

Normalized_severity

Calcule normalized_severity na entrada de terceira parte usando a severidade proveniente de **sn_vul_nvd_entry** tabela. Isso é definido usando regras de negócio para severidade normalizada de pesquisa em **sn_vul_entry** tabela.

Source_severity

Dados do **SEVERITY_LEVEL** está mapeado para **source_severity** enquanto **Integração da Base de conhecimento da Qualys** está em execução.

Prioridade

Os dados do campo Prioridade são obtidos de **Tabela DE SEVERIDADE** e mapeados para **prioridade** tabela enquanto **Integração do Qualys Host Detection** Está sendo executado usando a regra de negócio mapeada para dados da Qualys.

Nota: As regras de negócio são executadas em segundo plano e verificam a prioridade da Qualys e mapeiam a prioridade. Para mapear os dados da Qualys, o BR é responsável.

Mapeamento de gravidade da integração de vulnerabilidade do Tenable.io

Normalized_severity

Calcule normalized_severity na entrada de terceira parte usando a severidade proveniente de **sn_vul_nvd_entry** tabela. Isso é definido usando regras de negócio para severidade normalizada de pesquisa em **sn_vul_entry** tabela.

Source_severity

Dados de **risk_factor** a tabela está mapeada para **source_severity** enquanto **Integração do plug-in do Tenable.io** está em execução.

Prioridade

Dados de **severity_id** mapeado para **source_severity** . **Integração de vulnerabilidades abertas do Tenable.io** está em execução.

VPR

Dados de **pontuação** mapeado para **Source_risk_score** enquanto **Integração do plug-in do Tenable.io** está em execução.

Dados de **Calculado a partir da pontuação** mapeado para **Source_risk_rating** enquanto **Integração do plug-in do Tenable.io** está em execução.

Mapeamento de gravidade da integração de vulnerabilidade do Tenable.sc

Normalized_severity

Calcular **normalized_severity** na entrada de terceira parte usando a gravidade proveniente da tabela sn_vul_ntd_entry. Isso é definido usando regras de negócio para severidade normalizada de pesquisa em **sn_vul_entry** tabela.

Source_severity

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dados para **Fator de risco** a tabela está mapeada para **source_severity** . **Integração do plug-in do Tenable.io** está em execução.

Prioridade

Dados de **gravidade** recebido como **"ID": "0", "name": "Info", "description": "Informativo"** mapeado para **source_severity** . **Integração de vulnerabilidades abertas do Tenable.io** está em execução.

VPR

Dados de **VprScore** mapeado para **Source_risk_score** enquanto **Integração do plug-in do Tenable.io** está em execução.

Dados de **Calculado a partir do vprScore** mapeado para **Source_risk_rating** enquanto **Integração do plug-in do Tenable.io** está em execução.

Mapeamento de Severidade de TVM

Normalized_severity

Calcule normalized_severity na entrada de terceira parte usando a Severidade proveniente de **sn_vul_nvd_entry** tabela. Isso é definido usando regras de negócio para severidade normalizada de pesquisa em **sn_vul_entry** tabela.

Source_severity

Dados de **gravidade** a tabela está mapeada para **source_severity** enquanto **Microsoft TVM Vulnerability (CVE) integração** está em execução.

Prioridade

Este campo está vazio.

Crie um Resposta a vulnerabilidades mapa de severidade

Resposta a vulnerabilidades o mapeamento de gravidade transforma campos de gravidade de origem de terceiros em campos reconhecíveis em Resposta a vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades Fornecido com o National Vulnerability Database (NVD) para normalizado ServiceNow mapeamento de gravidade. ServiceNow integrações de terceiros, como Qualys Vulnerability Integration forneça mapeamentos de gravidade após a instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Criar ou editar um mapa de severidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Mapeamento de gravidade normalizado**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de gravidade.
Valor de origem	O valor da gravidade da origem.
Valor de meta	O valor da severidade de destino. As opções são: ○ 1- Crítica ○ 2 - Alta ○ 3 – Médio ○ 4 - Baixo(a) ○ 5 - Nenhum

4. Repita a Etapa 3 para cada nível de gravidade de origem.
5. Clique em **Enviar**.

Defina classificações de serviço para Resposta a vulnerabilidades relatórios e listas relacionadas

Dê mais foco à emissão de relatórios e às listas relacionadas em Resposta a vulnerabilidades definindo classificações de serviço. Reduzir o número de classificações de serviço solicitadas pode melhorar o desempenho do Resposta a vulnerabilidades coleta de dados.

Antes de Iniciar

Função necessária: administrador

Nota:

A edição das propriedades do sistema requer ambos ServiceNow e. Resposta a vulnerabilidades experiência.

Procedimento

1. Insira `sys_properties_list.do` na barra de navegação esquerda.
2. Clique em **Insira** .
3. Em **Pesquisa** menu, em **Nome** insira `sn_vul.service_classifications` .
4. Abra a propriedade do sistema *`sn_vul.service_classifications`*.
5. Em **Valor** caixa de texto, insira a lista separada por vírgulas das classificações de serviço desejadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando esta configuração está vazia, todos os serviços são listados.

Exemplos:

Para ver Serviços de negócio, Serviços técnicos e Serviços de aplicações e excluir ofertas de serviço, Serviços compartilhados e serviços não classificados, defina o valor como: **Serviço de negócios, Serviço técnico, Serviço de aplicações** .

Para ver os Serviços de aplicações, defina o valor como: **Serviço de aplicações** .

6. Clique em **Atualizar**.
   Os dados em cada relatório e lista relacionada de item vulnerável são filtrados por classificação de serviço durante a próxima execução do trabalho de análise de desempenho noturno.

Audite campos selecionados na tabela Itens vulneráveis

Habilite a auditoria para campos especificados na tabela Item vulnerável [sn_vul_vulnerable_item]. Este método de auditoria é útil quando você deseja auditar campos que não pode auditar por padrão.

Antes de Iniciar

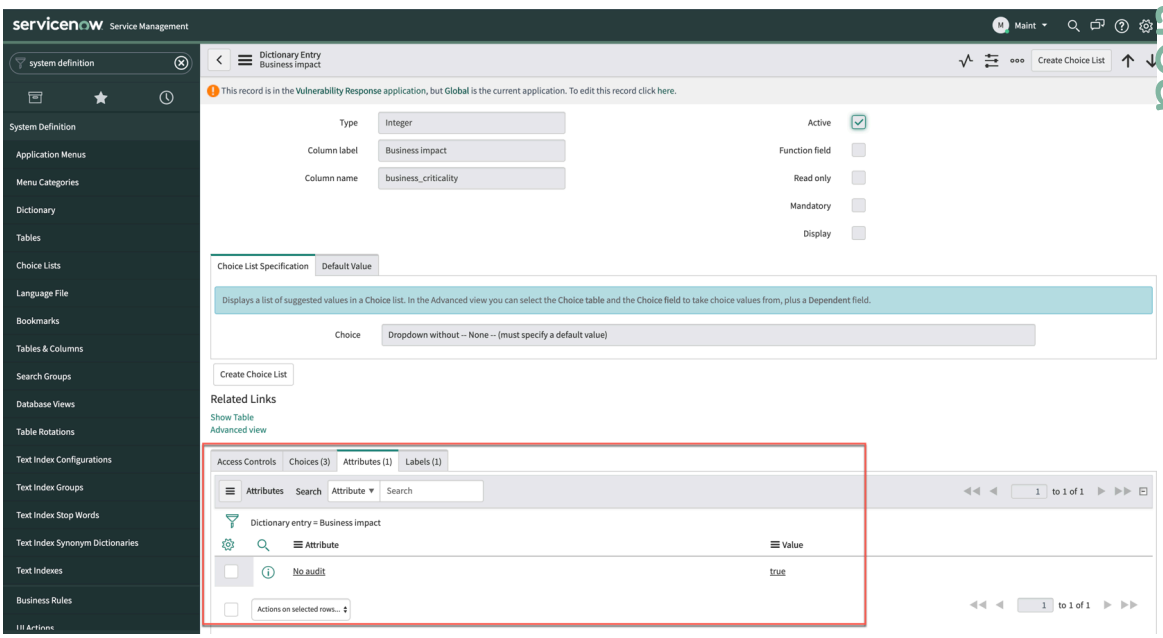
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A tabela sn_vul_vulnerable_item é auditável por padrão. Os campos que têm o atributo no_audit definido como verdadeiro não são auditáveis. Para obter mais informações sobre tabelas de auditoria, consulte Habilitar auditoria para uma tabela .

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Definição do Sistema** > **Tabelas** e pesquise a tabela sn_vul_vulnerable_item.
   A lista de entradas de dicionário da tabela é exibida.
2. Para habilitar a auditoria de um campo, clique no nome da entrada.
   A página Entrada do dicionário dessa entrada é exibida.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegar até **Atributos** > **Nenhuma auditoria**.
   A página Atributo de dicionário é exibida.
4. Para remover o atributo sem auditoria - true, clique em **Excluir** .
   A auditoria para este campo está habilitada.

Resposta a vulnerabilidades configuração da estrutura de trabalho em segundo plano

Defina a estrutura de trabalho em segundo plano em seu ServiceNow AI Platform® instância. Essas mudanças de configuração podem ajudar você a melhorar o desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

O que você pode editar na estrutura de trabalho em segundo plano

Com o módulo de configuração de trabalho em segundo plano, você tem as seguintes opções de configuração na estrutura:

- Você pode definir o número de trabalhos em segundo plano que são executados simultaneamente para Resposta a vulnerabilidades processos.
- Para trabalhos longos que são executados em segundo plano e processam grandes quantidades de dados, você pode criar partições para processar dados em blocos menores.
- Você pode cancelar um trabalho.

Por que configurar a estrutura de trabalho em segundo plano

Trabalhos em segundo plano em seu ServiceNow AI Platform® são projetados para serem executados por longos períodos de tempo para executar vários processos em seus registros no Resposta a vulnerabilidades. Anteriormente, esses trabalhos eram baseados em regras de negócios executadas de forma assíncrona. Não há limite para o número desses trabalhos que podem ser executados em segundo plano em sua instância para que as grandes quantidades de registros afetados por esses trabalhos possam ser processados. Quando vários trabalhos que demoram muito tempo para serem concluídos são executados simultaneamente em segundo plano, os recursos do sistema usados para executar seus trabalhos agendados são afetados, o que, por sua vez, pode afetar negativamente seu desempenho.

Configurar a estrutura de trabalho em segundo plano pode ajudar você a melhorar seu desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

Termos principais

Capacidade do trabalho

Descreve os trabalhos específicos. Por exemplo, um trabalho específico pode incluir os seguintes recursos:

- O trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo.
- O trabalho pode ser particionado.
- O trabalho pode ser cancelado durante a execução.

Simultaneidade

Refere-se a trabalhos ou partes de trabalhos executados em paralelo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Partição

Partições são partes de trabalhos que podem ser divididas para que possam ser processadas em paralelo para alcançar um melhor desempenho. Geralmente se refere a trabalhos com tempos de execução longos.

Configuração do trabalho

Refere-se às configurações de um trabalho agendado específico.

Trabalho programado

Trabalhos agendados são trabalhos automatizados que podem ser realizados em um horário específico ou em um cronograma recorrente.

Recursos do sistema

Refere-se à quantidade de recursos do sistema que você deve oferecer suporte a um determinado número de trabalhos em segundo plano e trabalhos agendados em seu ambiente.

Propriedade do sistema

As propriedades do sistema armazenam informações de configuração que raramente ou nunca mudam. Cada vez que você muda ou adiciona uma propriedade do sistema, o sistema limpa o cache para manter todos os nós no cluster sincronizados. Esta limpeza de cache afeta o desempenho.

Regra de negócio

Uma regra de negócio é um script do lado do servidor que é executado quando um registro é exibido, inserido, atualizado ou excluído ou quando uma tabela é consultada. As regras de negócio executam tarefas como alterar valores automaticamente nos campos de formulário quando determinadas condições são atendidas ou criar eventos para notificações por e-mail e ações de script.

Caso de uso para definir a estrutura de trabalho em segundo plano

Por exemplo, o trabalho em segundo plano que aplica regras de destino de correção para registros de item vulnerável (Vits) e registros de item vulnerável (AVITs) de resposta a vulnerabilidades da aplicação processa simultaneamente grandes quantidades de registros com várias tarefas.

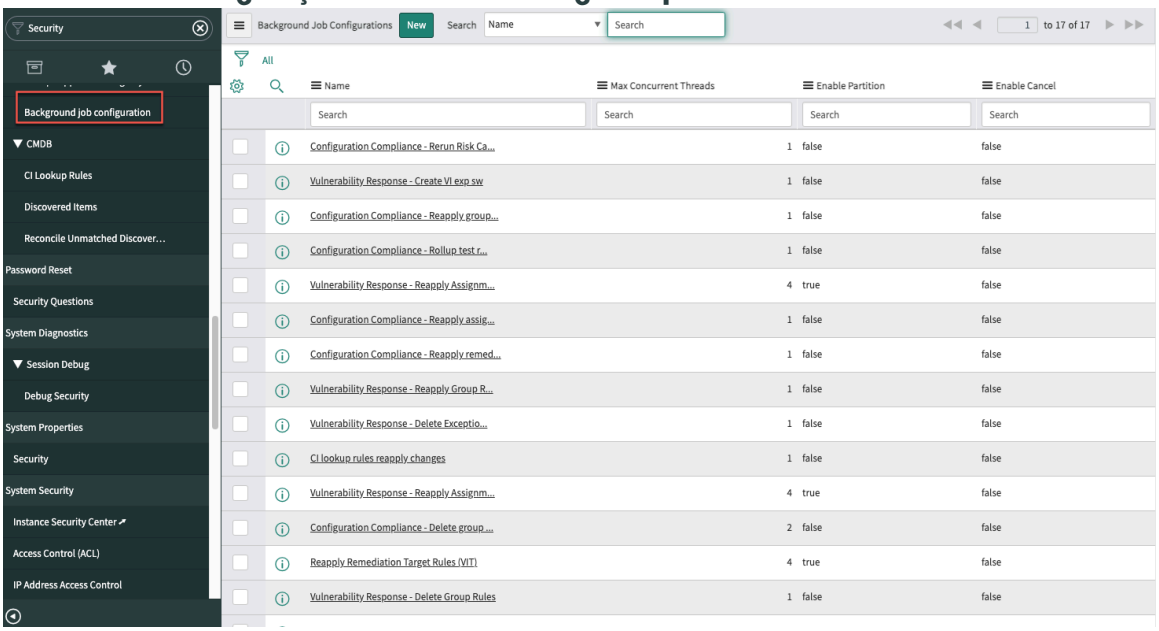
Dependendo do tamanho da importação e do número de registros que você tem em seu ambiente, este trabalho pode usar uma grande quantidade de recursos do sistema disponíveis e levar muito tempo para ser concluído com sucesso. Os trabalhos de manutenção do sistema ou outros trabalhos agendados podem ser executados mais lentamente.

O módulo de configuração de trabalho em segundo plano, os trabalhos são listados por nome e um ID de configuração exclusivo. Nesses registros, você pode definir quantas tarefas deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para processar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O módulo de configuração de trabalho em segundo plano



Para obter mais informações sobre as etapas necessárias para definir as configurações de trabalho em segundo plano, consulte Defina configurações de trabalho em segundo plano em Resposta a vulnerabilidades.

Defina configurações de trabalho em segundo plano em Resposta a vulnerabilidades

Defina quantas tarefas você deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para importar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou Gerentes de vulnerabilidades com a função granular sn_sec_cmn.manage_background_job

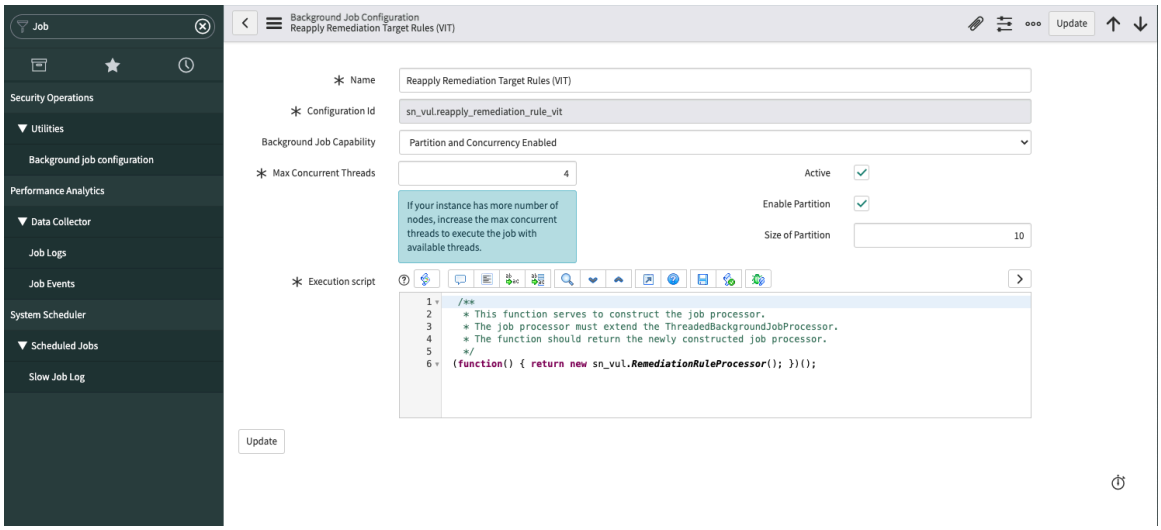
Consulte a seção abaixo das etapas para obter um exemplo.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Configurações de trabalho em segundo plano**.
2. Na coluna Nome, clique em um registro para abri-lo.
3. Edite os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Campo	Descrição
Nome	Nome do trabalho.
ID da configuração	Somente leitura. ID exclusivo usado para identificar o trabalho.
Capacidade de trabalho em segundo plano	Escolha um. ○ Partição e simultaneidade habilitadas - Um trabalho com um tempo de execução longo pode ser dividido e o trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo. ○ Simultaneidade habilitada - O trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo. ○ Cancelamento habilitado - O trabalho pode ser cancelado. ○ Simultaneidade e cancelamento habilitados - O trabalho pode ser executado em paralelo com outro trabalho e ser cancelado. ○ Partição, simultaneidade e cancelamento habilitados - Um trabalho com um tempo de execução longo pode ser dividido, o trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo e o trabalho pode ser cancelado. ○ Nenhum(a) O valor exibido indica se um trabalho é compatível com particionamento, simultaneidade e cancelamento.
Threads simultâneos máximos	Este campo será exibido somente se a simultaneidade for compatível. Insira o número máximo de trabalhos que você deseja que esta configuração execu–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	te em paralelo. Por padrão, o número de trabalhos agendados compatíveis com sua instância é 10. Você pode reduzir este valor se acreditar que pode usar ou ter recursos do sistema inferiores disponíveis para executar seus trabalhos em segundo plano.
Ativo	Habilite ou desabilite o trabalho Se um trabalho estiver desabilitado, você não poderá criar trabalhos desse tipo. Os trabalhos existentes na fila não serão processados.
Habilitar partição	Este campo será exibido somente se o particionamento for compatível. Esta opção permite limitar e definir o número de itens que este trabalho pode processar de uma só vez. O campo Tamanho da partição também é exibido. Se você deixar este campo desabilitado, os trabalhos em segundo plano que oferecem suporte ao particionamento processarão todos os itens em sua instância com este trabalho.
Tamanho da partição	Este campo será exibido somente se o particionamento for compatível. O padrão é 10 000 itens. Insira um valor para o número de itens por bloco de dados que você deseja que este trabalho processe. Esta opção está disponível para trabalhos que processam um grande número de registros, como VIS, tarefas de correção, resultados de testes e grupos de resultados de testes.
Script de execução	Exibe o processador de trabalho usado para executar este trabalho. Um método padrão para trabalhos que oferecem suporte ao particionamento é fornecido.
Cancelar	Este campo só será exibido se o cancelamento de trabalho for compatível. Esta opção é compatível com trabalhos que processam itens descobertos e reaplicam regras de IC.

4. Clique em **Atualizar** para salvar suas mudanças.
   Consulte o exemplo a seguir para saber como verificar os resultados das mudanças de configuração.

Há duas configurações de trabalho de regras de destino de correção incluídas com a aplicação, uma para itens vulneráveis e uma para itens vulneráveis da aplicação:

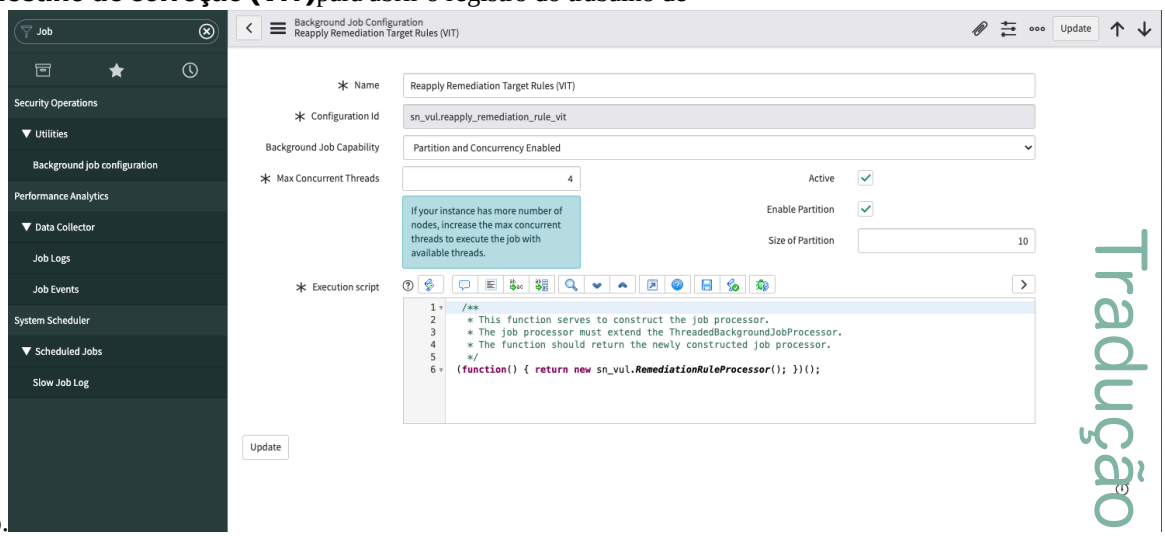
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Reaplicar regras de destino de correção (VIT)
- Reaplicar regras de destino de correção (AVIT)

Suponha que você mude para suas regras de destino de correção e deseja reaplicá-las sem usar a maioria dos recursos de processamento do sistema disponíveis. Para ajudá-lo a limitar os recursos de processamento, você pode controlar o número de trabalhos em segundo plano executados e o número de itens processados por trabalho no módulo Configurações de trabalho em segundo plano.

5. Para definir essas configurações, navegue até **Operações de segurança** > **Configurações de trabalho em segundo plano** e clique em **Reaplicar regras de destino de correção (VIT)**para abrir o registro do trabalho de configuração.

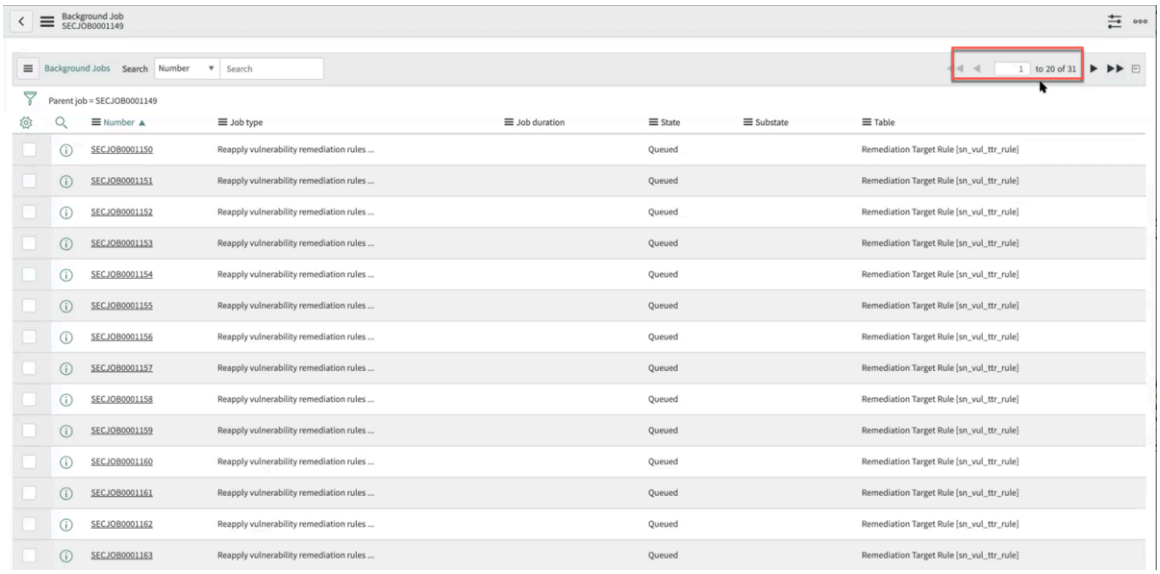


Por exemplo, digamos que você saiba que tem pouco mais de 300 VIS.

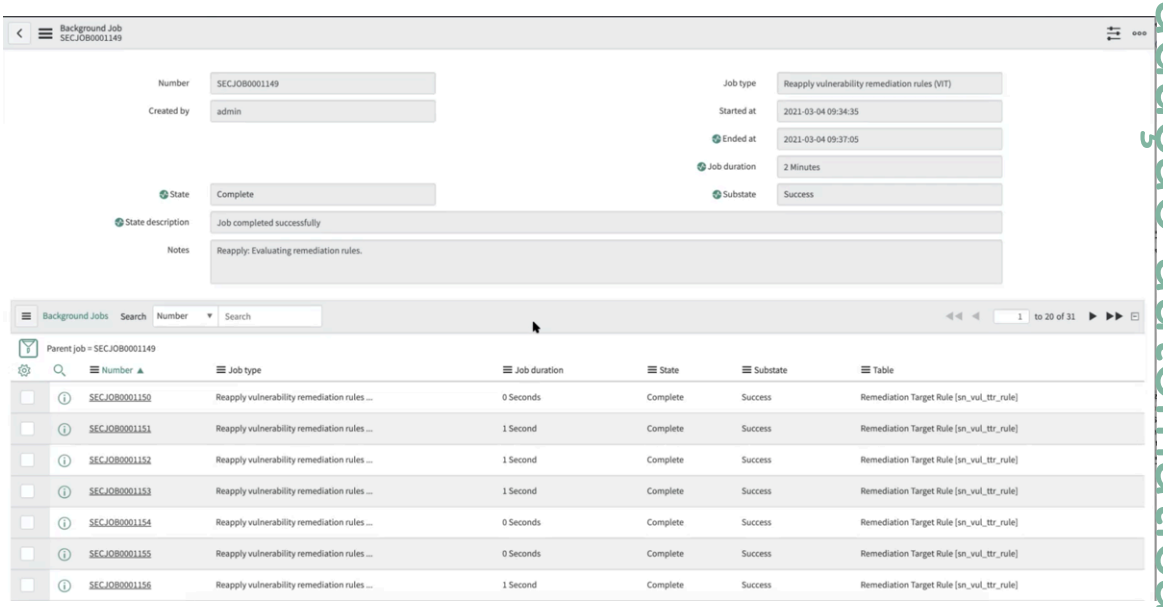
6. No registro de trabalho de configuração em aberto, altere o valor Tamanho da partição de **4** . **10** .
7. Navegar até **Resposta a vulnerabilidades** > **Regras de meta da correção**, Localize a regra de correção de vulnerabilidade Reaplicar que você alterou, selecione o registro na lista e clique em **Aplicar mudanças** Para reavaliar suas regras de destino para seu VIS existente.
   O trabalho Reaplicar regras de correção de vulnerabilidade (VIT) está enfileirado.
8. Clique em **Exibir status** Link para exibir o registro do trabalho em segundo plano e verificar se os trabalhos estão enfileirados, conforme mostrado na imagem a seguir.
   Para este exemplo, 31 trabalhos são criados para processar regras de destino para 307 VIS (máximo de 10 itens por trabalho). Esses trabalhos são trabalhos secundários do trabalho em segundo plano primário. Os trabalhos secundários processam os registros sequencialmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando todos os trabalhos são concluídos com sucesso, os campos são atualizados no registro Trabalho em segundo plano.



Tradução automática

9. Navegue até seus itens vulneráveis e verifique se eles refletem sua nova mudança de regra.

Processamento paralelo avançado para trabalhos em segundo plano no Resposta a vulnerabilidades

Com esta configuração avançada, controle o número total de trabalhos em segundo plano que estão sendo processados paralelamente, independentemente do tipo de trabalho.

Antes de Iniciar

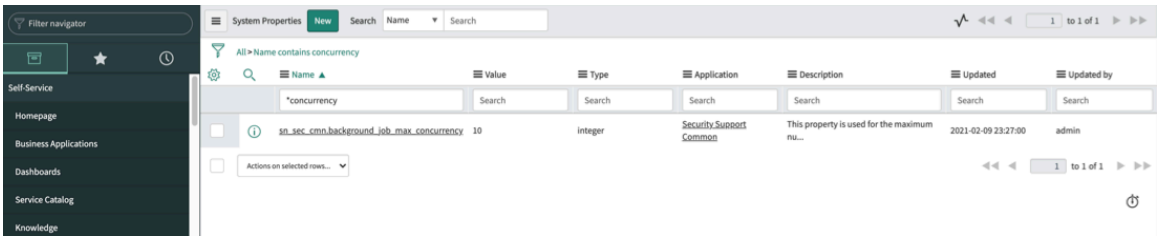
Função necessária: sn_vul.vulnerability_admin ou Gerentes de vulnerabilidades com a função granular sn_sec_cmn.manage_background_job

Nota: Este procedimento requer conhecimento avançado de programação.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No Navegador de filtros, insira **sys_properties.list** e localize *sn_sec_cmn.background_job_max_concurrency*propriedade do sistema.



2. Clique nele para abrir o registro.

   Por padrão, o *sn_sec_cmn.background_job_max_concurrency*a propriedade do sistema executa no máximo 10 trabalhos em segundo plano em paralelo.

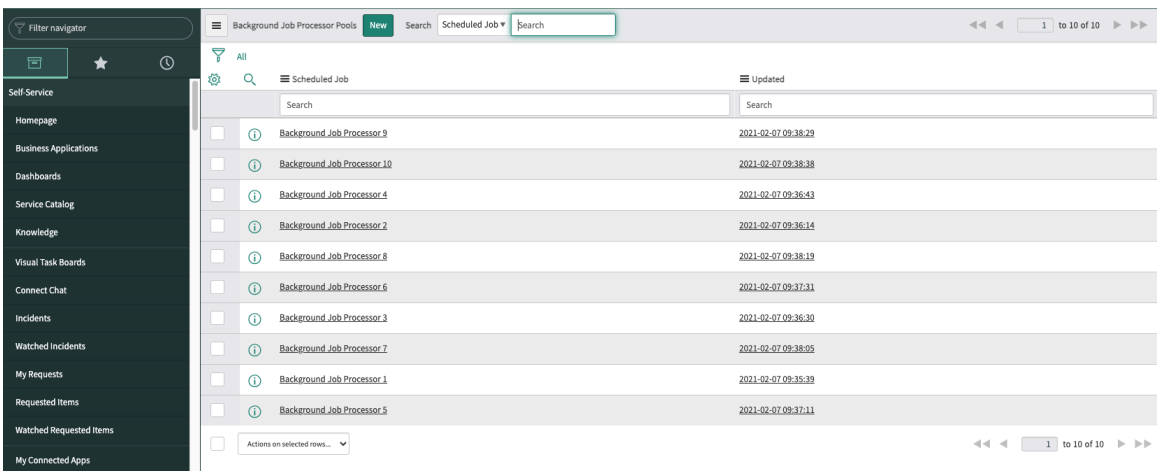
   Se sua instância tiver um número baixo de nós, você poderá reduzir esse valor na propriedade do sistema. Por exemplo, digamos que você tenha sete regras de atribuição em sua lista Regras de grupo. No registro de configuração de trabalho Reaplicar regras de atribuição, três trabalhos são definidos para o máximo de threads simultâneos. Seu valor de simultaneidade para sua estrutura é 10, mas seu sistema é uma instância de nó único, portanto, você pode processar dois trabalhos particionados do trabalho Reaplicar regras de atribuição simultaneamente. Se você definir o Máximo máximo de threads simultâneos para um registro de trabalho Regras de atribuição, todos os tipos de trabalho Reaplicar regras de atribuição serão processados sequencialmente.

   Por outro lado, se sua instância tiver mais nós, você poderá aumentar esse valor, mas também deverá adicionar mais trabalhos agendados para fazer essa mudança.

   Para aumentar o número de trabalhos agendados, duplique um trabalho agendado quantas vezes forem necessárias para corresponder ao valor em que você aumentou sua propriedade do sistema. Por exemplo, por padrão, há 10 trabalhos agendados. Se você quiser 20 trabalhos, você deve duplicar um trabalho 10 vezes.

   Os dez trabalhos agendados incluídos com ServiceNow AI Platform® para processamento são exibidos na tabela sn_sec_cmn_background_job_processor_pool.

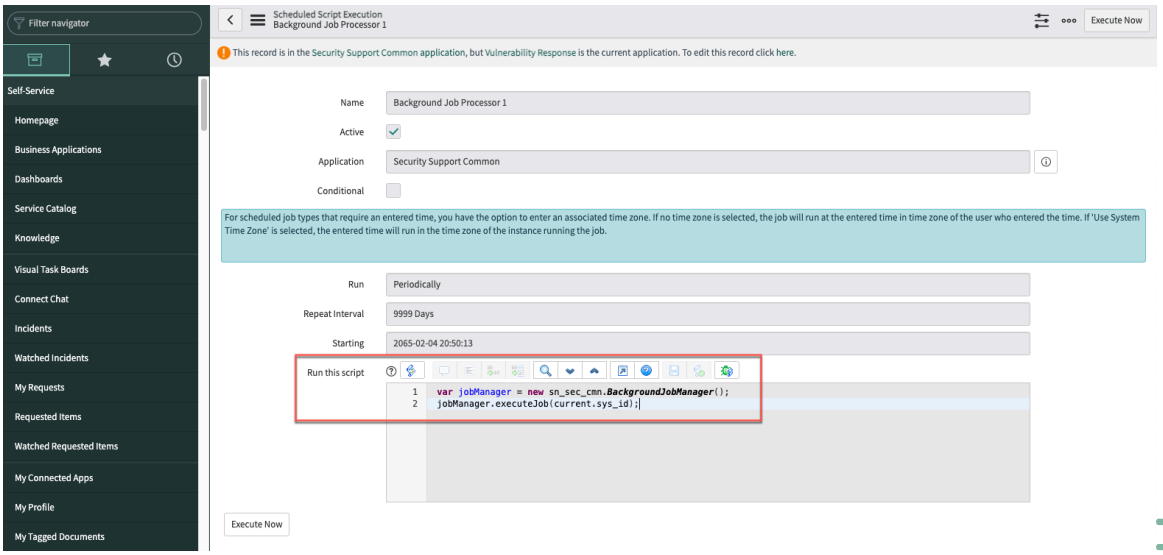
3. No Navegador de filtros, insira **sn_sec_cmn_background_job_processor_pool.list**



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em um trabalho para copiá-lo e duplicá-lo quantas vezes forem necessárias para que o número de trabalhos corresponda ao valor em que você aumentou sua propriedade do sistema.



5. Depois que o trabalho agendado for definido, adicione uma referência clicando em **Novo** na lista sn_sec_cmn_background_job_processor_pool do trabalho copiado.

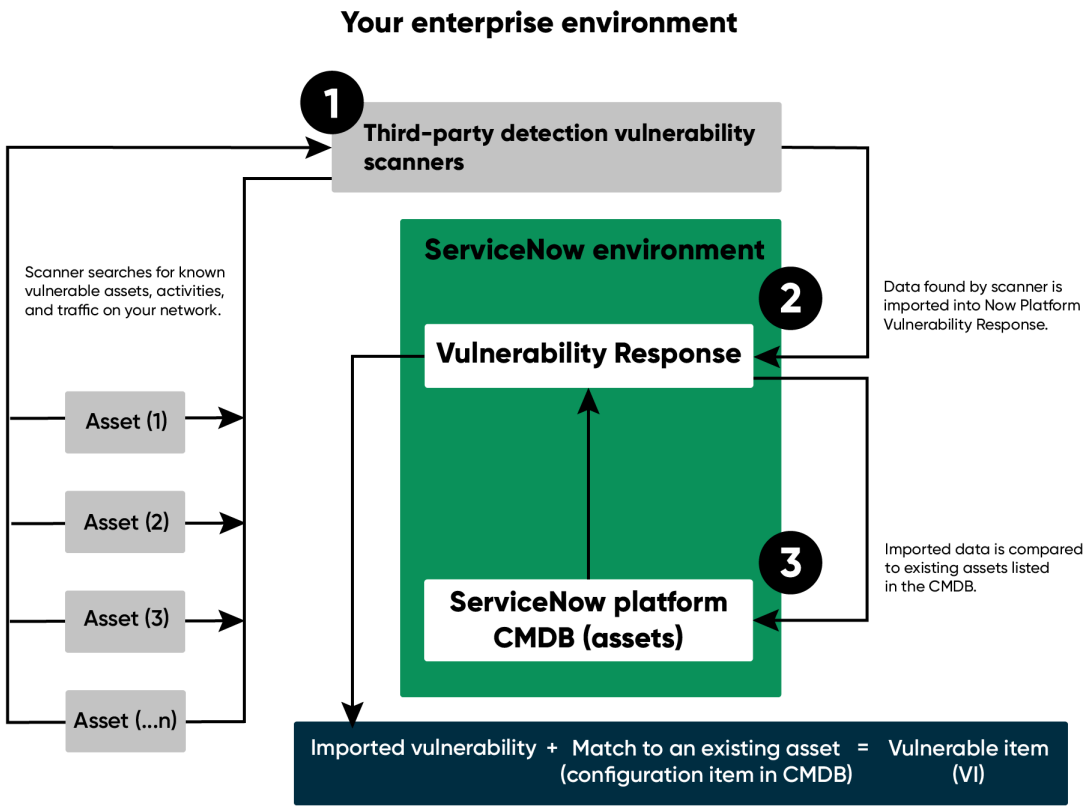
Integrações do Resposta a vulnerabilidades

Resposta a vulnerabilidades suporte para integrações de terceiros. Estão incluídas nesta seção algumas diretrizes básicas para desenvolver suas próprias integrações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de terceiros



Vulnerabilidades importadas do National Vulnerability Database (NVD) e dados de detecção de scanners de terceiros são reconciliados com os ativos no CMDB. Quando uma vulnerabilidade importada corresponde a um ativo existente, um item vulnerável é criado. Os itens vulneráveis são agrupados automaticamente em tarefas para correção, risco pontuado com contexto de negócios, priorizados e atribuídos às equipes apropriadas para correção.

Nota:

Integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável (VI) nas integrações. Por exemplo, desduplicação de VI entre Rapid7 e. Qualys não está disponível.

No entanto, as discrepâncias na contagem de detecção entre um scanner de terceiros (por exemplo, Qualys) Para ver seu ServiceNow As instâncias são esperadas, já que desduplicamos IPs, portas e assim por diante.

Para obter informações sobre integrações de terceiros compatíveis com Resposta a vulnerabilidades de aplicações consulte, Integração do Resposta a vulnerabilidades de aplicações a outras aplicações

- Integração de KEV (Knowned Exploit Vulnerability, vulnerabilidade de exploração conhecida da CISA)
- Noções básicas sobre a integração de vulnerabilidades do Microsoft Threat and Vulnerability Management
- Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM
- Noções básicas sobre as integrações de NVD
- Integração da vulnerabilidade da Qualys
- Noções básicas do Integração com Rapid7 Vulnerability
- Shodan Exploit Integration
- Noções básicas sobre a Integração de vulnerabilidades do Tenable
- Integrações da Solução do Microsoft Security Response Center Solution Integration

. Integração com a solução Microsoft Security Response Center está disponível com Solução de gestão de vulnerabilidade. Para obter informações sobre a instalação e configuração do Integração com a solução Microsoft Security Response Center e o. Red Hat Solution Integration, consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. Você pode configurar, editar, programar e iniciar sob demanda o. Integração com a solução Microsoft Security Response Center e o. Red Hat Solution Integration No Assistente de configuração.

Anotações adicionais para integrações

Se várias implantações forem compatíveis com uma integração, consulte Crie importações separadas por domínio para uma integração.

- Você pode instalar, configurar, programar e iniciar sob demanda muitas das aplicações de integração no Assistente de configuração.
- Você pode instalar o. Integração com Rapid7 Vulnerability Aplicação do Assistente de configuração, mas a configuração não é compatível com esta integração no Assistente de configuração. Para obter mais informações, consulte Instalar o Integração com Rapid7 Vulnerability.
- . Tenable para Resposta a vulnerabilidades A aplicação da Tenable é criada e mantida pela Tenable. Consulte a documentação em Tenable para Resposta a vulnerabilidades.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

A partir do VR v17.1, os seguintes nomes de estado do processo de integração foram atualizados:

Nome do estado anterior a V17.1	Nome do estado V17.1 em diante
Processando	Recuperando
WaitComplete	Aguardando/Processando

Nota: Você pode exibir os anexos baixados e processados. Quando o status da execução de integração é waitcomplete exibe a porcentagem de integração concluída.

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações. Para obter mais informações, consulte Resposta a vulnerabilidades aplicações e. CSDM tabelas.

Integrações criadas manualmente

Você pode adicionar outras integrações que não estão disponíveis como ServiceNow Store aplicações, conforme necessário. Para obter mais informações, consulte Criar manualmente uma integração de vulnerabilidade.

Noções básicas sobre as integrações de NVD

As integrações de NVD usam dados importados do produto National Vulnerability Database (NIST) do National Vulnerability Database (NVD) para ajudar você a determinar o impacto e a prioridade das falhas em seu código. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

O NIST NVD coleta dados CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e CPE (Common Platform Enumeration, enumeração de plataforma comum) e disponibiliza esses dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao Resposta a vulnerabilidades Mapear vulnerabilidades CVE e CPE enriquecendo os dados em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Após a instalação, a integração NIST National Vulnerability Database Integration-API (CVE somente) é invocada automaticamente como um trabalho agendado e é executada diariamente. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Dica: A ativação desse plug-in em instâncias de produção pode exigir uma licença separada.

Versões disponíveis

Versão de lançamento	Notas da versão
Resposta a vulnerabilidades Integração com NVD v1.2	

Importação inicial de dados de vulnerabilidade com as integrações NVD e CWE

1. Execute uma importação inicial de dados do CWE com a Integração abrangente do CWE 2000.

   Consulte Configure e execute o trabalho agendado para atualizar registros CWE. Você executa atualizações de CWE **Sob demanda** no registro de integração por padrão, e, você deve configurá-lo.

   Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados NVD. O dia padrão para a atualização do NVD é **Semanalmente** ativado **Segunda-feira** .

2. Verifique Resposta a vulnerabilidades A integração com a aplicação NVD está instalada e uma importação de dados inicial da API de integração do banco de dados de vulnerabilidades do NIST - (somente CVE) ou da API de integração do banco de dados de vulnerabilidades do NIST - API (CVE e CPE) é bem-sucedida.

   Para CPEs, verifique se uma importação de dados inicial da NIST National Vulnerability Database Integration - API (somente CPE) foi bem-sucedida.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois que o plug-in é instalado, a NIST National Vulnerability Database Integration - API (CVE somente) é ativada por padrão. Ele é executado diariamente. Para obter mais informações, consulte Instale o. Resposta a vulnerabilidades Integração com o NIST National Vulnerability Database.

3. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Noções básicas sobre dados de vulnerabilidade importados e itens vulneráveis

Em seu ServiceNow AI Platform cada vulnerabilidade importada é representada por uma entrada de vulnerabilidade nas bibliotecas de origem de produtos de scanner de terceiros, como Qualys, por exemplo. Itens vulneráveis (VI) importados e atualizados em sua instância são referências a bibliotecas de terceiros, como Qualys biblioteca. Uma biblioteca de terceiros pode, por sua vez, fazer referência ao NVD.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, quando você ingere dados de vulnerabilidade de terceiros de um produto como Qualys, Você está ingerindo VIS que fazem referência a um QID (Qualys Identificador). No caso de Qualys Esse QID, por sua vez, faz referência a um CVE da biblioteca NVD. Ao clicar nesse QID em uma tarefa de correção ou registro de item vulnerável no Resposta a vulnerabilidades E você executou as integrações NVD e CWE para ingerir dados, você está exibindo dados de vulnerabilidade atuais e aprimorados que permitem ver os relacionamentos existentes entre seus VIS e CVEs, CVEs e CPEs.

Antes de executar um produto de scanner de terceiros, como Qualys Que tenha sua própria biblioteca, primeiro você deve instalar e executar, no mínimo, a integração NIST National Vulnerability Database Integration- API (CVE somente) (também inclui detalhes relacionados à CISA) e Integração do CWE para ingerir dados de vulnerabilidade. Essas importações de dados de NVD e CWE enriquecem seu Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações dados antes de importar dados com um produto de terceiros.

Para obter mais informações sobre como gerenciar NVD, CWE e bibliotecas de terceiros e exibi-las, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros e. Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Depois de verificar a importação bem-sucedida de NVD, para enriquecer ainda mais seus dados de vulnerabilidade, Configure e execute o trabalho agendado para atualizar registros CWE.

Execute as importações de NVD e CWE antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Localizando as integrações de NVD

Para exibir as integrações de NVD, navegue até **Resposta a vulnerabilidades ou Resposta a vulnerabilidades da aplicação** > **Administração** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Nota: Integração do banco de dados de vulnerabilidades nacional do NIST - API (somente CVE) a integração está ativa, por padrão.

Integrações de NVD

Integração	Descrição
NIST National Vulnerability Database Integration - API (somente CVE)	Recupera somente dados de vulnerabilidade do NIST NIST NVD (CVE). Por padrão, esta integração é definida automaticamente para ser executada diariamente.
Integração do banco de dados de vulnerabilidades nacional do NIST - API (CPE somente)	Recupera dados de CPE do NIST NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em Software vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de NVD

Integração	Descrição
	Esta integração está definida para ser executada diariamente e está inativa por padrão. Para ativar esta integração, consulte Ativar o banco de dados nacional de vulnerabilidades do NIST - API (CPE somente).
Integração do banco de dados de vulnerabilidades nacional do NIST - API (CPE não mapeado)	Recupera dados de CPE associados ao CVE obtido do NIST NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em uma lista relacionada ao registro de entrada de vulnerabilidade NVD. Esta integração está definida para ser executada sob demanda e está inativa por padrão. Para ativar esta integração, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Importante: A integração "NIST National Vulnerability Database Integration-API (CVE e CPE)" foi descontinuada.

Para obter os status de execução de integração, consulte, Exiba o status da execução de importação da integração do NVD (National Vulnerability Database).

Preparando-se para as integrações de NVD

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. As integrações de NVD presumem que você esteja familiarizado com o NIST National Vulnerability Database (NVD).

Função necessária: administrador

Nota: Antes de executar as integrações de NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Configure e execute o trabalho agendado para atualizar registros CWE

D As importações de ata do CWE enriquecem ainda mais os dados de vulnerabilidade em sua instância. Use registros de enumeração de pontos fracos comuns (CWE) baixados do banco de dados do CWE para referência ao decidir se uma vulnerabilidade deve ser escalonada. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados NVD. O dia padrão para a atualização do NVD é **Semanalmente** ativado **Segunda-feira** .

Atualize registros de pontos fracos comuns do banco de dados de enumeração de pontos fracos comuns em uma base programada regularmente. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na página Enumerações de Pontos Fracos Comuns.

- Se você tiver a função de administrador, poderá adicionar repositórios ao trabalho agendado.
- Se você tiver sn_vul.vulnerability_read, poderá executar o trabalho agendado.
- Se você tiver sn_vul.vulnerability_write, poderá editar os detalhes do trabalho agendado.

Por Que e Quando Desempenhar Esta Tarefa
Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
2. Selecione **Integração abrangente do CWE 2000** trabalho agendado.
3. Modifique os campos, conforme necessário.

Formulário Integração de vulnerabilidades

Campo	Descrição
Nome	Nome do trabalho agendado.
Ativo	Se o trabalho agendado está ativo. Se você não quiser que o trabalho seja executado por um período específico, configure os parâmetros que deseja usar e desative o trabalho.
Executar	Frequência que você deseja que o trabalho seja executado. Os campos subsequentes são exibidos ou ocultos com base em sua configuração neste campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A atualização do CWE é **Sob demanda** por padrão. Definido como um período programado anterior às atualizações de NVD. As opções incluem: ◦ Diariamente: Escolha um **Hora** ◦ (Opção mais comum) Escolha um **Dia** e. **Hora** ◦ Mensal: Escolha **Dia** e. **Hora** ◦ Periodicamente: Escolha um **Intervalo de repetição** , **Iniciando** data e hora ◦ Uma vez: Escolha um **Iniciando** data e hora
Dia	O dia em que você deseja que o trabalho agendado seja executado. Se você selecionou **Semanalmente** em **Executar** este campo exibe os dias da semana. Se você selecionou **Mensal** em **Executar** este campo exibe os dias do mês. **Nota:** Programe a atualização do CWE para ser executada antes da atualização do banco de dados NVD. O dia padrão para a atualização do NVD é **Semanalmente** ativado **Segunda-feira** .
Hora	A hora em que você deseja que o trabalho agendado comece. **Nota:** Programe a atualização do CWE para ser executada antes da atualização do banco de dados NVD. O tempo padrão para a atualização do NVD é 01:00:00
Script de integração	O script para extrair dados das fontes de dados especificadas em **Fontes de dados** lista relacionada.
Integração de origem	[Somente leitura]
Instância de origem	[Somente leitura]
Aplicação	[Somente leitura] O nome da aplicação para a qual você está executando o trabalho agendado.
Intervalo de repetição	O número de dias e horas antes que o trabalho agendado seja executado novamente. Este campo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	aparece quando **Periodicamente** está selecionado em **Executar** lista.
Iniciando	A data e a hora para iniciar as atualizações periódicas. Este campo aparece quando **Periodicamente** está selecionado em **Executar** lista.
Condicional	Caixa de seleção para adicionar parâmetros condicionais.
Condição	As condições para executar o trabalho de programação. Este campo aparece quando **Condicional** a caixa de seleção está marcada.
Estratégia do processador de relatórios	A estratégia para extrair dados e processar o trabalho agendado. ○ Para extrair dados das fontes de dados no **Fontes de dados** lista relacionada usando o script no **Script de integração** campo, selecione **Anexo de fonte de dados** . ○ Para selecionar um processador personalizado no **Script do Processador de relatório** , selecione **Processador de relatório personalizado** .
Processador de relatórios	O script a ser executado quando o trabalho agendado for executado. Este campo aparece quando **Processador de relatório personalizado** está selecionado em **Estratégia do processador de relatório** lista.
Script de fábrica do processador	O script para criar o processador de relatório. Este campo aparece quando **Processador de relatório personalizado** está selecionado em **Estratégia do processador de relatório** lista.

Tradução automática

4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Para executar o trabalho agendado imediatamente, clique em **Executar agora** .
   Você retornará à exibição Integrações de vulnerabilidades.
6. Para observar o andamento da importação, selecione **Integração abrangente do CWE 2000** trabalho agendado novamente e selecione **Execuções de Integração de vulnerabilidades** guia.

   Consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades para ver as entradas importadas.

Instale o. Resposta a vulnerabilidades Integração com o NIST National Vulnerability Database

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto NIST National Vulnerability Database (NVD) se integre corretamente com o. Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao Gerenciador de vulnerabilidades no Resposta a vulnerabilidades Ou o grupo Gerenciador da App-Sec em Resposta a vulnerabilidades de aplicações. Para obter informações sobre Funções de grupo em Resposta a vulnerabilidades consulte, Gerencie funções granulares e de persona para Resposta a vulnerabilidades. Para obter informações sobre funções de grupo em Resposta a vulnerabilidades de aplicações consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O Gerenciador de vulnerabilidades ou o Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Nota: Antes de executar as integrações de NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login na instância em que você deseja instalar as integrações de NVD.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, Pesquise a aplicação Integração de resposta a vulnerabilidades com NVD.
4. Selecione o bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Selecione **App de solicitação** e insira seu Now Support credenciais de login.
6. Selecione **Obter** .
7. Insira **Nome da instância** e. **Motivo da instância** e selecione **Validar instância** .
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Tudo** > **Aplicações do sistema** > **Aplicações** > **Tudo**.
10. Localize a aplicação, selecione-a e selecione **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Após a instalação inicial, para obter modificações, consulte Modificação e atividades opcionais de integração de NVD.

Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado)

Para ingerir dados de CPE (Common Platform Enumeration, enumeração de plataforma comum) para dados CVE (Common Vulnerabilities and Exposures, vulnerabilidades comuns e exposições comuns) obtidos, você pode executar uma importação de dados completa com um trabalho agendado sob demanda.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NIST)–API (CPE não mapeado) captura dados (CPE) que inclui um formato de nome formal, um método para verificar nomes em um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em uma lista relacionada ao registro de entrada de vulnerabilidade NVD.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades da aplicação** > **NVD** > **Integrações**.
2. Selecione a integração NIST National Vulnerability Database Integration–API (CPE não mapeado).
3. Marque a caixa de seleção **Ativo**.

   Nota: A integração é pré-configurada para ser executada sob demanda. Ao ativar a integração, ela será executada automaticamente após a integração NIST NVD Integration-API (CVE somente). Mudar qualquer outro parâmetro de integração requer ambos ServiceNow e. Resposta a vulnerabilidades e experiência e pode resultar em dados incompletos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.

b. NIST National Vulnerability Database Integration–API (Unmapeated CPE) Integration.

c. Selecione **Detalhes da integração** guia.
Independentemente de **Importar desde** CPEs para todos os CVEs recuperados são recuperados.

4. Selecione **Executar agora** para executar uma execução de integração de suporte completo inicial.
Após a conclusão da importação inicial, as importações programadas de dados delta serão retomadas. Para obter os status de execução de integração, consulte Exiba o status da execução de importação da integração do NVD (National Vulnerability Database).

Ativar o banco de dados nacional de vulnerabilidades do NIST - API (CPE somente)

Para ingerir dados de CPE (Common Platform Enumeration, enumeração de plataforma comum), você pode executar uma importação de dados completa com um trabalho agendado diariamente.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NIST)–API (CPE) do National Institute of Standards and Technology (NIST) captura dados (CPE) que incluem um formato de nome formal, um método para verificar nomes em um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em uma tabela de software vulnerável.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades da aplicação** > **NVD** > **Integrações**.
2. Selecione a integração NIST National Vulnerability Database Integration–API (CPE only).
3. Marque a caixa de seleção **Ativo**.

- A integração é pré-configurada para ser executada diariamente. Mudar qualquer outro parâmetro de integração requer ambos ServiceNow e pode resultar em dados incompletos.
- Ativar esta integração ativará automaticamente as integrações NIST National Vulnerability Database Integration- API (CVE somente) e NIST National Vulnerability Database Integration- API (CPE não mapeado) e definirá seu campo de execução como Sob demanda.
- Além disso, uma execução de integração bem-sucedida da API de integração do banco de dados de vulnerabilidade nacional do NIST (somente CPE) acionará automaticamente a API de integração do banco de dados de vulnerabilidade nacional do NIST (somente CVE). E a conclusão bem-sucedida da API de integração do banco de dados de vulnerabilidades nacional do NIST (somente CVE) acionará automaticamente a API de integração do banco de dados de vulnerabilidades nacional do NIST (CPE não mapeado).

Nota: O campo Importar desde a data na Integração do banco de dados de vulnerabilidade nacional do NIST - API (CPE somente) está vazio por padrão. Mantenha-o em branco para buscar dados dos últimos 357 dias.

Para recuperar dados históricos durante a importação inicial da verificação de NVD, defina uma data de início no registro de integração do banco de dados de vulnerabilidades nacional do NIST - API (CPE somente).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.

b. NIST National Vulnerability Database Integration–API (CPE only) Integration.

c. Selecione **Detalhes da integração** guia.

d. Defina **Importar desde** valor do campo para a data mais antiga que você deseja recuperar. Cada importação bem-sucedida redefine essa data para a data e hora do dia selecionado.

4. Selecione **Executar agora** para executar uma execução de integração de suporte completo inicial. Após a conclusão da importação inicial, as importações programadas de dados delta serão retomadas. Para obter os status de execução de integração, consulte Exiba o status da execução de importação da integração do NVD (National Vulnerability Database).

Modificação e atividades opcionais de integração de NVD

Configure modificações opcionais especificamente para as integrações de NVD.

Nota: Alterar outras configurações de integração de NVD, diferentes das listadas aqui, requer avançado ServiceNow e. Resposta a vulnerabilidades e está além do escopo da documentação do produto.

Execute uma importação manual de integração de NVD

Se sua importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho agendado diário ou semanal.

Antes de Iniciar

Nota: NIST National Vulnerability Database Integration- API (CPE somente) e as integrações NIST National Vulnerability Database Integration-API (CPE não mapeado) estão inativas por padrão. Para obter mais informações, consulte Ativar o banco de dados nacional de vulnerabilidades do NIST - API (CPE somente) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades da aplicação** > **Administração** > **Integrações**.
2. Escolha e integração, por exemplo, a integração NIST National Vulnerability Database Integration - API (CVE somente).
3. Selecione **Executar agora**.

   Nota: Se a integração do banco de dados de vulnerabilidades nacional do NIST-API (CPE não mapeado) estiver ativada, os dados do CPE associados serão armazenados na lista relacionada ao Software vulnerável da entrada de vulnerabilidade do NVD. Consulte Resposta a vulnerabilidades campos do formulário vulnerabilidade.

4. Para obter os status de execução de integração, consulte, Exiba o status da execução de importação da integração do NVD (National Vulnerability Database).

Exiba o status da execução de importação da integração do NVD (National Vulnerability Database)

Use **Execuções de Integração de vulnerabilidades** lista relacionada para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Para exibir o status da execução de importação da integração NVD:

- Resposta a vulnerabilidades E a integração do Vulnerability Response com a aplicação de integração NVD deve ser instalada e configurada.
- As importações de integração NVD devem estar em execução. Integração do banco de dados de vulnerabilidades nacional do NIST - API (CVE somente) a integração é executada por padrão.

> **Nota:** NIST National Vulnerability Database Integration-API (CPE somente) e as integrações NIST National Vulnerability Database Integration-API (CPE não mapeado) estão inativas por padrão. Para obter mais informações, consulte Ativar o banco de dados nacional de vulnerabilidades do NIST - API (CPE somente) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite.

Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. O último registro processado com mais de uma hora indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos no processamento.

> **Nota:** . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:
>
> - `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
> - `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Se você não estiver usando o gráfico de status de execução de integração NVD, Navegar até **Tudo** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades da aplicação** > **Administração** > **Integrações**.
2. Selecione um **link** para uma integração.
3. Selecione **Execuções de Integração de vulnerabilidades** lista relacionada.
4. Verifique se todas as importações foram bem-sucedidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trouble?

As causas mais comuns para uma execução com falha incluem:

- Interrupção de rede.
- Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

Se você encontrar qualquer uma dessas condições, selecione **Executar agora** e execute novamente a integração.

Tópicos relacionados

Resposta a vulnerabilidades campos do formulário vulnerabilidade

Adicione CVEs a entradas de terceiros

As informações CVE (Common Vulnerability and Exposure, vulnerabilidade e exposição comum) podem estar relacionadas a uma única vulnerabilidade de terceiros. Geralmente, ele é adicionado durante uma importação de integração de terceiros. No entanto, você pode adicionar vários CVEs (vulnerabilidades) manualmente.

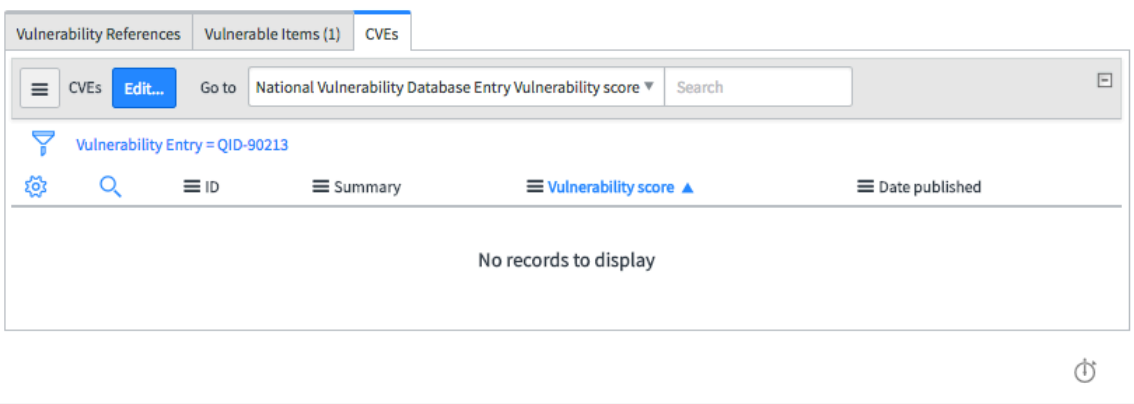
Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros**.
2. Abra um registro.
3. Clique em **CVEs** guia lista relacionada.



4. Clique em **Editar**.
5. Escolha quais CVEs adicionar.

> **Nota:** Você pode usar filtros de condição para refinar a coleção CVE.

6. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Resposta a vulnerabilidades campos do formulário vulnerabilidade

Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades

Você pode exibir dados de vulnerabilidade importados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou de terceiros para decidir se escalar uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Bibliotecas**.

   Para obter informações sobre campos específicos, consulte Resposta a vulnerabilidades campos do formulário vulnerabilidade.

   As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, isso é apenas para referência.
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

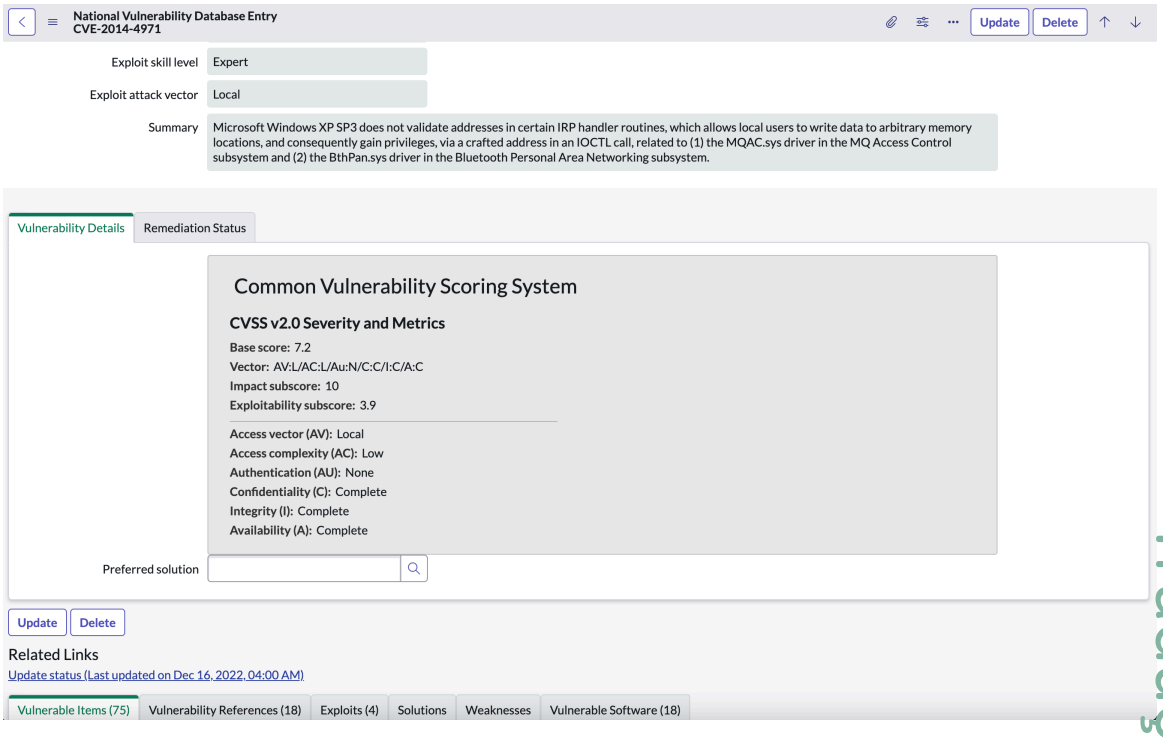
2. Escolha uma biblioteca para exibir vulnerabilidades.
3. Clique em um link na lista para abrir um registro.

   Um registro CVE na biblioteca de entradas do banco de dados de vulnerabilidades nacional. Mais informações estão disponíveis em **Links relacionados** . Após uma importação de dados, você pode escolher uma vulnerabilidade e explorar seus relacionamentos com itens vulneráveis, explorações, possíveis soluções, possíveis patches e quaisquer referências a artigos da base de conhecimento da HI. Se Solução de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

gestão de vulnerabilidade Se estiver instalado, você poderá exibir uma solução preferencial nos registros NVD, se houver uma disponível.



Integração de KEV (Knowned Exploit Vulnerability, vulnerabilidade de exploração conhecida da CISA)

. Resposta a vulnerabilidades A integração com o catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA ingere dados para ajudar você a priorizar e corrigir essas vulnerabilidades com eficácia.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

A CISA permite a correção urgente e priorizada de vulnerabilidades ativamente exploradas para agências governamentais e corporações.

Sobre a CISA

Cybersecurity & Infrastructure Security Agent (CISA) é uma agência de segurança cibernética e infraestrutura dos EUA que publica um relatório sobre as vulnerabilidades mais exploradas. Ele se integra facilmente ao Resposta a vulnerabilidades Mapear vulnerabilidades comuns de Vulnerabilidades e exposições (CVE) enriquecendo os dados em sua instância. Em seguida, essas informações são acumuladas para a tabela Entradas de vulnerabilidade de terceiros. A data de vencimento mais antiga é considerada para o acúmulo dos itens vulneráveis.

Nota: . **CISA existe** Caixa de seleção de CVEs recuperados pela CISA.

Valores recuperados da integração da CISA:

- ID do CVE
- Prazo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Data de inclusão
- Fornecedor/projeto
- Produto
- Ransomware conhecido (a partir de v21.0 de Resposta a vulnerabilidades um novo campo **Conhecido por ser usado em campanhas de ransomware** É ingerido do catálogo Vulnerabilidades exploradas conhecidas (KEVs) da CISA. É indicado pela sinalização de **Ransomware conhecido** Na tabela do banco de dados Entrada Nacional de Vulnerabilidade. O sinalizador é definido no nível CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e acumulado para a entrada de terceiros (TPE).

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Trabalhos agendados

A integração do CISA é invocada automaticamente como um trabalho agendado diariamente. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas da versão
Resposta a vulnerabilidades v 16,5, v18.0 Resposta a vulnerabilidades Integração com CISA v1.0, v1.2	

Exibindo a integração do CISA

Para exibir a integração do CISA, navegue até **Resposta a vulnerabilidades** > **Administração** > **Integrações** > **Integração de vulnerabilidades de exploração conhecidas da CISA**.

As integrações a seguir estão incluídas no sistema de base.

Nota: Por padrão, somente a Integração CISA está ativa.

Integração do CISA

Integração	Descrição
Integração da Agência de segurança cibernética e infraestrutura (CISA)	Recupera dados de vulnerabilidade da CISA (CVE) e enriquece os dados de vulnerabilidade existentes. Esta integração é definida automaticamente para ser executada diariamente.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Preparando para a integração do CISA

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. A integração de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades exploradas conhecidas da CISA pressupõe que você esteja familiarizado com a Agência de segurança cibernética e infraestrutura (CISA).

Função necessária: sn_vul.vulnerability_admin

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Nota: Antes de executar a integração do CISA, faça qualquer mudança de configuração necessária com base em seus requisitos.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Instale o. ServiceNow® Integração de Resposta a vulnerabilidades com a aplicação CISA

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o Consultor de vulnerabilidades exploradas conhecidas da CISA (Cybersecurity & Infrastructure Security Agent) se integre ao Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se o Resposta a vulnerabilidades A integração com a aplicação NVD está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instale o. Resposta a vulnerabilidades Integração com o NIST National Vulnerability Database.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao Gerenciador de vulnerabilidades no Resposta a vulnerabilidades. Para obter informações sobre Funções de grupo em Resposta a vulnerabilidades consulte, Gerencie funções granulares e de persona para Resposta a vulnerabilidades. • O Gerenciador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar Vulnerability Response integration with CISA ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Vulnerability Response integration with CISA aplicação.
4. Selecione o bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Selecione **App de solicitação** e insira seu Now Support credenciais de login.
6. Selecione **Obter** .
7. Insira **Nome da instância** e. **Motivo da instância** e selecione **Validar instância** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e selecione **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Nota: Nenhuma configuração é necessária para CISA integração.

Noções básicas sobre a integração do Sistema de pontuação de previsão de exploração (EPSS)

Visão geral da integração do EPSS com Resposta a vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral da integração

A integração do Exploit Prediction Scoing System (EPSS) importa dados EPSS relacionados a vulnerabilidades e exposições comuns (CVEs) de First.org para priorizar e corrigir vulnerabilidades. Para obter mais informações, consulte https://www.first.org . O Sistema de pontuação de previsão de exploração (EPSS) é um esforço orientado por dados para estimar a probabilidade (probabilidade) de que uma vulnerabilidade de software seja explorada em estado selvagem. O modelo EPSS produz uma pontuação de probabilidade entre 0 e 1 (0 e 100%). Quanto maior a pontuação, maior a probabilidade de que uma vulnerabilidade seja explorada.

As importações de dados da integração EPSS enriquecem ainda mais os dados NVD em sua instância. Se os registros NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Importante: Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é VR.System. Não mude este valor.

Importação inicial de dados com a integração EPSS

1. Execute uma importação inicial de dados de EPSS com a integração de First.org EPSS. Para obter mais informações, consulte Configure e execute um trabalho agendado para atualizar registros CVE com dados EPSS.

   Importante: Você executa atualizações de EPSS **Diariamente** no registro de integração por padrão, e você deve configurá-lo se quiser que ele seja executado como um trabalho agendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Para obter mais informações, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

> **Importante:** É recomendável executar integrações NIST National Vulnerability Database Integration - API (somente CVE) antes do EPSS.

Execute as importações de EPSS antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações de resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

> **Importante:** A integração a seguir está incluída no sistema de base. A integração está ativa por padrão.

Após a execução inicial, os trabalhos agendados do sistema de base executam as integrações automaticamente em ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Na ativação da integração do EPSS, os campos Pontuação do EPSS, Percentil do EPSS e EPSS Modificado pela última vez são adicionados à tabela Entradas de vulnerabilidade. Para CVEs existentes, esses campos são atualizados automaticamente após a conclusão bem-sucedida do trabalho de importação inicial. Se houver novos CVEs adicionados à tabela Entradas de vulnerabilidade após a conclusão do trabalho agendado do EPSS, os CVEs recém-adicionados indicarão sua origem como EPSS. As pontuações são acumuladas para TPEs existentes de CVEs da tabela NVD, usando o sistema de base `Rollup EPSS score from NVD to TPEs calculator`. Você também pode modificar a calculadora. Para obter mais informações, consulte Resposta a vulnerabilidades Calculadoras de acúmulo.

Tópicos relacionados

Crie um Resposta a vulnerabilidades calculadora

Configure e execute um trabalho agendado para atualizar registros CVE com dados EPSS

Personalize o trabalho agendado do sistema de base para atualizar registros CVE com dados EPSS.

Antes de Iniciar

> **Importante:** Você precisa baixar e ativar o. Vulnerability Response integration with CISA Plug-in (com.snc.vulnerability.cisa) para habilitar a integração do EPSS.

A seguir está a lista de novos campos adicionados na tabela NVD para armazenar dados EPSS.

- Pontuação de EPSS
- Percentual de EPSS
- Última modificação de EPSS

> **Nota:** Configure a exibição de lista ou a exibição de formulário de acordo com o requisito para exibir os campos recém-adicionados.

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

As importações de dados da integração EPSS enriquecem ainda mais os dados NVD em sua instância. Se os registros NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte da configuração inicial do Vulnerability Response e publique na importação de dados de vulnerabilidade para sua instância.

Nota: Por padrão, a integração do First.org EPSS está em **Ativo** estado. O trabalho agendado do sistema de base é configurado, por padrão, para ser executado diariamente.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
2. Encontre e selecione Integração EPSS First.org.
3. Modifique os campos, conforme necessário.
4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Selecione **Executar agora** para executar o trabalho agendado imediatamente.
   Você retornará à exibição Integrações de vulnerabilidades.
6. Selecionar **EPSS do First.org** > **Guia Execuções de integração de vulnerabilidades** para exibir o andamento da importação.
   Na conclusão bem-sucedida do trabalho agendado, as pontuações EPSS, o percentil e os carimbos de data/hora da pontuação EPSS modificados pela última vez são atualizados nos CVEs.

O que Fazer Depois

- Consulte Adicionar condição de pontuação EPSS na regra de negócio da calculadora de risco.
- Consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades para ver as entradas importadas.

Adicionar condição de pontuação EPSS na regra de negócio da calculadora de risco

Modifique Regra de negócio para adicionar a condição de pontuação EPSS à Calculadora de risco.

Antes de Iniciar

Nota: O procedimento a seguir é necessário para que as atualizações de EPSS em vulnerabilidades sejam revertidas para os itens vulneráveis.

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Regra de negócio**.
2. Pesquisar **Sinalizador de recalcular** .

   Nota: Há dois `Set recalculate flag`regras de negócio. Você pode usar qualquer um deles.

3. Navegue até **Quando executar** guia.
4. Selecione **Adicione cláusula "OR"** e selecione `Pontuação EPSS` de **escolha o campo** e. `mudanças` de **Escolha o operador** campo.
5. Selecione **Atualizar**.

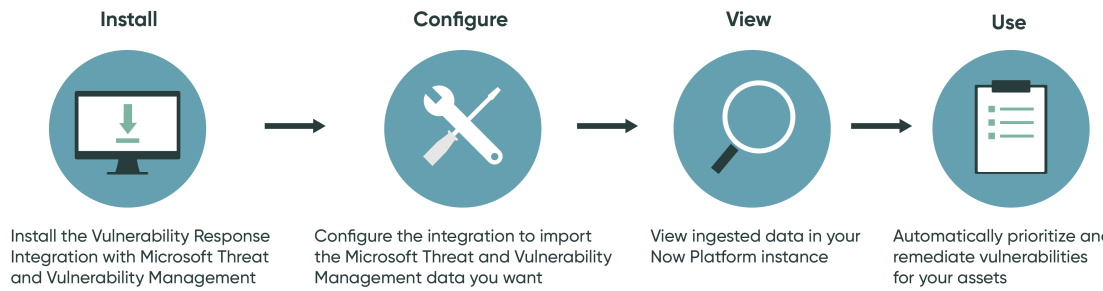
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre a integração de vulnerabilidades do Microsoft Threat and Vulnerability Management

. Resposta a vulnerabilidades A integração com a aplicação Microsoft Threat and Vulnerability Management (MS TVM) usa dados importados do MS TVM para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. O aplicativo está disponível com uma assinatura separada do ServiceNow Store.

Você pode usar a integração de Vulnerabilidade do MS TVM para importar dados do scanner de terceiros sobre seus ativos e vulnerabilidades. Em seguida, você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis no Resposta a vulnerabilidades painéis.



Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades Integração com MS TVM v2.2	Para obter mais informações sobre as versões lançadas da aplicação Vulnerability Response, compatibilidade e mudanças de esquema, consulte Matriz de compatibilidade de resposta a vulnerabilidades e mudanças no esquema de versão [KB0856498] na Base de conhecimento HI .

Domain Separation e MS TVM

Importe dados de integração de vulnerabilidade para um domínio especificado atribuindo um usuário nesse domínio para executar as integrações. Para criar importações separadas por domínio para o MS TVM Vulnerability Integration, consulte Crie importações separadas por domínio para uma integração.

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em seu ServiceNow AI Platform instância quando:

- Uma vulnerabilidade importada de um scanner de terceiros corresponde a um ativo existente (item de configuração) em seu CMDB). O produto MS TVM se refere a essas correspondências como vulnerabilidades.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um item de configuração (IC) incompatível também é criado com um item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido a um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação.

Entradas de vulnerabilidades de terceiros

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros, como o MS TVM, e são listadas na tabela Entradas de vulnerabilidade de terceiros em seu ServiceNow AI Platform instância. Entradas do banco de dados de vulnerabilidades nacionais (CVEs) são importadas do MS TVM. As informações de exploração associadas a esses dois tipos de entradas vêm do MS TVM. Essas informações de exploração podem ser usadas para cálculo de risco.

Nota: Uma vulnerabilidade de terceiros é recuperada somente para vulnerabilidades que não tenham um CVE atribuído a eles. O MS TVM pode adicionar um nome temporário para a vulnerabilidade, por exemplo, `TVM-XXXX-XXXX` . Este nome é atualizado depois que um ID CVE é atribuído.

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu CMDB.

Item descoberto

Itens descobertos são os ativos que são ingeridos da importação da máquina MS TVM que correspondem aos ICs existentes em seu CMDB.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Habilitar o plug-in Modelos de classe de IC do CMDB, o Mecanismo de identificação e reconciliação (IRE) cria ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros do item descoberto serão atualizados para refletir esse estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Resposta a vulnerabilidades usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no CMDB. As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os VIS são criados.

Instância

Uma instância se refere a várias contas do MS TVM. Cada conta pode ser uma instância na aplicação MS TVM.

Integração

Uma integração é um trabalho agendado que recupera informações de uma origem de terceiros, como a integração das máquinas MS TVM.

Implantação

Quando uma integração oferece suporte a várias origens, uma única existência de integração é chamada de implantação de sua integração. Uma implantação se refere às integrações e produtos em todo o seu ambiente. Por exemplo, você pode ter várias implantações do MS TVM em seu ambiente.

A integração do MS TVM também inclui os seguintes recursos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode identificar os ativos em seu ambiente e atualizar os ICs em seus itens descobertos existentes, itens vulneráveis e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações do MS TVM. Você também pode executar trabalhos agendados sob demanda.
- Você pode agrupar itens vulneráveis.
- Você pode configurar regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar ICs em seu CMDB.

Funções necessárias de ServiceNow AI Platform

As tarefas de integração exigem as seguintes funções em seu ServiceNow AI Platform instância.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

administrador

O administrador do sistema usa o Assistente de configuração para instalar a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do MS TVM no Assistente de configuração. Esta função tem acesso completo ao Resposta a vulnerabilidades aplicação e seus registros. O administrador de vulnerabilidades configura tudo Resposta a vulnerabilidades aplicações e regras para integrações de terceiros instaladas.

sn_vul_msft_tvm.configure_integration

Esta função contém `sn_vul_msft_tvm.read_integration` função granular. Usuários com esta função podem configurar a#Integração de resposta a vulnerabilidades com a aplicação Microsoft Threat and Vulnerability Management.

sn_vul_msft_tvm.read_integration

Usuários com esta função só podem exibir a#Integração de resposta a vulnerabilidades com os registros da aplicação Microsoft Threat and Vulnerability Management.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Integrações do MS TVM

Várias origens são compatíveis com todas as integrações do MS TVM. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura o. Resposta a vulnerabilidades Integração com a aplicação MS TVM do Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir as integrações do MS TVM, navegue até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integrações**. Resposta a vulnerabilidades Fornece integrações com endpoints do MS TVM para importar os dados de acordo com os intervalos de tempo programados. As integrações a seguir estão incluídas no sistema de base.

Integrações do MS TVM

Sequência de execução	Agendamento	Integração	Descrição
1	Diariamente	Integração de recomendações do Microsoft TVM	Recupera uma lista de todas as recomendações de segurança acionáveis para corrigir as vulnerabilidades.
2	Diariamente	Integração de Vulnerabilidade do Microsoft TVM (CVE)	Recupera uma lista das entradas do banco de dados de vulnerabilidades nacionais e entradas de vulnerabilidades de terceiros, bem como suas informações de exploração.
3	Diariamente	Microsoft TVM Machine Integration	Recupera todos os dados de ativo (máquina), incluindo marcadores de máquina, do Microsoft TVM e os processa em sua instância.
4	Semanalmente **Nota:** Após a instalação, esta integração é executada automaticamente após a importação das máquinas.	Microsoft TVM Machine Vulnerabilities Integration (importação completa)	Recupera todas as vulnerabilidades em aberto em todos os ativos.
5	Diariamente	Microsoft TVM Machine Vulnerabilities Integration (importação delta)	Recupera todas as informações que foram alteradas na importação completa de vulnerabilidades da organização, incluindo as vulnerabilidades novas, corrigidas e atualizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de grupo que você definiu e são atribuídos para correção com base em suas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção e Resposta a vulnerabilidades visão geral das regras de atribuição.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Resposta a vulnerabilidades usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os VIS são criados. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.

Nota: Depois de remover uma regra, você não poderá recuperá-la. Em vez de remover uma regra existente, você deve desabilitá-la.

As seguintes regras de pesquisa do MS TVM são enviadas com o sistema de base:

- MAC_ADDRESS
- FQDN
- IP

Nota: Você pode usar vários valores para ip_ADDRESS e MAC_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência.

Itens descobertos

Você pode ver os ICs que foram detectados durante uma importação da integração de máquinas MS TVM.

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

Para obter mais informações, consulte Itens descobertos.

Marcadores da máquina

Marcadores de máquina, também conhecidos como marcadores de host, são usados para organizar e rastrear os ativos em sua organização. Você atribui marcadores às suas máquinas.

Todos os marcadores de máquina são importados como parte da integração de máquinas MS TVM. Marcadores de máquina geralmente são usados para filtragem em Resposta a vulnerabilidades regras de atribuição e regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Execute a integração do MS TVM Machine antes de criar Resposta a vulnerabilidades regras de tarefa de atribuição ou correção no Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Se um marcador Paris for criado, um marcador PARIS não poderá ser armazenado na tabela de marcadores Máquina. Paris e. PARIS são considerados a mesma etiqueta da máquina pelo sistema. Qualquer marcador importado primeiro é o marcador que é armazenado e reconhecido.
- Usar marcadores de máquina como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Chaves de grupo são colunas na tabela Tarefas de correção, enquanto os marcadores de máquina são destinados ao uso somente no construtor de condições.
- Os marcadores de máquina são controlados pela propriedade global do sistema sn_vul.import_host_tags. Esta propriedade é definida como verdadeira por padrão. Desabilitar marcadores os desabilita em todos ServiceNow AI Platform® instâncias.

O que fazer a seguir

Depois de baixar o. Resposta a vulnerabilidades Integração com o Microsoft Threat and Vulnerability Management do ServiceNow® Store A instalação e a configuração são compatíveis com o Assistente de configuração no Resposta a vulnerabilidades. Para obter mais informações, consulte Instale e configure a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

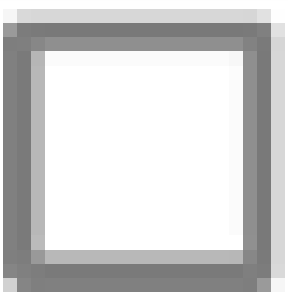
Preparando-se para a Integração de vulnerabilidades do Microsoft Threat and Vulnerability Management

Você pode se preparar para ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Integração de vulnerabilidades executando tarefas de configuração.

Antes de começar a usar uma check-list

Para instalar e configurar o. Resposta a vulnerabilidades Integração com a aplicação MS TVM, você pode imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para seu ServiceNow AI Platform® instância.

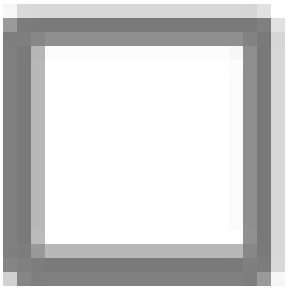
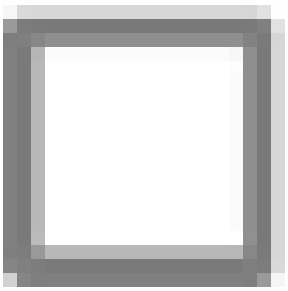
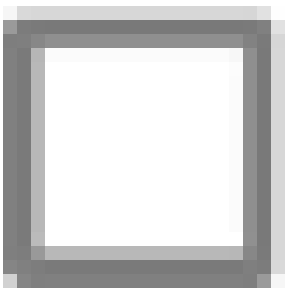
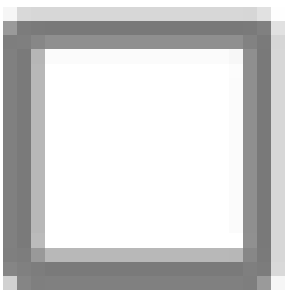
Check-list de preparação da integração

Tarefa	Descrição
	Verifique se você tem um dos seguintes conjuntos de informações: • ClientSecret, ClientID e TenantId para sua conta do MS TVM • Nome de usuário, senha, ID do cliente e Id do locatário para sua conta do MS TVM. Para obter essas informações, consulte Configurar Microsoft Integração do Azure para MS TVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

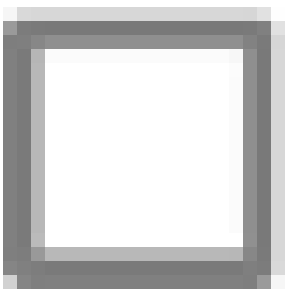
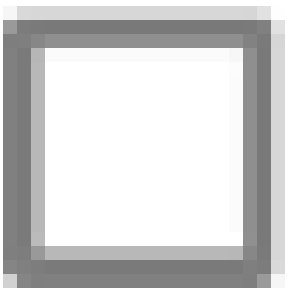
Check-list de preparação da integração

Tarefa	Descrição
	Se ainda não estiver instalado e ativado, instale o. Resposta a vulnerabilidades aplicação antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 14,0 de Resposta a vulnerabilidades ou posterior.
	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe o. Resposta a vulnerabilidades Integração com a aplicação MS TVM para seu ServiceNow AI Platform® instância. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com ServiceNow® Suporte técnico.
	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis: **administrador** Usa o Assistente de configuração para instalar a integração do Resposta a vulnerabilidades com a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Conclui a configuração da integração do MS TVM. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Este administrador configura todos os aplicativos e regras de VR e configura integrações de terceiros. **sn_vul_msft_tvm.configure_integration** Configura a Integração de vulnerabilidades do MS TVM. Esta função contém a função granular sn_vul_msft_tvm.read_integration. **sn_vul_msft_tvm.read_integration** Exibe (lê) registros da Integração de vulnerabilidades do MS TVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
	Grupo de Resposta a vulnerabilidades Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Para obter mais informações, consulte Crie um grupo de usuários . Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver no Resposta a vulnerabilidades aplicação. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.
	Instale o. Resposta a vulnerabilidades Integração com NVD e execute a API de integração do banco de dados nacional de vulnerabilidades do NIST - (somente CVE).
	Para promover um desempenho aprimorado para sua primeira importação, você pode desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não usá-las. Essas calculadoras, além de todas as que você definiu, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Para obter mais informações, consulte Desabilite a calculadora de vulnerabilidades padrão se não for usada . • Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem fazer com que muitas notificações sejam geradas, o que pode afetar o desempenho da ingestão.

Você está pronto para Instale e configure a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

Configurar Microsoft Integração do Azure para MS TVM

Configure sua conta no Microsoft Portal do Azure para acessar a API Microsoft Threat and Vulnerability Management (MS TVM) remotamente. Você precisa desta conta para acessar o locatário do MS TVM para coletar informações de máquinas, vulnerabilidades e recomendações de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: Microsoft Administrador do portal do Azure.

Por Que e Quando Desempenhar Esta Tarefa
Conclua as tarefas de configuração a seguir em seu Microsoft Portal do Azure antes de instalar o. ServiceNow® aplicação para esta integração.

Para verificar se você tem acesso ao conteúdo mais atual, consulte Documento da Microsoft site. Se você não criou um ID de aplicação para autenticação OAuth 2,0 no Microsoft Portal do Azure, siga as etapas deste procedimento.

Procedimento
1. Faça login no Microsoft Portal do Azure usando suas credenciais de administrador do portal do Azure.
2. No painel de navegação esquerdo do painel inicial, clique em **Azure Active Directory** .
3. No painel Visão geral, clique em **Registros da aplicação (visualização)** .
4. No painel Registros de aplicações (visualização), clique em **Novo registro** .
   O formulário Registrar uma aplicação é exibido.
5. No formulário, preencha os campos.

Registrar um formulário de candidatura

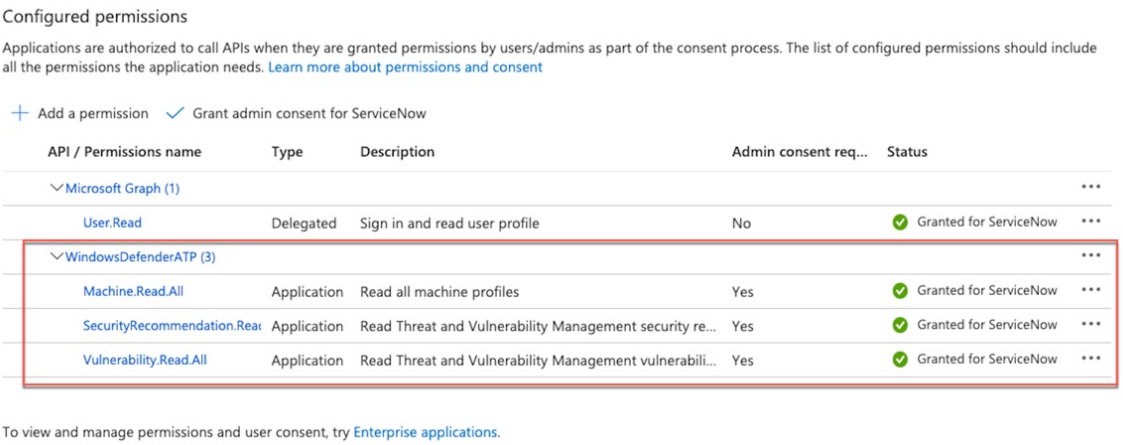
Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, Integração do MS TVM da ServiceNow inserido.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, clique em **Somente contas neste diretório organizacional (somente ServiceNow - locatário único)** .
URL de redirecionamento (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.

6. Clique em **Registrar**.
   O ID da aplicação (cliente) e o ID do diretório (locatário) são criados. Insira esses valores na página de configuração do **ID do cliente** e. **ID do locatário** campos durante a etapa de configuração no ServiceNow Assistente de configuração de integração VR-TVM. Esta etapa foi descrita em Instale e configure a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.
7. Quando você vê o ID da aplicação (cliente) exibido no ServiceNow Painel Integração MS TVM, clique em **Exibir permissões de API** .
8. Navegar até **Solicitar permissões de API** > **APIs que minha organização usa**e, em seguida, clique em **Windows Defender ATP** .
9. No painel Integração da ServiceNow MS TVM - Permissões de API, clique em **Adicione uma permissão** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Forneça acesso de leitura a máquinas, vulnerabilidades e recomendações de



segurança.

11. Clique em **Conceda consentimento do administrador para o nome da sua organização** .

Nota: Para autenticar como uma aplicação de um ServiceNow, execute as seguintes ações:

a. Navegar até **ServiceNow MS TVM Integration** > **Certificados e segredos**e, em seguida, clique em **Novo segredo do cliente** .

b. No formulário, preencha os campos.

Formulário segredos do cliente

Campo	Descrição
Descrição	Nome da aplicação.
Expira	Data de vencimento.

c. Clique em **Adicionar**.

. **Valor** o campo é preenchido com o novo segredo do cliente, que é sua nova senha.

Nota: Você precisará dessa senha ao configurar a integração no ServiceNow AI Platform instância. Para obter mais informações, consulte Instale e configure a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

d. Salve esta senha em um local seguro. Esta senha não estará disponível depois de sair desta página.

Você criou com sucesso um ID de aplicação para autenticação no Microsoft Portal do Azure.

O que Fazer Depois

Você está pronto para configurar seu ServiceNow AI Platform® instância da integração.

Instale e configure a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração

Instale e configure o. Resposta a vulnerabilidades Integração com o aplicativo Microsoft Threat and Vulnerability Management (MS TVM) para que você possa usar os dados importados do MS TVM para priorizar e corrigir vulnerabilidades de seus ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de executar o. ServiceNow® Microsoft Threat and Vulnerability Management Integração de vulnerabilidades, você deve baixar a Integração de resposta a vulnerabilidades com a aplicação Microsoft Threat and Vulnerability Management do ServiceNow Store E instale e configure-o usando o Assistente de configuração no Resposta a vulnerabilidades aplicação.

Antes de instalar a aplicação MS TVM, verifique se você concluiu todos os itens em Preparando-se para a Integração de vulnerabilidades do Microsoft Threat and Vulnerability Management check-list. Para obter informações sobre como configurar seu Microsoft Conta do Azure, consulte Configurar Microsoft Integração do Azure para MS TVM.

Funções necessárias:

- administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Microsoft Threat and Vulnerability Management no Assistente de configuração
- Administrador de vulnerabilidades (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)) para configurar a aplicação no Assistente de configuração depois que ela for instalada.

Por Que e Quando Desempenhar Esta Tarefa

Execute o procedimento a seguir antes de instalar e configurar a Integração MS TVM.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações que estão disponíveis para instalação em sua instância serão exibidas.

2. Localize **Microsoft Threat and Vulnerability Management** lado a lado e clique **Instalar** .

   . Resposta a vulnerabilidades Integração com a aplicação Microsoft Threat and Vulnerability Management que você baixou do ServiceNow Store instalado.

3. Siga as instruções no Assistente de configuração para continuar com a instalação.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de Integração** > **Integrações do Scanner** No Assistente de configuração para continuar com a configuração. Para obter mais informações para complementar os avisos fornecidos no Assistente de configuração, consulte Configure a Integração de vulnerabilidades do MS TVM usando o Assistente de configuração.

Configurações de recuperação de dados para o Microsoft Threat and Vulnerability Management Integration

Você pode usar as configurações de recuperação de dados para ajudar a determinar o tipo e o escopo dos dados que você deseja importar do ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Integração de vulnerabilidades ao seu ServiceNow AI Platform® instância.

As configurações de recuperação de dados ajudam você a controlar os dados que você deseja importar. Você pode definir os valores desses filtros em instâncias de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir as instâncias de integração, navegue até **Microsoft Threat and Vulnerability Management Integração de vulnerabilidades** > **Instâncias de Integração** E clique na integração do MS TVM.

Na página Instância de integração, clique em **Parâmetros da instância de integração** para exibir uma lista de parâmetros ou clique em **Integrações de vulnerabilidades** Guia para uma programação, detalhes de REST, detalhes de integração, fontes de dados e informações de execução de integração.

Configurações de recuperação de dados e filtros para as integrações do MS TVM em seu ServiceNow AI Platform instância

As configurações a seguir estão disponíveis para as integrações do MS TVM em seu ServiceNow AI Platform instância. Essas e outras definições de configuração são exibidas na página Instância de integração do seu ServiceNow AI Platform instância. Você pode preferir deixar essas configurações em suas configurações padrão nas primeiras execuções de integração.

MS TVM.

vi_size_limit

Define o número de registros de item vulnerável a serem incluídos no conjunto de resultados da integração de vulnerabilidades de máquina MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2 000.

vulnerability_size_limit

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de Vulnerabilidade do MS TVM (CVE). Esta configuração deve estar no formato int32. O valor padrão é 2 000.

recommendations_size_limit

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da Integração de recomendações do MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2 000.

asset_size_limit

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de máquinas MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2 000.

machine_filter

Filtra as máquinas que vêm do MS TVM. Este filtro é aplicado à integração de máquinas MS TVM. O valor padrão é trazer máquinas em que onBoardingStatus está integrado.

Mensagens REST para o Microsoft Threat and Vulnerability Management Vulnerability Integration

Você pode usar as mensagens REST para ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability Integration para fazer chamadas para a API MS TVM.

Token de acesso MS TVM

Você também pode usar as mensagens REST para o token de acesso do MS TVM para recuperar o token de acesso da API do MS TVM para que você possa autenticar solicitações da REST API. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas ao MS TVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração do MS TVM

Você pode usar a mensagem REST para a integração do MS TVM para recuperar informações do MS TVM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao MS TVM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição do método
OBTENHA vulnerabilidades	Recupera informações de vulnerabilidade e exploração do MS TVM.
OBTER vulnerabilidades de software por máquina	Recupera todas as vulnerabilidades em aberto.
OBTER recomendações	Recupera a lista de todas as recomendações de segurança acionáveis que afetam a organização.
OBTER máquinas	Recupera a coleção de ativos.
OBTER mudanças de vulnerabilidades de software por máquina	Recupera todas as informações que foram alteradas na importação completa de vulnerabilidades da organização, incluindo vulnerabilidades novas, corrigidas e atualizadas.

Transformação de dados para o Microsoft Threat and Vulnerability Management Vulnerability Integration

Depois de identificar os dados que você deseja importar, os dados serão recuperados do ServiceNow® Aplicação Microsoft Threat and Vulnerability Management (MS TVM), processada por meio de um conjunto de fontes de dados e transformada em sua instância.

Durante a instalação, os mapas de gravidade normalizados são instalados no módulo Mapeamento de gravidade normalizado. Esses mapas são transformados importados Microsoft níveis de gravidade de vulnerabilidade de terceiros para níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de gravidade, consulte Crie um Resposta a vulnerabilidades mapa de severidade.

Importação de máquinas MS TVM

Os dados das máquinas importadas são carregados primeiro na tabela Importação de máquinas MS TVM [sn_vul_msft_tvm_machines_import].

A transformação de máquinas MS TVM é usada para transformar as informações das máquinas importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de máquinas MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de máquinas do Microsoft TVM** .

A tabela a seguir lista os campos do mapa de transformação por integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de máquinas MS TVM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo dos ativos. Este ID é mapeado para o source_id do registro do item descoberto.
u_ipaddresses.macAddress	mac_address	Endereço MAC mapeado da API para o campo de endereço mac do host do registro cmdb_ci.
u_ipaddresses.ipaddress	ip_address	Campo Endereço IP mapeado para o campo Endereço IP do registro cmdb_ci.
u_lastseen	last_scan_date	Campo mapeado para o campo last_scan_date no registro do item descoberto.
u_machinetags		Marcadores salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	os	Campo que mapeia para o campo SO no registro cmdb_ci.
u_computerdnsname	fqdn	Campo que mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Tempo e finalidade do script de mapa de transformação das máquinas MS TVM

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) do processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para atualizar valores no host e verificar se o host existe. Com base nos resultados, este script modifica os valores na variável de escopo (sn_vul_msft_tvm). Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

A inclusão de script MicrosoftTVMMachinesProcessor é chamada a partir do script de transformação onBefore. Ele pega a saída da integração das máquinas Microsoft TVM e a transforma em um IC. Qualquer mudança nesta inclusão de script pode alterar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a transformação dos dados das máquinas Microsoft TVM na tabela de IC e itens descobertos.

Integração de vulnerabilidades do MS TVM

Os dados de vulnerabilidades importados são carregados primeiro na tabela Microsoft TVM CVE (Vulnerabilidades) Import [sn_vul_msft_tvm_vulnerability_import].

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades do MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de vulnerabilidades do Microsoft TVM** .

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de vulnerabilidades do Microsoft TVM

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia para a coluna ID do registro sn_vul_entry.
u_severity	source_severity	Mapeia o campo Severidade para a Severidade. O valor padrão é 5.
u_publishedon	date_published	Mapeia o campo u_publishedon para a data de publicação.
u_publicexploit	public_exploit	Mapeia o u_publicexploit fornecido pelo verificador para a coluna exploit público na tabela de entrada de vulnerabilidade.
u_cvssv3	v3_base_score	Mapeia a pontuação cvssv3 para a pontuação de base v3 no registro de entrada de vulnerabilidade.
u_description	resumo	Mapeia a descrição para o campo de resumo no registro de entrada de vulnerabilidade.
u_exploitinkit	malware_kit	Mapeia o campo u_exploitinkit para o kit de malware na tabela de exploração.
u_exploittypes	tipo	Mapeia o tipo de exploração para o tipo na tabela de exploração.
u_exploitverificado	_exploit_verified	Mapeia o campo u_exploitverified para o exploit verificado na tabela de exploração.
u_exploituris	exploit_links	Mapeia o campo u_exploituris para os links de exploração na tabela de exploração.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) do processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para criar ou atualizar os valores na tabela de entrada de terceiros ou NVD. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir os valores dos novos itens que foram criados e os itens que foram atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de recomendações do MS TVM

Os dados de recomendação importados são carregados primeiro na tabela Importação de recomendações do MS TVM [sn_vul_msft_tvm_recom_import].

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de recomendações do MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de recomendação do MS TVM** .

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_recommendedvendor	recommended_vendor	Mapeia o campo u_recommendedvendor para a coluna Fornecedor.
u_weaknesses	pontos fracos	Mapeia o campo u_weakks para a coluna Weakks.
u_exposedmachinescount	src_exposed_machines_cnt	Mapeia o campo u_exposedmachinescount para a coluna Contagem de máquinas expostas.
u_status	status	Mapeia o status para o campo Status no registro de recomendação.
u_productname	product_name	Mapeia o campo u_productname para o Nome do produto no registro de recomendação.
u_nonprodutiv_impactessets	non_prod_impacted_assets	Mapeia o campo u_nonproducti_impactedassets para a coluna Ativos afetados no registro de recomendação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_activealert	active_alert	Mapeia o campo u_activealert para a coluna Alerta ativo no registro de recomendação.
u_recommendedversion	recommended_version	Mapeia o campo u_recommendedversion para a coluna Versão recomendada no registro de recomendação.
u_totalmachinecount	total_machine_count	Mapeia o campo u_totalmachinecount para a coluna Contagem total de máquinas no registro de recomendação.
u_exposureimpacto	exposure_impact	Mapeia o campo u_exposureimpact para a coluna Impacto da exposição no registro de recomendação.
u_recommendationname	recommendation_name	Mapeia o campo u_recommendationname para a coluna Nome da recomendação no registro de recomendação.
subcategory	subcategoria	Mapeia o campo u_subcategoria para a coluna Subcategoria no registro de recomendação.
u_id	source_id	Mapeia o ID de recomendação do MS TVM para a coluna ID de origem.
u_remediationtype	remediation_type	Mapeia o campo u_remediationtype para a coluna Tipo de correção no registro de recomendação.
componente u_related	related_component	Mapeia o campo u_relatedcomponent para a coluna Componente relacionado no registro de recomendação.
u_recommendedprogram	recommended_program	Mapeia o campo u_recommendedprogram para a coluna Programa recomendado no registro de recomendação.
u_recommendationcategory	recommendation_category	Mapeia o campo u_recommendationcategory para a coluna Categoria de recomendação no registro de recomendação.
u_publicexploit	public_exploit	Mapeia o campo u_publicexploit para a coluna Exploração pública no registro de recomendação.
u_vendor	fornecedor	Mapeia o campo u_vendor para a coluna Fornecedor no registro de recomendação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
[Script]	integration_instance	Nome da instância da qual a recomendação é importada.
[Script]	sys_domain	Domínio no qual este registro é importado.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Script do mapa de transformação de recomendação do MS TVM

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) do processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para atualizar valores nas recomendações e verificar se as recomendações existem. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir os valores de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de vulnerabilidades de máquina MS TVM

O mapa de transformação de vulnerabilidades da máquina MS TVM é usado para transformar informações de vulnerabilidades abertas e corrigidas importadas do MS TVM.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades de máquina MS TVM são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e corrigidas do MS TVM, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de vulnerabilidades da máquina MS TVM** .

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de vulnerabilidades da máquina MS TVM

Campo de origem	Campo de destino	Descrição
u_id	detection_key	Mapeia o campo u_id para a coluna Chave de detecção na tabela de detecção.
u_diskpaths	prova	Mapeia o campo u_diskpaths para a coluna de prova na tabela de detecção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de vulnerabilidades da máquina MS TVM

Campo de origem	Campo de destino	Descrição
u_registrycaminhos	prova	Mapeia o campo u_registrypaths para a coluna de prova na tabela de detecção.
u_recommendedsecurityupdateid	preferred_solution	Mapeia o campo u_recommendedsecurityupdateid para a coluna de solução preferencial na tabela de item vulnerável, se a solução existir com o mesmo ID na tabela sn_vul_solution.
referência u_recommendation	recomendação	Mapeia o campo u_recommendationreference para a coluna Recomendação na tabela de item vulnerável.
u_cveid	vulnerabilidade	Mapeia o campo u_cveid para a coluna Vulnerabilidade na tabela de itens vulneráveis.
u_status	source_status	Mapeia o campo u_status para a coluna Status de origem na tabela de detecção.
u_eventtimestamp	temporal_score	Mapeia o campo u_eventtimestamp para a coluna Mais recente encontrado na tabela de item vulnerável.
u_lastseentimemcarimbo	last_seen	Mapeia o campo u_lastseentimestamp para a coluna Visto pela última vez na tabela de item vulnerável.
u_firstseentimentimcarimbo	first_seen	Mapeia o campo u_firstseentimestamp para a coluna Visto pela primeira vez na tabela de itens vulneráveis.
u_recommendedseguridadualização	solution_summary	Mapeia o campo u_recommendedsecurityupdate para a coluna Resumo da solução na tabela de itens vulneráveis.
u_recommendedsecurityupdateurl	solution_summary	Mapeia o campo u_recommendedsecurityupdateurl

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de vulnerabilidades da máquina MS TVM

Campo de origem	Campo de destino	Descrição
		para a coluna Resumo da solução na tabela de itens vulneráveis.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) do processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para verificar se a entrada de vulnerabilidade e as detecções existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para atualizar a contagem de VIS e detecções conforme importado do MS TVM. Este script é para uso interno e não deve ser modificado ou excluído.

Gráfico de status de execução de integração para a Integração de vulnerabilidades do Microsoft Threat and Vulnerability Management

Você pode usar o módulo Status de execução de integração do Microsoft Threat and Vulnerability Management (MS TVM) para fornecer uma exibição gráfica do status das execuções de integração do MS TVM.

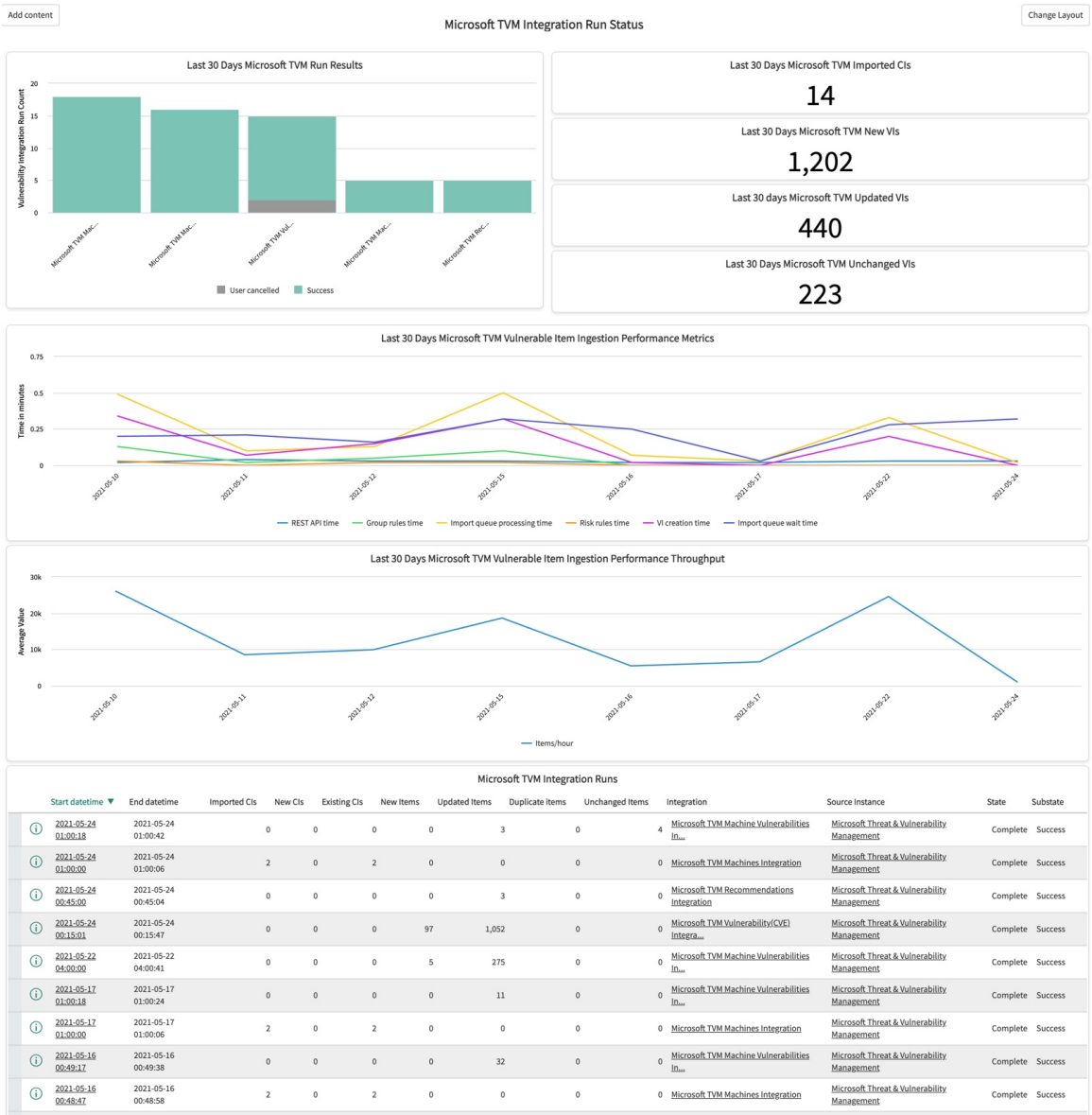
A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, você pode apontar para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer peça no gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios de gráfico de status de execução de integração do MS TVM

Nome	Descrição
Resultados do Microsoft TVM nos últimos 30 dias	Número de execuções de integração concluídas para cada integração. Este relatório mostra as execuções bem-sucedidas e com falha. Cada execução é exibida como uma barra no gráfico.
Microsoft TVM nos últimos 30 dias	Número de novos itens vulneráveis importados nos últimos 30 dias.
Microsoft TVM atualizados nos últimos 30 dias	Número de itens vulneráveis atualizados que foram importados nos últimos 30 dias.
Microsoft TVM inalterado nos últimos 30 dias	Número de itens vulneráveis duplicados que foram importados nos últimos 30 dias.
Execuções de integração do MS TVM	Registros de execução de integração em uma lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: V16.1: Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no *sn_vul_detection*tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.
Métricas de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Rendimento de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Rendimento diário de ingestão de item vulnerável que foi medido para a integração do Microsoft TVM Host Detection nos últimos 30 dias.
ICs importados do Microsoft TVM nos últimos 30 dias	Número de novos itens de configuração que foram importados nos últimos 30 dias.

Verifique o status da execução de importação da integração do Microsoft Threat and Vulnerability Management

Use o status de execução de importação do Microsoft Threat and Vulnerability Management (MS TVM) para verificar o sucesso das execuções de integração e localizar quaisquer problemas.

Antes de Iniciar

Este procedimento faz as seguintes suposições:

- Você tem Resposta a vulnerabilidades E o MS TVM Vulnerability Integration instalado e configurado.
- As importações de Integração de vulnerabilidades do MS TVM estão programadas e em execução.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Microsoft Threat and Vulnerability Management** > **Integrações**.
   a. Escolha uma integração.
   b. Clique na lista relacionada Execuções de integração de vulnerabilidades.
2. Verifique se o estado das importações está concluído, com o subestado como Sucesso.
   As causas mais comuns para uma execução com falha são as seguintes:
   - Interrupção de rede.
   - Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação.
3. **Opcional:** Se você vir uma dessas condições que causou uma falha na execução, clique em **Executar agora** e execute novamente a integração.

Divida detecções do Microsoft TVM com base na instância de vulnerabilidade para dividir itens vulneráveis

ServiceNow® O Vulnerability Response permite a divisão de detecções de scanners do Microsoft Threat and Vulnerability Management (MS TVM), permitindo a criação de um item vulnerável exclusivo (VIT) para cada instância de vulnerabilidade detectada. Essa divisão permite a atribuição de Vits a várias equipes de correção, aprimorando o gerenciamento e o acompanhamento de vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A carga útil do scanner do Microsoft Threat and Vulnerability Management (MS TVM) contém dados de detecção, com cada caminho na prova usado para dividir as detecções. O marcador diskpath na carga identifica o local da vulnerabilidade, facilitando a identificação e o gerenciamento precisos de vulnerabilidades de acordo com seus caminhos específicos.

Procedimento

1. Na tabela Integrações de terceiros [sn_sec_int_integration], defina **Incluir prova na chave vi** valor da coluna como verdadeiro para Tenable.io e. Tenable.sc.
2. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.
3. No formulário Incluir porta, marque a caixa de seleção Incluir porta e marque **clique aqui** link.
4. Na lista Adicionar prova às chaves VI, selecione **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário Adicionar prova à chave VI - Novo registro, em **Vulnerabilidade** Adicione o Microsoft Threat and Vulnerability Management (MS TVM) CVE para o qual você deseja incluir a prova e selecione **Enviar** .
   A vulnerabilidade selecionada aparece na lista Adicionar prova às chaves VI.

Example: Divisão de detecções do scanner Microsoft Threat and Vulnerability Management (MS TVM)

A detecção a seguir do scanner Microsoft Threat and Vulnerability Management (MS TVM) mostra prova no marcador Diskpath.


```
          "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
          "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

          "rbacGroupId":
     "rbacGroupName": "Unassigned",
      "deviceName": "ip-0a1409fd.secops.com",
       "osPlatform": "WindowsServer2019",
         "oVersion": "10.0.17763.5936",
       "osArchitecture": "x64",
        "softwareVendor": "mozilla",
       "softwareName": "firefox",
       "softwareVersion": "126.0.1.0",

           "cveId"; "CVE-2024-7528",
          #vulnerabilitySeverityLevel": "High",
        #recommendedSecurityUpdate":; "mfsa2024-33",

        "recommendedSecurityUpdateId": null,

           "recommendedSecurityUpdateUrl": null,
            "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

         "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
lMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


        #lastSeenTimestamp": "2024-08-28 19:36:07",

         "firstSeenTimestamp": "2024-08-06 20:32:34",

       "end0fSupportStatus": null,
          "end0fSupportDate": null,
      "exploitabilityLevel": "NoExploit",
          "recommendationReference": "va-_-mozilla-_-firefox",

         "cvssScore": 8.8,
      "securityUpdateAvailable": true,
         "cveMitigationStatus": null
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades

Você pode gerenciar patches e implantações de patches para vulnerabilidades críticas para grandes grupos de ativos com Resposta a vulnerabilidades Integração da Orquestração de patches com o produto HCL BigFix.

Orquestração de patches com Resposta a vulnerabilidades

Orquestração de patches com Resposta a vulnerabilidades usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidades. Os dados de detecção do scanner correspondem os ativos em seu ambiente às vulnerabilidades e às atualizações de patch que podem corrigi-las. Envie solicitações de patch para aprovação, programe atualizações de patch para resolver itens vulneráveis e monitore o andamento da correção, tudo a partir de registros no Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform®.

Orquestração de patch de resposta a vulnerabilidades com o HCL BigFix

Quando a aplicação de integração Orquestração de patch de resposta a vulnerabilidades com BigFix do HCL é usada com o. ServiceNow® Solução de gestão de vulnerabilidade, Orquestração de patch, e. Resposta a vulnerabilidades gerentes de vulnerabilidades e analistas podem executar as seguintes tarefas:

- Veja mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore dados de vulnerabilidades e soluções, bem como o andamento da correção de vulnerabilidades de registros no Resposta a vulnerabilidades Espaços de trabalho.

Os especialistas DE TI e os responsáveis pela correção podem executar as seguintes tarefas:

- Implante patches compatíveis com o produto BigFix para seus Windows, CentOS, MAC, Oracle e outros ativos em intervalos regulares e programados fora do horário comercial para evitar conflitos de trabalho.
- Identifique ativos não corrigidos com vulnerabilidades ou ativos que ou não foram atualizados com êxito por patches programados de dados de detecção importados de scanners de terceiros.
- Programe patches disponíveis no Espaço de correção de TI ou no ambiente clássico para ativos vulneráveis e não corrigidos da atualização de patch, tarefa de correção e registros de itens descobertos.

Termos-chave no Resposta a vulnerabilidades E aplicações BigFix

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu Configuration Management Database (CMDB). O BigFix chama ICs, computadores.

Grupos de computadores

Terminologia usada no produto BigFix que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma conta distinta da aplicação BigFix. Cada conta de usuário pode ser uma instância na aplicação BigFix. Este termo também se refere a um endereço da web exclusivo e seguro para um ServiceNow AI Platform instância.

Integração

Uma integração é um trabalho agendado no ServiceNow AI Platform Que recupera informações de uma origem de terceiros, como a integração com as máquinas BigFix.

Solução

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

Patch

Atualizações de software que corrigem vulnerabilidades. Na aplicação BigFix, os patches são chamados Fixlets. Por exemplo, o BigFix tem Fixlets para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que se destinam a corrigir vulnerabilidades específicas. Depois de implantados, os patches são mapeados para os itens vulneráveis relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção

Listas de itens vulneráveis no Resposta a vulnerabilidades aplicação de ações necessárias para corrigir vulnerabilidades.

Implantação

A implantação para fins desta integração se refere a quando você aplica, inicia ou agenda um patch em uma máquina. O BigFix chama essas implantações de ações. Você pode implantar (criar ações) para os patches baixados do BigFix em seu ServiceNow AI Platform. Navegue até Itens descobertos, patches ou tarefas de correção de registros individuais em Resposta a vulnerabilidades. Você pode implantar patches com trabalhos agendados em máquinas individuais ou em grupos de computadores.

Implantação no ServiceNow AI Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em todo o seu ambiente. Por exemplo, você pode ter várias implantações da integração do BigFix Vulnerability em seu ambiente.

Gestão de soluções de vulnerabilidade e Orquestração de patch de resposta a vulnerabilidades com integração do HCL BigFix

O gerenciamento de soluções é fornecido pelo Solução de gestão de vulnerabilidade aplicação, a. ServiceNow AI Platform aplicação que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrige. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, o Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidades E as aplicações Orquestração de patch de resposta a vulnerabilidades com HCL BigFix trabalham juntos para implantar patches preferenciais da solução para a vulnerabilidade e para o item vulnerável para ajudar você a corrigir e fechar vulnerabilidades em seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidades E a Orquestração de patch de resposta a vulnerabilidades com HCL BigFix Integration estão disponíveis no ServiceNow® Store.

Funções necessárias de ServiceNow AI Platform

As tarefas de instalação, configuração e correção de integração exigem as seguintes funções no ServiceNow AI Platform instância.

administrador

Usuários com esta função obtêm direitos para aplicações no ServiceNow Store e os baixa para ServiceNow AI Platform instâncias.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações no ServiceNow AI Platform e conclui a configuração do Resposta a vulnerabilidades aplicação. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_bigfix.configure_integration

Os usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém a função granular sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Usuários com esta função podem exibir (somente leitura) os#registros doResposta a vulnerabilidades E a aplicação BigFix Patch Orchestration Integration e os dados de orquestração de patches.

sn_vul_patch_orch.configure_patch

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir informações de patch (somente leitura).

Aprovadores

Atribua usos aos grupos de aprovadores de aprovador de nível 1 e de aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre Resposta a vulnerabilidades funções em seu ServiceNow AI Platform, consulte Resposta a vulnerabilidades personas e funções granulares.

Regras de pesquisa de IC

Quando os dados são importados da aplicação BigFix, o. Resposta a vulnerabilidades a aplicação pesquisa automaticamente correspondências no Configuration Management Database (CMDB) usando dados da máquina (ativo). As regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (VI) quando os VIS são criados.

As regras de pesquisa de IC a seguir são enviadas com o sistema de base e são usadas para identificar ICs (ativos) e adicioná-los ao Resposta a vulnerabilidades aplicação:

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar vários valores para ip_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência. Para obter mais informações sobre como as regras de pesquisa de IC e como elas funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.

MID Server

. Resposta a vulnerabilidades A Orquestração de patches com a integração do HCL BigFix é uma integração no local. Requer um MID Server autônomo que não faça parte de um cluster do MID Server. O MID Server deve executar scripts em máquinas remotas da sua instância para importar dados do servidor BigFix. As APIs para esta integração são chamadas usando MID Servers que você configurou em seu ServiceNow AI Platform instância. Para obter mais informações, consulte Prepare-se para Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix.

Integrações e dependências do Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix

Os seguintes produtos e aplicações de dependência são necessários para a Orquestração de patch de resposta a vulnerabilidades com integração do HCL BigFix. Essas aplicações estão disponíveis no ServiceNow® Store.

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

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços de trabalho em Resposta a vulnerabilidades as seguintes aplicações são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre compatibilidade de versões com as aplicações e versões de família necessárias, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão artigo na Base de conhecimento HI.

Aplicação e versão de lançamento
Resposta a vulnerabilidades
Solução de gestão de vulnerabilidade
Aplicação de Orquestração de patch de resposta a vulnerabilidades
Resposta a vulnerabilidades Orquestração de patches com a aplicação HCL BigFix
Security Support Common
Orquestração do suporte de segurança
Uma aplicação de verificação de vulnerabilidades de terceiros compatível

Resposta a vulnerabilidades Tabelas da aplicação de Orquestração de patches

. Resposta a vulnerabilidades A aplicação de Orquestração de patches contém as seguintes tabelas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização do dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Integrações de Orquestração de patch de Resposta a vulnerabilidades com o HCL BigFix

As integrações desenvolvidas por ServiceNow® A engenharia compõe a implantação da solução orquestrada com o produto BigFix. As integrações a seguir estão incluídas com Resposta a vulnerabilidades Integração da Orquestração de patches com a aplicação HCL BigFix que você baixa do ServiceNow® Store.

Depois de instalar a aplicação de integração no seu ServiceNow AI Platform para exibir essas integrações, navegue até **Integrações** > **Integração da Orquestração de patches do BigFix** > **Integrações**. . Resposta a vulnerabilidades A aplicação processa dados em intervalos de tempo programados importados por essas integrações com endpoints do BigFix.

Integração	Descrição
Integração do BigFix Collection	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução de integração encadeada. • Recupera os computadores e os grupos de computadores que compõem os grupos de computadores (itens de configuração) da aplicação BigFix.
Integração do BigFix Fixlet	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Collection. Você também pode executá-lo sob demanda. • Recupera informações sobre todos os fixlets disponíveis (patches) do servidor BigFix.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
BigFix Device Fixlet Integration	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os fixlets que estão atualmente em computadores (ativos) do servidor BigFix.
Integração do BigFix Actions	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Device Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe DE TI no servidor BigFix.

Prepare-se para Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix

Prepare-se para a integração executando as tarefas de configuração a seguir.

Antes de Iniciar

Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Por Que e Quando Desempenhar Esta Tarefa

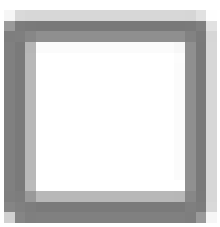
Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração.

Você está pronto para Instale o. Resposta a vulnerabilidades Orquestração de patches com a aplicação HCL BigFix.

Procedimento

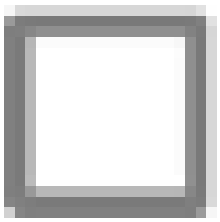
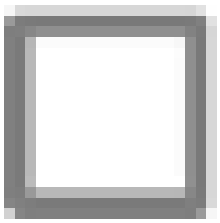
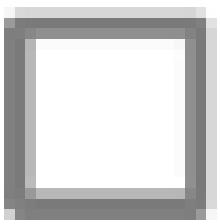
1. Para uma instalação e configuração suaves do Resposta a vulnerabilidades Orquestração de patches com a aplicação HCL BigFix, siga a check-list fornecida.
2. Antes de instalar a aplicação, você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos.

   Após a instalação e a configuração, importe informações relacionadas a vulnerabilidades e patches para seu ServiceNow AI Platform® instância.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,0 de Resposta a vulnerabilidades ou posterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Se ainda não estiver instalado, obtenha direitos e instale um aplicativo de scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Resposta a vulnerabilidades para obter mais informações sobre scanners de terceiros compatíveis com Resposta a vulnerabilidades. Consulte .
	Se ainda não estiver instalado, obtenha direitos e baixe a aplicação Orquestração de patch de resposta a vulnerabilidades com HCL BigFix para seu ServiceNow AI Platform® instância. Consulte .
	Obtenha credenciais do BigFix. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos BigFix para que você tenha acesso a eles.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **administrador** O administrador do sistema obtém direitos, baixa e instala o aplicativo BigFix Patch Orchestration e os outros aplicativos necessários para a integração. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Resposta a vulnerabilidades Ou no módulo Administração de usuários. **sn_vul.vulnerability_admin** Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do BigFix e das outras aplicações de terceiros. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Orquestração de patch de resposta a vulnerabilidades e aplicações de Gestão de soluções de vulnerabilidade. **sn_vul_bigfix.configure_integration** Os usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_bigfix.read_integration e connection_admin que permitem que o usuário se conecte ao console do

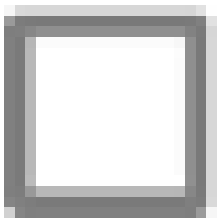
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	BigFix e configure as instâncias de integração em seu ServiceNow AI Platform. **sn_vul_bigfix.read_integration** Usuários com esta função podem exibir (somente leitura) os#registros doResposta a vulnerabilidades E a aplicação BigFix Patch Orchestration Integration e os dados de orquestração de patches. **sn_vul_patch_orch.configure_patch** Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário dos registros de item vulnerável e Atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores forem atribuídos. **sn_vul_patch_orch.read_patch** Usuários com esta função podem exibir (somente leitura) informações de patch em registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades. **Aprovadores** Os usuários atribuídos ao aprovador de nível 1 e, opcionalmente, aprovador de nível 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de aprovadores de nível 1 para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Orquestração de patches com Resposta a vulnerabilidades. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o grupo Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais para funções de especialista em correção e analista de vulnerabilidades e adicionar usuários com o módulo Administração de usuários em sua instância. Consulte Crie um grupo de usuários .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ○ A Orquestração de patch de resposta a vulnerabilidades com HCL BigFix é uma integração no local que requer o uso de um MID Server autônomo. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . ○ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

O que Fazer Depois

Agora você está pronto para Instale o. Resposta a vulnerabilidades Orquestração de patches com a aplicação HCL BigFix.

Instale o. Resposta a vulnerabilidades Orquestração de patches com a aplicação HCL BigFix

Baixe a aplicação Orquestração de patch de resposta a vulnerabilidades com HCL BigFix do ServiceNow® Store.

Antes de Iniciar

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. O administrador de vulnerabilidades (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)) para configurar a Orquestração de patch de resposta a vulnerabilidades com o HCL BigFix e outros aplicativos depois que eles forem instalados.

Por Que e Quando Desempenhar Esta Tarefa

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Prepare-se para Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Procedimento

1. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
2. Localize **Orquestração de patch de resposta a vulnerabilidades com o HCL BigFix** aplicação e clique **Instalar** .

   Esta ação instala a aplicação que você baixou do ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Tudo** > **Integração da Orquestração de patches do BigFix** > **Configuração** para continuar com a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o. Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix

Depois de instalar a aplicação, configure-a com as informações da conta do BigFix e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_bigfix.configure_integration

Procedimento

1. Navegar até **Integração da Orquestração de patches do BigFix** > **Configuração**.
2. Preencha os campos com suas informações e credenciais do BigFix.

Campo	Descrição
Instância de integração	O nome da conta da instância do BigFix que você deseja usar, por exemplo, Integração do BigFix Patch Management .
Nome do host	Insira o URL do host do BigFix.
Nome do usuário	Insira o nome de usuário da sua conta do BigFix.
Senha	Insira a senha da sua conta do BigFix.
MID Server	Insira o nome do MID Server autônomo na lista que você deseja usar. Consulte Prepare-se para Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix Para obter mais informações sobre MID Servers e configurar tarefas em seu ServiceNow AI Platform®.

3. Clique em Salvar e testar credenciais.
   O status da conexão entre o BigFix e o. ServiceNow AI Platform® A instância#é exibida no campo Status de validação. Se você não vir um teste bem-sucedido, siga as instruções.
4. **Opcional:** Domain Separation é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:
   a. Navegar até **Integração da Orquestração de patches do BigFix Instâncias de integração** .
   b. Verificar o escopo da aplicação, Orquestração de patch de resposta a vulnerabilidades com o HCL BigFix É exibido no campo Escopo da aplicação.
   c. Clique em **Nova**.
   d. Preencha o formulário.

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Orquestração de patch de resposta a vulnerabilidades com o HCL BigFix

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Integração	BigFix Patch Management é o padrão.
Ativo	O padrão é Ativado (selecionado). Se estiver desmarcada, a instância não estará ativa.

e. Clique em **Enviar**.
Sua nova instância de integração é exibida na lista Instâncias de integração.

f. Repita as etapas de 1-3 a 5 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.
Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] É ativado para que, quando as implantações de patch são programadas, elas sejam enviadas para revisão e aprovação aos usuários atribuídos ao grupo de aprovação de atualização de patch de nível 1.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative [**sn_vul_patch_orch.patch_approval_required** propriedade]. Você pode preferir deixar as aprovações ativadas para que os patches agendados não entrem em conflito com o horário normal de trabalho.

Nota: Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **sys.properties.list**.

b. Localizar **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `falso` .

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, deverá atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.

b. . **Implantar aprovação de atualização de patch** A regra de aprovação não é exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch** .

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Aprovação de atualização de patch de configuração padrão** .

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Adicione usuários neste grupo.

Os usuários atribuídos a este grupo aprovam solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em **Atualização** para salvar suas mudanças.

8. **Opcional:** Você pode configurar aprovações multinível para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

a. Com o registro Aprovação de atualização de patch de configuração padrão exibido, clique em **Novo** .

b. Preencha os campos.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 - Aprovação de atualização de patch** .
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções especificadas.
Usuários	Edite os usuários listados nos grupos.

c. Clique em **Enviar** para salvar suas edições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibindo dados de patch para Resposta a vulnerabilidades Integração da Orquestração de patches com o HCL BigFix

Dados de patch e dados de acúmulo de patch, bem como informações de vulnerabilidade e status de correção de suas vulnerabilidades, são exibidos em registros em sua instância.

Exibição de dados de patch no Resposta a vulnerabilidades Espaços de trabalho

Funções necessárias:

- função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades

No Espaço de correção de TI, você pode exibir patches:

- Na exibição Página inicial, em que você pode clicar em cartões de pontuação para exibir registros de soluções preferenciais em VIS, ICs vulneráveis e patches preferenciais em VIS.
- Na exibição de lista, em que você pode exibir todos os registros de atualização de patch (VPUs) dos links de patches e os itens vulneráveis (Vits) atribuídos a você que têm patches.

Você pode programar patches a partir dos seguintes registros:

- Da Atualização de Patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Espaço do Gerenciador de vulnerabilidades, você pode exibir patches:

- Na exibição Página inicial nos tópicos de exibição, onde você pode exibir patches preferenciais e potenciais, datas programadas de patch e, se o patch foi baixado, todos no **Itens vulneráveis** guia.
- Na Exibição de lista sobre esforços de correção, em que você pode exibir dados de patch em registros de VI do **Itens vulneráveis** guia.

Na exibição de ambiente clássica, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Patches**.

Registros de atualização de patch nos Espaços de VR e na exibição de ambiente clássica

Os dados do patch e os dados e status do rollup de patch são exibidos nos registros em sua instância. Os registros de patch estão incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exibir registros de Patch (VPU) em Resposta a vulnerabilidades Exibição de lista no Espaço de correção de TI. Registros de atualização de patch na exibição clássica e Resposta a vulnerabilidades Os espaços de trabalho incluem os seguintes dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Dados e informações da solução de vulnerabilidade de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos com atualizações ausentes.
- Status de correção que inclui % de VIS corrigidos e o total de VIS que têm um patch como patch preferencial.
- Dispositivos associados, Itens vulneráveis, Implantações de patch e Solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros no Resposta a vulnerabilidades Espaços de trabalho.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Acúmulo de estado em registros de item vulnerável

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e rollup de estado para orquestração de patches em Resposta a vulnerabilidades.

Registros que acumulam contagens de VI ativas

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado seleciona somente as mudanças na contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados nos seguintes registros em Resposta a vulnerabilidades:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Dados de patch com Resposta a vulnerabilidades

Os painéis de Gestão de vulnerabilidades (PA) e CISO estão incluídos com uma assinatura do Performance Analytics para Resposta a vulnerabilidades aplicação. Se você tiver uma assinatura para Performance Analytics, Mas não tem uma integração de orquestração de patch instalada, a guia Correção é exibida no painel do CISO, mas não é preenchida com dados.

Para o painel de Gestão de vulnerabilidades (PA), navegue até **Tudo** > **Resposta a vulnerabilidades** > **Visão geral**. Clique em **Correção** E role até a parte inferior da página para exibir os dados de Atualizações de patch: Patches programados e não programados, patches que não têm datas de destino e contagens semanais.

Para o Painel do CISO, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura de patch: Criticidade, patches programados e não programados e patches sem datas de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre Resposta a vulnerabilidades painéis, consulte Usando o padrão Resposta a vulnerabilidades painéis, Orquestração de patches com Resposta a vulnerabilidades Espaços de trabalho e Exibição de dados de orquestração de patches no Resposta a vulnerabilidades painéis.

Programar patches com Resposta a vulnerabilidades Integração de orquestração de patches HCL BigFix

Programe patches dos registros de tarefa de correção e Atualização de patch no Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform instância.

Antes de Iniciar

A partir da versão 16,1, você pode programar patches do Resposta a vulnerabilidades Ou do ambiente clássico.

Funções necessárias:

- função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades

Procedimento

1. Na Vulnerabilidade Resposta a vulnerabilidades Espaços de trabalho, como um usuário com a função sn_vul.remediation_owner, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Na página inicial, clique em **Patch preferencial no VIS** .
   A lista de registros de Atualização de patch para o VIS com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço, clique em **Patches** > **Tudo** E localize um registro de Atualização de patch.
   O registro de Atualização de patch é exibido. Você pode preferir revisar os dados antes de programar um patch, porque pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos e o que você pode fazer.

Tarefa	Descrição
Clique em um link de Itens relacionados	○ Visão geral - Exibir detalhes como o número do registro de atualização do patch, os IDs do artigo e do boletim, a data da versão e a categoria da atualização, o nome do site do patch, classificação de risco, pontuação de risco, descrição, solução (se fornecida), e status de correção. ○ Dispositivos associados - A lista de itens de configuração afetados pelo patch e pelo status. ○ Itens vulneráveis - A lista de itens vulneráveis associados à vulnerabilidade e ao patch.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	○ Implantações de patch - Os nomes e as informações relacionadas às implanta–ções deste patch em ativos ou grupos de ativos deste patch. ○ Solicitações de patch - Uma lista de so–licitações de patch já enviadas para este patch. Isso é exibido.
Clique em um link para abrir um registro	Nas listas exibidas em registros abertos nos links de Itens relacionados, exiba mais detalhes, incluindo mensagens sobre metas perdidas. Uma vez abertos, os registros permanecem abertos como guias até que você os feche.
Programar patch	Quando você estiver pronto para progra–mar um patch ou enviar uma solicitação, clique em **Patch de programação** . Na cai–xa de diálogo exibida, preencha os campos. Consulte as etapas abaixo para obter mais detalhes.
Adicione uma anotação de trabalho ou anexe um arquivo	Na extrema direita da tela, clique em **Atividade** (ícone de iluminação) e insira uma anotação de tra-balho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.

6. Clique em **Patch de programação** .
7. Na caixa de diálogo, preencha os campos.

Campo	Descrição
Selecione Destino	
Ativos	Escolha um na lista para continuar. Grupo de computadores é exibido por padrão. ○ Grupo de computadores: Selecione es–ta opção se quiser escolher uma coleção (um grupo de ativos) para este patch. #Os grupos são compostos pelos itens de configuração importados da aplicação BigFix. ○ Lista de computadores: Selecione esta opção se quiser escolher computadores individuais (ativos) para este patch. Você pode ver dados sobre o fabricante, local, classe, quando foi atualizado pela última vez e o cronograma de manutenção na caixa de diálogo exibida. Clique em **Próximo** para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de computadores ou Lista de computadores	Dependendo da sua seleção de ativos, um dos campos será exibido. Escolha uma das listas.
Agendamento	
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda você a rastrear suas atualizações.
Tipo de implantação	Escolha uma opção na lista.
Hora do vencimento	Defina o valor do tempo do prazo. Este valor é a hora em que o patch está disponível pela última vez para implantação.
Horário disponível	Defina o valor para a hora em que o patch ficará disponível.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Permitir reinicialização	O padrão é Desativado. Ative (selecione) esta opção para instruir as máquinas no grupo a reiniciar automaticamente após a conclusão do patch com sucesso.
Descrição	Adicione mais texto para Sobre o patch. Essas informações são exibidas no campo Descrição dos registros de Atualização de patch.

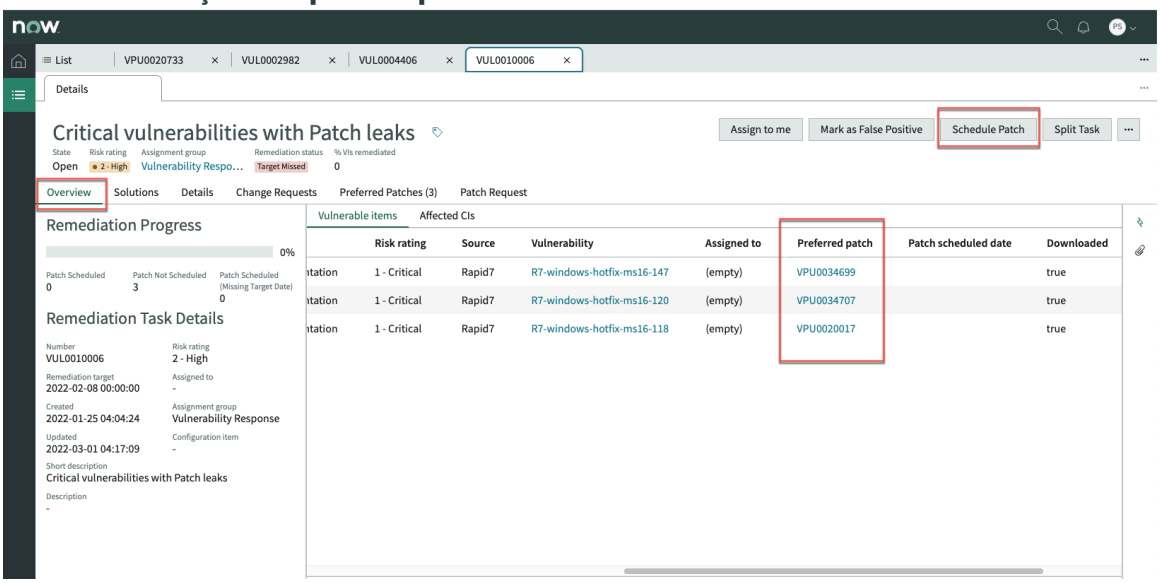
8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas de **Solicitações de exceção** > **Minhas solicitações** Na exibição de lista.
9. Como alternativa, você pode programar patches de tarefas de correção (RT) atribuídas a você ou ao seu grupo.

   Nota: A opção de programar um patch a partir de um registro de tarefa de correção estará disponível somente se houver patches mapeados para (associados a) o VIS na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de registros de tarefa de correção com a guia Visão geral selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção com patches preferenciais



10. Clique em **Patch de programação** No registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. Você pode programar patches para as etapas listadas anteriormente no ambiente clássico.
    Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Resposta a vulnerabilidades** > **Patches** > **Tudo**.

    b. Na lista exibida, localize um registro de Atualização de patch.

    c. Para tarefas de correção, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** e localize um registro.
    Rastreie o status de correção na guia Status de correção. Na parte inferior do registro, os dados do patch são exibidos nos links relacionados.

    d. Clique em Programar patch e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda você a rastrear suas atualizações.
Atualização de patch	Escolha um dos patches disponíveis na lista.
Ativos	Selecione um: ▪ Grupo de computadores: Selecione esta opção se quiser escolher uma coleção (um grupo de ativos) para este patch. #Os grupos são compostos pelos itens de configuração importados da aplicação BigFix. ▪ Lista de computadores: Selecione esta opção se quiser escolher computadores individuais (ativos) para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	este patch. Você pode ver dados sobre o fabricante, local, classe, quando foi atualizado pela última vez e o cronograma de manutenção na caixa de diálogo exibida.
Hora de início e hora de término	Insira as horas de início e término da janela de tempo. Insira quando você deseja que o patch inicie sua implantação e, no último dia, o patch poderá ser instalado.

Mensagens REST para a integração da Orquestração de patch de Resposta a vulnerabilidades com o HCL BigFix

. Resposta a vulnerabilidades Integração da Orquestração de patches com as mensagens REST do BigFix do HCL são usadas para fazer chamadas para a API do BigFix.

Login do BigFix

Você também pode usar as mensagens REST para o login do BigFix para autenticar solicitações da REST API. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas ao BigFix.

Nome do parâmetro	Valor	Descrição
sourceType	cumulativo	Indica que a integração de origem extrai dados do . Usado pelo código. Mudanças não são recomendadas.
SortDIR	desc	Indica a direção de classificação dos dados extraídos da integração. Mudanças não são recomendadas.
ClassificarCampo	severidade	Indica o campo no qual a classificação de dados se baseia. Mudanças não são recomendadas.
tipo	vuln	Indica o tipo de dados a serem obtidos da integração para a integração de ativos. Mudanças não são recomendadas.

Integração do BigFix

Você pode usar a mensagem REST para a integração do BigFix para recuperar informações do BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição
OBTER dados de busca	Recupera as informações do BigFix sobre um dos seguintes itens com base na consulta fornecida:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos REST

Método REST	Descrição
	• Computadores/Grupos de computadores • Fixos • Fixlets relevantes em computadores • Ações

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos baseados no usuário	Indica o endpoint do console do BigFix

BigFix Deploy patch

Você pode usar a mensagem REST para a integração do BigFix para programar patches do seu ServiceNow AI Platform® Para o BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch PÓS-implantação	Programa o patch no console do BigFix em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos baseados no usuário	Indica o endpoint do console do BigFix.
título	Valores dinâmicos baseados no usuário	Título da implantação.
settings_tag	Configurações nomeadas por marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o BigFix durante o agendamento do patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site em que o Fixlet está presente.
fixlet_id	Valor da atualização do patch	ID do Fixlet.

Transformação de dados para a integração de orquestração de patches com o HCL BigFix

Os dados são recuperados do Resposta a vulnerabilidades Orquestração de patches com integração do HCL BigFix, processada por meio de um conjunto de fontes de dados e transformada em seu ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação da coleção do BigFix

Os dados dos ativos importados (computadores e grupos de computadores) são carregados na tabela BigFix Collection Import [sn_vul_bigfix_collection_import]. BigFix Computer and Computer Groups Import TM (mapa de transformação?) é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação da BigFix Collection são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** E localize BigFix Computer and Computer Groups Import TM. A tabela a seguir lista os campos do mapa de transformação por integração.

BigFix Computador e Grupos de computadores importam o tempo do script do mapa de transformação

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para criar e atualizar ICs com base nas regras e coleções de pesquisa de IC, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação do BigFix Fixlet

Os dados dos fixlets importados são carregados na tabela Importação de Fixlet do BigFix [sn_vul_bigfix_patch_update_import].

O BigFix Fixlet Import TM é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação do BigFix Fixlet são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** E localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de mapa de transformação de importação do BigFix Fixlet

Campo de origem	Campo de destino	Descrição
u_id	article_id	ID exclusivo de um fixlet em um site.
u_id	source_id	ID exclusivo de um fixlet em um site.
U_site_name	SN_vul_bigfix_site_name	Nome do site no BigFix em que o Fixlet depende.
U_display_name	Título	Título do Fixlet.
[Script]	Bulletin_id	ID de origem da solução.
[Script]	SN_vul_solution	Solução baseada no ID de origem.
U_source	bulletin_source	Fornecedor de origem da solução.
[Script]	Date_release	Data de lançamento do fixlet.
U_category	Update_category	Categoria do fixador.
[Script]	Is_highest_suplantdence	Booliano para se o fixlet for a substituição mais alta ou não.
[Script]	_baixado	Se o fixlet foi baixado ou não.
[Script]	Integration_instance	Nome da instância da qual o fixlet é importado.
U_source_severity	Source_severity	Gravidade do fixador.
U_applicable_count	Num_total	Número total de dispositivos com fixlets ausentes.
[Script]	Last_modified	Data da última modificação do fixlet.

Tempo do script do mapa de transformação de importação do BigFix Fixlet

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de fixlets criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de Fixlet do dispositivo BigFix

Os dados dos fixlets relevantes importados nos computadores são carregados na tabela Importação de Fixlet do dispositivo BigFix [sn_vul_bigfix_device_patch_import].

O BigFix Device Fixlet TM é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação do BigFix Device Fixlet são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** E localize o BigFix Device Fixlet TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação do BigFix Device Fixlet

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para criar e atualizar ICs com base nas regras e coleções de pesquisa de IC, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de ações do BigFix

Os dados das ações importadas são carregados na tabela Importação de ações do BigFix [sn_vul_bigfix_deployment_import].

O BigFix Actions Import TM é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de ações do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** E localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação de ações do BigFix

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de importação de ações do BigFix

Campo de origem	Campo de destino	Descrição
U_name	nome	Nome da ação
[Script]	SN_vul_bigfix_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	SN_vul_patch_orch_update	Referência do patch
U_apply_count	Count_success	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Deployment_time	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Source_created	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Tempo do script do mapa de transformação de importação de ações do BigFix

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de ações criadas, atualizadas e ignoradas. Este script é para uso interno e não deve ser modificado ou excluído.

Exemplo de fluxo de trabalho para a integração da Orquestração de patch de Resposta a vulnerabilidades com o HCL BigFix

Um exemplo de como a orquestração de patches funciona com o produto HCL BigFix.

Antes de Iniciar

Digamos, por exemplo, que todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Espaço do Gerenciador de vulnerabilidades.
- sn_vul.remediation_owner para exibir o espaço do responsável pela correção de TI.
- função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente ou analista de vulnerabilidades que trabalha no Espaço do gerenciador de vulnerabilidades, você pode considerar criar tópicos de observação ou editar tópicos de observação existentes para ajudar a capturar VIS importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patch. Use estes exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Crie um tópico de observação no Espaço do gerente de vulnerabilidade para obter mais informações sobre como configurar o tópico de observação.

Exemplos de tópicos de observação para orquestração de patches no Espaço do Gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	A classificação de risco é 1 - crítica E. O motivo é Patch não programado
Vulnerabilidades críticas com patches programados (ANS ausente)	Patch programado (data de destino ausente)
Vulnerabilidades críticas com patches agendados	A classificação de risco é 1 - crítica E. A data programada do patch não está vazia E. O motivo é Patch programado

- Como gerente ou analista de vulnerabilidades, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Nos registros de VI e tarefas de correção, você pode detalhar a guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto BigFix.
- Como analista de vulnerabilidades ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) a partir de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode programar o patch a partir de um registro de Atualização de patch (nº VPU).
- Se os itens vulneráveis (VI) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique em **Tarefas de correção atribuídas** cartão de pontuação para exibir os registros.

   Para este exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (nº VUL) em busca de qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você pode saber que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para capturar VIS (VIT nº) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar o VIS, os patches preferenciais e ver se você ou algum de seu grupo já enviou solicitações de patch para aprovação.
3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

   Nota: . Se o VIS associado ao registro não tiver patches mapeados para eles, o **Patch de programação** o botão não está disponível no registro.
4. Clique em **Patch de programação** e preencha os campos na caixa de diálogo.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com Resposta a vulnerabilidades Integração de orquestração de patches HCL BigFix.
5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros.

   Neste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos VIS com esta vulnerabilidade está atribuído a você ou aos seus grupos. Nos registros de Atualização de patch, você pode enviar solicitações de patch. Nos registros de VI, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.
6. Se você não tiver acesso aos espaços ou preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Patches** > **Tudo**.

   b. Localize o registro de Atualização de patch desejado.
   Você pode preferir filtrar os registros com Crítico Pontuações de risco.

   c. Revise os campos VIS associados e % vis corrigidos na guia Status de correção.
   Se o VIS tiver patches disponíveis, o. **Patch de programação** o botão é exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Patch de programação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como programar um patch, consulte Programar patches com Resposta a vulnerabilidades Integração de orquestração de patches HCL BigFix.

e. Como alternativa, digamos que você não tenha as informações de ID do patch, mas você pode verificar o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo em busca de qualquer texto relacionado à sua vulnerabilidade crítica.

f. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**.

g. Localize o registro desejado e clique nele para abri-lo.
No registro em aberto, revise a guia Status de correção para Vis e % Vis corrigidos. Clique nos links relacionados para registros de VI, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

Nota: . Se o VIS associado ao registro não tiver patches mapeados para eles, o **Patch de programação** o botão não está disponível no registro.

h. Clique em **Patch de programação** se você quiser enviar uma solicitação de patch.

Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM

Gerencie patches e implantações de patches para as vulnerabilidades críticas em seus ativos com Resposta a vulnerabilidades integração com Microsoft System Center Configuration Manager (SCCM).

Orquestração de patches com Resposta a vulnerabilidades

Orquestração de patches com Resposta a vulnerabilidades usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidades. Os dados de detecção do scanner correspondem os ativos em seu ambiente às vulnerabilidades e às atualizações de patch que podem corrigi-las. Você envia solicitações de patch para aprovação, agenda atualizações de patch para resolver itens vulneráveis e monitora o andamento da correção, tudo a partir de ServiceNow AI Platform® instância.

Resposta a vulnerabilidades orquestração de patches com Microsoft SCCM

Quando a Orquestração de patch de resposta a vulnerabilidades com Microsoft A aplicação SCCM é usada com ServiceNow® Solução de gestão de vulnerabilidade, Orquestração de patch, e. Resposta a vulnerabilidades gerentes de vulnerabilidades e analistas podem executar as seguintes tarefas:

- Veja mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore dados de vulnerabilidades e soluções, bem como o andamento da correção de vulnerabilidades de registros no Resposta a vulnerabilidades Espaços de trabalho.

Os especialistas DE TI e os responsáveis pela correção podem executar as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Implantar patches compatíveis com Microsoft Produto SCCM para seu Windows, CentOS, macOS, Oracle e outros ativos em intervalos regulares e programados durante folga para evitar conflitos com o trabalho.
- Identifique ativos não corrigidos com vulnerabilidades ou ativos que ou não foram atualizados com êxito por patches programados de dados de detecção importados de scanners de terceiros.
- Programe patches disponíveis no Espaço de correção de TI ou na IU clássica para ativos vulneráveis e não corrigidos da atualização de patch, tarefa de correção e registros de itens descobertos.

Termos-chave no Resposta a vulnerabilidades e. Microsoft Aplicações SCCM

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu Configuration Management Database (CMDB). Microsoft ICs e dispositivos de chamadas do SCCM.

Coleções e coleções de dispositivos

Terminologia usada no Microsoft Produto SCCM que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Uma conta distinta de Microsoft Aplicação SCCM. Cada conta de usuário pode ser uma instância no Microsoft Aplicação SCCM. Este termo também se refere a um endereço da web exclusivo e seguro para um ServiceNow AI Platform instância.

Integração

Uma integração é um trabalho agendado no ServiceNow AI Platform que recupera informações de uma origem de terceiros, como a integração com Microsoft Máquinas SCCM.

Solução

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

Patches

Atualizações de software que corrigem vulnerabilidades. Em Microsoft Aplicação SCCM, patches são chamados, patches. Por exemplo, Microsoft O SCCM tem patches para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que se destinam a corrigir vulnerabilidades específicas. Depois de implantados, os patches são mapeados para os itens vulneráveis relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção ou anterior à v15.0 de Resposta a vulnerabilidades, grupos de vulnerabilidades

Listas de itens vulneráveis no Resposta a vulnerabilidades aplicação de ações necessárias para corrigir vulnerabilidades.

Implantação

A implantação para fins desta integração se refere a quando você aplica, inicia ou agenda um patch em uma máquina. Você pode implantar os patches de que você baixou Microsoft SCCM em seu ServiceNow AI Platform navegando até itens descobertos, patches ou tarefas de correção de registros individuais em Resposta a vulnerabilidades. Você pode implantar patches com trabalhos agendados em máquinas individuais ou em grupos de computadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Implantação no ServiceNow AI Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em todo o seu ambiente. Por exemplo, você pode ter várias implantações do Microsoft Integração de vulnerabilidades do SCCM em seu ambiente.

Solução de gestão de vulnerabilidade e o. Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM

. Solução de gestão de vulnerabilidade a aplicação é um ServiceNow AI Platform aplicação que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrigem. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, o Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidades E a Orquestração de patch de resposta a vulnerabilidades com Microsoft As aplicações SCCM trabalham juntas para acumular patches preferenciais da solução para a vulnerabilidade e para o item vulnerável para ajudar você a corrigir e fechar vulnerabilidades em seu ambiente. . Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidades e Resposta a vulnerabilidades Orquestração de patches Microsoft Todos os aplicativos de integração do SCCM estão disponíveis no ServiceNow® Store.

Funções necessárias de ServiceNow AI Platform

As tarefas de instalação, configuração e correção de integração exigem as seguintes funções no ServiceNow AI Platform instância.

administrador

Usuários com esta função obtêm direitos para aplicações no ServiceNow Store e os baixa para ServiceNow AI Platform instâncias.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações no ServiceNow AI Platform e conclui a configuração do Resposta a vulnerabilidades aplicação. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_sccm.configure_integration

Usuários com esta função configuram o. Microsoft Aplicação de integração de Orquestração de patch do SCCM. Esta função contém a função granular sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Usuários com esta função podem exibir (somente leitura) os#registros doResposta a vulnerabilidades e o. Microsoft Integração da Orquestração de patch do SCCM e dados de orquestração de patches.

sn_vul_patch_orch.configure_patch

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir informações de patch (somente leitura).

Aprovadores

Atribua usos aos grupos de aprovadores de aprovador de nível 1 e de aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

Regras de pesquisa de IC

Quando os dados são importados do Microsoft Aplicação SCCM, o. Resposta a vulnerabilidades a aplicação pesquisa automaticamente correspondências no Configuration Management Database (CMDB) Usando dados de ID do recurso. As regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (VI) quando os VIS são criados. As regras de pesquisa de IC a seguir são enviadas com o sistema de base e são usadas para identificar ICs (ativos) e adicioná-los aos itens descobertos.

Esta regra de pesquisa depende dos dados trazidos pelo Conector do Service Graph com o SCCM. Você deve instalar e executar a integração do CMDB antes de executar as integrações do SCCM. Se você tiver várias instalações do servidor SCCM, poderá configurar o alias de conexão do Conector do Service Graph na página de configuração da Orquestração de patches do SCCM.

MID Server

Orquestração de patch de resposta a vulnerabilidades com Microsoft O SCCM é uma integração no local. Ele requer um autônomo Windows MID Server que não faz parte de um cluster do MID Server. O MID Server deve executar scripts em máquinas remotas da sua instância para importar dados do servidor SCCM. As APIs para esta integração são chamadas usando MID Servers que você configurou em seu ServiceNow AI Platform instância. Prepare-se para Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.

Integrações e dependências da Orquestração de patch de resposta a vulnerabilidades com o. Microsoft Aplicação SCCM

Os seguintes produtos e aplicações de dependência são necessários para a Orquestração de patch de resposta a vulnerabilidades com Microsoft Integração do System Center Configuration Manager (SCCM). Essas aplicações estão disponíveis no ServiceNow® Store

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

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços de trabalho e na IU clássica em Resposta a vulnerabilidades as seguintes aplicações são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre compatibilidade de versões com as aplicações e versões de família necessárias, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão artigo na Base de conhecimento HI.

Aplicação e versão de lançamento
Resposta a vulnerabilidades
Solução de gestão de vulnerabilidade
Aplicação de Orquestração de patch de resposta a vulnerabilidades
Orquestração de patch de resposta a vulnerabilidades com a aplicação Microsoft SCCM

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação e versão de lançamento
Security Support Common
Orquestração do suporte de segurança
Conector do Service Graph com SCCM

Resposta a vulnerabilidades tabelas da aplicação de orquestração de patches

. Resposta a vulnerabilidades A aplicação de Orquestração de patches contém as seguintes tabelas:

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização do dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Orquestração de patch de resposta a vulnerabilidades com Microsoft Integrações do SCCM

As integrações desenvolvidas por ServiceNow® a engenharia compõe a implantação da solução orquestrada com o. Microsoft Produto SCCM. As integrações a seguir estão incluídas com o aplicativo Microsoft SCCM Patch Orchestration Integration que você baixa do ServiceNow® Store.

Depois de instalar a aplicação de integração no seu ServiceNow AI Platform para exibir essas integrações, navegue até **Integrações** > **Integração de Orquestração de Patch do SCCM** > **Integrações**. . Resposta a vulnerabilidades a aplicação processa dados em intervalos de tempo programados importados por essas integrações com Microsoft Endpoints do SCCM.

Integração	Descrição
Microsoft Integração da coleção do SCCM	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução de integração encadeada. • Recupera as coleções de dispositivos das Coleções do SCCM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Microsoft Integração da coleção de dispositivos SCCM	• Quando programada, esta integração é acionada pela conclusão da Integração da coleção do SCCM. Você também pode executá-lo sob demanda. • Esta integração busca os dispositivos em cada coleção. Esta integração cria registros na tabela Itens descobertos e na tabela Coleção de dispositivos.
Microsoft Integração de atualização de patch do SCCM	• Quando programada, esta integração é acionada pela conclusão da Integração da coleção de dispositivos SCCM. Você também pode executá-lo sob demanda. • Recupera informações do servidor SCCM sobre os patches instalados ou ausentes em dispositivos (ativos).
Microsoft Integração de implantações do SCCM	• Quando programada, esta integração é acionada pela conclusão da integração de atualização de patch. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe DE TI no servidor SCCM.

Prepare-se para Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM

Prepare-se para a integração executando as tarefas de configuração a seguir.

Antes de Iniciar

Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Por Que e Quando Desempenhar Esta Tarefa

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração.

Procedimento

1. Para uma instalação e configuração suaves da Orquestração de patch de resposta a vulnerabilidades com Microsoft Aplicação SCCM, siga a check-list fornecida abaixo.
2. Você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar informações relacionadas a vulnerabilidades e patches para seu ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
☐	(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,1 de Resposta a vulnerabilidades ou posterior.
☐	Se ainda não estiver instalado, obtenha direitos e instale um aplicativo de scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Resposta a vulnerabilidades para obter mais informações sobre scanners de terceiros compatíveis com Resposta a vulnerabilidades. Consulte .
☐	Se ainda não estiver instalado, obtenha direitos e baixe a Orquestração de patch de resposta a vulnerabilidades com Microsoft Aplicação SCCM para seu ServiceNow AI Platform® instância. Consulte .
☐	Obter Microsoft Credenciais do SCCM. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seu Microsoft para que você tenha acesso a eles.
☐	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **administrador** O administrador do sistema obtém direitos, baixa e instala o. Microsoft Aplicação de Orquestração de patches do SCCM e os outros aplicativos necessários para a integração. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Resposta a vulnerabilidades Ou no módulo Administração de usuários. **sn_vul.vulnerability_admin**

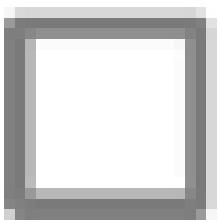
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Uma vez atribuído, o administrador de vulnerabilidades conclui a configuração do Microsoft Integrações do SCCM e outras aplicações de terceiros. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Resposta a vulnerabilidades Orquestração de patches e aplicações de Gestão de soluções de vulnerabilidade. **sn_vul_sccm.configure_integration** Usuários com esta função configuram o. Microsoft Aplicação de integração de Orquestração de patch do SCCM. Esta função contém as funções granulares sn_vul_sccm.read_integration e connection_admin que permitem que o usuário se conecte ao console do SCCM e configure as instâncias de integração no seu ServiceNow AI Platform. **sn_vul_sccm.read_integration** Usuários com esta função podem exibir (somente leitura) os#registros doResposta a vulnerabilidades e o. Microsoft Integração da Orquestração de patch do SCCM e dados de orquestração de patches. **sn_vul_patch_orch.configure_patch** Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário dos registros de item vulnerável e Atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores forem atribuídos. **sn_vul_patch_orch.read_patch** Usuários com esta função podem exibir (somente leitura) informações de patch em registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades. **Aprovadores** Os usuários atribuídos ao aprovador de nível 1 e, opcionalmente, aprovador de nível 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de aprovadores de nível 1 para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Configure a Orquestração de patch de resposta a vulnerabilidades com Microsoft Integração do SCCM. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o Resposta a vulnerabilidades o grupo está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais para funções de especialista em correção e analista de vulnerabilidades e adicionar usuários com o módulo Administração de usuários em sua instância. Consulte Crie um grupo de usuários .
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ○ Orquestração de patch de resposta a vulnerabilidades com Microsoft O SCCM é uma integração no local que requer que você use um autônomo Windows MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . ○ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

Instale o. Resposta a vulnerabilidades Orquestração de patches com Microsoft Aplicação SCCM

Baixe a aplicação do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Prepare-se para Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. Administrador de vulnerabilidades (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar o. Resposta a vulnerabilidades Orquestração de patches Microsoft SCCM e outros aplicativos depois que eles são instalados.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter o direito para prosseguir Ativar um ServiceNow Store aplicação.

Procedimento

1. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
2. Localize **Orquestração de patch de resposta a vulnerabilidades com o Microsoft SCCM** aplicação e clique **Instalar** .

   Esta ação instala a aplicação que você baixou do ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Tudo** > **Integração de Orquestração de Patch do Microsoft SCCM** > **Configuração** para continuar com a configuração.

Configure a Orquestração de patch de resposta a vulnerabilidades com Microsoft Integração do SCCM

Depois de instalar a aplicação, configure-a com as informações da sua conta e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_sccm.configure_integration

Procedimento

1. Navegar até **Tudo** > **Integração de Orquestração de Patch do Microsoft SCCM** > **Configuração**.
2. Preencha os campos com seu Microsoft Informações e credenciais do SCCM.

Campo	Descrição
Instância de integração	O nome do Microsoft Conta de instância do SCCM que você deseja usar, por exemplo, Integração do Microsoft SCCM Patch Management .
Nome do host	Insira o URL do Microsoft Host do SCCM.
Nome do usuário	Insira seu Microsoft Nome de usuário da conta SCCM.
Senha	Insira seu Microsoft Senha da conta do SCCM.
MID Server	Insira o nome do MID Server autônomo na lista que você deseja usar. Consulte Prepare-se para Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM Para obter mais informações sobre MID Servers e configurar tarefas em seu ServiceNow AI Platform®.

3. Clique em Salvar e testar credenciais.
   O status da sua conexão entre Microsoft SCCM e seu ServiceNow AI Platform® A instância#é exibida no campo Status de validação. Se você não vir um teste bem-sucedido, siga as instruções.
4. **Opcional:** Domain Separation é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:
   a. Navegar até **Tudo** > **Integração de Orquestração de Patch do Microsoft SCCM Instâncias de integração** .
   b. Verificar o escopo da aplicação, Orquestração de patch de resposta a vulnerabilidades com o Microsoft SCCM É exibido no campo Escopo da aplicação.
   c. Clique em **Nova**.
   d. Preencha o formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Orquestração de patch de resposta a vulnerabilidades com Microsoft SCCM
Integração	[Somente leitura] Microsoft A Gestão de patches do SCCM é o padrão.
Ativo	O padrão é Ativado. Se estiver desmarcada, a instância não estará ativa.

e. Clique em **Enviar**.
Sua nova instância de integração é exibida na lista Instâncias de integração.

f. Repita as etapas de 1-3 a 5 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.
Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] É ativado para que, quando as implantações de patch são programadas, elas sejam enviadas para revisão e aprovação aos usuários atribuídos ao grupo de aprovação de atualização de patch de nível 1.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative [**sn_vul_patch_orch.patch_approval_required** propriedade]. Você pode preferir deixar as aprovações ativadas para que os patches agendados não entrem em conflito com o horário normal de trabalho.

Nota: Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **Tudo** > **sys.properties.list**.

b. Localizar **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `falso` .

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, será necessário atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.

b. . **Implantar aprovação de atualização de patch** A regra de aprovação não é exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch** .

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Aprovação de atualização de patch de configuração padrão** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch** .

f. Adicione usuários neste grupo.

Os usuários atribuídos a este grupo aprovam solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em **Atualização** para salvar suas mudanças.

8. **Opcional:** Você pode configurar aprovações multinível para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

a. Com o registro Aprovação de atualização de patch de configuração padrão exibido, clique em **Novo** .

b. Preencha os campos.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 - Aprovação de atualização de patch** .
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções especificadas.
Usuários	Edite os usuários listados nos grupos.

c. Clique em **Enviar** para salvar suas edições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de dados de patch e acúmulo de dados de patch para Resposta a vulnerabilidades Integração da Orquestração de patches com Microsoft SCCM

Dados de patch e dados de acúmulo de patch, bem como informações de vulnerabilidade e status de correção de suas vulnerabilidades são exibidos em registros em sua instância.

Exibição de dados de patch no Resposta a vulnerabilidades Espaços de trabalho

Funções necessárias:

- função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades

No Espaço de correção de TI, você pode exibir os patches:

- Na exibição Página inicial, em que você pode clicar em cartões de pontuação para exibir registros de soluções preferenciais em VIS, ICs vulneráveis e patches preferenciais em VIS.
- Na exibição de lista, em que você pode exibir todos os registros de atualização de patch (VPUs) dos links de patches e os itens vulneráveis (Vits) atribuídos a você que têm patches.

Você pode programar patches a partir dos seguintes registros:

- Da Atualização de Patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Espaço do Gerenciador de vulnerabilidades, você pode exibir patches:

- Na exibição Página inicial nos tópicos de exibição, onde você pode exibir patches preferenciais e potenciais, datas programadas de patch e, se o patch foi baixado, todos no **Itens vulneráveis** guia.
- Na Exibição de lista sobre esforços de correção, em que você pode exibir dados de patch em registros de VI do **Itens vulneráveis** guia.

Na exibição de ambiente clássica, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Patches**.

Registros de atualização de patch nos Espaços de VR e na exibição de ambiente clássica

Os dados do patch e os dados e status do rollup de patch são exibidos nos registros em sua instância. Os registros de patch estão incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exibir registros de Patch (VPU) em Resposta a vulnerabilidades Exibição de lista no Espaço de correção de TI. Registros de atualização de patch no ambiente clássico e Resposta a vulnerabilidades Os espaços de trabalho incluem os seguintes dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Dados e informações da solução de vulnerabilidade de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch. Além disso, ele também inclui e todos os dispositivos com atualizações ausentes.
- Status de correção que inclui % de VIS corrigidos e o total de VIS que têm um patch como patch preferencial.
- Dispositivos associados, Itens vulneráveis, Implantações de patch e Solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros no Resposta a vulnerabilidades Espaços de trabalho.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Acúmulo de estado em registros de item vulnerável

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e rollup de estado para orquestração de patches em Resposta a vulnerabilidades.

Registros que acumulam contagens de VI ativas

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado seleciona somente as mudanças na contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados nos seguintes registros em Resposta a vulnerabilidades:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Dados de patch com Resposta a vulnerabilidades

Os painéis de Gestão de vulnerabilidades (PA) e CISO estão incluídos com uma assinatura do Performance Analytics para Resposta a vulnerabilidades aplicação. Se você tiver uma assinatura para Performance Analytics, Mas não tem uma integração de orquestração de patch instalada, a guia Correção é exibida no painel do CISO, mas não é preenchida com dados.

Para o painel de Gestão de vulnerabilidades (PA), navegue até **Tudo** > **Resposta a vulnerabilidades** > **Visão geral**. Clique em **Correção** E role até a parte inferior da página para exibir os dados de Atualizações de patch: Patches programados e não programados, patches que não têm datas de destino e contagens semanais.

Para o Painel do CISO, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura de patch: Criticidade, patches programados e não programados e patches sem datas de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre Resposta a vulnerabilidades painéis, consulte Usando o padrão Resposta a vulnerabilidades painéis, Orquestração de patches com Resposta a vulnerabilidades Espaços de trabalho e Exibição de dados de orquestração de patches no Resposta a vulnerabilidades painéis.

Programar patches com Microsoft Integração do SCCM com Resposta a vulnerabilidades

Programe patches dos registros de tarefa de correção e Atualização de patch no Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform instância.

Antes de Iniciar

A partir da versão 16,1, você pode programar patches do Resposta a vulnerabilidades Ou do ambiente clássico.

Funções necessárias:

- função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades

Procedimento

1. Na Vulnerabilidade Resposta a vulnerabilidades Espaços de trabalho, como um usuário com a função sn_vul.remediation_owner, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Na página inicial, clique em **Patch preferencial no VIS** .
   A lista de registros de Atualização de patch para o VIS com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço, clique em **Patches** > **Tudo** E localize um registro de Atualização de patch.
   O registro de Atualização de patch é exibido. Você pode preferir revisar os dados antes de programar um patch, porque pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos no Espaço de correção de TI e o que você pode fazer.

Tarefa	Descrição
Clique em um link de Itens relacionados	○ Visão geral - Exibir detalhes como o número do registro de atualização do patch, os IDs do artigo e do boletim, a data da versão e a categoria da atualização, o nome do site do patch, classificação de risco, pontuação de risco, descrição, solução (se fornecida), e status de correção. ○ Dispositivos associados - A lista de itens de configuração afetados pelo patch e pelo status. ○ Itens vulneráveis - A lista de itens vulneráveis associados à vulnerabilidade e ao patch. ○ Implantações de patch - Os nomes e as informações relacionadas às implanta–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	ções deste patch em ativos ou grupos de ativos deste patch. ○ Solicitações de patch - Uma lista de solicitações de patch já enviadas para este patch.
Clique em um link para abrir um registro	Nas listas exibidas em registros abertos nos links de Itens relacionados, exiba mais detalhes, incluindo mensagens sobre metas perdidas. Uma vez abertos, os registros permanecem abertos como guias até que você os feche.
Programar patch	Quando você estiver pronto para programar um patch ou enviar uma solicitação, clique em **Patch de programação** . Na caixa de diálogo exibida, preencha os campos. Consulte as etapas abaixo para obter mais detalhes.
Adicione uma anotação de trabalho ou anexe um arquivo	Na extrema direita da tela, clique em **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.

6. Clique em **Patch de programação** .
7. Na caixa de diálogo, preencha os campos.

Campo	Descrição
Etapa 1 Selecione Destino	
Coleção	Escolha uma coleção (grupo de ativos) na lista para continuar. Estas são as coleções importadas do SCCM.
Etapa 2 Programação	
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda você a rastrear suas atualizações.
Tipo de implantação	Escolha uma opção na lista. ○ Obrigatório - Este patch é uma atualização obrigatória. ○ Disponível - Este patch não é necessário, mas está disponível para implantação.
Hora do vencimento	Defina o prazo. Este valor indica o último dia em que o patch pode ser instalado.
Horário disponível	Defina o valor da hora em que o patch se torna disponível para implantação pela primeira vez.

Tradução automática

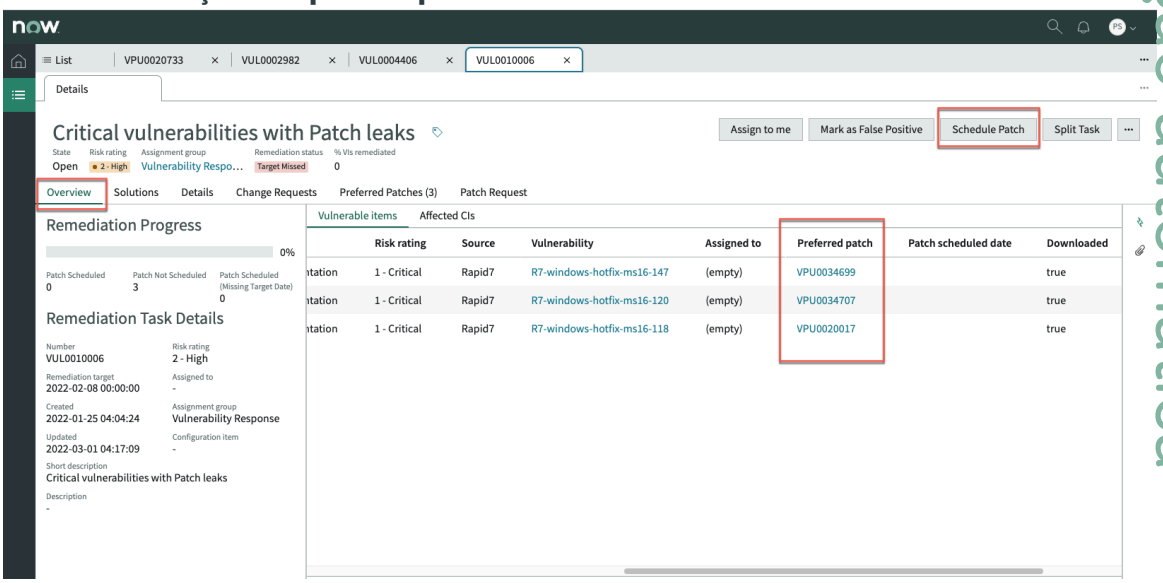
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Permitir reinicialização	O padrão é Desativado. Ative (selecione) esta opção para instruir as máquinas no grupo a reiniciar automaticamente após a conclusão do patch com sucesso.
Descrição	Adicione mais texto para Sobre o patch. Essas informações são exibidas no campo Descrição do registro de Atualização de patch.

8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas de **Solicitações de exceção** > **Minhas solicitações** Na exibição de lista.
9. Como alternativa, você pode programar patches de tarefas de correção (RT) atribuídas a você ou ao seu grupo.

   Nota: A opção de programar um patch a partir de um registro de tarefa de correção estará disponível somente se houver patches mapeados para (associados a) o VIS na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de registros de tarefa de correção com a guia Visão geral selecionada.

Tarefa de correção com patches preferenciais



10. Clique em **Patch de programação** No registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. **Opcional:** Você pode programar patches para as etapas anteriormente no ambiente clássico.
    Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Patches** > **Tudo**.

    b. Na lista exibida, localize um registro de Atualização de patch.

    c. Para tarefas de correção, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** e localize um registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rastreie o status de correção na guia Status de correção. Na parte inferior do registro, os dados do patch são exibidos nos links relacionados.

d. Clique em **Patch de programação** e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda você a rastrear suas atualizações.
Descrição	Adicione mais texto para Sobre o patch. Essas informações são exibidas no campo Descrição do registro de Atualização de patch.
Tipo de implantação	Escolha uma opção na lista. ▪ Obrigatório - Este patch é uma atualização obrigatória. ▪ Disponível - Este patch não é necessário, mas está disponível para implantação.
Coleção	Escolha uma coleção (grupo de ativos) na lista para continuar. Esses grupos são as coleções de ativos importadas do SCCM.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Tempo disponível	Defina o valor da hora em que o patch se torna disponível para implantação pela primeira vez.
Vencimento	Defina o prazo. Este valor indica o último dia em que o patch pode ser instalado.

e. Clique em **Implantar**.

Mensagens REST para Resposta a vulnerabilidades Orquestração de patches com Microsoft SCCM

Orquestração de patch de resposta a vulnerabilidades com Microsoft O SCCM usa as classes SCCM Windows Management Instrumentation (WMI) para fazer chamadas para a API do Servidor SCCM.

Visão geral das mensagens REST

. Provedor de SMS Fornece à API um acesso de interoperabilidade por HTTPS, chamado de serviço de administração. O serviço de administração é uma API REST (Representational State Transfer, transferência de estado representacional) baseada no protocolo Open Data (OData) v4.

Consulte O que é o serviço de administração no Configuration Manager para obter mais informações sobre o serviço de administração, use com esta integração.

Como a autenticação necessária usa o protocolo NTLM do Windows New Technology LAN Manager, as chamadas para as APIs são feitas por meio do MID Server usando scripts PowerShell.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Integração do SCCM

Você pode usar a mensagem REST para Microsoft Integração do SCCM da qual recuperar informações Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas Microsoft SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Nomes das classes WMI:

- SMS_Collection
- DeploymentSummary

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos baseados no usuário	Indica o endpoint do Console do SCCM

Microsoft Patch de implantação do SCCM

Você pode usar a mensagem REST para a integração do Microsoft SCCM para programar patches do seu ServiceNow AI Platform® para Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch PÓS-implantação	Programa o patch para o console do SCCM em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos baseados no usuário	Indica o endpoint do Console do SCCM.
título	Valores dinâmicos baseados no usuário	Título da implantação.
settings_tag	Configurações nomeadas por marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o SCCM durante o agendamento do patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site em que o Patch está presente.
Patch_id	Valor da atualização do patch	ID do patch.

Transformação de dados para a Orquestração de patches com Microsoft Integração do SCCM

Os dados são recuperados da Orquestração de patches com Microsoft Integração do SCCM, processada por meio de um conjunto de fontes de dados e transformada em ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação da coleção do SCCM

Os dados das coleções importadas são carregados na tabela Importação de coleção do SCCM [sn_vul_sccm_collection_import]. As Coleções do SCCM (mapa de transformação) são usadas para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação da coleção do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Tudo** > **Conjuntos para importação do sistema** > **Mapas de transformação** E localize Transformação de coleção do SCCM. A tabela a seguir lista os campos do mapa de transformação por integração.

Campo de origem	Campo de destino	Descrição
u_collectionid	source_id	ID exclusivo da coleção.
u_name	nome	Nome da coleção.
u_membercount	device_count	Número de dispositivos nesta coleção.
[script]	integration_instance	Nome da instância da qual o patch é importado.

Tempo do script do mapa de transformação de importação da coleção do SCCM

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de atualização de patch do SCCM

Os dados dos patches importados são carregados na tabela Importação de atualização de patch do SCCM [sn_vul_sccm_patch_update_import].

A transformação de atualização de patch do SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de atualização de patch do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Tudo** > **Conjuntos para importação do sistema** > **Mapas de transformação** E localize a transformação de atualização de patch do SCCM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação de atualização de patch do SCCM

Campo de origem	Campo de destino	Descrição
[Script]	urls	URLs do patch.
u_nummissing	num_missing	Número de dispositivos sem este patch.
[Script]	date_release	Data da versão do patch.
u_bulletinid	bulletin_id	ID do boletim do patch.
u_numtotal	num_total	Número total de dispositivos.
u_localizeddescription	descrição	Descrição do patch.
[Script]	is_highest_suplantdence	É o patch com a substituição mais alta.
u_numnotaplicável	num_not_applicable	Número de dispositivos não aplicáveis a este patch.
u_iscontentprovisionado	_baixado	Se o patch for baixado para o Servidor SCCM.
u_numunknown	num_unknown	Número total de dispositivos desconhecidos.
u_articleid	article_id	ID do artigo do patch.
u_localizeddisplayname	título	Título do patch.
u_ci_id	source_id	ID exclusivo do patch no SCCM.
u_numpresente	num_present	Número de dispositivos em que o patch está instalado.
[Script]	integration_instance	Nome da instância da qual o patch é importado.
[Script]	sn_vul_solution	Solução baseada no ID de origem.
[Script]	last_modified	Data da última modificação do patch.
u_severity	source_severity	Gravidade do patch.

Tempo do script do mapa de transformação de importação de atualização de patch do SCCM

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo do script do mapa de transformação de importação de atualização de patch do SCCM

Script	Descrição
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de atualização de patch do dispositivo SCCM

Os dados dos patches relevantes importados nos dispositivos são carregados na tabela Importação de atualização de patch do dispositivo SCCM [sn_vul_sccm_device_patch_import].

A transformação de atualização de patch do dispositivo SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de atualização de patch do dispositivo SCCM são processados.

Para acessar este mapa de transformação, navegue até **Tudo** > **Conjuntos para importação do sistema** > **Mapas de transformação** E localize a transformação Atualização de patch do dispositivo SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação de atualização de patch do dispositivo SCCM

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	Script usado para criar e atualizar ICs com base em regras de pesquisa de IC e patches, bem como o relacionamento entre eles. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de coleção de dispositivos do SCCM

Os dados das coleções de dispositivos importadas são carregados na tabela Importação de coleção de dispositivos SCCM [sn_vul_sccm_device_collection_import].

A transformação de importação da coleção de dispositivos SCCM é usada para transformar as informações importadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação da coleção de dispositivos SCCM são processados.

Para acessar este mapa de transformação, navegue até **Tudo** > **Conjuntos para importação do sistema** > **Mapas de transformação** E localize a transformação da coleção de dispositivos SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação de importação da coleção de dispositivos

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para criar e atualizar ICs com base nas regras e coleções de pesquisa de IC, bem como no relacionamento entre elas. Com base nos resultados, este script modifica valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Campos do mapa de transformação de importação da coleção de dispositivos SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.
U_name	nome	Nome da ação
[Script]	SN_vul_sccm_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	SN_vul_patch_orch_update	Referência do patch
U_apply_count	Count_success	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Deployment_time	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Source_created	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de implantação do SCCM

Os dados das implantações importadas são carregados na tabela Importação de implantação do SCCM [sn_vul_sccm_deployment_import].

A transformação de importação de implantação do SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de implantação do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Tudo** > **Conjuntos para importação do sistema** > **Mapas de transformação** E localize a Transformação de implantação do SCCM.

Campos do mapa de transformação de implantação do SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma implantação.
u_name	nome	Nome da implantação.
[Script]	prazo	Hora do prazo para a implantação.
u_numberemandamento	count_progress	Contagem de dispositivos em andamento para a implantação.
[Script]	deployment_time	Hora de início da implantação.
[Script]	integration_instance	Nome da instância da qual a implantação é importada.
[Script]	source_created	Hora de criação da implantação.
[Script]	sn_vul_patch_orch_update	Referência do patch
[Script]	sn_vul_patch_orch_collection	Referência do item descoberto no qual o patch está implantado.
u_softwarename	nome	Nome da implantação.
u_numberoutro	count_other	Outra contagem de dispositivos para a implantação.
u_numberdesconhecido	count_unknown	Contagem de estado desconhecida de dispositivos para a implantação.
u_deploymentid	source_id	Identificador exclusivo da implantação.
u_numbersucesso	count_success	Contagem de sucesso de dispositivos para a implantação.
u_numbererrs	count_error	Contagem de erros de dispositivos para a implantação.
u_numbertargeted	count_total	Contagem total de dispositivos para a implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo do script do mapa de transformação de importação da implantação do SCCM

Script	Descrição
OnStart (quando um conjunto de importação cria transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes de um conjunto de importação concluir a transformação.	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
OnComplete (quando um conjunto de importação conclui a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Fluxo de trabalho de exemplo para Resposta a vulnerabilidades Integração da Orquestração de patches com Microsoft SCCM

Um exemplo de como a orquestração de patches funciona com Microsoft SCCM.

Antes de Iniciar

Digamos, por exemplo, que todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Espaço do Gerenciador de vulnerabilidades.
- sn_vul.remediation_owner para exibir o espaço do responsável pela correção de TI.
- função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços de correção DE TI e Gerenciador de vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente ou analista de vulnerabilidades que trabalha no Espaço do gerenciador de vulnerabilidades, você pode considerar criar tópicos de observação ou editar tópicos de observação existentes para ajudar a capturar VIS importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patch. Use estes exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Crie um tópico de observação no Espaço do gerente de vulnerabilidade para obter mais informações sobre como configurar o tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de tópicos de observação para orquestração de patches no Espaço do Gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	A classificação de risco é 1 - crítica E. O motivo é Patch não programado
Vulnerabilidades críticas com patches programados (ANS ausente)	Patch programado (data de destino ausente)
Vulnerabilidades críticas com patches agendados	A classificação de risco é 1 - crítica E. A data programada do patch não está vazia E. O motivo é Patch programado

- Como gerente ou analista de vulnerabilidades, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Nos registros de VI e tarefas de correção, você pode detalhar a guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto SCCM.
- Como analista de vulnerabilidades ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) a partir de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

- Você pode programar o patch a partir de um registro de Atualização de patch (nº VPU).
- Se os itens vulneráveis (VI) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique em **Tarefas de correção atribuídas** cartão de pontuação para exibir os registros.

   Para este exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (nº VUL) em busca de qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você pode saber que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para capturar VIS (VIT nº) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar o VIS, os patches preferenciais e ver se você ou algum de seu grupo já enviou solicitações de patch para aprovação.
3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . Se o VIS associado ao registro não tiver patches mapeados para eles, o **Patch de programação** o botão não está disponível no registro.

4. Clique em **Patch de programação** e preencha os campos na caixa de diálogo.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com Microsoft Integração do SCCM com Resposta a vulnerabilidades.
5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros.
   Neste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos VIS com esta vulnerabilidade está atribuído a você ou aos seus grupos. Nos registros de Atualização de patch, você pode enviar solicitações de patch. Nos registros de VI, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.
6. Se você não tiver acesso aos espaços ou preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Resposta a vulnerabilidades** > **Patches** > **Tudo**.

   b. Localize o registro de Atualização de patch desejado.
   Você pode preferir filtrar os registros com Crítico Pontuações de risco.

   c. Revise os campos VIS associados e % vis corrigidos na guia Status de correção.
   Se o VIS tiver patches disponíveis, o. **Patch de programação** o botão é exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Patch de programação** .
   Para obter mais informações sobre como programar um patch, consulte Programar patches com Microsoft Integração do SCCM com Resposta a vulnerabilidades.

   e. Como alternativa, digamos que você não tenha as informações de ID do patch, mas você pode verificar o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo em busca de qualquer texto relacionado à sua vulnerabilidade crítica.

   f. Navegar até **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**.

   g. Localize o registro desejado e clique nele para abri-lo.
   No registro em aberto, revise a guia Status de correção para Vis e % Vis corrigidos. Clique nos links relacionados para registros de VI, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

   Nota: . Se o VIS associado ao registro não tiver patches mapeados para eles, o **Patch de programação** o botão não está disponível no registro.

   h. Clique em **Patch de programação** se você quiser enviar uma solicitação de patch.

Noções básicas do Qualys Vulnerability Integration

. Qualys os sensores de produto coletam os dados e os enviam automaticamente para o. Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente ao Resposta a vulnerabilidades. Qualys Vulnerability Integration Mapear vulnerabilidades para ICs e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

serviços de negócios para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Configure seu Qualys Vulnerability Integration usando **Vulnerabilidade** > **Administração** > **Assistente de configuração** tornar a recuperação de dados mais flexível e escalonável.

Se você tiver várias implantações do Qualys Cloud Platform, você pode adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados originados de cada implantação são identificados e disponibilizados em uma única instância do Resposta a vulnerabilidades. Qualys Vulnerability Integration Os registros da Base de conhecimento são normalizados em todas as implantações, garantindo que as instâncias da mesma vulnerabilidade em todas as implantações sejam tratadas como a mesma vulnerabilidade.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Nota: . Qualys Vulnerability Integration Cria integrações para Lista de dispositivos, Grupo de ativos, Lista de pesquisa dinâmica e Lista de pesquisa estática, elas não são necessárias para a operação normal.

Versões disponíveis

Versão de lançamento para Zurich	Notas da versão
Qualys Vulnerability Integration v12.7, v12.8	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Componentes instalados

Para obter uma lista atual de funções, trabalhos de integração e tabelas instaladas com a integração, bem como um link para instruções sobre como exibir o que está instalado atualmente em sua instância, consulte Componentes instalados com Qualys Vulnerability Integration.

Integrações primárias e de suporte

Qualys As integrações primárias e de suporte enriquecem os dados de vulnerabilidade em sua instância recuperando dados da Integração de vulnerabilidades da Qualys. Uma série de trabalhos agendados invocam as integrações automaticamente. Você também pode executá-los manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. As integrações primárias e de suporte podem ser modificadas.

. Qualys as integrações são executadas como trabalhos agendados. Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Este valor não deve ser alterado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Não definir um usuário de execução válida resulta em vários anexos de recuperação de dados, geralmente duplicados, nos registros da fonte de dados, sempre que a integração é executada. Vários anexos na fonte de dados aumentam o tempo de processamento, resultando em resultados de transformação inconsistentes.

Os registros CVE, que ainda não estão presentes, são criados como registros NVD e referenciados em entradas de terceiros para Qualys por padrão.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Integrações primárias

Uma integração primária é um ponto de entrada para Qualys Cloud Platform interagindo com Qualys API invocada em uma programação.

Navegue até as integrações primárias **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.

Integrações de suporte

Uma integração de suporte é um processo que não se destina a ser executado em uma programação nem sem invocação por uma integração primária.

Navegue até as integrações de suporte **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações de Suporte**.

Conector do Service Graph para Qualys

A partir da versão 2,2, o Conector do Service Graph para Qualys está disponível no ServiceNow® Store. Para obter mais informações, consulte Conector do Service Graph para Qualys .

Os dados dos campos de fonte de dados da Qualys são importados com a API Ativo global e a Gestão de ativos e a API Marcação.

API de ativo global:

- Uma licença do CSAM é necessária.
- As informações de ativos incluem detalhes como Categoria de hardware e Categoria de SO.

API Gestão de ativos e marcação:

- Não requer uma licença do CSAM
- As informações de ativos não incluem detalhes sobre Categoria de hardware e Categoria de SO.

Para obter mais informações, consulte Conector do Service Graph para Qualys APIs .

.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de identificação e reconciliação para criar novos ICs quando um IC existente não puder ser correspondido a um host importado de um scanner de terceiros. Habilite o plug-in Modelos de classe de IC do CMDB para criar ICs usando as novas classes, caso contrário ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Listas de pesquisa

Listas de pesquisa são usadas em Qualys para criar grupos personalizados de vulnerabilidades. Você pode salvá-los e usá-los para criação de tíquete e personalizar verificações e relatórios de vulnerabilidade. O módulo Listas de pesquisa permite que você baixe dados da lista de pesquisa da Qualys para sua instância de forma programada.

As listas de pesquisa são extraídas de Qualys usando o. Importação da lista de pesquisa dinâmica e/ou Importação da lista de pesquisa estática mapas de transformação de dados. Em cada uma dessas transformações, você pode definir cronogramas para executar a importação.

Perfis de opção

Os perfis de opção estão disponíveis com Qualys configurações de verificação. Um perfil de opção é necessário quando você inicia uma verificação do seu ServiceNow AI Platform.

Os perfis de opção são importados do Qualys Produto pela Integração da lista de perfis de opção. Você pode preferir executar a Integração da lista de perfis de opção após uma importação das Integrações de listas de pesquisa, o. Qualys Lista de pesquisa dinâmica e. Qualys Integrações de lista de pesquisa estática para que você possa ver quais listas de pesquisa estão associadas a perfis de opção.

Grupos de ativos

Os grupos de ativos são configurados no Qualys plataforma. Os grupos de ativos identificam quais dispositivos de scanner são usados para verificar endereços IP correspondentes quando uma verificação é iniciada a partir do ServiceNow AI Platform.

Os grupos de ativos que têm dispositivos associados são extraídos de Qualys Pela Integração da lista do grupo de ativos.

Inicie a Integração da lista de soluções depois de importar grupos de ativos para preencher os campos Nome da solução e Status da solução no Qualys Registros de aplicações padrão em seu ServiceNow AI Platform.

Marcadores de host

Todos os marcadores de host são importados como parte do Qualys Integração da lista de hosts. Marcadores de host são usados principalmente para filtragem no Resposta a vulnerabilidades Regras de tarefa de atribuição e correção. Eles são exibidos no formulário Item descoberto.

Nota: . Qualys A integração da Lista de hosts deve ser executada antes de criar regras de tarefa de atribuição ou correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Se for um **San Diego** o marcador é criado e, em seguida, um **SAN DIEGO** O marcador não pode ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. O marcador que foi importado pela primeira vez vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags** . Esta propriedade é definida como verdadeira por padrão. Desativar os marcadores os desativa em todas as instâncias.

Marcadores de host (também chamados de marcadores de ativo) são usados para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos de host. Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host do Qualys para sua instância em uma base programada.

Reabra itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvido" em seu ServiceNow AI Platform As execuções de integração de terceiros são reabertas se forem detectadas durante novas verificações.

Para Qualys Detecções, se o scanner continuar a encontrar os VIS que foram definidos como "Resolvido", mas não foram transferidos para "Encerrado/Corrigido" por verificações subsequentes, esses VIS serão movidos de volta para "Aberto" quando a data da última descoberta for posterior à data de resolução.

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados do Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando seu processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection - Padrão/POST** . Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método POST com os seguintes valores:

- Nome: Gravidades
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tópicos relacionados

Qualys Mensagens REST

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparando para Qualys Vulnerability Integration

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. É essencial que você se prepare para a integração executando esses procedimentos. . Qualys Vulnerability Integration Presume que você esteja familiarizado e execute verificações da Qualys Cloud Platform em seu ambiente.

Nota: Faça as mudanças de configuração necessárias com base em seus requisitos antes de executar as integrações.

Pré-requisitos importantes

Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

Use a filtragem para limitar o número de itens para importação inicial e preparar sua implantação ajustando os filtros nas importações subsequentes.

. Qualys os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Ações a serem executadas

- Determine uma data de início inicial para **Importação da lista de detecção de host** integrações.

  Considere configurar **Hora de início** campo para algumas horas ou dias no passado. Escolha a data da última verificação da Qualys. A data de início pode incluir vulnerabilidades descobertas antes de usar a solução de gestão de vulnerabilidades. Defina a hora de início mais antiga usada para o início do ciclo de digitalização. Portanto, se levar uma semana antes que todos os hosts sejam verificados, defina esse valor como uma semana antes desse horário.

- Adicione usuários às funções de admin, sn_vuln.admin e sn_vul_qualys.admin. Para obter mais informações, consulte, Atribua uma função a um usuário .

- Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

- Se você não usar calculadoras de vulnerabilidade, Desabilite a calculadora de vulnerabilidades padrão se não for usada, além de todos os outros que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
- Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, desabilite as regras de negócio .
- Se você quiser usar um scanner diferente do padrão da Qualys, consulte configurar dispositivos de scanner .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tenha o URL do servidor Qualys e as credenciais de autenticação prontas. As credenciais devem fornecer permissões adequadas para recuperar informações de conhecimento, verificação e detecção para uma assinatura da Qualys.
- Se você planeja usar marcadores de host em Resposta a vulnerabilidades Regras de tarefa de atribuição ou correção, certifique-se de Qualys A integração da Lista de hosts foi executada antes da criação de regras.

Instalar o Qualys Vulnerability Integration

Antes de executar o. Qualys Vulnerability Integration em sua instância, você deve instalar e configurar o. Qualys Vulnerability Integration aplicação. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Função necessária: administrador para baixar e instalar a aplicação

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Obtenha direitos para Qualys Vulnerability Integration e baixe-o para seu ServiceNow AI Platform® instância.	Se a aplicação ainda não tiver sido baixada em sua instância, consulte .
Prepare-se para a integração.	Consulte Preparando para Qualys Vulnerability Integration.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.

   Após alguns momentos, as aplicações que estão disponíveis para instalação em sua instância serão exibidas.

2. Localize Qualys Vulnerability Integration lado a lado e clique **Instalar** .

3. Siga as instruções no Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegue até **Configuração de integração>Integrações do scanner** No Assistente de configuração para continuar com a configuração.
   Para obter mais informações sobre como complementar os prompts fornecidos no Assistente de configuração, consulte Configure o. Qualys Vulnerability Integration Usando o Assistente de configuração.

O que Fazer Depois
Ative os scanners, pois eles estão inativos por padrão no Resposta a vulnerabilidades aplicação. Para obter mais informações sobre como ativar o. Qualys scanners, consulte Ative o. Qualys scanners.

Ative o. Qualys scanners

Você deve ativar os scanners após instalar o. Qualys Vulnerability Integration porque os scanners estão desativados por padrão no Resposta a vulnerabilidades aplicação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Procedimento
1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto do scanner que você deseja ativar e selecione o registro para abri-lo.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. O produto que você ativou é exibido em **Origem** campo em um item vulnerável e registros de tarefa de correção após a próxima importação, e. **Nova verificação** Está disponível como uma ação de IU.

Atualize itens de configuração com o identificador de partição de rede para Qualys Vulnerability Integration

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão, em Resposta a vulnerabilidades Uma maneira de identificar seus ativos é pelo endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (ICs) em seu ambiente podem compartilhar endereços IP, mas têm ids exclusivos de rede e repositório. No entanto, por padrão, esses ativos geralmente são identificados e armazenados como um único IC (IC 1) Durante a pesquisa de endereço IP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_ID	Item de configuração
Qualys Vulnerability Integration Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	REPOSITORY_ID	Item de configuração
Qualys Vulnerability Integration Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para poder identificá-los como ativos distintos. A partir de uma importação de dados nova, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as Integrações Ativos e Vulnerabilidades fixas e abertas para Qualys Vulnerability Integration No Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o Identificador de partição de rede [network_partition_identifier] aos registros de IC existentes de dados importados. ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar seus dados existentes.

A partir da v14.0 de Resposta a vulnerabilidades e v12.1 do Qualys Vulnerability Integration Integração de vulnerabilidades, os modelos de classe de IC do CMDB (1,0.21.) é compatível. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de IRE (Identificação e reconciliação).

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. ICs para o seu existente Qualys Vulnerability Integration os dados são criados ou atualizados para incluir a granularidade do identificador da partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são atualizados com os novos ICs.
Aguarde as importações de dados atualizados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são atualizados para incluir a nova

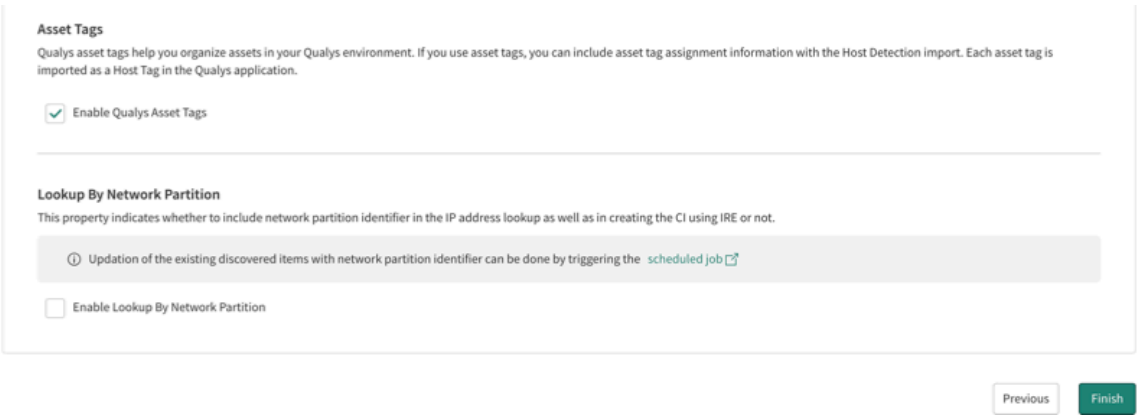
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Editar** a integração necessária.
4. Escolher **Configuração de detecção do host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITÓRIO _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de endereço IP e de IC de endereço IP incompleto incluem o atributo identificador de partição de rede automaticamente para uma importação de dados das Integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Depois de ativar o trabalho agendado e salvar os registros, você também pode atualizar seus itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos agendados sob demanda. Os ICs no item descoberto existente, item vulnerável e registros de detecção são atualizados automaticamente.

Modificações opcionais da Qualys

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração da Qualys.

Você pode redefinir essa data de início no Assistente de configuração ou na integração primária ou modificar as regras de negócios para desabilitá-las durante uma importação inicial.

Desabilite regras de negócios relacionadas a notificações antes da importação inicial de registro

Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desabilitá-las durante a importação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.
2. Pesquisar **Notificações de ic afetado** .
3. Abra a regra de negócio e insira esta condição: `"sn_vul_vulnerable_item"` .
4. Clique em **Atualizar**.
5. Repita este procedimento para as seguintes regras de negócios:
   - Notificações do centro de custos afetado
   - Notificações de grupo afetado
   - Notificações de local afetado

Nota: Após a conclusão da importação de registro inicial, você tem a opção de reativar essas regras de negócios. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Ative o. Qualys Integração de pontuação QVS

Usando o. Qualys Integração de pontuação QVS Você pode preencher automaticamente as pontuações QVS para CVEs para ajudá-lo a avaliar o risco de vulnerabilidade com mais precisão na tabela sn_vul_nvd_entry.LIST.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Integrações da Qualys** > **Integração de pontuação QVS da Qualys**.
2. Selecione **Ativo** caixa de seleção para habilitar a integração.

Nota: Este recurso está inativo por padrão.

Resultado
Quando a integração é executada, ela consulta Qualys Para obter as pontuações QVS mais recentes dos CVEs atualizadas nos últimos 15 dias e preenche o. **Pontuação de vulnerabilidade da Qualys** Coluna na tabela [sn_vul_nvd_entry.LIST].

Nota: Se a pontuação QVS estiver vazia, o CVE não foi atualizado nos últimos 15 dias.

Modifique uma data de início inicial

Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Qualys. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado abaixo.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa
Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique em **Integração do Qualys Host Detection** .
3. Clique em **Detalhes da integração** .
4. Defina **Hora de início** para um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde esse momento sejam detectadas.

   Se você configurou Qualys Usando o Assistente de configuração, o. **Hora de início** o campo é preenchido previamente, inicialmente até três meses antes da data de hoje e, posteriormente, até a data de hoje.

   Nota: Considere definir o valor como um máximo de um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como acione tempos limite de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. **Opcional:** Clique em **Executar agora** para executar imediatamente.

Avançado Qualys configurações e modificações

Configure modificações opcionais avançadas e simplifique alguns dos dados especificamente para Qualys integração. A maioria dessas modificações requer codificação ou avançado ServiceNow ou Qualys Cloud Platform experiência.

Para obter mais dicas para Qualys importações, consulte Dicas de ajuste de desempenho para trabalhos de importação da Qualys artigo de conhecimento na Base de conhecimento HI.

Modifique os valores de mapeamento de prioridade e estado da Qualys para ServiceNow

Modifique os valores de mapeamento de prioridade e estado para seus requisitos.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Esta é uma opção de personalização avançada.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.
2. Pesquisar **Mapear valores da Qualys** e abra-o.
3. Clique em **Avançado** guia.
4. Modifique de acordo com seus requisitos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As modificações mais comuns incluem adicionar novos valores de estado ou revisar criticidade ou prioridade.

5. Clique em **Atualizar**.

Restringir a capacidade de gravar em um registro com base em um grupo de atribuição

Você pode restringir os direitos de gravação/leitura em registros com base na associação a um grupo atribuído. Modifique condições e script com base em requisitos específicos.

Antes de Iniciar

Função necessária: Security_admin (função elevada do administrador)

Nota: Esta ação é executada no Escopo da vulnerabilidade.

Procedimento

1. Navegar até **Tudo** > **Segurança do sistema** > **Controle de Acesso (ACL)**.
2. PESQUISE ACLs que começam com `sn_vul` .
3. Escolha um registro de Controle de acesso, por exemplo, sn_vul_vulnerable_item , **Operação gravar** .
4. Verifique **Avançado** no registro, se necessário, para exibir o. **Função** entradas.
5. Modifique o. **Função** script para seus requisitos.
   Exemplo de script de modificação de acesso por grupo.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Clique em **Atualizar**.

Configurar dispositivos de scanner

Se você estiver iniciando verificações do seu ServiceNow AI Platform® Em vez de diretamente da Qualys, você pode configurar verificações para intervalos de endereços IP.

Antes de Iniciar

Os dados vêm do Qualys integração baseada em Qualys grupos de ativos e seus dispositivos padrão relacionados (scanners).

Se nenhuma solução estiver configurada para os intervalos de endereços IP de destino, a solução definida como padrão para a instância de integração será usada para a verificação.

Função necessária: sn_vul_qualys.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
2. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome do dispositivo	Você será solicitado a preencher este campo ao criar um registro manualmente. Insira o nome do Qualys dispositivo de scanner a ser usado para invocar verificações para itens de configuração correspondentes. Use Externo valor quando você deseja que a verificação seja iniciada com um scanner externo.
ID de dispositivo	Insira o identificador da solução para Qualys dispositivo de scanner a ser usado para invocar verificações para itens de configuração correspondentes. Você será solicitado a preencher este campo ao criar um registro manualmente. Use 0 valor quando você deseja que a verificação seja iniciada com um scanner externo.
Status do dispositivo	Exibe o último status da solução de scanner nos dados retornados pelo Qualys integração. Para registros criados manualmente, o status será atualizado somente se for válido **ID do dispositivo** especificado.
ID de grupo de ativos	Exibe o. Qualys identificador do grupo de ativos que criou este registro. Este campo exibe um valor somente para registros criados pelo Qualys integração.
Nome do grupo de ativos	Exibe o. Qualys nome do grupo de ativos que criou este registro. Este campo exibe um valor somente para registros criados pelo Qualys integração.
Ordem	Insira um valor a ser usado para determinar a prioridade de verificação. Para a solução que tem critérios conflitantes, uma solução com um valor de ordem inferior recebe uma prioridade mais alta.
Criado manualmente	Indica se este registro foi criado manualmente pelo usuário.
Usar grupo de filtros	Marque esta caixa de seleção para especificar um grupo de filtros para encontrar itens de configuração correspondentes para verificação.
Grupo de filtros	Selecione o grupo de filtros que você deseja usar para encontrar itens de configuração correspondentes para verificação. Este campo aparecerá somente se você selecionou **Usar grupo de filtros** .
IPs	Uma lista separada por vírgulas de endereços IP ou intervalos de endereços IP a serem usados por esta solução ao invocar verificações.
Instância de integração	. Qualys instância de integração associada a esta solução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Perfil de opção	Selecione o perfil de opção que você deseja usar para verificações de itens de configuração correspondentes.

3. Clique em **Atualizar**.

Configurar e gerenciar Qualys verificações e verificações de vulnerabilidades

Qualys Verificações de vulnerabilidades podem ser realizadas para encontrar vulnerabilidades de software que afetam seus ICs. Você pode iniciar verificações a partir de um registro de item vulnerável ou criando um registro de verificação diretamente para itens de configuração (ICs) e endereços IP.

Se você verificar Qualys Itens vulneráveis diretamente na tela Itens vulneráveis, você também tem a opção de verificar vários itens vulneráveis ao mesmo tempo.

Se Resposta a incidentes de segurança estiver ativado, você também pode iniciar uma verificação do catálogo de incidentes de segurança, de um registro de incidente de segurança ou de uma solicitação de verificação de segurança.

Verificações enviadas de Qualys itens vulneráveis, o. Catálogo de incidentes de segurança, incidentes de segurança ou solicitações de verificação de segurança são realizadas por padrão Qualys scanner.

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário quando você inicia um Qualys digitalize a partir do ServiceNow AI Platform®.

Configure o iniciado pela ServiceNow Qualys Verificação de IP

. Qualys O scanner incluído com o sistema de base fornece uma integração de linha de base para iniciar verificações com base em endereços IP.

Antes de Iniciar

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário quando você inicia uma verificação da Qualys a partir de ServiceNow AI Platform®.

Função necessária: sn_vul_qualys.admin

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Abra o. Qualys registro.
3. Selecione **Ativo** e. **Padrão** caixas de seleção.

   Selecionando **Ativo** é necessário para usar Qualys scanner a ser verificado Qualys VIS automaticamente. Você também não precisa selecionar **Padrão** para que ele seja executado automaticamente.

   Anterior à v12.0, **Ativo** é necessário para usar o scanner. Se **Padrão** também estiver selecionado, o scanner será usado automaticamente sem precisar ser selecionado durante a varredura.

4. Para o campo Integração de origem, clique no ícone de pesquisa e selecione a opção para **Qualys** , por exemplo, **Qualys Cloud Platform** .
5. Clique em **Atualizar**.
6. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
7. Abra o. **Integração da lista do grupo de ativos da Qualys** .
   a. Marque a caixa de seleção **Ativo**.
   b. Clique em **Executar Agora**.
8. Siga estas etapas para preencher seus dispositivos de scanner.

   Nota: Você pode preferir executar a Integração da lista de perfis de opção após uma importação das Integrações de listas de pesquisa, da Lista de pesquisa dinâmica da Qualys e das Integrações da lista de pesquisa estática da Qualys, para que você possa ver quais listas de pesquisa estão associadas aos perfis de opção.

   a. Abra o. **Integração da lista de perfis de opções da Qualys** .
   b. Marque a caixa de seleção **Ativo**.
   c. Clique em **Executar Agora**.
   d. Siga as etapas listadas em Configurar dispositivos de scanner para configurar seus dispositivos de scanner. Retorne aqui depois de concluir essas etapas para continuar com a configuração.
   e. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
   f. Abra o. **Integração da lista de dispositivos da Qualys** .
   g. Marque a caixa de seleção **Ativo**.
   h. Clique em **Executar Agora**.
   . Qualys os dispositivos do scanner agora estão preenchidos corretamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Noções básicas do Qualys Vulnerability Integration

Verificação múltipla Qualys vulnerabilidades ou itens vulneráveis

Simultaneamente, você pode verificar vários Qualys Vulnerabilidades ou itens vulneráveis que contêm pelo menos um item de configuração (IC) afetado ou um endereço IP preenchido no formulário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Siga um destes procedimentos:
   - Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
   - Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Todos os Itens vulneráveis**.
2. Marque as caixas de seleção dos registros que você deseja verificar.
3. Clique em **Ações nas linhas selecionadas** e clique em **Verificar novamente itens vulneráveis** . Uma mensagem é exibida com um link para a verificação e as anotações de trabalho são atualizadas.
4. Clique no link para ver o andamento ou os resultados da verificação.

Configure o. Qualys verificação automática de tarefas de correção resolvidas

Você pode programar a verificação que é executada automaticamente para atualizar seu Qualys itens vulneráveis.

Antes de Iniciar

Após a transição de uma tarefa de correção para **Resolvido** , uma verificação é iniciada automaticamente para atualizar o estado dos itens vulneráveis associados.

- A verificação está desabilitada por padrão.
- Habilite a verificação com **scan_on_resolved** parâmetro de instância de integração no **Qualys** registro localizado em **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**. Para obter mais informações, consulte as etapas a seguir.
- Esta verificação é específica da instância. Se você tiver várias instâncias e quiser habilitar ou desabilitar esta verificação, deverá desabilitar **scan_on_resolved** parâmetro nos parâmetros da instância de integração em cada instância que você deseja mudar.
- Quando a verificação está habilitada, você pode iniciar a verificação sob demanda ou programar a verificação para ser executada somente dentro de uma janela de tempo especificada. Consulte Configurar Qualys nova verificação para executar somente dentro dos intervalos programados para saber como definir as horas de início e término da janela de tempo.

Função necessária: sn_vul_qualys.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Selecione **Qualys** para abrir o registro.
   Os Parâmetros de instância de integração para Qualys são exibidos em uma guia.
3. Para habilitar a verificação automática, localize *scan_on_resolved*parâmetro.
4. Na coluna Valor da propriedade, insira verdadeiro .
5. Clique em **Atualizar**.

Configurar Qualys nova verificação para executar somente dentro dos intervalos programados

Para Qualys Integração de vulnerabilidades, defina os parâmetros de hora de início e término da verificação para que novas verificações sejam executadas ou estejam disponíveis somente durante as horas desejadas.

Antes de Iniciar

Esta configuração se aplica às novas verificações programadas e às novas verificações iniciadas manualmente no Qualys produto do seu ServiceNow AI Platform® instância.

Definir os parâmetros de hora de início e término da verificação para instâncias de integração permite especificar janelas de tempo quando novas varreduras no Qualys produtos estão disponíveis. Por exemplo, você pode preferir especificar que as novas varreduras só estão disponíveis fora do horário comercial, por exemplo, meia-noite às 10 horas.

Esta configuração é específica da instância. Se você tiver várias instâncias, deverá configurar os valores scan_start_time e scan_end_time nos parâmetros de instância de integração em cada instância que você deseja mudar.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**.
2. Clique em **Qualys** para abrir o registro.
   Os parâmetros de instância de integração para Qualys são exibidos.
3. Para o parâmetro scan_start_time, na coluna Valor, insira a hora no fuso horário UTC no formato de 24 horas (00:00 a 24:00) para a hora de início da janela que você deseja verificar novamente.
4. Para scan_end_time, na coluna Valor, insira as horas no mesmo formato (00:00 a 24:00) para a hora de término da janela disponível.
   Por exemplo, se você inserir uma hora de início de 00:00 para o parâmetro scan_start_time e um scan_end_time de 10:00 na mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de horário da meia-noite às 10 horas serão enfileiradas e iniciadas na hora de início da janela de tempo do dia seguinte, 00:00.

   No mesmo exemplo, se um responsável pela correção iniciar manualmente uma nova verificação às 11:00 da manhã, a nova verificação não será iniciada imediatamente, porque está fora dos tempos de verificação configurados disponíveis. A solicitação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo, (00:00).

5. Clique em **Atualização** para salvar suas configurações.

Qualys limites de taxa de verificação de vulnerabilidades

Você pode definir a taxa em que diferentes tipos de verificações são executados para limitar o número de solicitações enviadas para um scanner externo. Depois de definir os limites de taxa, você pode aplicá-los ao Qualys scanners.

Definir Qualys limites de taxa de verificação

Você pode definir a taxa em que diferentes tipos de verificações são executados para equilibrar a carga na fila de verificação. As condições definidas no limite de taxa determinam se os limites de taxa são aplicados às entradas na fila.

Antes de Iniciar

Função necessária: sn_vul.admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Definições de Limite de Taxa**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Definição do limite de taxa

Campo	Descrição
Nome	Forneça um nome descritivo que identifique as condições que a entrada da fila deve atender. Por exemplo, verificações por minuto
Condições de fila	Insira as condições usadas para determinar se uma entrada de verificação enfileirada está sujeita a este limite de taxa. As condições não devem ser específicas para um scanner específico.
Script de avaliação	Grave um script com a lógica para avaliar a entrada enfileirada. É importante que o script retorne verdadeiro/falso para definir se a entrada será processada. Baseie o script de avaliação na entrada enfileirada que está sendo avaliada.

4. Clique em **Enviar**.

Aplicar limites de taxa de varredura a. Qualys scanners

Depois de definir os limites de taxa de varredura usando **Definições de Limite de Taxa** , você pode aplicar limites de taxa a específicos Qualys scanners.

Antes de Iniciar

Função necessária: sn.vul_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Limites de Taxa do Scanner**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Limite de taxa do scanner

Campo	Descrição
Scanner	Selecione o scanner ao qual você deseja aplicar um limite de taxa.
Limite de taxa	Selecione o limite de taxa que você deseja aplicar a este scanner.
Limite	Insira o limite ao qual você deseja submeter o scanner selecionado para o limite de taxa selecionado. Por exemplo, se o scanner permitir 4 verificações por minuto e o limite de taxa for definido como solicitações por minuto, o limite será 4.

4. Clique em **Enviar**.

Exiba Qualys fila de verificação de vulnerabilidades

Solicitações de verificação de vulnerabilidades enviadas para Qualys a integração de verificação de vulnerabilidades é enfileirada para não sobrecarregar os recursos do sistema. Você pode exibir o status das solicitações enfileiradas, conforme necessário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Na lista de verificações enfileiradas, cada verificação inclui um nome de verificação gerado automaticamente que identifica o IC que foi verificado.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Fila de Verificação**.
   Todos Qualys as solicitações de verificação que foram enviadas são mostradas em uma lista. . **Estado** a coluna mostra o estado atual de cada entrada enfileirada. Um estado de **Concluído** indica que a verificação saiu da fila. Isso não indica necessariamente que a verificação concluiu o processamento. Quando as verificações forem concluídas ou se falharam, o. **Processando** a coluna mostra o texto de anotações de trabalho apropriado.

   Nota: . Se um valor de hash foi enviado para verificação e o scanner não conseguiu encontrar um resultado, o. **Estado** mostra **Concluído** e a anotação de trabalho no **Processando** a coluna indica **Desconhecido** .

2. Após a conclusão do processamento de uma verificação, clique em um registro enfileirado para exibir os detalhes da solicitação de verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilite o filtro do sistema de base para importações de detecção confirmadas

Habilite um filtro padrão usando parâmetros de integração para importar somente detecções confirmadas de Qualys Cloud Platform.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin, sn_vul.vr_import_admin

Por Que e Quando Desempenhar Esta Tarefa

Um parâmetro de instância de integração do sistema de base "include_only_confirmed" está disponível para importar uma lista filtrada de detecções Qualys Cloud Platform. Por padrão, este parâmetro é definido como `FALSO` e todas as detecções potenciais, confirmadas ou informativas são importadas.

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Abra a integração da plataforma Qualys Cloud na lista Instâncias de integração.
3. Na lista Parâmetros de instância de integração, abra ' `include_only_confirmed`parâmetro '.
4. Atualize o valor padrão para `Verdadeiro` .
5. Clique em **Atualizar**.
   Você habilitou o filtro para importar detecções confirmadas do Qualys Cloud Platform integração.

Resultado

Por padrão, somente detecções confirmadas do Qualys Cloud Platform As integrações são importadas quando a próxima importação de vulnerabilidades da Qualys é executada. Todas as outras detecções, como informativas e potenciais, são ignoradas e não importadas. Para obter mais informações, consulte Exibir dados de detecção de item vulnerável da Resposta a vulnerabilidades .

Iniciar uma nova verificação para Qualys Vulnerability Integration

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas varreduras no Qualys produto do seu ServiceNow AI Platform sob demanda.

Antes de Iniciar

Você pode iniciar novas varreduras nos espaços de trabalho de Resposta a vulnerabilidades. Para obter mais informações, consulte Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Para novas varreduras no ambiente clássico, consulte as seções a seguir para saber como iniciar novas varreduras.

Configuração necessária para novas varreduras no Qualys produto iniciado a partir de ServiceNow AI Platform:

Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Qualys produto do seu ServiceNow AI Platform® instância.

Ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidades, ou os gerentes de vulnerabilidades podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configuração) em seus ambientes. Você pode iniciar novas varreduras no Qualys Produto de item vulnerável (VI), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de item descoberto do seu ServiceNow AI Platform instância.

Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

Caso de uso:

Por exemplo, digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Qualys itens vulneráveis.

Você pode iniciar novas varreduras para VIS que têm Qualys como a origem em estados diferentes de encerrado. Consulte Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Verifique se você concluiu a configuração a seguir necessária para novas varreduras. Consulte as etapas que começam com Configurar e gerenciar Qualys verificadores de vulnerabilidades e verificações listadas nas seções anteriores para obter mais informações.

Função necessária: sn_vul_manually_initiate_rescan

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas varreduras para VIS com Qualys como a origem. Verificar Qualysé exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se a coluna Origem não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique em **Personalizar lista** (Ícone de engrenagem) e use o Slushbucket para mover **Origem** de **Disponível** . **Selecionado** .

3. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**, **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros**ou para **Itens descobertos** para a tarefa de correção, entrada de terceiros ou registros de itens descobertos, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve ser do Qualys produto e em qualquer estado diferente de **Encerrado** . Para vários registros de VI, todos os VIS devem ter Qualys como a origem e em qualquer estado diferente de **Encerrado** .
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ter Qualys como a origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado em qualquer estado diferente de **Encerrado** com Qualys como a origem.
- Em um registro de item descoberto, o item de configuração tem pelo menos um VI associado a. Qualys como a origem em qualquer estado diferente de **Encerrado** .

4. No canto superior direito do registro escolhido, clique em **Nova verificação** .
Na caixa de diálogo exibida, escolha uma para continuar.

Opção	Descrição
Selecione **Especifique perfis de opção** caixa de seleção.	Na lista, escolha o perfil de opção para Qualys scanner que você deseja usar para a nova verificação. Estes são os dispositivos (scanners) que você configurou e listou em **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
Limpe **Especifique perfis de opção** caixa de seleção (não marcada).	. Qualys O perfil de opção do scanner que você definiu como scanner padrão na lista Dispositivos do scanner é usado para a verificação. Para obter mais informações sobre como configurar os scanners padrão que você inicia no ServiceNow AI Platform Configure os dispositivos do scanner listados na seção anterior para obter mais informações.

5. Clique em **Verificação de solicitação** .

É exibida uma mensagem indicando que sua verificação está sendo processada. O status de todas as novas varreduras pode ser encontrado a qualquer momento nas listas relacionadas de Varredura nos registros VI, RT, TPE e de item descoberto que você usou para iniciar as novas varreduras. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e exibir todas as outras novas verificações iniciadas a partir de um determinado registro.

Sua instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida.

Depois que a nova verificação for concluída com sucesso, o. Qualys A integração de detecção de host é iniciada automaticamente para atualizar seus itens vulneráveis. Dependendo de quantos VIS você tiver, suas detecções, VIS e RTS serão atualizados após a conclusão do Qualys Verificação de integração de detecção de host. Navegue até esses registros para exibir as atualizações após a conclusão da integração de detecção de host.

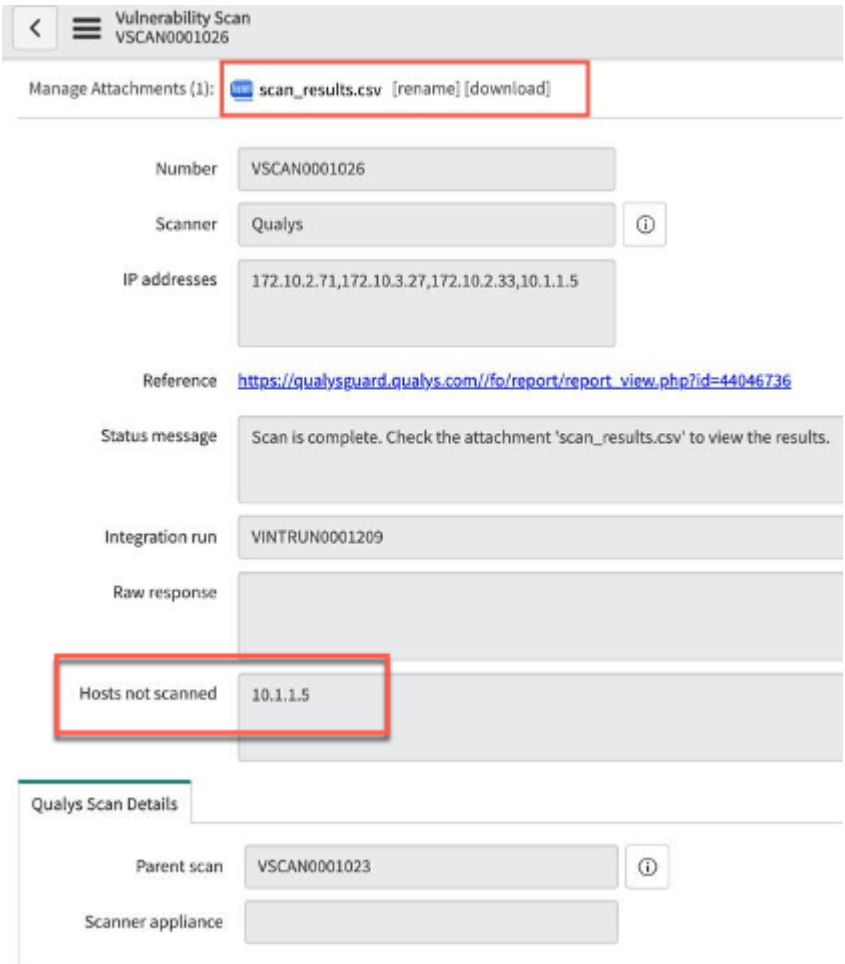
Esta verificação é específica da instância e pode ser desabilitada. Para obter mais informações sobre Qualys integrações e como exibir as integrações, consulte Noções básicas do Qualys Vulnerability Integration.

O que Fazer Depois

Você pode exibir um anexo .csv no registro de verificação para ver detalhes sobre as novas varreduras.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como mostrado na imagem anterior, durante a nova verificação, se os hosts (itens de configuração) em seu ambiente não estiverem acessíveis, quaisquer detecções e VIS associados a esses ativos não serão atualizados quando a nova verificação for concluída. Para ajudar você a entender por que eles não estão incluídos, depois que a nova verificação for concluída, os endereços IP do ativo desses ICs serão listados nos registros de vulnerabilidade no campo Hosts não verificados.

Qualys metadados de vulnerabilidades

. Qualys A integração de detecção de host foi aprimorada para incluir mais campos de Qualys. Esses campos ajudam na filtragem do não explorável Linux vulnerabilidades. Essa melhoria melhora a integração no nível de detecção e no nível do item vulnerável (VI).

Importar metadados adicionais de Qualys

Importe metadados adicionais para itens de vulnerabilidade (VI) para filtrar vulnerabilidades com base no impacto em um kernel ou serviço.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.
2. Em Configuração de integração, clique em **Integrações do scanner** .
3. Em Aplicação instalada, clique em **Editar** para Qualys aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Configuração de detecção de host** .
5. Navegar até **Importar metadados adicionais para detecções**.
6. Para importar metadados adicionais de Qualys, marque manualmente qualquer uma das seguintes caixas de seleção necessárias.
   - **Metadados do kernel** Identifica vulnerabilidades encontradas em kernels Linux em execução ou não em execução.

     Se o valor dos metadados retornados for **Não** significa que a vulnerabilidade não pode ser explorada devido a um kernel não em execução. Para obter informações sobre os valores recuperados, consulte Qualys valores de metadados para vulnerabilidades.
   - **Metadados de serviço** Identifica vulnerabilidades encontradas em portas ou serviços em execução ou não em execução.
   - **Metadados de configuração exploráveis** Identifica vulnerabilidades que podem ou não ser exploráveis devido à configuração atual do host.

   Nota: Essas caixas de seleção não estão marcadas por padrão.
7. Execute o. Qualys Integração de detecção de host com um backdate.
   Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais da Qualys.

Resultado
Os metadados foram importados.

O que Fazer Depois
Para exibir os metadados importados, insira `sn_vul_detection.list` Na Navegação de filtro. A lista Detecções de item vulnerável é exibida. Para obter mais informações sobre os valores exibidos nas colunas recém-adicionadas, consulte Qualys valores de metadados para vulnerabilidades.

Qualys valores de metadados para vulnerabilidades

Quando os metadados do kernel, os metadados de serviço e os metadados de configuração são importados, alguns valores também são recuperados. Os valores **0** , **1** e. **Não disponível** são processados no back-end e convertidos para **Não** , **Sim** e. **Vazio** respectivamente.

Esses valores são preenchidos nas seguintes colunas na lista Detecções de item de vulnerabilidade e Itens de vulnerabilidade:

- Afeta a coluna de serviço em execução
- Afeta a coluna de configuração explível
- Afeta colunas do kernel em execução

Nota:

- Essas colunas não estão visíveis por padrão. Para obter mais informações sobre como configurar o layout do formulário, consulte Configure o layout do formulário
- Para detecções mais antigas, os valores dessas colunas podem estar vazios. Para atualizar os dados, execute uma Integração de detecção de host da Qualys com data anterior. Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais da Qualys.

A tabela a seguir mostra os valores recuperados e sua importância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valores de campo recuperados e sua importância

Campo	Valor	Significância
AFFECT_RUNNING_KERNEL	0	A vulnerabilidade foi encontrada em um kernel não em execução. A vulnerabilidade não pode ser explorada.
AFFECT_RUNNING_KERNEL	1	A vulnerabilidade foi encontrada em um kernel em execução. A vulnerabilidade pode ser explorada.
AFFECT_RUNNING_KERNEL	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada ao kernel.
AFFECT_RUNNING_SERVICE	1	A vulnerabilidade foi encontrada em portas ou serviços não em execução. A vulnerabilidade não pode ser explorada.
AFFECT_RUNNING_SERVICE	0	A vulnerabilidade foi encontrada em portas ou serviços em execução. A vulnerabilidade pode ser explorada.
AFFECT_RUNNING_SERVICE	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.
AFFECT_EXPLOLIABLE_CONFIG	1	A vulnerabilidade não pode ser explorada devido à configuração do host.
AFFECT_EXPLOLIABLE_CONFIG	0	A vulnerabilidade pode ser explorada devido à configuração do host.
AFFECT_EXPLOLIABLE_CONFIG	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.

Defina parâmetros de filtro adicionais para Qualys importações

Personalize os parâmetros de filtragem para suas consultas programadas com Qualys Vulnerability Integration para ajudar você a refinar ainda mais os dados de vulnerabilidade importados com o compatível Qualys integrações.

Antes de Iniciar

Casos de uso: Como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você deseja exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou, você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudar você a coletar esses dados, você pode adicionar Qualys parâmetros para ajudá-lo a importar os detalhes específicos da vulnerabilidade de que você precisa.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite personalizar suas informações de solicitação HTTP com Qualys parâmetros em seu ServiceNow AI Platform. Você modifica ou adiciona esses valores no registro do método HTTP no método REST do compatível Qualys integrações do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

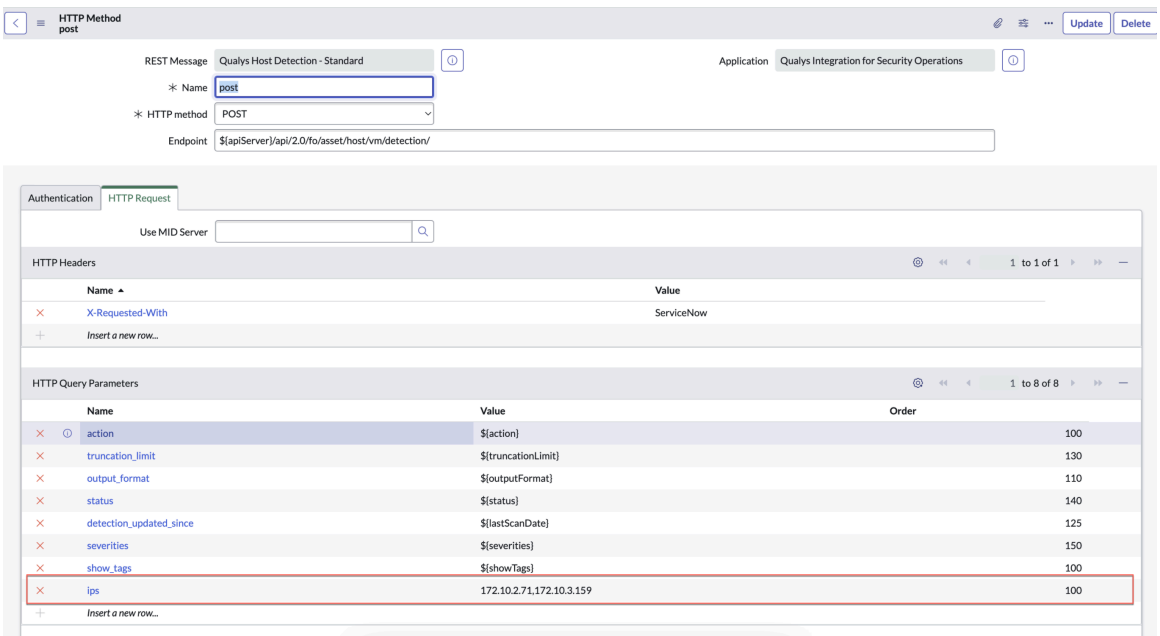
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Localize os parâmetros compatíveis com Qualys produto no site do desenvolvedor que você deseja usar para filtragem.
   Parâmetros e valores inseridos no Qualys os produtos são compatíveis somente no nível de instância de integração em seu ServiceNow AI Platform. Todos Qualys As integrações oferecem suporte à filtragem usando parâmetros de consulta.
2. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
3. Em Qualys Página de lista de integrações, clique no registro da integração em que você deseja abrir o registro.
4. Com Qualys Guia Detalhes DO REST selecionada, localize e clique no ícone de informações (I) do método REST seguido por **Registro em aberto** Para abrir o registro do método HTTP.
5. Selecione **Solicitação HTTP** guia.
6. Nos Parâmetros de consulta HTTP para o corpo da solicitação, adicione os valores obtidos do Qualys site do desenvolvedor.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços/intervalos IP, *ips={value}*foi adicionado. Nesse caso, **valor** É um ou mais IPs/intervalos especificados. Várias entradas são separadas por vírgulas, 172.10.2.71, 172.10.3.159 e um intervalo é especificado com um hífen, 10.10.10.1-10.10.10.100 . Consulte Qualys site do desenvolvedor para obter mais informações.



   Se você quiser inserir mais de um parâmetro, consulte Qualys para obter mais informações sobre como separar cada valor.

   Nota: Você deve estar ciente dos seus requisitos de API. Pode ser necessário adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

   Alguns outros parâmetros que você pode achar úteis no Qualys site do desenvolvedor:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- `ag_ids` - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente as máquinas no seu escopo sejam introduzidas.
- `qids` - Este parâmetro limita os resultados a apenas determinadas vulnerabilidades (QID na tabela de entrada de terceiros). Esta configuração evita inundar seu sistema com registros informativos.

7. Clique em **Atualizar**.

Resolvendo problemas de integração de vulnerabilidades da Qualys

Alguns problemas comumente encontrados, juntamente com soluções alternativas, são discutidos.

Anexos que não aparecem após a importação

Se os anexos não estiverem aparecendo conforme o esperado para fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso de IP podem impedir que anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir anexos em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Os mapas de transformação são fornecidos com configurações básicas e geralmente são suficientes. Você pode modificar mapeamentos de transformação dependendo das necessidades da sua organização.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin e import_admin

Procedimento

1. Navegar até **Tudo** > **Conjuntos para importação do sistema** > **Administração** > **Mapas de transformação** Para exibir as mensagens REST.
2. Filtre a lista resultante por aplicação e limite a lista ao **Integração de vulnerabilidades da Qualys** aplicação.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

   Para obter detalhes sobre os dados fornecidos pela API da Qualys, consulte Documentação da API da Qualys .

Verifique o tamanho da propriedade do anexo XML

Verifica se a propriedade do anexo XML é suficiente para arquivos grandes.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Propriedades do sistema** > **Importação/Exportação**.
2. Role para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Se necessário, altere o valor para 250 e clique em **Salvar** .

Tópicos relacionados

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados da Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando seu processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection - Padrão/POST** . Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método POST com os seguintes valores:

- Nome: Gravidades
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

Resolvendo falha na integração da Base de conhecimento da Qualys

Resolver Qualys Falha na integração da base de conhecimento ao reduzir o tamanho do anexo da carga recebida de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo da carga esteja dentro do limite especificado.
   a. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione **Parâmetros da instância de integração** guia.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys** .
   c. Selecione **Detalhes da integração** guia.
   d. Em **Hora de início** , selecione a data atual para ignorar a execução da execução desse dia.
   e. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Selecione **Parâmetros da instância de integração** guia.

g. Selecione **kb_backfill_full_import** e modificam o valor padrão para verdadeiro.

Resultado
Executar a integração de backpreenchimento da Base de conhecimento da Qualys atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração do Qualys Host Detection cria uma entrada de espaço reservado, a integração de backpreenchimento da Base de conhecimento da Qualys a atualiza.

Qualys Vulnerability Integration emissão de relatórios

. Qualys Cloud Platform a visão geral é uma exibição executiva da atividade de vulnerabilidade. Ao fornecer tendências, relatórios e detalhamentos em dados específicos, um administrador ou analista pode identificar rapidamente áreas de preocupação. Os gráficos são preenchidos com dados após Itens vulneráveis e Qualys os dados da base de conhecimento foram recuperados.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços de trabalho, Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Versões anteriores de Resposta a vulnerabilidades

Os analistas de vulnerabilidades também podem usar os painéis padrão no ambiente clássico para monitorar dados de vulnerabilidade. Para obter mais informações, consulte Usando o padrão Resposta a vulnerabilidades painéis.

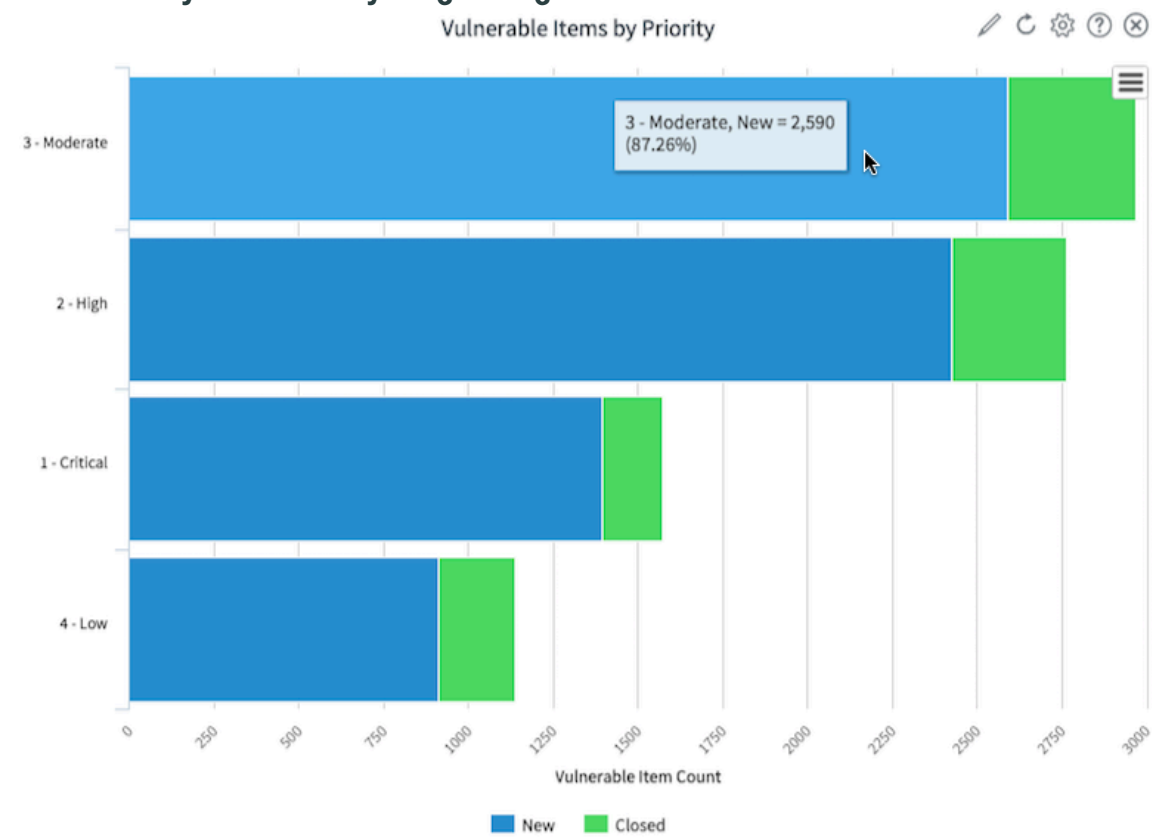
Nota: Usando o. Qualys Cloud Platform A integração de vulnerabilidades pressupõe que o ajuste, o teste e a implantação ocorreram em sua instância. Essas funções são áreas além do escopo da documentação do produto. Para obter assistência, entre em contato Suporte e atendimento ao cliente.

Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Amostra Qualys Vulnerability Integration gráfico



Os relatórios a seguir estão disponíveis no Qualys Cloud Platform página inicial.

Qualys Vulnerability Integration Relatórios de visão geral

Nome	Visual	Descrição
ICs sincronizados com a Qualys	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada IC, do mais para o menos.
Itens vulneráveis do Qualys em aberto	Barra	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros CVE), do mais para o menos.
Total de itens vulneráveis da Qualys	Barra	Exibe o número de itens vulneráveis ignorados programados para expirar em 7 dias.
Itens vulneráveis por prioridade	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Prevalência de QID	Barra	Exibe o número de itens vulneráveis registrados para cada modelo, do mais para o menos.
Itens vulneráveis do Qualys em aberto	Lista	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.

Qualys gráfico de status de execução de integração

. Qualys O módulo Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

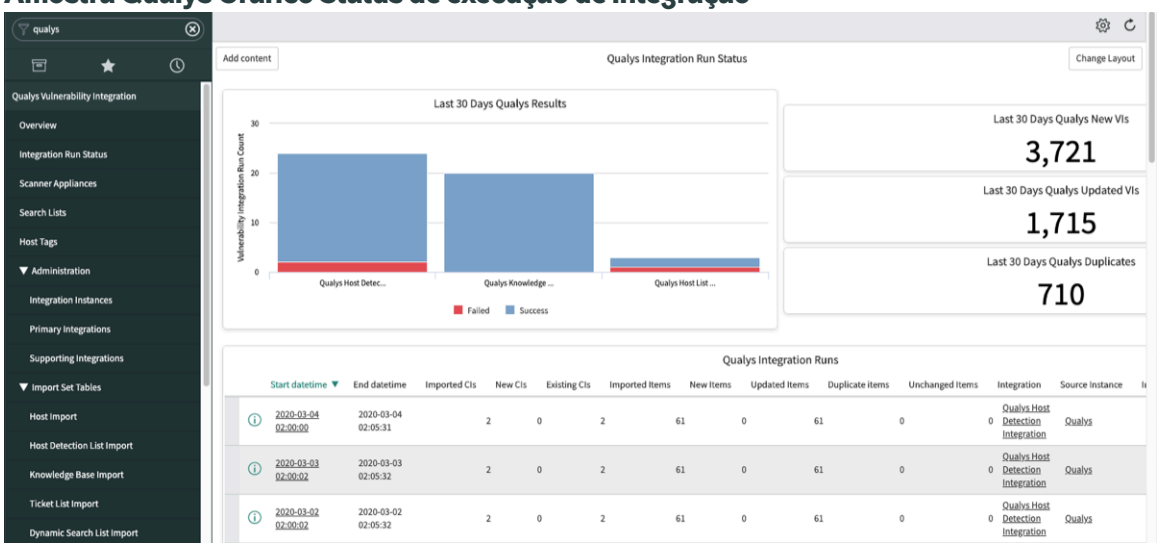
Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

. Qualys Status de execução da integração exibe o status de execução da integração da vulnerabilidade nos últimos 30 dias. A contagem de VIS atualizada da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O VI é atualizado com a nova detecção.

Nota: A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que são definidas como estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Amostra Qualys Gráfico Status de execução de integração



- Os valores na coluna Itens importados representam o número total de registros criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos atualizados. Se, por exemplo, um registro é atualizado duas vezes durante a execução da integração, é contado duas vezes e exibido como 2 itens atualizados.
- A coluna Itens inalterados exibe registros encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Nota: A integração é executada com zero resultados para todos os quatro dos seguintes valores: **Novos ICs** , **ICs existentes** , **Novos itens** e **Itens atualizados** são filtrados de **Execuções de integração da Qualys** lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualys relatórios de gráfico de status de execução de integração

Nome	Descrição
Últimos 30 dias Qualys Resultados	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novo VIS	O número de novos registros importado nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys VIS. Atualizado	O número de registros atualizados importado nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys Duplicatas	O número de registros duplicados importado nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota: V16.1:** Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no *sn_vul_detection*tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Qualys Rendimento de desempenho de ingestão de item vulnerável	Rendimento diário de ingestão de item vulnerável medido para Qualys Integração de detecção de host nos últimos 30 dias.

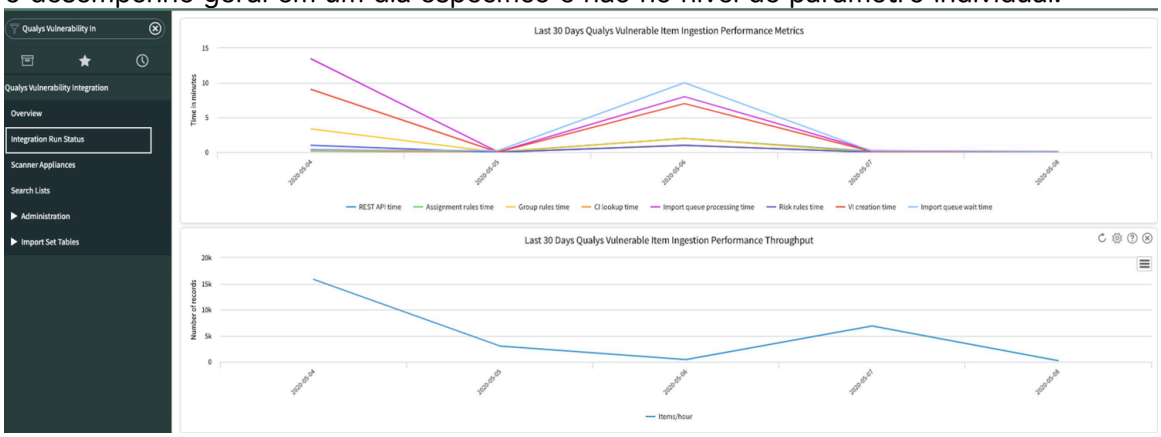
Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

- Qualys Métricas de desempenho de ingestão de item vulnerável: Comparar métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila, e outras estatísticas para itens vulneráveis nos últimos 30 dias, para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo necessário para cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cores para facilitar a identificação.
- Qualys Rendimento de desempenho de ingestão de item vulnerável: Compare o rendimento de ingestão de item vulnerável diário para Qualys Integração de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

detecção de host. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.



Transformação de dados da Qualys

Os dados recuperados da Qualys são processados por meio de um conjunto de fontes de dados e transformações.

A maioria das transformações para Qualys Vulnerability Integration são executados usando scripts de transformação. A exclusão desses scripts não é recomendada para uso interno. Modificações exigem codificação ou avançadas ServiceNow ou Qualys Vulnerability Integration experiência. Os mapas restantes são listados nesta seção e usam mapas de campo.

Nota: Mapas de gravidade normalizados que são importados por transformação durante a instalação Qualys Cloud Platform níveis de gravidade para o padrão ServiceNow os níveis de gravidade, são instalados no Resposta a vulnerabilidades Módulo de Mapeamento de gravidade normalizado. Para obter mais informações, consulte Crie um Resposta a vulnerabilidades mapa de severidade.

Importação de lista de pesquisa dinâmica

O mapa de transformação da lista de pesquisa dinâmica da Qualys é usado para transformar e importar listas de pesquisa dinâmica da Qualys. As mudanças nesta transformação alteram como as listas de pesquisa dinâmica são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação da lista de pesquisa Dynmaic**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos de mapa de transformação da lista de pesquisa dinâmica da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como o identificador da Lista de pesquisa dinâmica da Qualys.
[Script]	list_type	O tipo de lista de pesquisa. Dinâmico é o padrão para a transformação da lista de pesquisa dinâmica.
u_title	título	O nome na Qualys desta lista de pesquisa.

Além dos mapeamentos de campo, há também um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa dinâmica da Qualys

Quando o script é executado	Finalidade do script
OnAfter (depois que um conjunto de importação conclui a transformação).	Cria os relacionamentos entre as listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Não é recomendado modificar ou excluir.

Importação de lista de pesquisa estática

O mapa de transformação da lista de pesquisa estática da Qualys é usado para transformar e importar listas de pesquisa estática da Qualys. As mudanças nesta transformação alteram como as listas de pesquisa estática são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de lista de pesquisa estática**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos de mapa de transformação da lista de pesquisa estática da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como o identificador da Lista de pesquisa estática da Qualys.
u_title	título	O nome na Qualys desta lista de pesquisa.
[Script]	list_type	O tipo de lista de pesquisa. Estático é o padrão para a transformação da lista de pesquisa estática.

Além dos mapeamentos de campo, há também um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa estática da Qualys

Quando o script é executado	Finalidade do script
OnAfter (depois que um conjunto de importação conclui a transformação).	Cria os relacionamentos entre as listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Não é recomendado modificar ou excluir.

Importação de grupo de ativos

O Mapa de transformação do dispositivo Qualys Asset Group é usado para transformar dados do Qualys Asset Group para criar registros de dispositivo de scanner. As mudanças nesta transformação alteram como os dispositivos de scanner são criados e modificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de grupo de ativos**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos de mapa de transformação do grupo de ativos da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como identificador para o Grupo de ativos da Qualys.
[Script]	manual	Valor de script para determinar como o registro de destino foi criado. Quando criado por meio de transformações, este campo é sempre falso.
[Script]	ips	Os endereços IP associados ao grupo de ativos que está sendo transformado.
u_default_appliance_id	appliance_id	O identificador do dispositivo da Qualys para o dispositivo padrão neste grupo de ativos.
u_title	asset_group_name	O nome do grupo de ativos da Qualys.

Além dos mapeamentos de campo, há também um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do grupo de ativos da Qualys

Quando o script é executado	Finalidade do script
Antes de um conjunto de importação concluir a transformação.	O script que restringe as importações do grupo de ativos somente para grupos de ativos com um dispositivo padrão e um conjunto de endereços IP mapeados. Para uso interno. Não é recomendado modificar ou excluir.

Importação de dispositivo

O mapa de transformação da solução Qualys é usado para transformar dados da solução Qualys em registros da solução. Isso é usado para atualizar os registros da solução que seriam criados inicialmente a partir da importação do grupo de ativos. As mudanças nesta transformação alteram como os registros da solução são atualizados com os detalhes da solução.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de dispositivo**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos de mapa de transformação da aplicação Qualys

Campo de origem	Campo de destino	Descrição
u_name	appliance_name	O nome do dispositivo de scanner da Qualys.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de mapa de transformação da aplicação Qualys

Campo de origem	Campo de destino	Descrição
u_status	appliance_status	O último status relatado do dispositivo de scanner da Qualys.
u_id	appliance_id	O identificador do dispositivo Qualys.

Além dos mapeamentos de campo, há também um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do dispositivo Qualys

Quando o script é executado	Finalidade do script
Antes de um conjunto de importação concluir a transformação.	Usado para atualizar nomes e status da solução para o ID fornecido. Para uso interno. Não é recomendado modificar ou excluir.

Qualys Mensagens REST

As mensagens REST da Qualys são usadas para fazer chamadas para a API da Qualys.

A partir da versão 12.9.2 de Qualys, Você tem a opção de escolher entre Autenticação básica ou OAuth. O Método de autenticação do Qualys Cloud do parâmetro de instância é pré-configurado para Autenticação básica. Se você preferir usar o OAuth, modifique o parâmetro da instância de integração e configure a mensagem REST diretamente para o OAuth.

Mensagem REST de detecção de host da Qualys

A mensagem REST DO Qualys Host Detection faz a chamada inicial para a API de detecção de lista de hosts para a integração do Qualys Host Detection.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são necessárias.
output_format	XML	Define o formato do relatório retornado pela Qualys. Os vários scripts e transformações assumem XML, portanto, mudanças no valor não são recomendadas.
detection_processed_after	(LastScanDate)	Mostra somente detecções cujo status de detecção foi alterado após uma determinada data e hora. Para detecções que nunca foram alteradas, a data é aplicada à data da última detecção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do Parâmetro	Valor	Descrição
truncation_limit	500	O número de hosts dos quais recuperar dados, de acordo com a solicitação. Este parâmetro é usado para fins de paginação. O valor padrão é 500, mas valores maiores ou menores podem ser usados. Não defina em menos de 100, pois isso aumenta significativamente a carga do sistema. Valores menores exigem mais chamadas para a API da Qualys, e valores maiores resultam em conjuntos de resultados maiores para processar e possíveis tempos limite de recuperação/processamento de dados.
status	Novo, Fixo, Ativo, reaberto	Status de detecção a serem recuperados da Qualys. O padrão é recuperar todos os status. Para extrações de dados grandes (geralmente a extração inicial de dados), pode ser benéfico excluir status fixos desta lista. É importante incluir o status Corrigido ao atualizar vulnerabilidades que já estão no sistema.

Mensagem REST de paginação de detecção de host da Qualys

A mensagem REST DE paginação de detecção de host lida com solicitações de paginação para a API de detecção de host.

Quando a detecção do host primário é executada, se a API da Qualys fornecer uma URL para buscar a próxima página de dados, esta mensagem REST recuperará esses dados adicionais. Esses dados são usados pelo manipulador de paginação de detecção de host.

REST DE paginação de detecção de host é uma mensagem REST especializada e não deve ser modificada.

Mensagem REST da base de conhecimento da Qualys (preenchimento)

A mensagem REST da Base de conhecimento da Qualys (preenchimento) recupera os dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados de vulnerabilidade para a integração da Base de conhecimento da Qualys.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação que são enviados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (preenchimento)

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Tudo	Indica o nível de detalhe mostrado para vulnerabilidades recuperadas. Modificar conforme necessário.
IDs	(qids)	Especifica quais QIDs recuperar da Qualys. Referenciado no código. Modificações não são recomendadas.

Mensagem REST da base de conhecimento da Qualys (baseada em data)

A mensagem REST da Base de conhecimento da Qualys (baseada em data) é usada para recuperar dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados da vulnerabilidade. Esta mensagem é usada pela integração da Base de conhecimento da Qualys.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (baseados em data)

Campo de origem	Campo de destino	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Tudo	Indica o nível de detalhe mostrado para vulnerabilidades recuperadas. Modificar conforme necessário.
last_modified_after	(DateStart)	Indica quando começar a recuperar dados históricos. Usado pelo código para determinar a hora de início e para ajudar na paginação. Modificações ou remoção não são recomendadas.
last_modifiedbefore	(DateEnd)	Indica quando terminar a recuperação de dados históricos. Usado pelo código para determinar a hora de término e para ajudar na paginação. Modificações ou remoção não são recomendadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST de tíquetes da Qualys

A mensagem REST DE tíquetes da Qualys recupera as informações do tíquete da Qualys para a Integração de tíquete da Qualys. As mudanças no registro do método de mensagem REST afetam as solicitações feitas à Qualys para recuperar informações do tíquete.

A tabela mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST de tíquetes da Qualys

Nome do Parâmetro	Valor	Descrição
modified_since_datetime	(LastRunDatetime)	Indica a data da última execução da integração e a data após a qual os dados serão extraídos. Usado pelo código. Mudanças não são recomendadas.
since_ticket_number	(LastTicketNumber)	Indica qual tíquete foi recuperado pela última vez da Qualys. Usado para paginação. Mudanças não são recomendadas.
show_vuln_details	1	Indica se os detalhes da vulnerabilidade são recuperados.

Divida detecções da Qualys com base na instância de vulnerabilidade

A Resposta a vulnerabilidades permite dividir detecções de scanners da Qualys, criando um item vulnerável (VIT) exclusivo para cada instância de vulnerabilidade detectada. Isso oferece suporte à atribuição mais precisa às equipes de correção e melhora o gerenciamento e o acompanhamento de vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A carga útil do scanner da Qualys inclui dados de detecção com detalhes de prova. Cada caminho na prova é usado para identificar e dividir instâncias de vulnerabilidade. O marcador de saída na carga indica o local da vulnerabilidade, permitindo a separação e o gerenciamento precisos de detecções.

Procedimento

1. Habilitar divisão de detecção
   a. Navegue até a tabela Integração de terceiros [sn_sec_int_integration].
   b. Abra o registro para `Qualys Cloud Platform` .
   c. Defina `Include proof VI key`. *verdadeiro* .
   d. Salve o registro.
2. **Opcional:** Exclua QIDs específicos da divisão de detecção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Abra a propriedade do sistema [sn_vul_qualys.skip_split_detection_ids].

b. Em **Valor** , insira uma lista separada por vírgulas de QIDs que você deseja excluir da divisão.

> **Nota:** Por padrão, os seguintes QIDs são excluídos da divisão devido ao volume de suas descobertas: QID-989920, QID-993308, QID-5001711, QID-5001632.

c. Salve a propriedade.

3. Certifique-se de que os QIDs estejam listados para divisão

a. Navegue até a tabela Lista de vulnerabilidades de chave de prova [sn_vul_proof_key_vulnerability_list].

b. Verifique se os QIDs que você deseja dividir estão listados.

Resultado

Depois de executar o. `Integração do Qualys Host Detection` As detecções são divididas com base na prova, criando Itens vulneráveis individuais (Vits) para cada instância de vulnerabilidade. Você pode verificar os resultados na tabela Detecções de item de vulnerabilidade [sn_vul_detection_list], em que cada detecção aparece como um registro separado.

Componentes instalados com Qualys Vulnerability Integration

As funções, trabalhos de integração e tabelas a seguir são instalados com Qualys Vulnerability Integration.

> **Nota:** A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, trabalhos agendados e tabelas instaladas com uma aplicação sejam exibidas. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.

2. Selecione o Construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.

3. No Construtor de condições, para adicionar um segundo filtro, selecione **E.** e, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função** , **Trabalho agendado** ou **Tabela** .

4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura ao Qualys Vulnerability Integration registros.	
sn_vul_qualys.user	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador de Qualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o. Qualys Vulnerability Integration	sn_vul_qualys.admin

Trabalhos de integração instalados

Trabalho de integração	Descrição
Qualys Integração da lista de pesquisa estática	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis. Recupera somente registros do tipo de lista estática.
Qualys Integração abrangente de detecção de host	Recupera dados de host e vulnerabilidade do Qualys e o processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção de host. A saída desta integração é Itens vulneráveis. Esta integração importa todos os estados da vulnerabilidade: Novo, Corrigido, Ativo e Reaberto. Por padrão, esta integração está inativa e é executada semanalmente. **Nota:** Depois que essa integração é ativada, o trabalho abrangente diário importa somente os estados Novo, Fixo e Reaberto.
Qualys Integração da lista de hosts	Recupera dados de verificação de host autenticados e não autenticados e marcadores de host do Qualys Uma vez por semana e armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente.
Qualys Integração de detecção de host	Recupera dados de host e vulnerabilidade do Qualys e o processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção de lista de hosts.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
	As saídas desta integração são itens vulneráveis. Qualys marcadores de host são importados nesta integração.
Qualys Integração de tíquete	Recupera Qualys tíquetes e os adiciona à sua instância. Ele coordena as chamadas de mensagem REST para a API de lista de tíquetes. Desde então, há menos tíquetes do que as detecções de host Qualys as configurações podem restringir as detecções que resultam em um tíquete.
Qualys Integração da lista de perfis de opção	Recupera perfis de opção do Qualys produto. Os perfis de opção incluem configurações de verificação que são necessárias quando você inicia verificações no ServiceNow AI Platform instância.
Qualys Integração da lista de dispositivos	Recupera informações da solução do scanner de Qualys.
Qualys Integração do grupo de ativos	Recupera informações do grupo de ativos de Qualys. Os grupos de ativos são usados para identificar quais dispositivos de scanner usar para verificar itens de configuração correspondentes.
Qualys Base de conhecimento (preenchimento)	Recupera Qualys entradas da base de conhecimento. Programado para ser executado após Qualys Integração de detecção de host. Atualiza sua instância com quaisquer QIDs que foram referenciados na integração de detecção de host, mas não existiam no sistema.
Qualys Base de conhecimento	Recupera Qualys entradas da base de conhecimento. Os dados recuperados são baseados na data em que as vulnerabilidades foram atualizadas Qualys e desde a última vez em que a integração foi executada. Esses dados são úteis para preencher dados históricos em sua instância, bem como garantir o. Qualys Os identificadores (QIDs) estão atualizados.
Qualys Integração da lista de pesquisa dinâmica	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis e recupera registros de tipo de lista dinâmica.
Corrigindo as detecções de chave atualizada para Qualys	Uma combinação com hash de campos que forneceu uma maneira de identificar e vincular uma detecção a um Qualys item vulnerável.
Qualys Atualize itens descobertos existentes com o identificador de partição de rede	Atualiza seus itens descobertos existentes. ICs para o seu existente Qualys Os dados de Integração de vulnerabilidades são criados ou atualizados para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
	incluir a granularidade do identificador da partição de rede.

Tabelas instaladas

Tabela	Descrição
Vulnerabilidade da Lista de Pesquisa sn_vul_qualys_m2m_search_list_vul	Armazena o mapeamento entre Qualys lista de pesquisa e uma vulnerabilidade.
Qualys Verificador de vulnerabilidades sn_vul_qualys_scanner	Tabela que estende os Scanners de vulnerabilidades para armazenar informações do scanner para Qualys recurso de verificação novamente.
Qualys Listas de pesquisa sn_vul_qualys_search_list	Armazena listas de pesquisa recuperadas pelo Qualys integração da lista de pesquisa.
Qualys Importação do dispositivo sn_vul_qualys_appliance_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys IC sn_vul_qualys_ci	Tabela não mais usada.
Paginação de Detecção de Host sn_vul_qualys_host_detection_pagination	Tabela não mais usada.
Qualys Execução de integração sn_vul_qualys_integration_run	Tabela não mais usada.
Qualys Integração sn_vul_qualys_integration	Tabela que estende a integração de vulnerabilidade e armazena todas as integrações correspondentes a. Qualys.
Qualys Importação da lista de pesquisa estática sn_vul_qualys_static_search_list_imp	Tabela que estende a linha do conjunto de importação. Os mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Base de conhecimento sn_vul_qualys_knowledge_base	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys Lista de tíquetes sn_vul_qualys_ticket_list_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys Perfil de opção sn_vul_qualys_option_profile	Tabela que armazena os perfis de opção recuperados Qualys. Esta tabela é usada com a nova verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Qualys Importação da lista de pesquisa dinâmica sn_vul_qualys_dynamic_search_list_imp	Tabela que estende a linha do conjunto de importação. Os mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Reexecução do conjunto de importação sn_vul_qualys_import_rerun	Tabela não mais usada.
Qualys Importação de perfil de opção sn_vul_qualys_option_profile_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.

Noções básicas do Integração com Rapid7 Vulnerability

. ServiceNow® Integração com Rapid7 Vulnerability usa dados importados do Rapid7 depósito de dados ou Rapid7 InsightVM produtos para ajudá-lo a determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Rapid7 Nexpose os sensores coletam dados e os enviam automaticamente para Rapid7 depósito de dados (no local) ou Rapid7 InsightVM produtos (baseados em nuvem), que analisam e correlacionam continuamente as informações. Ele se integra facilmente ao ServiceNow® Resposta a vulnerabilidades Mapear vulnerabilidades para ICs e serviços. . Integração com Rapid7 Vulnerability aprimora os dados de vulnerabilidade em sua instância.

Rapid7 integrações são pontos de entrada que interagem com Rapid7 depósito de dados ou Rapid7 InsightVM produtos, invocados como trabalhos agendados. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Os trabalhos agendados são executados automaticamente e na ordem especificada. Você também pode executar trabalhos agendados individuais manualmente.

Nota:

Se você usar ambos Rapid7 depósito de dados e. Rapid7 InsightVM como fontes de seus dados, você corre o risco de registros de vulnerabilidade duplicados.

Nota: Ao migrar do **Depósito de dados** tipo de integração com **InsightVM** tipo, você pode desduplicar seus registros de depósito de dados existentes. Para obter mais informações, consulte Desduplicar Integração com Rapid7 Vulnerability registros do depósito de dados.

Se você tiver várias implantações do Rapid7 InsightVM integração de vulnerabilidade, você pode adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados originados de cada implantação são identificados e disponibilizados em uma única instância do Resposta a vulnerabilidades.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos desativados são desabilitadas por padrão.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis

Versão de lançamento para Zurich	Notas da versão
Integração com Rapid7 Vulnerability v13.6, 13,7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Rapid7 as tarefas de integração de vulnerabilidades envolvem as seguintes funções.

- sn_vul_r7.admin: Pode ler, gravar e excluir registros.
- sn_vul_r7.user: Pode ler e gravar registros.
- sn_vul_r7.read: Pode ler registros.

Integrações do Integração com Rapid7 Vulnerability

Para exibir o. Integração com Rapid7 Vulnerability, navegue até **Rapid7** > **Administração** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Rapid7 integrações de data warehouse

Integração	Descrição
Integração com Rapid7 Vulnerability	Recupera dados de vulnerabilidade de Rapid7 Nexpose e o processa em sua instância.
Rapid7 Integração da lista de ativos	Recupera dados de verificação uma vez por semana de Rapid7 Nexpose Depósito de dados e armazena-o no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando **Última verificação** data. Exiba **Última verificação** Tempo na lista de itens descobertos em Resposta a vulnerabilidades.
Rapid7 Integração de categoria	Recupera informações de categoria de Rapid7 Nexpose. As categorias fornecem classificação de alto nível para vulnerabilidades.
Rapid7 Integração de exploração	Recupera informações de exploração de Rapid7 Nexpose.
Rapid7 Integração do kit de malware	Recupera informações do kit de malware do Rapid7 Nexpose.
Rapid7 Integração de referência	Recupera referências a documentos de autoridade externa, como CVEs ou referências de vulnerabilidade específicas do fornecedor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rapid7 integrações de data warehouse

Integração	Descrição
Rapid7 Integração da solução	Recupera dados da solução de Rapid7 Nexpose, que fornece soluções recomendadas para vulnerabilidades específicas.
Rapid7 Integração da solução de substituição	Recupera informações sobre quais soluções são substituídas por outras soluções.
Rapid7 Integração de solução de pré-requisito	Recupera informações sobre as soluções que são pré-requisitos para outras soluções. Quando esta integração é executada, ela busca o mapeamento de soluções e soluções de pré-requisito do Rapid7 depósito de dados. **Nota:** Esta integração funciona somente se o Solução de gestão de vulnerabilidade o plug-in está ativado.
Rapid7 Integração do mapa de soluções de vulnerabilidade	Recupera o mapeamento para associar soluções a vulnerabilidades.
Rapid7 Integração de item vulnerável	Recupera dados de item vulnerável de Rapid7 Nexpose e o processa em sua instância. As saídas desta integração são itens vulneráveis.
Rapid7 Integração de resolução de item vulnerável	Recupera informações sobre os itens vulneráveis marcados como encerrados Rapid7 Nexpose e fecha os itens vulneráveis correspondentes em Resposta a vulnerabilidades.
Rapid7 Integração do site	Recupera dados do site de Rapid7 Nexpose. Um site é uma coleção de ativos que são direcionados para uma verificação.
Rapid7 Integração da lista de ativos	Recupera marcadores de host e dados de verificação uma vez por semana do Rapid7 Depósito de dados e armazena-o no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando **Última verificação** data. Exiba **Última verificação** Tempo na lista de itens descobertos em Resposta a vulnerabilidades
Rapid7 Integração abrangente de item vulnerável	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis não encontrados recentemente durante as verificações são transferidos automaticamente para "Encerrado" quando o módulo Fechar itens vulneráveis obsoletos automaticamente está habilitado.

Integrações do Rapid7 InsightVM

Integração	Descrição
Rapid7 Integração	Recupera dados de item vulnerável de Rapid7 InsightVM e processa-o em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Rapid7 InsightVM

Integração	Descrição
de item vulnerável - API	
Integração com Rapid7 Vulnerability API	Recupera dados de referência, categoria, exploração, kit de malware e vulnerabilidade do Rapid7 InsightVM e processa-o em sua instância.
Rapid7 Integração da lista de ativos - API	Recupera marcadores de host e dados de verificação uma vez por semana do Rapid7 InsightVM E o armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando **Última verificação** data. Exiba **Última verificação** Tempo na lista de itens descobertos em Resposta a vulnerabilidades.
Rapid7 Integração abrangente de item vulnerável - API	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis não encontrados recentemente durante as verificações são transferidos automaticamente para "Encerrado" quando o módulo Fechar itens vulneráveis obsoletos automaticamente está habilitado.
Rapid7 Integração do site	Recupera dados do site do Rapid7 InsightVM produto. Esta integração está definida para ser executada semanalmente às 00:00:00.

Durante a importação, os registros CVE ainda não presentes são criados como registros NVD e referenciados em entradas de terceiros para Rapid7 por padrão. A integração do modelo para Rapid7 não pode ser excluído. Em vez disso, desabilite-o.

Conector do Service Graph para Rapid7

A partir da versão 2,0, o Conector do Service Graph para Rapid7 está disponível no ServiceNow® Store. Para obter mais informações, consulte Conector do Service Graph para Rapid7 .

Regras de pesquisa de IC

As regras de pesquisa de IC determinam como preencher **Item de configuração** campo em um registro de item vulnerável.

Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.

Para criar ou editar regras de pesquisa, consulte Crie uma regra de pesquisa de IC de resposta a vulnerabilidades.

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

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação do Rapid7 Integrações de item vulnerável (data warehouse ou API InsightVM) e o. Rapid7 Integração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da lista de ativos - API. . Rapid7 Integração da lista de ativos - A API importa todos os ativos do Rapid7 verificados em busca de vulnerabilidades desde a última execução da integração. . Rapid7 A integração da lista de ativos do depósito de dados está incluída.

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

Consulte Itens descobertos em Resposta a vulnerabilidades Para obter mais informações sobre o módulo Itens descobertos.

Marcadores de host

Os marcadores de host são importados como parte do Rapid7 Integração da lista de ativos - Integração de API para Rapid7 InsightVM. Eles são usados principalmente para filtragem no Resposta a vulnerabilidades Atribuição e regras de tarefa de correção em Rapid7 InsightVM. Eles são exibidos no formulário Item descoberto.

Marcadores de host

Nota: . Rapid7 Integração da lista de ativos - A integração da API deve ser executada antes da criação das regras de tarefa de atribuição ou correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Se for um **San Diego** o marcador é criado e, em seguida, um **SAN DIEGO** O marcador não pode ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. O marcador que foi importado pela primeira vez vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags** . Esta propriedade é definida como verdadeira por padrão. Desativar os marcadores os desativa em todas as instâncias.

Sites

Um site é uma coleção de ativos destinados a uma verificação. Um site consiste em ativos de destino, um modelo de verificação, um ou mais mecanismos de verificação e outras configurações relacionadas à verificação, como cronogramas ou alertas. Os sites são gerenciados por Rapid7 aplicações.

Integração com Rapid7 Vulnerability a filtragem de site durante a configuração permite categorizar e solicitar ativos por site durante a importação. Consulte Filtrando por Rapid7 sites para obter mais informações sobre como filtrar importações.

. Rapid7 depósito de dados e. Rapid7 InsightVM As integrações de sites importam sites como um trabalho programado semanalmente.

Para exibir os sites importados em uma lista, navegue até **Rapid7** > **Sites**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reabra itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvido" em seu ServiceNow AI Platform A instância, mas não transitada para "Encerrado/Corrigido" pelas execuções de integração subsequentes, será reaberta se forem detectadas durante novas verificações.

Para Rapid7 Detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir os VIS resolvidos por idade. Se habilitado, o VIS definido como "Resolvido", mas não será alterado para "Encerrado/Corrigido" pelas verificações subsequentes, a transição de volta para "Aberto" após o número de dias que você inserir.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de identificação e reconciliação para criar novos ICs quando um IC existente não puder ser correspondido a um host importado de um scanner de terceiros. Habilite o plug-in Modelos de classe de IC do CMDB para criar ICs usando as novas classes, caso contrário ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Verificar novamente itens vulneráveis

Iniciar novas varreduras no Rapid7 plataforma para verificar se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Consulte Iniciar uma nova verificação para Rapid7 Integração de vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Rapid7 gestão de soluções

Se você ativou o. Solução de gestão de vulnerabilidade plug-in e, em seguida, o. Rapid7 soluções para ambos Rapid7 depósito de dados e. Rapid7 InsightVM Preenchido na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não tiver ativado o. Solução de gestão de vulnerabilidade plug-in e, em seguida Integração com Rapid7 Vulnerability funciona como está e importa as soluções na tabela personalizada [sn_vul_r7_solution]. Para obter mais informações, consulte Rapid7 gestão de soluções.

Preparando para Integração com Rapid7 Vulnerability

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Integração com Rapid7 Vulnerability presume que você esteja familiarizado com e execute Rapid7 depósito de dados ou Rapid7 InsightVM verificações de produto em seu ambiente.

Função necessária: administrador

. Rapid7 os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de baixar o. Integração com Rapid7 Vulnerability aplicação do ServiceNow® Store e instale-o em sua instância, revise as seguintes informações sobre os tipos de integração e as informações de configuração:

Há dois tipos de integrações incluídos com Integração com Rapid7 Vulnerability que está disponível em ServiceNow® Store:

- Rapid7 InsightVM
- Rapid7 depósito de dados

. Rapid7 tipo de depósito de dados:

- Requer seu Rapid7 URL do servidor de depósito de dados e credenciais de autenticação
- Requer um MID Server
- Usa um driver PostgresSQL para executar consultas no depósito de dados
- Não é compatível com várias instâncias

. Rapid7 InsightVM tipo de integração:

- É baseado em nuvem e usa uma REST API. Esta integração requer uma chave de API de no seu Rapid7 Conta do InSight.
- Oferece suporte a várias instâncias.

Consulte Configurar para Rapid7 Integração de data warehouse(depósito de dados) e. Configurar para Rapid7 InsightVM Integração para obter mais informações sobre os requisitos de configuração para esses tipos de integração.

Configurar para Rapid7 Integração de data warehouse

. Rapid7 depósito de dados A integração é um dos tipos de integração incluídos com Integração com Rapid7 Vulnerability Integração com Rapid7 Vulnerability.

Antes de Iniciar

Antes de executar o. Rapid7 integração do depósito de dados, conclua as seguintes tarefas de configuração:

- Obtenha o. Rapid7 complemento do data warehouse. Consulte Rapid7 site e documentação para adquirir e instalar este complemento.
- Obtenha o driver PostgresSQL mais atual. Vá para https://jdbc.postgresql.org/ e baixe o driver mais recente.
- MID Server para executar consultas ao depósito de dados. Consulte MID Server Para obter mais informações sobre como configurar um MID Server.

  Anote o nome do depósito de dados. . Rapid7 O tipo de integração de depósito de dados oferece suporte somente a MID Servers autônomos. MID Servers em cluster não são compatíveis.

- Obtenha seu Rapid7 URL do servidor de depósito de dados e credenciais de autenticação e disponibilize-as.

Função necessária: O administrador do sistema [admin] baixa e instala o app. Sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login no ServiceNow AI Platform instância da qual você deseja instalar Integração com Rapid7 Vulnerability aplicação em.
2. Instale o arquivo JAR do PostgreSQL que você baixou nas tarefas de configuração listadas anteriormente.
   a. Em seu ServiceNow AI Platform instância, navegue até **Tudo** > **MID Server** > **Arquivos JAR**.
   b. Clique em **Nova**.
   c. Insira o nome do driver PostgresSQL que você baixou anteriormente.

      Opcionalmente, insira **Versão** , **Origem** e **Descrição** informações. Saia do **Ativo** caixa de seleção marcada.

   d. Anexe o arquivo JAR baixado usando o ícone de clipe de papel no cabeçalho.
   e. Clique em **Enviar**.

Você concluiu a configuração do Rapid7 Integração de data warehouse. Se você não revisou os requisitos do Rapid7 InsightVM Antes de instalar o. Integração com Rapid7 Vulnerability, consulte Configurar para Rapid7 InsightVM Integração e. Preparando para Integração com Rapid7 Vulnerability.

Para obter as etapas para obter direitos, baixe e instale o. Integração com Rapid7 Vulnerability, consulte Instalar o Integração com Rapid7 Vulnerability.

Configurar para Rapid7 InsightVM Integração

. Rapid7 InsightVM A integração é um dos tipos de integração incluídos com Integração com Rapid7 Vulnerability Integração com Rapid7 Vulnerability.

Antes de Iniciar

Antes de executar o. Rapid7 InsightVM conclua as tarefas de configuração a seguir.

Função necessária: O administrador do sistema [admin] baixa e instala o app. Sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Para Rapid7 InsightVM Tipo de integração, tenha sua região e chave de API prontas.
   Contato Rapid7 Para obter a região apropriada e a chave de API.
   Você concluiu a configuração do Rapid7 InsightVM Integração. Se você não revisou os requisitos do Rapid7 integração do data warehouse, antes de instalar o. Integração com Rapid7 Vulnerability, consulte Configurar para Rapid7 Integração de data warehouse e. Preparando para Integração com Rapid7 Vulnerability.
2. Para obter as etapas para obter direitos, baixe e instale o. Integração com Rapid7 Vulnerability, consulte Instalar o Integração com Rapid7 Vulnerability.

Instalar o Integração com Rapid7 Vulnerability

Depois de concluir as etapas de configuração da integração para que ela se integre corretamente ao Resposta a vulnerabilidades, obtenha direitos, baixe e instale o aplicativo em seu ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Funções necessárias: administrador para downlaod e instalação, sn_vuln.admin supervisiona a configuração e verifica os resultados esperados.

1. Consulte Preparando para Integração com Rapid7 Vulnerability, Configurar para Rapid7 Integração de data warehouse e. Configurar para Rapid7 InsightVM Integração para obter mais informações sobre os tipos de integração e os requisitos de configuração do Integração com Rapid7 Vulnerability.
2. Conclua a check-list de configuração a seguir antes de baixar e instalar. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.
3. Depois que a aplicação for ativada, siga as etapas listadas abaixo para configurar o. Integração com Rapid7 Vulnerability.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow AI Platform funções para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados. Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades. • O administrador do sistema [admin] instala o app. Se ainda não estiver atribuído, o administrador atribuirá a função Administrador de vulnerabilidades [sn_vul.vulnerability_admin ou sn_vul.admin]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	. Rapid7 a função de administrador é herdada quando você recebe uma função administrativa no Resposta a vulnerabilidades(VR).
Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar.	Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.
Configurar filtragem	Use a filtragem para limitar o número de itens para importação inicial e preparar sua implantação ajustando os filtros nas importações subsequentes.
Desabilitar Calculadoras de Vulnerabilidade	Se você não usar calculadoras de vulnerabilidade, Desabilite a calculadora de vulnerabilidades padrão se não for usada, além de todos os outros que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
Mantenha o valor padrão para executar como usuário	Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.
Usando marcadores de host	Se você planeja usar marcadores de host em Resposta a vulnerabilidades Regras de tarefa de atribuição ou correção, execute a integração da Lista de ativos do Rapid7 antes de criar regras.
Desduplicar registros de dados existentes	Ao migrar do **Depósito de dados** tipo de integração com **InsightVM** você pode desduplicar seus registros de depósito de dados existentes. Para obter mais informações, consulte Desduplicar Integração com Rapid7 Vulnerability registros do depósito de dados.

Tradução automática

Procedimento

1. Faça login na instância em que você deseja instalar Integração com Rapid7 Vulnerability aplicação em.
2. Navegue até ServiceNow Store e faça login.
3. Em ServiceNow Store, pesquise Integração com Rapid7 Vulnerability aplicação.

   Nota: Em ServiceNow Store, a aplicação é chamada, Rapid7 Integração para Operações de segurança. Esta aplicação requer uma assinatura.

4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Obter**.
7. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Em seu ServiceNow AI Platform instância, navegue até **Aplicações do sistema** > **Todas as aplicações** > **Tudo**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .
    Na caixa de diálogo Instalar, seu status de dependência é exibido. Se você precisar de uma aplicação de dependência, a aplicação necessária será exibida. Siga as instruções na caixa de diálogo para instalar o. Integração com Rapid7 Vulnerability em sua instância.

Nota: Agora, o administrador de vulnerabilidades pode concluir a configuração da aplicação. Consulte Configure o Integração com Rapid7 Vulnerability.

Configure o Integração com Rapid7 Vulnerability

Configure o. Integração com Rapid7 Vulnerability depois que o aplicativo é instalado e ativado em seu ServiceNow AI Platform®.

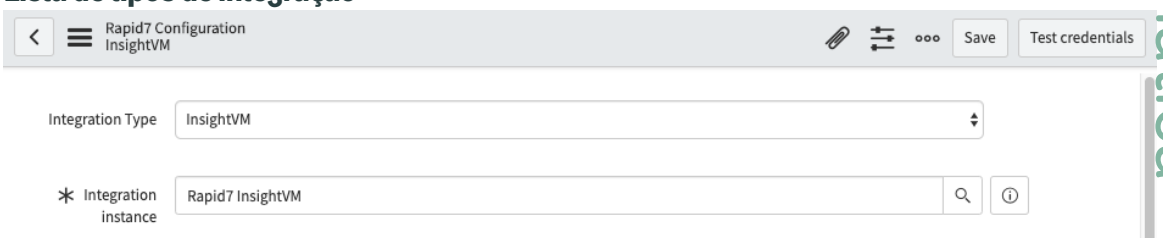
Antes de Iniciar

Função necessária: O administrador [admin] baixa e instala o app. Sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Depois que a aplicação for ativada (instalada), navegue até **Integração com Rapid7 Vulnerability** > **Administração** > **Configuração**.
2. Selecione um tipo de integração na lista.

Lista de tipos de integração



3. Selecione uma instância de integração.
   O padrão Rapid7 InsightVM a instância de integração é selecionada por padrão. Se esse for o tipo de integração desejado, siga estas etapas. Se você quiser configurar o. Rapid7 tipo de integração de depósito de dados, prossiga para a etapa 4.

   a. Com **Configuração de integração** selecionado no formulário exibido, preencha os campos:

Guia Configuração de integração para o tipo de integração InsightVM

Campo	Descrição
Região do InsightVM	O URL do servidor que você adquiriu do Rapid7 site.
Chave de API	A chave de API que você adquiriu do seu Rapid7 Conta do InSight.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status de Validação	Somente leitura: Status do processo de validação de credenciais.

b. Verifique a configuração bem-sucedida clicando em **Credenciais de teste** .
Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.

c. Após um teste bem-sucedido, clique em **Salvar** .

d. Clique em **Configuração de importação** guia.

No formulário exibido, preencha os campos.

Guia Configuração de importação para InsightVM

Campo	Descrição
Pontuação mín. do CVSS	Pontuação mínima de CVSS do item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máxima de CVSS	Pontuação máxima de CVSS do item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados ao Rapid7 InsightVMSites escolhidos na lista Sites. Consulte Filtrando por Rapid7 sites. Você pode escolher mais de um site. O padrão (vazio) traz todos os sites. Para preencher previamente a lista de sites, execute Rapid7 Site Integration - API antes de definir este campo. Para obter informações sobre como usar a filtragem de sites, consulte Filtrando por Rapid7 sites.
Criar entrada CVE automaticamente	A propriedade do sistema para criar uma entrada CVE está ativa (verdadeira) por padrão. Os espaços reservados CVE são criados automaticamente com a ingestão de conhecimento do Rapid7 se o ID CVE não existir. Se você quiser que este recurso fique inativo, desative a propriedade [sn_vul_r7.create_cvs_for_vulnerability] na lista Propriedades do sistema.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que foram resolvidos, mas não encerrados corresponde ao valor exibido em **Resolvido após** campo.

e. Clique em **Salvar**.

Para várias implantações do Rapid7 InsightVM tipo de integração:

f. Ativado **Instância de integração** Abra a lista de pesquisa e selecione uma instância de integração existente ou clique em **Novo** no menu pop-up.

g. Para **Novo** , insira um **Nome** para a instância de integração e clique em **Enviar** .
O tipo de integração aparece em Rapid7 formulário de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode excluir qualquer instância de integração, exceto o padrão. A exclusão de uma instância exclui o seguinte (excluindo VIS):

- Integrações
- Parâmetros de instância
- Execuções de integração
- Processos de integração
- A coluna de instância no VI está marcada em branco

h. Verifique a configuração bem-sucedida clicando em **Credenciais de teste** .

i. Após um teste bem-sucedido, clique em **Salvar** .

4. No campo Tipo de integração, expanda a lista e clique em **Depósito de dados** .

a. Selecione **Configuração de integração** guia.

No formulário exibido, preencha os campos.

Guia Configuração de integração para o tipo de integração do Data Warehouse

Campo	Descrição
Nome da credencial JDBC	Nome das suas credenciais de depósito de dados.
Nome de usuário	Nome de usuário do depósito de dados do Rapid7.
Senha	Senha do depósito de dados do Rapid7.
Status de Validação	Somente leitura: Status do processo de validação de credenciais.
Detalhe da Validação	Somente leitura: Somente depósito de dados. Mostra informações adicionais sobre a verificação de validação depois que você clica em Testar credenciais pelo menos uma vez. Isso pode ser útil para depurar sua configuração (por exemplo, validar se o MID Server está configurado incorretamente ou se você simplesmente tem as credenciais incorretas.
Servidor de banco de dados DNS/ IP	DNS ou endereço IP do seu depósito de dados.
Porta do banco de dados	Porta a ser usada para sua integração de depósito de dados.
Nome do banco de dados	Nome do seu depósito de dados.
Deslocamento de atraso de dados (Dias)	Os fatores de deslocamento de atraso de dados no atraso entre os dados em tempo real no Rapid7 Nexpose scanner e os dados no depósito de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
MID Server	MID Server a ser usado. MID Servers autônomos são compatíveis. MID Servers em cluster não são compatíveis.
Tempo limite do MID Server (mín.)	Número de minutos de espera para que o MID Server responda antes de a execução da integração expirar.

b. Verifique a configuração bem-sucedida clicando em **Credenciais de teste** .

c. Após um teste bem-sucedido, clique em **Salvar** .

d. Clique em **Configuração de importação** guia.

No formulário exibido, preencha os campos.

Guia Configuração de importação para Data Warehouse

Campo	Descrição
Caixa de seleção Criar entrada CVE anterior à v12.0	Quando marcado, os espaços reservados para CVEs, ainda não presentes, são criados como registros NVD e referenciados na entrada de terceiros para Rapid7. Esses CVEs são ignorados.
Pontuação mín. do CVSS	Pontuação mínima de CVSS do item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máxima de CVSS	Pontuação máxima de CVSS do item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados de integração de sites importados aos sites escolhidos. Você pode escolher mais de um. **Nota:** Como a configuração padrão é importar dados de todos os sites, você não precisa usar o filtro se quiser todos os sites. Fazer isso torna a solicitação mais lenta.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que foram resolvidos, mas não encerrados corresponde ao valor exibido em **Resolvido após** campo.

5. Clique em **Salvar**.

6. Opcional: Se você quiser definir uma data de início no Rapid7 Integração de vulnerabilidade - API e integração de item vulnerável do Rapid7 - registros de integração de API para recuperar dados históricos durante sua importação inicial do Rapid7 verificar, siga estas etapas.
Você pode usar esses dados para ajudá-lo com Fechando detecções obsoletas em Resposta a vulnerabilidades.

a. Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**.
. Rapid7 A lista de integrações é exibida.

b. Clique em um dos registros de integração para abri-lo.

(Optional) Perto da parte superior do formulário, clique em **aqui** link para editar o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. **Importar desde** campo de data em Rapid7 as integrações estão em branco, por padrão, exceto para Rapid7 Integração de vulnerabilidades - API e Integração de item vulnerável do Rapid7 - API. Para essas integrações, esses campos são definidos como 1998-12-31 ou 1999-01-01.

Para recuperar dados históricos durante sua importação inicial do Rapid7 defina uma data de início nos registros de integração apropriados. Este processo funciona para qualquer um Rapid7 integração com as seguintes exceções:

- . Rapid7 As integrações de Exploit e Kit de malware não mostram **Importar desde** porque eles não fazem atualizações delta e, portanto, não usam esse campo.
- . Rapid7 A integração da lista de ativos ignora o campo, pois sua intenção é recuperar todos os dados.
- Para a execução inicial do Rapid7 InsightVM Integração abrangente de item vulnerável - API quando o módulo Fechar automaticamente itens vulneráveis obsoletos está habilitado e **Importar desde** o campo é deixado em branco.

  Quando você habilita o recurso de fechamento automático, é necessária uma execução bem-sucedida da Integração abrangente de item vulnerável do Rapid7 ou da Integração abrangente de item vulnerável do Rapid7 - API. Essas integrações estão desabilitadas por padrão.

  Quando você habilita Rapid7 InsightVM Integração abrangente de item vulnerável - API, se você sair do **Importar desde** campo em branco na página de configuração de integração, o valor em **dias atrás** O campo do formulário Fechar automaticamente itens vulneráveis obsoletos também é usado para **Importar desde** data da primeira execução da integração. O valor padrão para Fechar itens vulneráveis obsoletos automaticamente é (90 dias).

  Por exemplo, se o **dias atrás** O campo no formulário Fechar itens vulneráveis obsoletos automaticamente é 90 e **Importar desde** O campo na página de configuração Integração abrangente de item vulnerável do Rapid7 - API está em branco, a primeira execução de integração importa os dados dos últimos 90 dias.

  Este relacionamento entre **Importar desde** e. **dias atrás** os campos se aplicam somente à primeira execução de integração. Depois disso, mude **dias atrás** O campo no formulário Fechar automaticamente itens vulneráveis obsoletos não afeta **Importar desde** Campo na página de configuração Integração abrangente de item vulnerável do Rapid7 - API. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta

  . **Importar desde** o campo é editável e você pode inserir os valores desejados para cada uma das integrações.

7. Navegar até **Tudo** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

a. . **import_startime_buffer_comprehensive** o parâmetro de instância de integração define um tempo de buffer de 24 horas antes do tempo especificado no **Importar desde** para que os ativos verificados a partir deste tempo de buffer sejam obtidos durante **Integração abrangente de item vulnerável do Rapid7 - API** execução de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode modificar este tempo de buffer de acordo com sua necessidade.

b. Opcional: Defina **close_stale_detections** parâmetro para *verdadeiro* Para fechar as detecções obsoletas que não chegam mais pela API Rapid7 para os ativos verificados e recuperados por meio da API Rapid7 por meio de **Integração abrangente de item vulnerável do Rapid7 - API** .

Você concluiu com sucesso as etapas de configuração, instalação e configuração do Integração com Rapid7 Vulnerability. Agora você está pronto para revisar e verificar os dados importados.

O que Fazer Depois

. Rapid7 e. Qualys os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto do scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

O produto que você ativou é exibido no campo Origem nos registros de item vulnerável e tarefa de correção após a próxima importação, e. **Nova verificação** Está disponível como uma ação de IU.

Se o seu ambiente exigir importações separadas por domínio, consulte Crie importações separadas por domínio para uma integração.

Para criar ou refinar suas regras de pesquisa antes da importação, consulte Crie uma regra de pesquisa de IC de resposta a vulnerabilidades.

Filtrando por Rapid7 sites

Filtrar por local para Rapid7 InsightVM tipos de integração, bem como Rapid7 Nexpose tipos de integração de data warehouse.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Nota: O uso da filtragem de site pode afetar o desempenho. Para obter informações sobre desempenho e outras considerações antes de usar a filtragem de site, consulte KB0789221 .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Tudo** > **Integração com Rapid7 Vulnerability** > **Configuração**.
2. Selecione uma instância de integração.
3. Clique em **Configuração de importação** guia.

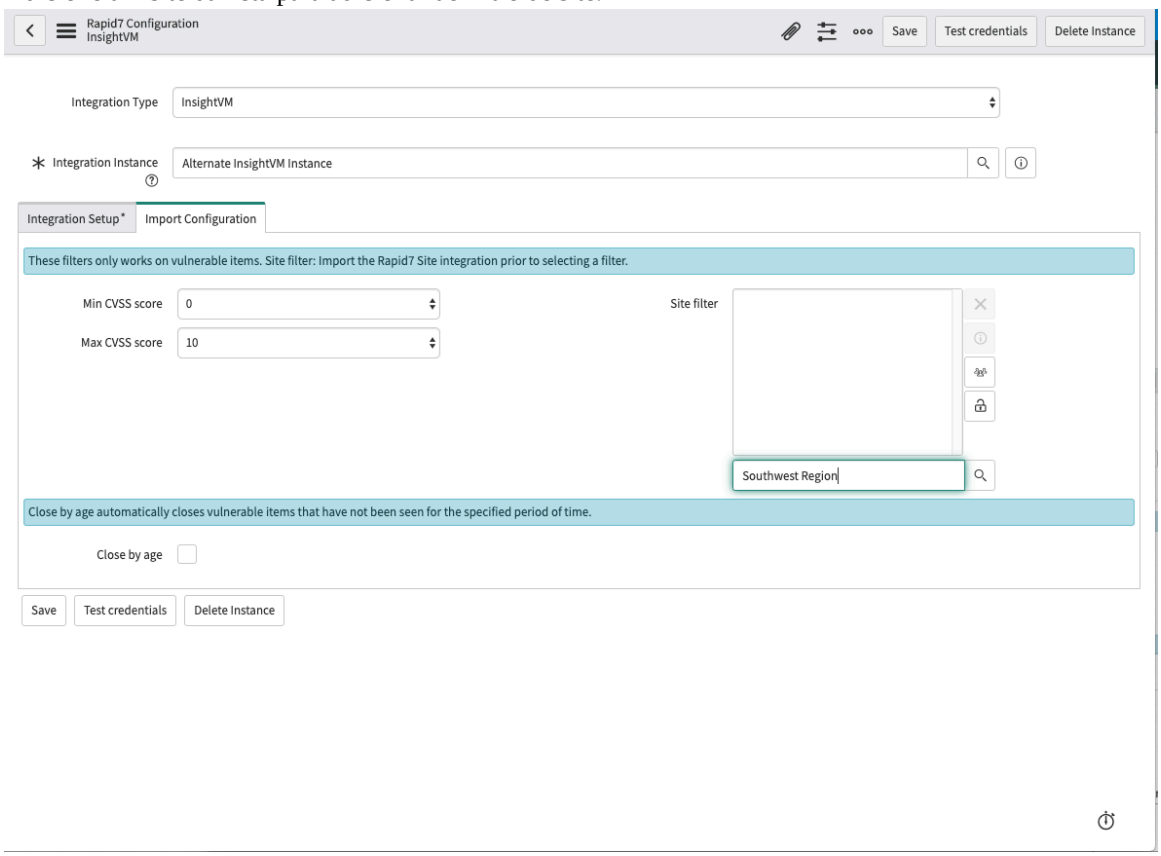
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você quiser todos os sites, deixe o campo de filtro de site vazio. Nenhum filtro de site é equivalente a adicionar todos os sites.

Os sites são específicos da instância de integração. A lista de pesquisa para filtragem de sites exibe ambos Rapid7 InsightVM e. Rapid7 Nexpose sites da instância de integração do depósito de dados. Certifique-se de que o site escolhido corresponda à instância de integração selecionada. Por exemplo, se você escolher um site de depósito de dados, por engano, esse site não funcionará para filtragem de site por Rapid7 InsightVM.

4. Clique na lista de pesquisa para exibir os registros do site da instância de integração atual.
5. Adicione um site da lista para adicionar ao filtro de site.



6. Repita a seleção para adicionar sites adicionais.
7. Clique em **Salvar**.
   Esses sites são usados para filtrar por local durante a próxima importação. Consulte Preceda O SITE aos marcadores do site Rapid7 InsightVM Para obter informações sobre como adicionar o prefixo de SITE aos dados do site.

Preceda O SITE aos marcadores do site Rapid7 InsightVM

Adicione o prefixo, SITE, ao seu Rapid7 InsightVM marcadores do site para destacá-los na sua lista de marcadores.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Nota: Se necessário, alterne seu escopo para o Rapid7 Integration for Security Operations.

Procedimento

1. Na caixa de navegação à esquerda, digite: *sys_properties.list*.
2. Em **Nome** , pesquise por: *sn_vul_r7.prefix_site_to_rapid7_tags*.
3. Abra o *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Mudança **Valor** . **verdadeiro** .
5. Clique em **Atualizar**.
   Marcadores de site novos e existentes são prefixados durante a próxima importação de Rapid7 InsightVM.

Integração com Rapid7 Vulnerability executar gráfico de status

Rapid7 Nexpose os sensores coletam os dados e os enviam automaticamente para o. Rapid7 Nexpose ou Rapid7 InsightVM, que analisam e correlacionam continuamente as informações.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços de trabalho, Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Integração com Rapid7 Vulnerability funciona facilmente com Resposta a vulnerabilidades Mapear vulnerabilidades para ICs e serviços de negócios para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas. . Integração com Rapid7 Vulnerability O módulo Status de execução é uma exibição gráfica do status de Integração com Rapid7 Vulnerability execuções.

Para exibir esses dados na exibição legada, navegue até **Tudo** > **Integração de vulnerabilidades do All Rapid7** > **Status da Execução da Integração**.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Versões anteriores de Resposta a vulnerabilidades

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois novos gráficos foram adicionados para comparar as métricas de desempenho:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Rapid7 Métricas de desempenho de ingestão de item vulnerável: Comparar métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila, e outras estatísticas para itens vulneráveis nos últimos 30 dias, para identificar a causa de quaisquer desvios no desempenho.
- Rapid7 Rendimento de desempenho de ingestão de item vulnerável: Compare o rendimento de ingestão de item vulnerável diário para Rapid7 Integração de item vulnerável - API. O rendimento é medido em itens por hora.

Nota: Em Rapid7 Esses gráficos são compatíveis somente com a integração da VM do Insight.

Status de execução da integração do Rapid7



Amostra Integração com Rapid7 Vulnerability executar gráfico de status



- O valor na coluna Itens importados representa o número total de itens vulneráveis criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de itens vulneráveis criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os itens vulneráveis são atualizados durante uma execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.

- A coluna Itens inalterados exibe itens vulneráveis encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Nota: A integração é executada com zero resultados para todos os quatro dos seguintes valores: **Novos ICs** , **ICs existentes** , **Novos itens** e **Itens atualizados** são filtrados de **Execuções de integração do Rapid7** lista.

Integração com Rapid7 Vulnerability executar relatórios de gráfico de status

Nome	Descrição
Últimos 30 dias Rapid7 Resultados	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Rapid7 Novo VIS	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Rapid7 VIS. Atualizado	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Rapid7 Duplicatas	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Rapid7 Execuções de integração	Os registros de execução de integração em uma lista. **Nota: V16.1:** Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no `sn_vul_detection`tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.
Últimos 30 dias Rapid7 Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Rapid7 Rendimento de desempenho de ingestão de item vulnerável	Rendimento diário de ingestão de item vulnerável para Rapid7 Integração de item vulnerável - API medida nos últimos 30 dias.

Exiba Integração com Rapid7 Vulnerability painel de status de execuções de importação

Use Rapid7 painel de status de execução de importação de vulnerabilidades para verificar o sucesso das execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Antes de Iniciar

Funções necessárias: sn_vuln.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Este procedimento faz as seguintes suposições.

- Você tem Resposta a vulnerabilidades e o. Integração com Rapid7 Vulnerability instalado e configurado.
- Integração com Rapid7 Vulnerability as importações estão programadas e em execução.
- Rapid7 os gráficos de status de execução de integração estão em uso.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 19,0 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Rapid7** > **Status da Execução da Integração**.

   A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

   Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

2. Se você não estiver usando Rapid7 gráfico de status de execução de integração, navegue até **Rapid7** > **Integrações**.
   a. Escolha uma integração.
   b. Clique em **Execuções de Integração de vulnerabilidades** lista relacionada.
3. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns para uma execução com falha:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Interrupção de rede
- Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação

Para todas essas condições, clique em **Executar agora** e execute novamente a integração.

Desduplicar Integração com Rapid7 Vulnerability registros do depósito de dados

Ao migrar para **InsightVM** tipo de integração do **Depósito de dados** tipo de integração, você pode desduplicar itens vulneráveis do depósito de dados existentes, desde que pertençam aos mesmos dados de origem que seu Rapid7 InsightVM dados.

Antes de Iniciar

Função necessária: sn_vul_r7.admin ou, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

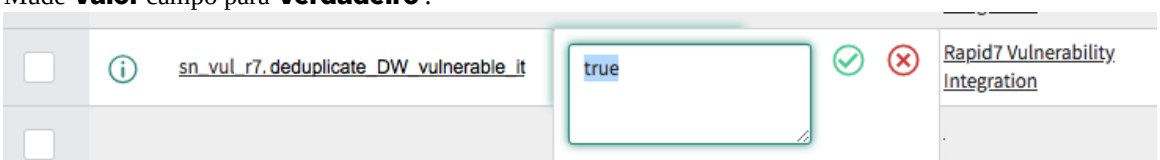
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Esta desduplicação só funciona ao migrar do Rapid7 Nexpose depósito de dados para Rapid7 InsightVM Integração de item vulnerável.

Procedimento

1. Navegar até **Tudo** > **Rápido 7** > **Integrações**.
2. Definir tudo Rapid7 Nexpose integrações de data warehouse **Ativo** configurações de coluna para **Falso** desabilitando as integrações.
3. Insira sys_properties.list no painel de navegação esquerdo.
4. PESQUISE **Nome** : sn_vul_r7.deduplicate_DW_vulnerable_item .
5. Mude **Valor** campo para **Verdadeiro** .



6. Clique no ícone de marca de seleção verde .
   Durante o próximo Rapid7 InsightVM importação de integração de item vulnerável, qualquer correspondência com registros de depósito de dados existentes impede que um item vulnerável duplicado seja criado.

Iniciar uma nova verificação para Rapid7 Integração de vulnerabilidades

Iniciar novas varreduras no Rapid7 plataforma para verificar se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados.

Antes de Iniciar

Nota: Novas varreduras para Rapid7 itens vulneráveis do depósito de dados não são compatíveis.

Você pode iniciar novas varreduras nos espaços de trabalho de Resposta a vulnerabilidades. Para obter mais informações, consulte Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias: Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Por Que e Quando Desempenhar Esta Tarefa
Para novas varreduras no ambiente clássico, consulte as seções a seguir.

Novas varreduras são compatíveis. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis importados de Rapid7 InsightVM integrações do seu ServiceNow AI Platform® instância.

Nota: . Rapid7 o scanner é desativado por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm Rapid7 Aplicação Como origem, o botão Reverificar não está disponível.

Ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidades, ou os gerentes de vulnerabilidades podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas varreduras de itens vulneráveis (VI), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de itens descobertos do seu ServiceNow AI Platform® instância.

Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

Por exemplo, todo o seu ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Rapid7 itens vulneráveis. Você pode exibir resultados atualizados em seus itens vulneráveis com a próxima importação programada de Rapid7 InsightVM Vulnerabilidades e Integrações de itens vulneráveis.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

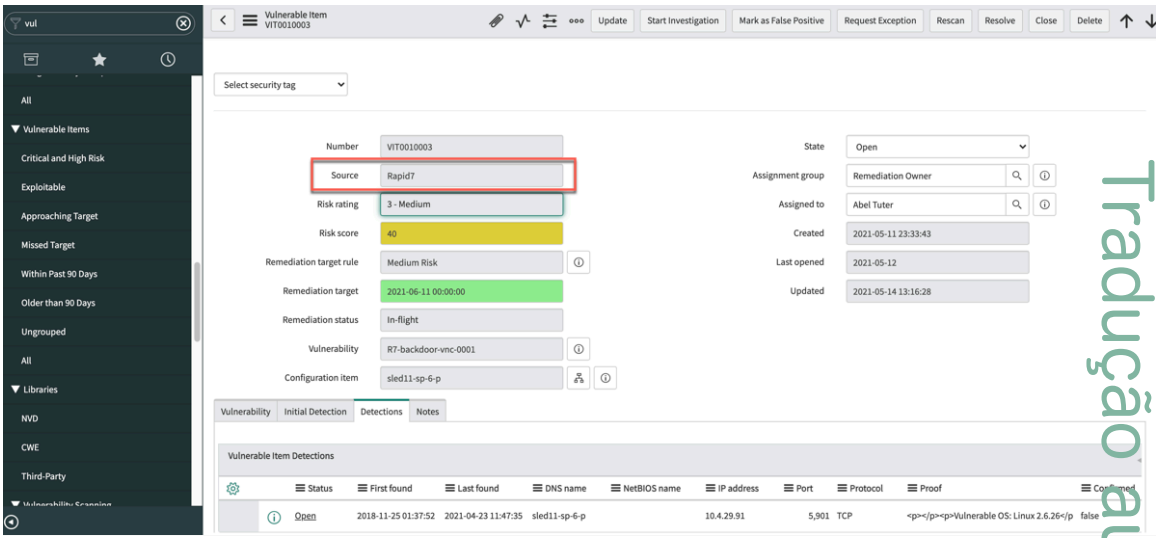
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Iniciar novas varreduras do VIS com Rapid7 como a origem. Verificar Rapid7é exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se for **Origem** A coluna não é exibida na exibição Lista de VI. No canto superior esquerdo da lista, clique no ícone de engrenagem e mova **Origem** de **Disponível** . **Selecionado** .

Ao iniciar novas varreduras, evite acionar simultaneamente varreduras para um ID de origem de várias origens. A solicitação de verificação mais recente ocorrerá um erro.

Por exemplo, se você iniciar uma nova verificação de uma VI a partir de um registro de VI e também solicitar outra nova verificação de um registro de tarefa de correção que contém essa mesma VI, é provável que a segunda solicitação falhe.



3. Como alternativa, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **terceiro** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve ser do Rapid7 Produto e em qualquer estado diferente de Encerrado. Para vários registros de VI, todos os VIS selecionados na exibição de lista devem ser de Rapid7 Produto e em qualquer estado diferente de Encerrado.
   - Em um registro de tarefa de correção, a tarefa de correção pode estar em qualquer estado diferente de Encerrado e todos os VIS associados devem ser do Rapid7 produto.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do Rapid7 Produto em qualquer estado diferente de Encerrado.
   - Em um registro de item descoberto, o VI deve ser do Rapid7 produto e em qualquer estado diferente de **Encerrado** .

4. No canto superior direito do registro, clique em **Nova verificação** .
   Para exibições de lista, selecione o VIS na lista que você deseja verificar novamente e, em **Ação nas linhas selecionadas** , selecione **Nova verificação** .

5. No pop-up exibido, confirme a nova verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

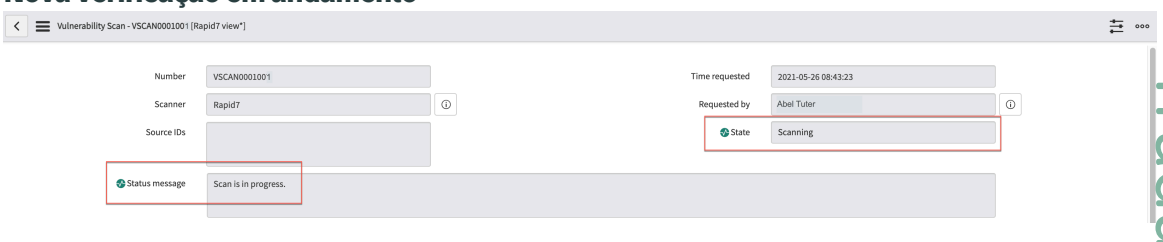
É exibida uma mensagem indicando que sua verificação está sendo processada (**Em fila**). Na mensagem, clique em **Exibir detalhes** link para verificar o status da nova verificação (verificação secundária) e exibir outras novas varreduras iniciadas a partir do registro. O status de todas as novas varreduras pode ser encontrado a qualquer momento na lista relacionada Verificações na parte inferior dos registros de VI, tarefa de correção, TPE e item descoberto que você usa para iniciar as novas varreduras.

Quando a verificação está em andamento, o campo Estado muda para **Verificando** E o campo Mensagem de status é exibido **A verificação está em andamento** .

Nota: Cada nova varredura oferece suporte a 500 ativos por verificação. Se sua solicitação tiver mais de 500 ativos, mais verificações secundárias serão solicitadas.

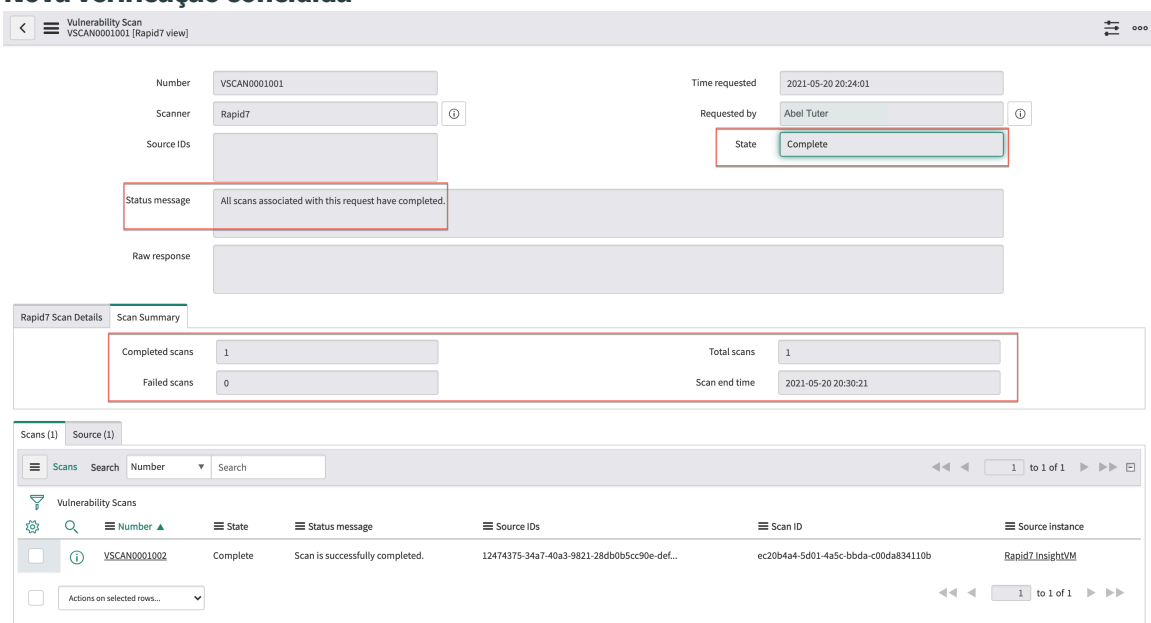
. ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro.

Nova verificação em andamento



O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida. Todos os VIS que fizeram a transição, ou farão a transição, para Encerrado/Fixo são importados com a próxima importação programada do Rapid7 integrações.

Nova verificação concluída



Como alternativa, você pode iniciar uma nova verificação sob demanda para uma vulnerabilidade específica em um ativo específico. Você pode exibir os resultados dessas verificações depois que a verificação for concluída no VI atualizado, na tarefa de correção, no TPE e nos registros de item descoberto a partir dos quais você iniciou a verificação.

Tradução automática

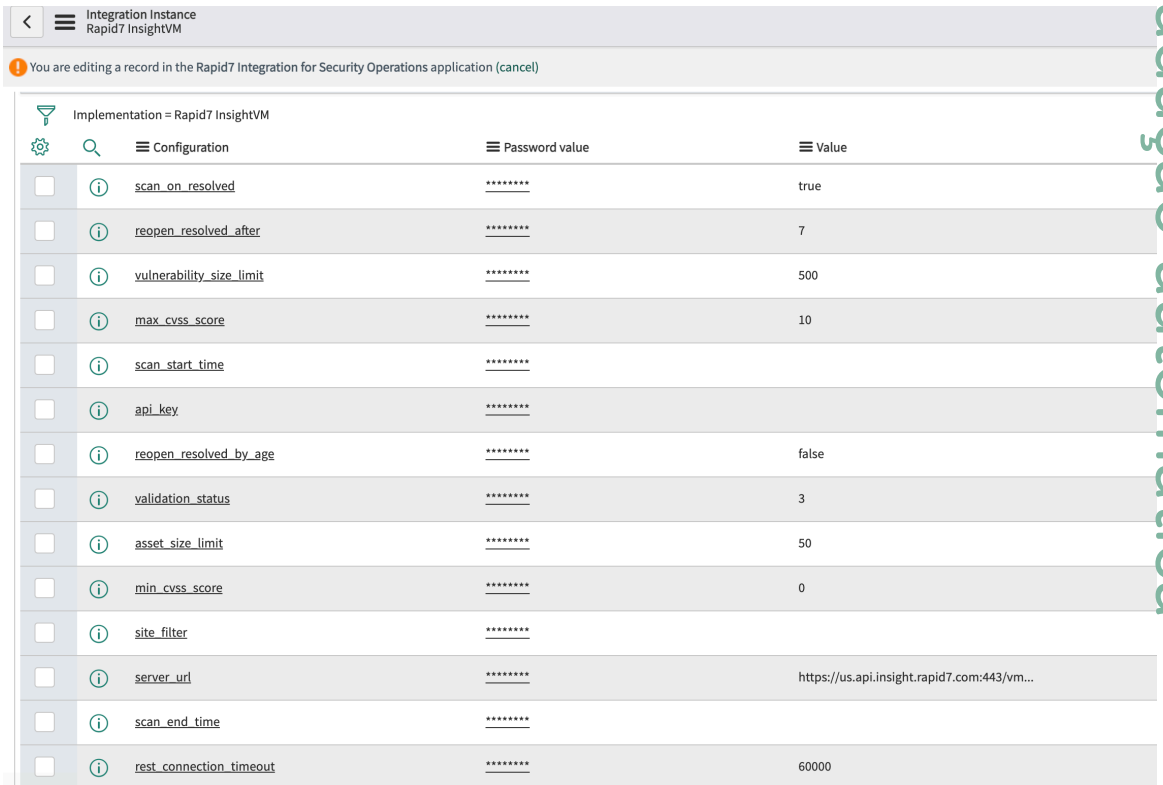
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor do campo Estado nos registros de Verificação de vulnerabilidades é importado de Rapid7. Quando a verificação é concluída com sucesso, o estado é definido como Concluído. Se a verificação não for concluída com sucesso, um valor de erro será exibido.

Verificações automáticas e programadas

Como gerente ou analista de vulnerabilidades, você pode especificar e programar quando novas varreduras são iniciadas para VIS e RTS. Você também pode habilitar verificações automáticas para tarefas de VIS e correção definidas como Resolver.

6. Para modificar os parâmetros de integração na instância de integração, navegue até **Integração com Rapid7 Vulnerability** > **Administração** > **Configuração**.
7. No registro Configuração do Rapid7, se não estiver selecionado, no **Tipo de integração** , selecione **Rapid7 InsightVM** .
8. À direita do **Instância de integração** , clique no ícone de informações, seguido por **Registro em aberto** .
9. No registro Integration Instance Rapid7 InsightVM, localize os parâmetros para programar verificações e edite conforme necessário.



scan_on_resolved indica se a verificação é iniciada quando uma vulnerabilidade é resolvida. O padrão é **falso** (desabilitado).

Se este parâmetro estiver definido como `verdadeiro` Sempre que um VI ou RT é definido como Resolvido, o fluxo de trabalho para verificar novamente o respectivo VI e a tarefa de correção é acionado automaticamente.

scan_start_time

Defina a hora de início da varredura em **HH:MM** (Formato de 24 horas) no Fuso horário UTC para a hora de início da janela que você deseja disponibilizar novamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor padrão é 00:00 .

scan_end_time

Defina a hora de término da verificação em **HH:MM** (Formato de 24 horas) no Fuso horário UTC para a hora de término da janela de verificação disponível.

O valor padrão é 23:59 .

Se uma verificação for iniciada dentro da janela de tempo programada, ela será iniciada instantaneamente. Se a verificação for iniciada fora da janela, ela será enfileirada para a próxima janela programada.

Por exemplo, se você inserir uma hora de início de 00:00 para *scan_start_time*e um *scan_end_time*Das 10:00 da mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de tempo da meia-noite às 10 horas são enfileiradas e iniciadas na hora de início da janela de tempo do dia seguinte 00:00 .

No mesmo exemplo, se você iniciar manualmente uma nova verificação às 11:00 AM, a nova verificação não será iniciada imediatamente, porque está fora dos tempos de verificação configurados disponíveis. A solicitação de verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo 00:00 .

Defina parâmetros de filtro adicionais para Rapid7 InsightVM importações

Personalize os parâmetros de filtragem para suas consultas programadas com Integração Rapid7 para Operações de segurança para ajudar você a refinar ainda mais os dados de vulnerabilidade importados com Rapid7 InsightVM produto.

Antes de Iniciar

Casos de uso: Como gerente ou analista de vulnerabilidades, convém filtrar dados de suas consultas para revisar somente detalhes específicos da vulnerabilidade. Por exemplo, talvez você queira exibir somente as vulnerabilidades importadas que são Crítico e. Grave .

Para ajudar você a coletar esses dados, adicione Rapid7 parâmetros para ajudá-lo a importar os detalhes específicos da vulnerabilidade de que você precisa.

Sem adicionar chamadas de API ou codificação adicionais, a partir da v13.4, o recurso permite personalizar as informações da solicitação HTTP com Rapid7 InsightVM parâmetros em seu ServiceNow AI Platform. A seguir Rapid7 InsightVM As integrações oferecem suporte à filtragem adicionando conteúdo JSON ao corpo da solicitação:

- Rapid7 InsightVM API de integração de item vulnerável
- Rapid7 InsightVM API de integração de vulnerabilidades
- Rapid7 InsightVM

Você deve saber como usar JSON cadeias de caracteres para este recurso.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Localize os parâmetros compatíveis com Rapid7 InsightVM produto no Rapid7 site do desenvolvedor que você deseja usar para sua filtragem.

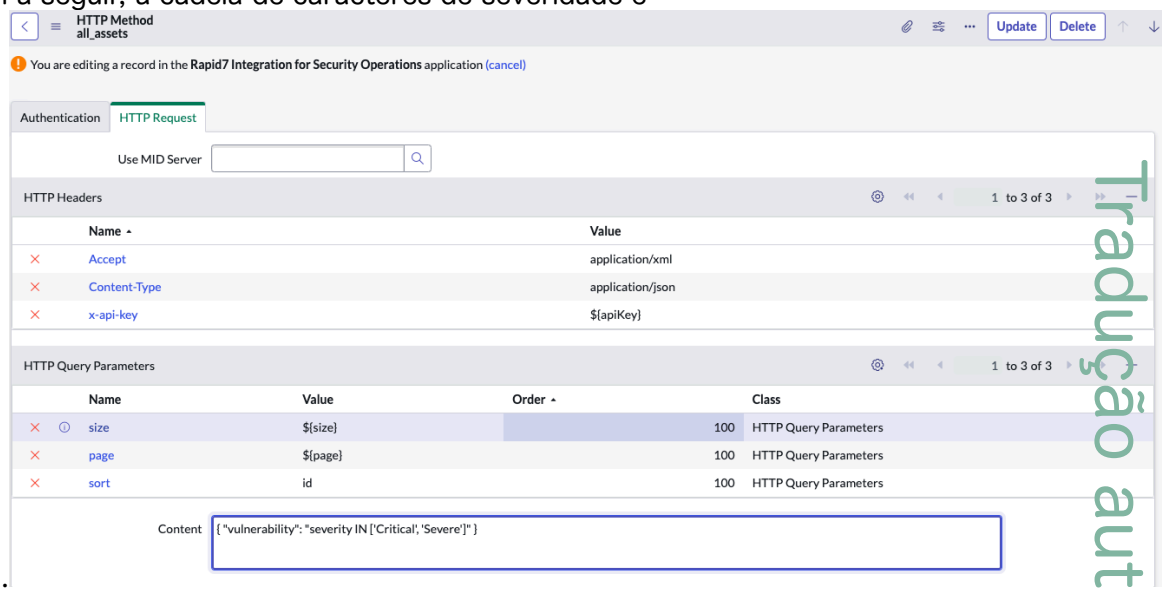
   Você pode criar os parâmetros para o corpo da solicitação consultando Rapid7 documentação. Parâmetros e valores inseridos no Rapid7 InsightVM os produtos são compatíveis somente no nível da instância de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Navegar até **Tudo** > **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**.
3. Na página de lista Integrações do Rapid7, clique no registro do Rapid7 InsightVM integração que você deseja abrir.
4. À direita da página, clique no ícone de informações (i) da mensagem REST seguida por **Registro em aberto** .
5. Com a guia Solicitação HTTP selecionada, em Métodos HTTP, na coluna Nome, clique em um item para abrir seus parâmetros de consulta HTTP.
6. Em Registro de método HTTP, em Parâmetros de consulta HTTP, no campo Conteúdo, insira os valores de parâmetro encontrados em Rapid7 site do desenvolvedor.

   Na imagem a seguir, a cadeia de caracteres de severidade é adicionada.



   Se você quiser inserir mais de um parâmetro, consulte Rapid7 para obter mais informações sobre como separar cada valor.

7. Clique em **Atualizar**.

Noções básicas sobre a integração do Shodan Exploit

. ServiceNow® Shodan A aplicação Integração de exploração usa dados importados do Shodan mecanismo de pesquisa para ajudar você a determinar o impacto e a prioridade de explorações potencialmente mal-intencionadas.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Shodan Exploit Integration

. Shodan O mecanismo de pesquisa coleta dados de exploração e a API do Shodan disponibiliza esse banco de dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao ServiceNow® Resposta a vulnerabilidades aplicação para mapear explorações para vulnerabilidades de terceiros, enriquecendo os dados de exploração em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que são listadas. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento para Zurich	Notas da versão
Integração com Shodan Exploits 10.6, 10,7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Shodan As tarefas de integração de exploração envolvem as seguintes funções.

- sn_vul_shodan.admin: Usuários com esta função podem ler, gravar e excluir registros.
- sn_vul_shodan.user: usuários com esta função podem ler e gravar registros.
- sn_vul_shodan.read: Usuários com esta função podem ler registros.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Integrações de exploração do Shodan

Para exibir o. Shodan integrações de exploração, navegue até **Tudo** > **Shodan Exploit Integration** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base. Essas integrações estão ativas por padrão.

Integrações de exploração do Shodan

Integração	Descrição
Shodan ExploitDB Integration	Recupera dados do ExploitDB de Shodan e enriquece seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente às 03:15:00.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de exploração do Shodan

Integração	Descrição
Integração de Metasploit do Shodan	Recupera informações de Metasploit de Shodan e enriquece seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente às 01:15:00.

Para mudar a hora de início padrão das importações de integração programadas, consulte Definido Shodan Tempo de importação da integração de exploração.

Para exibir dados de exploração em vulnerabilidades de terceiros, consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Alterando outro Shodan As configurações de integração de exploração exigem avançado ServiceNow e. Resposta a vulnerabilidades e está além do escopo da documentação do produto.

Preparando para Shodan Integração de exploração

Bem-sucedida Shodan A integração de exploração requer planejamento e execução cuidadosa de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Shodan A Integração de exploração pressupõe que você esteja familiarizado com Shodan Mecanismo de pesquisa e API.

Antes de Iniciar

. Shodan A integração de exploração requer uma chave de API. Registre-se com Shodan site para obter uma assinatura gratuita para adquirir esta chave.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

- Se você não importou dados do NIST Vulnerability Database (NVD) para Resposta a vulnerabilidades, faça isso antes de instalar o. Shodan Integração de exploração. Importar os dados de NVD garante que os dados CVE (Common Vulnerability and Exposure) preencham automaticamente os registros de exploração.

  Sem dados de NVD, um espaço reservado é criado no registro de exploração e não inserido até a próxima atualização de NVD. Para obter mais informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

- Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Instale e configure o. Integração com Shodan Exploits para Operações de segurança

Antes de executar o. Integração com Shodan Exploits em sua instância, baixe e instale-o do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

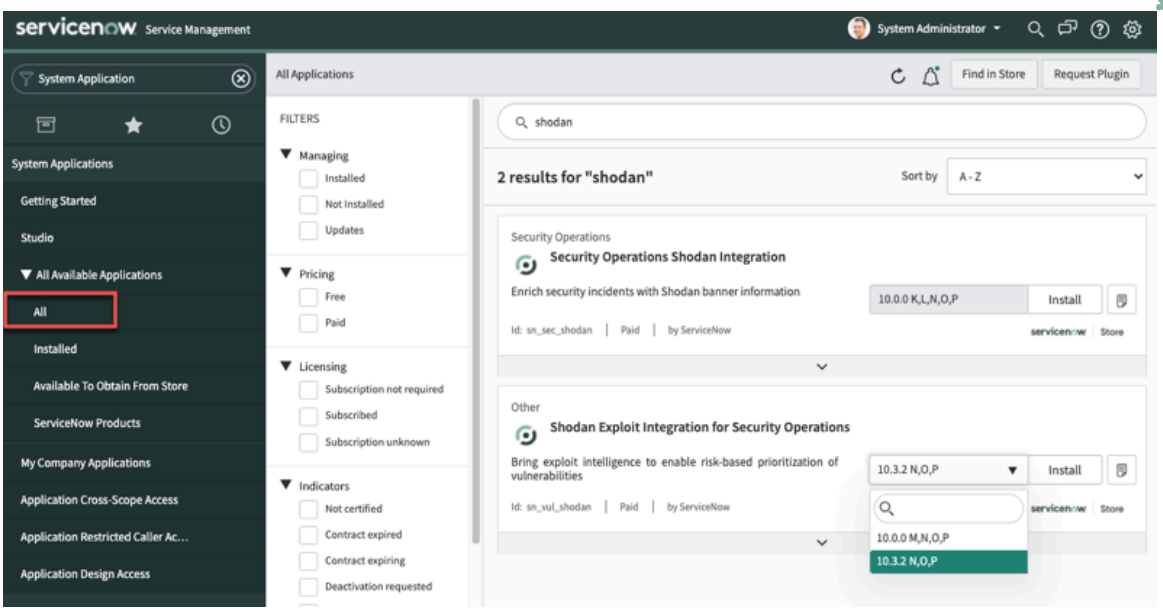
Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se você tem válido ServiceNow direitos para Resposta a vulnerabilidades e Integração com Shodan Exploits para Operações de segurança aplicação.	Para verificar direitos, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para um Operações de segurança aplicação do ServiceNow Store, consulte Obtenha direito para um Operações de segurança produto ou aplicação.
(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instalar Resposta a vulnerabilidades.
. Shodan Chave de API de integração de exploração útil.	Consulte Preparando para Shodan Integração de exploração.

Função necessária: administrador

Procedimento

1. Faça login no ServiceNow AI Platform instância da qual você deseja instalar Integração com Shodan Exploits aplicação em.
2. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
3. Localize Integração com Shodan Exploits para Operações de segurança, selecione a versão desejada e clique em **Instalar** .



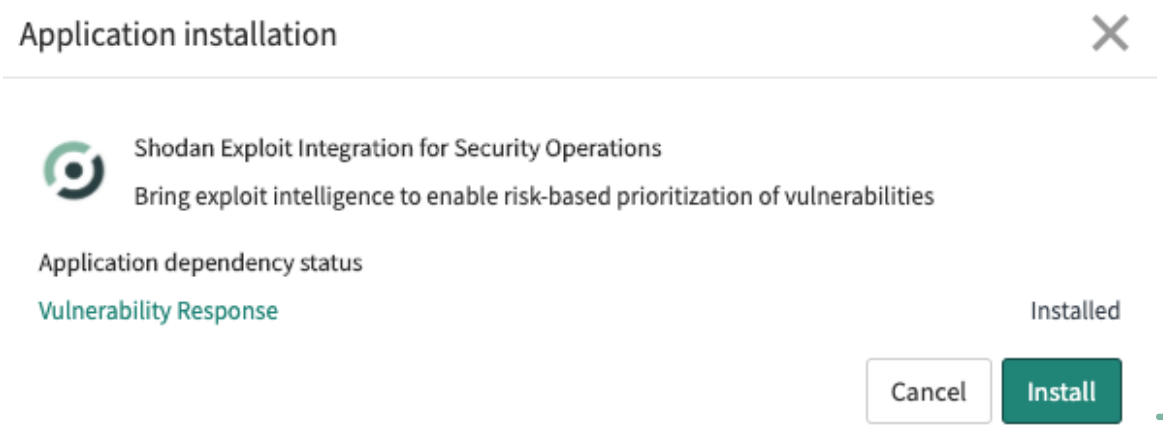
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você tiver direito a uma atualização para esta aplicação, o **Atualização** o botão é exibido.

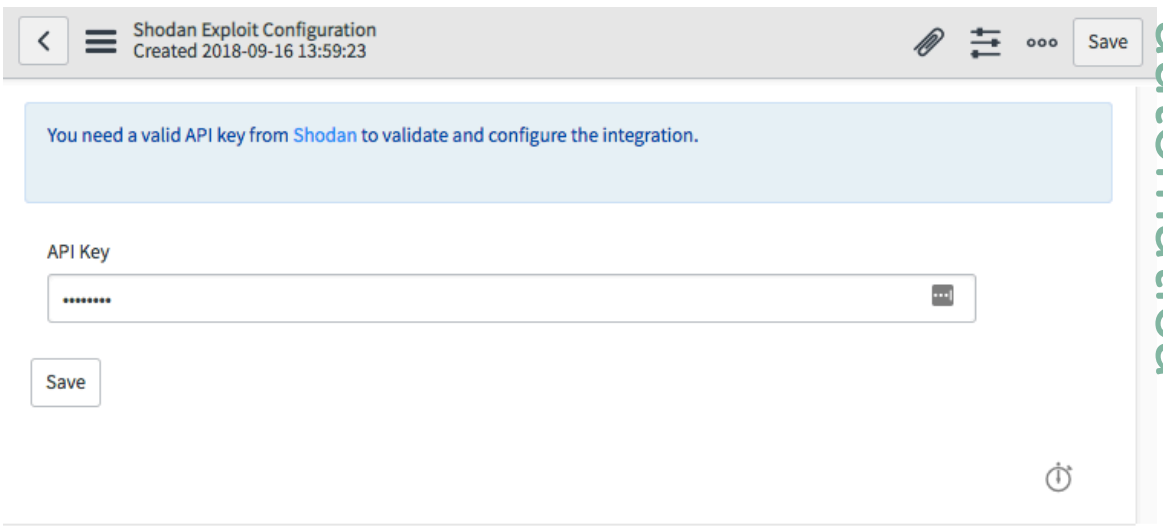
A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo, clique em **Instalar** .



A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo Instalar.
6. Navegar até **Shodan Exploit Integration** > **Configuração**.
7. Insira seu Shodan Chave de API.



8. Clique em **Salvar**.
. Integração com Shodan Exploits a configuração está concluída.

Definido Shodan Tempo de importação da integração de exploração

Para sua conveniência, você pode redefinir a hora de início do Shodan integrações de exploração.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, Shodan as integrações de exploração trazem dados delta, a menos que uma importação completa seja solicitada. Consulte Execute um manual Shodan importação de exploração para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Tudo** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Clique no link para editar o registro.
4. Definir o novo **Executar** e. **Hora** opções.
   O tempo é calculado como horas no horário local. A hora padrão do Shodan importações de exploração é 03:15:00.
5. Clique em **Atualizar**.
   A nova hora é usada para a próxima importação programada.

Execute um manual Shodan importação de exploração

Se sua importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho agendado diariamente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Selecione **Importação de dados completa** caixa de seleção.
4. Clique em **Executar Agora**.
   Quando a importação estiver concluída, a caixa de seleção será desmarcada e as importações delta serão retomadas.

Exiba Shodan Status da execução de importação da integração de exploração

Use a lista relacionada Execuções de integração de vulnerabilidades para verificar o sucesso de suas execuções de integração e localizar quaisquer problemas , e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status da execução de importação do Shodan:

- . Resposta a vulnerabilidades e Shodan A integração de exploração deve ser instalada e configurada.
- . Shodan As importações de integração de exploração devem ser programadas e em execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vuln.admin

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Shodan Exploit Integration** > **Integrações**.
2. Selecione uma integração.
3. Clique em **Execuções de Integração de vulnerabilidades** lista relacionada.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns para uma execução com falha incluem:

- Interrupção de rede
- Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação

Se você encontrar qualquer uma dessas condições, selecione **Importação de dados completa** caixa de seleção, clique em **Executar agora** e execute novamente a integração.

Noções básicas sobre a Integração de vulnerabilidades do Tenable

. Integração de Resposta a vulnerabilidades com Tenable aplicação desenvolvida por ServiceNow A Engenharia para a Integração de vulnerabilidades do Tenable usa dados importados do Tenable.io, Tenable.sc e Tenable.cs produtos para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. O aplicativo está disponível com uma assinatura separada do ServiceNow® Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

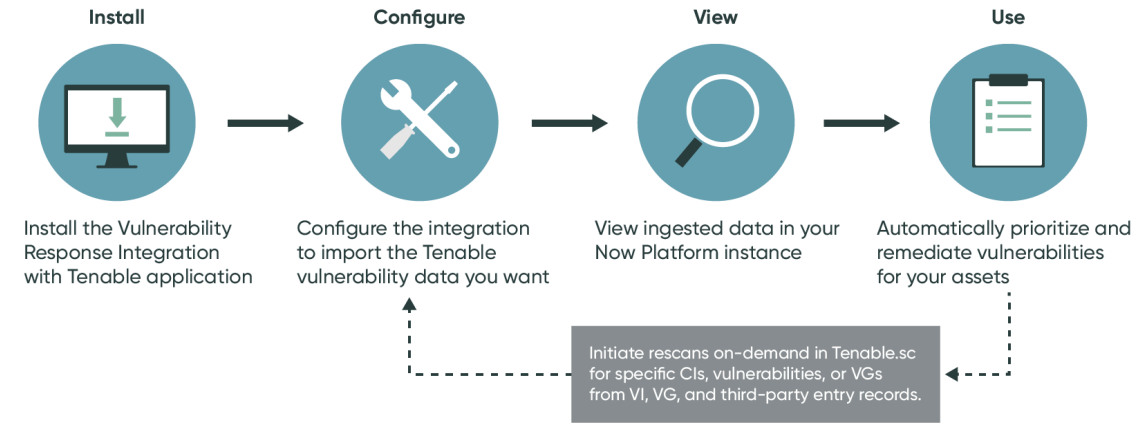
A Integração de vulnerabilidades do Tenable emprega três integrações do Tenable, Tenable.io, Tenable.sc e. Tenable.cs, para importar dados do scanner de terceiros sobre seus ativos e vulnerabilidades. . Integração de Resposta a vulnerabilidades com Tenable a aplicação oferece suporte ao Tenable.sc produto a partir da versão 5,13 e. Tenable.cs produto a partir da versão 5,0.1.

- Tenable.io é uma integração empresarial baseada em nuvem.
- Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Tenable.sc e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente.
- . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server.
- Tenable.cs é uma integração empresarial baseada em nuvem.

. Integração de Resposta a vulnerabilidades com Tenable a aplicação está disponível no ServiceNow Store com uma assinatura separada.

Para listas e descrições das integrações no Integrações de vulnerabilidade da Tenable, consulte Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações e. Tenable.sc integrações com Resposta a vulnerabilidades aplicação.

Integração com a gestão de vulnerabilidades do Tenable



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis para Zurich

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Tenable v3.13.1, v4.1, v5.0.1	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Principais recursos e termos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em seu ServiceNow AI Platform instância quando:

- Uma vulnerabilidade importada de um scanner de terceiros corresponde a um ativo existente (um item de configuração em seu CMDB). O produto Tenable se refere a essas correspondências como **vulnerabilidades** .
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs incompatíveis, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido a um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação.

Entradas de vulnerabilidade de terceiros e plug-ins

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros em seu ServiceNow AI Platform instância. A partir da v24.0 de Resposta a vulnerabilidades, A coluna Softwares na tabela Entradas de vulnerabilidade de terceiros preenche as Enumerações de plataforma comum (CPEs) associadas a um terceiro entrada . Entradas de vulnerabilidade de terceiros do Tenable são ingeridas no Resposta a vulnerabilidades e correspondidos aos ativos existentes listados em seu CMDB. Tenable se refere a entradas de vulnerabilidade de terceiros como **Plug-ins** .

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Item descoberto

Os ativos ingeridos da importação de ativos do Tenable correspondem aos itens de configuração existentes em seu CMDB. Ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in Modelos de classe de IC do CMDB estiver habilitado, o Mecanismo de identificação e reconciliação (IRE) criará ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros de item descoberto serão atualizados para refletir o estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando os dados são importados de uma integração de terceiros, o Vulnerability Response usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os Vits são criados para ajudar você na correção.

Nova verificação e correção

Você pode iniciar um comando de nova varredura direcionada em um item de configuração específico, tarefa de correção ou entrada de terceiros diretamente dos registros de item vulnerável, tarefa de correção e entrada de vulnerabilidade de terceiros em seu ServiceNow AI Platform instância. A Tenable se refere a esta nova verificação como um **verificação de correção** .

Fechar automaticamente o VIS mais antigo

Com o módulo Fechar automaticamente itens vulneráveis obsoletos em seu ServiceNow AI Platform, Você pode limpar itens vulneráveis (VI) mais antigos e obsoletos não encontrados recentemente por suas integrações de terceiros. Movendo esses VIS para **Encerrado** ajuda a reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração de Resposta a vulnerabilidades com Tenable Para fechar automaticamente o VIS obsoleto.

Instância

Este termo se refere a uma ocorrência distinta do seu ServiceNow AI Platform® aplicação.

Integração

Uma integração é uma referência específica do produto a uma integração, como Tenable.io Integração de ativos ou Tenable.sc Integração de plug-in. Essas são as integrações separadas que pertencem a produtos Tenable específicos na Integração de vulnerabilidades do Tenable em sua instância.

Instância de integração

Este termo se refere às integrações separadas do Tenable listadas por Tenable.io e. Tenable.sc produtos.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação de sua integração. O termo é usado para se referir às integrações e aos produtos em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações do Tenable.io e. Tenable.sc produtos em seu ambiente.

. Tenable.io, Tenable.sc e Tenable.cs as integrações também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas, podem ser importados para o. Conformidade de configurações aplicação com Tenable.io produto. Consulte Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações e. Explorando Conformidade de configurações para obter mais informações sobre como esta integração funciona com Conformidade de configurações aplicação.
- A partir da v2.1 do Integrações de vulnerabilidade da Tenable, Crie itens de configuração (ICs) exclusivos que incluem identificadores de partição de rede diferentes para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todos os Tenable.io, Tenable.sc e. Tenable.cs integrações. Você também pode executar trabalhos agendados manualmente sob demanda.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para importações de ativos com Tenable.io, você pode habilitar etiquetas de ativo para organizar e rastrear os ativos listados em seu CMDB em Tenable.io ambiente.
- . Tenable.io, Tenable.sc e. Tenable.cs As integrações permitem que você configure Regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu ServiceNow AI Platform CMDB.
- . Tenable.io, Tenable.sc e. Tenable.cs As integrações permitem que você defina filtros de importação na importação de vulnerabilidades para importar somente as vulnerabilidades desejadas do Tenable. Para Tenable.io, você tem a opção de importar **Corrigido** Vulnerabilidades da Tenable com a importação de vulnerabilidades.
- Para Tenable.sc, você tem a opção de iniciar novas varreduras sob demanda diretamente de um item vulnerável, tarefa de correção e registros de entrada de terceiros em seu ServiceNow AI Platform instância. Se os VIS tiverem sido transferidos para **Encerrado/ Corrigido** mas ainda não foram atualizados em sua instância, você pode verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar uma nova verificação para Tenable.sc integração.

As seções a seguir listam mais detalhes sobre as integrações do Tenable.

Funções necessárias de ServiceNow AI Platform

As tarefas de integração exigem as seguintes funções em seu ServiceNow AI Platform instância.

administrador

O administrador do sistema usa o Assistente de configuração para instalar o. Integração de Resposta a vulnerabilidades com Tenable aplicação. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do Tenable no Assistente de configuração. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações e regras de VR para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Esta função contém a função granular sn_vul_tenable.read_integration e os usuários com esta função podem configurar o. Integração de Resposta a vulnerabilidades com Tenable aplicação.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros do Integração de Resposta a vulnerabilidades com Tenable aplicação.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de tarefa de correção e atribuídos para correção com base em suas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção e Resposta a vulnerabilidades visão geral das regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de pesquisa de item de configuração (IC)

As regras de pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.

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

A seguir Tenable.io as regras de pesquisa são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nome do host
- DNS
- IP

Nota: . Tenable.io As regras de pesquisa de IC priorizam e preenchem os valores de interface de rede não vazios (FDQN, IPV4 e MacAddress) sobre os valores regulares de FDQN, IPV4 e MacAddress para um item descoberto. Quando esses valores de interface de rede estão vazios, os valores regulares de FDQN, IPV4 e MacAddress são preenchidos para um item descoberto.

A seguir Tenable.sc as regras de pesquisa são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Nota: Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando IRE.

. Tenable.cs O ID do recurso em nuvem da regra de pesquisa é enviado com o sistema de base.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, Há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços MAC como parte das regras de pesquisa de IC:

IgnoreIPAddress

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

IgnoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de Item vulnerável do Tenable e das integrações de Ativo do Tenable.

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

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens descobertos.

Etiquetas do ativo

Etiquetas de ativo (também chamadas de marcadores de host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos ativos que deseja verificar. O módulo de etiquetas de ativo permite que você baixe dados de etiqueta de ativo do Tenable.io para sua instância em uma base programada. Os dados do ativo que incluem etiquetas de ativo são extraídos de Tenable.io e transformados usando Transformação de ativo do Tenable.io mapas de transformação de integração.

Todas as etiquetas de ativo são importadas como parte do Tenable.io Integração de ativos. As etiquetas de ativo são usadas para filtragem no Resposta a vulnerabilidades Regras de atribuição e Regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Nota: Execute o. Tenable.io Integração de ativos antes de criar Resposta a vulnerabilidades regras de atribuição ou regras de tarefa de correção no Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local em San Diego e criar San Diego , você também não pode criar um SAN DIEGO Marque e armazene-o na tabela Rótulo do ativo. San Diego e. SAN DIEGO são considerados a mesma etiqueta de ativo pelo sistema. Qualquer marcador importado primeiro é o marcador que será armazenado e reconhecido daqui para frente.
- Usar marcadores de ativo como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas de ativo devem ser usadas somente no Construtor de condições.
- As etiquetas de ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como verdadeira por padrão. Desabilitar marcadores os desabilita em todos ServiceNow AI Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para seu ServiceNow AI Platform® instância. Para obter uma lista das configurações mais usadas, consulte Configurações de recuperação de dados para a Integração de vulnerabilidades do Tenable.

Classificação de prioridade de vulnerabilidade (VPR)

A Classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable importado e usado com uma nova calculadora de risco padrão em Resposta a vulnerabilidades. A Regra de Risco do Tenable é instalada com Integração de Resposta a vulnerabilidades com Tenable Aplicação como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidades de Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta regra de risco está inativa por padrão.

Ao habilitar a regra da calculadora de risco do Tenable, os valores de VPR importados são usados para calcular a Pontuação de risco para itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR é 70%, Ativo é 15% e Criticalidade dos negócios é 15%. Habilitar esta regra da Calculadora de risco do Tenable pode afetar o desempenho de ingestão de dados. Para obter mais informações sobre Resposta a vulnerabilidades E a regra da calculadora de risco do Tenable, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Instalação e configuração

Depois de baixar o. Integração de Resposta a vulnerabilidades com Tenable em ServiceNow® Store A instalação e a configuração são compatíveis com o Assistente de configuração em Resposta a vulnerabilidades. Para obter mais informações, consulte Configurando Resposta a vulnerabilidades Usando o Assistente de configuração.

Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações

. Tenable.io integrações no Integração de Resposta a vulnerabilidades com Tenable as aplicações estão disponíveis no Resposta a vulnerabilidades e. Conformidade de configurações aplicações.

Lista de Tenable.io integrações

O recurso de várias origens é compatível com todos os Tenable.io e. Tenable.sc integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

Tenable.io é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com Tenable.io produto.

. Tenable.io Integração de resultados de conformidade e Tenable.io A integração de preenchimento de resultados de conformidade está inativa por padrão.

Para ativá-los:

1. Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações do Tenable, clique em um nome de integração para abrir o registro e selecione **Ativo** marque a caixa para habilitá-la. Você pode preferir deixar as configurações de programação nos valores padrão para que essas integrações sejam iniciadas.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados do ativo, incluindo etiquetas do ativo, do Tenable.io e processa-o em sua instância. • A partir da v3.0, se o Tenable.io A Integração de resultados de conformidade está ativada, você pode importar dados de avaliação de configuração segura junto com dados de ativos importados. Esses dados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	podem ajudar você a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativo. • A saída desta integração é Itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da v3.0, os dados de avaliação de configuração segura importados da Integração de resultados de conformidade junto com os dados importados da Integração de ativos podem ajudar você a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em seu ServiceNow AI Platform instância. Os dados importados incluem resultados de teste junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Os dados de avaliação de ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de teste for importado e seu ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) é listado em **ICs ignorados** . **Configuração** no registro de execução de integração para esta integração.
Tenable.io Integração de preenchimento de resultados de conformidade	• Quando ativada, esta integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com ativos ausentes listados na tabela [sn_vul_tenable_missing_asset].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância depois que a importação de integração de ativos é concluída com sucesso. • Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos aos dados de avaliação de configuração correspondentes.
Tenable.io Integração de credenciais de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API Credenciais. • A saída desta integração são credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas no ServiceNow AI Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante uma nova verificação. Esta integração recupera disponível Tenable.io credenciais a serem usadas para novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do Tenable.io produto. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por um Tenable.io execução de integração. • Essa importação garante que o Tenable.io Identificadores (dez IDs) são atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base nos filtros de gravidade do Tenable.io e processa-o em sua instância. Itens vulneráveis são criados para registros de detecção que estão no **Aberto** e. **Reaberto** porque esses registros

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **Corrigido** , mas itens vulneráveis não são criados para **Corrigido** Detecções por padrão, porque a Tenable considera **Corrigido** vulnerabilidades **Mitigado** . • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidades fixas** Está ativado no Assistente de configuração, novos VIS são criados no **Corrigido** estado para que você tenha visibilidade das detecções que as criaram. Porque os VIS foram criados para **Corrigido** detecções que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para isso **Corrigido** as detecções atualizam somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. Esta execução de integração está programada. É uma integração encadeada, o que significa que, depois que uma execução é concluída com sucesso, a integração de vulnerabilidades em aberto descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações sobre as execuções de integração de vulnerabilidades: • **Total de blocos:** Número total de blocos gerados pela Tenable • **Blocos disponíveis:** Número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de vulnerabilidades em aberto	• Esta integração é acionada após a conclusão bem-sucedida do Tenable.io Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.io e processa-o em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Novo/reaberto** Itens vulneráveis (VIS). Ele também cria itens de configuração e entradas de terceiros, se eles não existirem. A Tenable considera vulnerabilidades ativas **Cumulativo** (atual). • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações sobre as execuções de integração de vulnerabilidades: • **Total de blocos:** Número total de blocos gerados pela Tenable • **Blocos disponíveis:** Número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de metadados /scan	Esta integração recupera metadados do endpoint /vars. Extrai informações de verificação com base em last_schedule_id dos dados de ativos existentes em Tenable.io. A integração do endpoint /varns de Tenable.io envolve as seguintes etapas de implementação: • **Criação de tabela** : Uma nova tabela personalizada, **sn_vul_tenable_scan** , é criado para armazenar metadados de verificação recuperados do Tenable.io endpoint /verifica. Isso inclui detalhes como ID de verificação, nome, status, hora de início, hora de término, e tipo de verificação. • **Associação de dados** : Um campo de referência é estabelecido entre os itens descobertos (itens de configuração ou vulnerabilidades) e o registro de verificação mais recente correspondente no **sn_vul_tenable_scan** tabela. Este vínculo permite que você:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	○ Exiba as informações de verificação mais recentes associadas a cada item descoberto. ○ Melhorar o contexto para triagem de vulnerabilidades e decisões de correção. ○ Aprimore a auditabilidade e os recursos de emissão de relatórios mantendo um registro histórico das atividades de verificação.

Tenable.sc integrações com Resposta a vulnerabilidades aplicação

. Tenable.sc integrações no Integração de Resposta a vulnerabilidades com Tenable aplicação.

Começando com Resposta a vulnerabilidades V20.0, se um ativo for verificado por um agente, a coluna "Existe agente" na lista de itens descobertos exibirá o valor como "verdadeiro". Indica que a verificação é autêntica.

Lista de Tenable.sc integrações

O recurso de várias origens é compatível com todos os Tenable.io e. Tenable.sc integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também pode instalar e configurar o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

- Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Tenable.sc e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente.
- . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativos importados, a Integração de ativos do Tenable.sc o produto é composto por duas integrações. **. Tenable.sc Integração de ativos em aberto** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativo** (atual), ou **Aberto** . Os itens vulneráveis (VIS) que são criados em sua instância com estes dados de ativo importados são considerados abertos, ou seja, em **Aberto** estado. Esses itens vulneráveis exigem investigação e podem precisar de correção. **. Tenable.sc Integração de ativos fixos** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Mitigado** (não está mais vulnerável) ou **Corrigido** . Os itens vulneráveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	para esses ativos fazem a transição do **Aberto** estado para **Encerrado/Corrigido** em sua instância, porque os resultados das verificações mostram que elas não estão mais vulneráveis. • Recupera todos os dados de ativos do Tenable.sc e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Ativos. • A saída desta integração é Itens descobertos. • O filtro de consulta do Tenable selecionado no Assistente de configuração também se aplica ao Tenable.sc Integração de ativos. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do Tenable.sc produto. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por um Tenable.sc execução de integração. • Essa importação garante que o Tenable.sc Identificadores (dez IDs) são atuais e somente vulnerabilidades ativas são importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base nos filtros de gravidade do Tenable.sc e processa-o em sua instância. Itens vulneráveis são criados para registros de detecção que estão no **Aberto** e. **Reaberto** porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **Corrigido** , mas itens vulneráveis não são criados para **Corrigido** Detecções por padrão, porque a Tenable considera **Corrigido** vulnerabilidades **Mitigado** . • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidades fixas** Está ativado no Assistente de configuração, ele cria VIS no **Corrigido** estado para que você tenha visibilidade das detecções que as criaram. Como os VIS são criados para **Corrigido**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	detecções que não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para isso **Corrigido** as detecções atualizam somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem. Esta execução de integração é uma execução programada. É uma integração encadeada, o que significa que depois que uma execução é concluída com sucesso, o. Tenable.sc A Integração de vulnerabilidades em aberto descrita a seguir é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de vulnerabilidades em aberto	• Esta integração é acionada após a conclusão bem-sucedida do Tenable.sc Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados no Tenable.sc e processa-o em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Atualizar/criar novo** Itens vulneráveis (VIS) se eles não existirem. Ele também cria itens de configuração e entradas de terceiros, se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de credenciais de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API Credenciais. • A saída desta integração são credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas no ServiceNow AI Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de preenchimento importa todas as vulnerabilidades abertas e corrigidas que possam ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está inativa por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, você pode preferir programar as Integrações de vulnerabilidades fixas e vulnerabilidades abertas do Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é: ○ **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem. ○ . **Atualizar/criar novo** Itens vulneráveis (VIS) se eles não existirem. Ele também cria itens de configuração e entradas de terceiros, se eles não existirem.

Autenticação de usuário e. Tenable.sc

A autenticação de usuário é compatível com ServiceNow AI Platform® e versão 5,13 do Tenable.sc produto. A autenticação do usuário será necessária se você estiver usando a versão 5,12 e anterior do Tenable.sc produto.

Quando você seleciona a autenticação de usuário para Tenable.sc tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Falha: A validação do token falhou . Nenhuma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ação será necessária se esta mensagem for exibida. Tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Tenable.cs integrações com Resposta a vulnerabilidades e. Contêiner de Resposta a vulnerabilidades aplicação

. Tenable.cs integrações no Integração de Resposta a vulnerabilidades com Tenable Estão disponíveis no Vulnerability Response e Contêiner de Resposta a vulnerabilidades aplicações.

A partir da v20.0 Resposta a vulnerabilidades Se um ativo for verificado por um agente, a coluna "Existe agente" na lista Itens descobertos exibirá "Verdadeiro", indicando que a verificação é autêntica.

Lista de Tenable.cs integrações

O recurso de várias origens é compatível com todos os Tenable.io, Tenable.sc e Tenable.cs integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também pode instalar e configurar o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

Tenable.cs é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com Tenable.cs produto.

Integrações do Tenable.cs

Integração	Descrição
Tenable.cs Integração de ativos de contêiner em nuvem	• Recupera todos os dados de ativos de contêiner do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. Coordena as chamadas de mensagem REST para a API de ativo. A saída desta integração são imagens de contêiner descobertas, imagens do Docker e repositórios de contêiner.
Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta	Quando ativada, esta integração é executada automaticamente depois que a integração de ativos de contêiner é concluída com sucesso como parte de uma execução de integração encadeada. • Recupera dados de vulnerabilidade do contêiner com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Novos/ReopenedContainer Vulnerable Items (CVIS). Se eles não existirem, ele também criará imagens de contêiner descobertas, imagens do docker, repositórios de contêiner, descobertas de imagem,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.cs

Integração	Descrição
	entradas de terceiros, e Vulnerabilidades e exposições comuns (CVE).
Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida	Esta integração é acionada após a conclusão bem-sucedida do Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta. • Recupera dados de vulnerabilidade do contêiner com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Novos/ReopenedContainer Vulnerable Items (CVIS). Se eles não existirem, ele também criará imagens de contêiner Discover, imagens do docker, repositórios de contêiner, descobertas de imagem, entradas de terceiros, e CVEs. As descobertas de imagem são criadas no estado Encerrado.
Tenable.cs Integração de vulnerabilidades de host na nuvem	• Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Itens vulneráveis novos/ reabertos (VIS). Se eles não existirem, ele também criará itens de configuração, entradas de terceiros e CVEs. Detecções de vulnerabilidades são criadas no estado Aberto.
Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida	Esta integração é acionada após a conclusão bem-sucedida do Tenable.cs Integração de vulnerabilidades de host na nuvem. • Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Fechar Itens Vulneráveis (VIS). Se eles não existirem, ele também criará itens de configuração, entradas de terceiros e CVEs. Detecções de vulnerabilidades são criadas no estado Encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticação de usuário e. Tenable.sc

A autenticação de usuário é compatível com ServiceNow AI Platform® e versão 5,13 do Tenable.sc produto. A autenticação do usuário será necessária se você estiver usando a versão 5,12 e anterior do Tenable.sc produto.

Quando você seleciona a autenticação de usuário para Tenable.sc tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Falha: A validação do token falhou . Se esta mensagem for exibida, nenhuma ação será necessária. Tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Preparando para a Integração de vulnerabilidades do Tenable

Prepare-se para ServiceNow® Integração do Tenable Vulnerability executando as tarefas de configuração a seguir.

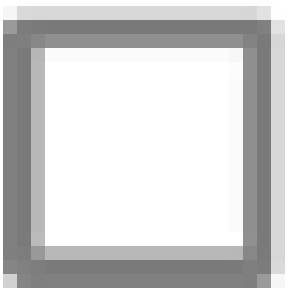
Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. Para uma instalação e configuração suaves do Integração de Resposta a vulnerabilidades com Tenable, você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para seu ServiceNow AI Platform® instância.

Nota: Se você estiver importando dados com a integração criada pelo Tenable e quiser começar a usar o. ServiceNow® Integração de Resposta a vulnerabilidades com a Tenable, consulte

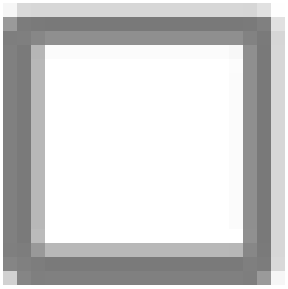
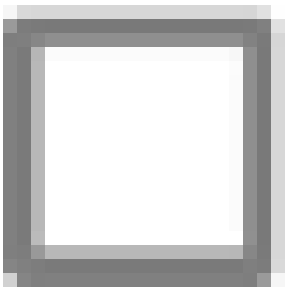
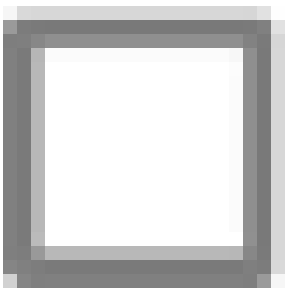
Para obter informações atuais de limpeza e migração de dados da integração criada pelo Tenable para a integração criada por ServiceNow, consulte Diretrizes para migrar da Integração do Tenable Vulnerability Response para a Integração do ServiceNow Vulnerability Response com o Tenable [KB0960106] artigo.

Função necessária: Administrador para baixar e instalar a aplicação.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instalar Resposta a vulnerabilidades. Esta integração requer a versão 12,1 de Resposta a vulnerabilidades ou posterior.

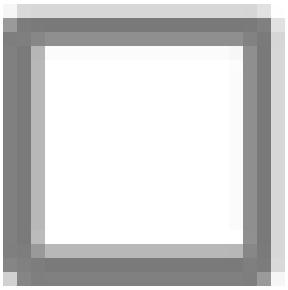
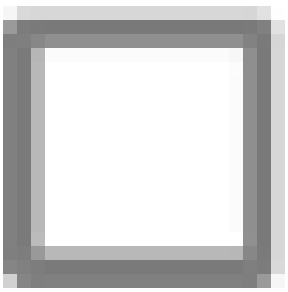
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe o. Integração de Resposta a vulnerabilidades com Tenable aplicação para seu ServiceNow AI Platform® instância. . Integração de Resposta a vulnerabilidades com Tenable a aplicação oferece suporte ao Tenable.sc produto a partir da versão 5,13 e. Tenable.cs produto a partir da versão 5,0.1. .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou, se precisar de assistência, entre em contato com ServiceNow® Suporte técnico.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **administrador** O administrador do sistema usa o Assistente de configuração para instalar o. Integração de Resposta a vulnerabilidades com Tenable aplicação. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do Tenable. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Configura todos os aplicativos e regras de VR e configura integrações de terceiros. **sn_vul_tenable.configure_integration** Pode configurar a Integração de vulnerabilidades do Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration** Pode exibir (ler) registros da Integração de vulnerabilidades do Tenable. **Grupo de Resposta a vulnerabilidades** Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo Resposta a vulnerabilidades

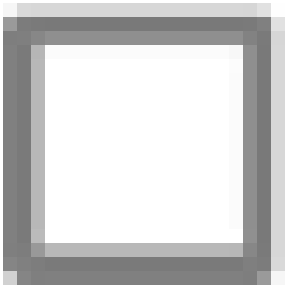
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Crie um grupo de usuários . As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.
	Para promover um desempenho aprimorado para sua primeira importação, você pode preferir desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não usá-las. Essas calculadoras, além de todas as que você definiu, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade . • Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, você pode preferir Desabilitar regras de negócios relacionadas a notificações, conforme descrito em Importar modificações para a Integração de vulnerabilidades do Tenable.
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Integração de Resposta a vulnerabilidades com Tenable e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente. . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . • Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ativa etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Obtenha credenciais do Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos Tenable para que você tenha acesso a eles. Tenable.io Requer acesso de administrador com um atributo de permissão maior ou igual a 64. Tenable.sc Requer acesso de analista de segurança ou gerente. **Nota:** A partir da v3.8 de Integração de Resposta a vulnerabilidades com Tenable acessando Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instale o. Integração de Resposta a vulnerabilidades com Tenable Usando o Assistente de configuração.

Instale o. Integração de Resposta a vulnerabilidades com Tenable Usando o Assistente de configuração

Antes de executar o. ServiceNow® Integração de vulnerabilidades do Tenable, você precisa baixar o. Integração de Resposta a vulnerabilidades com Tenable aplicação do ServiceNow Store E instale e configure-o usando o Assistente de configuração no Resposta a vulnerabilidades aplicação.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens da check-list em Preparando para a Integração de vulnerabilidades do Tenable.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidades (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar a aplicação no Assistente de configuração depois que ela for instalada.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações que estão disponíveis para instalação em sua instância serão exibidas.

2. Localize **Tenable (plataforma Tenable)** lado a lado e clique **Instalar** .

   Esta ação instala o. Integração de Resposta a vulnerabilidades com Tenable aplicação que você baixou do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Siga as instruções fornecidas no Assistente de configuração para continuar com a instalação.
4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** No Assistente de configuração para continuar com a configuração. Para obter mais informações para complementar os prompts fornecidos no Assistente de configuração, consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração.

Configurações de recuperação de dados para a Integração de vulnerabilidades do Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar do ServiceNow® Integração de vulnerabilidade do Tenable ao seu ServiceNow AI Platform® instância.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Instâncias de Integração** e selecione sua integração, Tenable.io, Tenable.sc ou Tenable.cs.

Na página Instância de integração exibida, selecione os Parâmetros de instância de integração para exibir uma lista de parâmetros ou as guias Integrações de vulnerabilidade para uma programação, Detalhes DO REST, Detalhes DE integração, Fontes de dados e informações de execução de integração.

Gravidade comum e configurações de recuperação e filtros para Tenable.io, Tenable.sc e. Tenable.cs em seu ServiceNow AI Platform instância

As configurações a seguir estão disponíveis para Tenable.io, Tenable.sc e Tenable.cs integrações em seu ServiceNow AI Platform instância. Essas e outras definições de configuração são exibidas na página Instância de integração do seu ServiceNow AI Platform instância. Você pode preferir deixar essas configurações em seus padrões nas primeiras execuções de integração.

Tenable.io

insert_fixed

Se você habilitar **insert_fixed** No Assistente de configuração para a integração Importação de vulnerabilidades, novos VIS são criados para detecções no **Corrigido** estado que não existe em sua instância.

severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_high

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de nível médio do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informações do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de baixo nível do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

tamanho

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados do Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1 000. O tamanho máximo é 10 000.

num_assets

O número máximo de vulnerabilidades por bloco exportado do Tenable.io Vulnerabilidades corrigidas e. Tenable.io Integrações de vulnerabilidades em aberto. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pelo Tenable.io Integração de ativos. O padrão é 1 000.

Tenable.sc

async_request

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Uma vez habilitado, este parâmetro é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request ao existente Tenable.sc instâncias de integração. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

insert_fixed

Se você habilitar **insert_fixed** No Assistente de configuração para a integração Importação de vulnerabilidades, novos VIS são criados para detecções no **Corrigido** estado que não existe em sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Os filtros de consulta são configurados no console do Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração em seu ServiceNow AI Platform instância. Esses filtros são aplicados ao recuperar os dados do Tenable.sc integrações.

Tenable.cs

compute_severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_high

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de nível médio do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informações do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de baixo nível do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

container_severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de contêiner de severidade crítica do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_high

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de contêiner de gravidade de alto nível do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber Vulnerabilidades de contêiner de gravidade de nível médio do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber Vulnerabilidades de gravidade no nível de informações das Vulnerabilidades de contêiner do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de contêiner de gravidade de baixo nível do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

asset_page_limit

Esta configuração define o número de registros de ativos de contêiner a serem incluídos no conjunto de resultados do Tenable.cs Integração de ativos de contêiner em nuvem. O valor padrão é 1 000. O tamanho máximo é 1 000.

vuln_page_limit

Esta configuração define o número de registros de vulnerabilidades a serem incluídos no conjunto de resultados do Tenable.cs Integração de vulnerabilidades de host em nuvem aberta, Tenable.cs Integração de vulnerabilidades de host em nuvem fixa, Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta, e. Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida. O valor padrão é 1 000. O tamanho máximo é 10 000.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagens REST para a Integração de vulnerabilidades do Tenable

. ServiceNow® As mensagens REST da Integração de vulnerabilidades do Tenable são usadas para fazer chamadas para a API do Tenable.

Tenable.io Mensagem REST de ativos

. Tenable.io A mensagem REST DE ativos recupera informações de ativos para Tenable.io Integração de ativos. As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tenable.io Mensagem REST de plug-ins

. Tenable.io A mensagem REST DE plug-ins recupera informações de plug-in para Tenable.io Integração de plug-in. As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

. Tenable.io A mensagem REST DE vulnerabilidades recupera informações de vulnerabilidade para vulnerabilidades abertas e encerradas do Tenable.io Integração de vulnerabilidades. As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST DE consultas DO Tenable.sc

A mensagem REST Consultas do Tenable.sc recupera as informações do filtro de consulta da integração de ativos do Tenable.sc e da integração de vulnerabilidades do Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

. Tenable.sc A mensagem REST do plug-in recupera informações de plug-in para Tenable.sc Integração de plug-ins. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas Tenable.sc para recuperar informações de plug-ins.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado pelo código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore,TemporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, nome, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, família, riskfator,	Indica a lista de campos importados da Tenable.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
	cpe, veeTambém, solução, exploitAvailable, exploitFrameworks, tipo, copyright, versão, sourceFile, dependências, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	

Tenable.sc Mensagem REST de vulnerabilidades

. Tenable.sc A mensagem REST DE vulnerabilidades recupera informações de vulnerabilidade do Tenable.sc Integração. Mudanças no método Buscar vulnerabilidades ou Buscar vulnerabilidades com patch da mensagem REST ou, começando com v14.0 Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable, o registro Buscar vulnerabilidades de preenchimento afetam as solicitações feitas Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Verificar mensagem REST de credenciais

Tenable.sc Mensagem REST da política

. Tenable.sc A mensagem REST POST DA política adiciona uma política para plug-ins solicitados. A política gerada é usada em Tenable.sc solicitações de verificação.

Tenable.sc Verificar mensagem REST

A mensagem REST POST DA verificação do Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tenable.sc Mensagem REST do resultado da verificação

. Tenable.sc OBTER mensagem REST do resultado da verificação fornece detalhes da verificação gerada usando a mensagem REST DA verificação. Ele usa o scanResultId na resposta das mensagens REST da verificação e recupera os detalhes da verificação para a verificação acionada.

Tenable.sc Verificar credenciais

. Tenable.sc A mensagem REST DE credenciais de verificação recupera as informações de credenciais do Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	id,nome,descrição,tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis do Tenable.sc Mudanças em qualquer um dos parâmetros não são recomendadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs GraphQl mensagem REST: O. Tenable.cs A mensagem REST do GraphQl recupera informações de ativos do contêiner, host e informações de vulnerabilidade do contêiner para Tenable.cs Integração. As mudanças no registro Obter ativos do contêiner da mensagem REST, Buscar vulnerabilidades do contêiner, Buscar vulnerabilidades do método de computação afetam as solicitações feitas Tenable.cs para recuperar informações de ativos e vulnerabilidades.

Transformação de dados para a Integração de vulnerabilidades do Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de gravidade normalizados são instalados no módulo Mapeamento de gravidade normalizado. Esses mapas transformam os níveis de severidade importados do Tenable em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de gravidade, consulte Criar um mapa de gravidade de resposta a vulnerabilidades em Resposta a vulnerabilidades documentação.

Importação de ativos do Tenable.io

Os dados de ativos importados são carregados primeiro na tabela Importação de ativos do Tenable.io [sn_vul_Tenable_io_asset_import].

O mapa de transformação de integração de ativos do Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de Ativo do Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar `Transformação de ativo do Tenable.io` .

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos de mapa de transformação de ativo do Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e mapeia para o registro do item descoberto e é usada para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor ip para o campo ip_address no registro do item descoberto.
u_mac_addresses	mac_address	Mapeia o primeiro valor mac_address para o campo de endereço mac no registro do item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor de fqdn para o campo fqdn no registro do item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netbios para o campo netbios no registro do item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de mapa de transformação de ativo do Tenable.io

Campo de origem	Campo de destino	Descrição
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo SO no registro do item descoberto.
(Anterior à v14.0 Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable) u_last_scan_time	last_scan_date	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tempo e finalidade do script do mapa de transformação de ativos do Tenable.io

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores no host e verifica se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados.Este script é para uso interno e não é recomendável modificá-los ou excluí-los.

Integração de plug-ins do Tenable.io

O mapa de transformação de plug-ins do Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins do Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE a transformação do plug-in Tenable.io.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A carga útil dos plug-ins do Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plug-in_import. O campo Atributos é analisado e mapeado para os registros da tabela de entrada de terceiros conforme listado na tabela a seguir.

Campo de origem	Campo de destino	Descrição
id	id	Mapeia o ID da origem e adiciona o prefixo DEZ a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será DEZ-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	A origem da entrada de terceiros importada (TPE) é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família de plug-in para a coluna de categoria
plug-in_modified_date	last_modified	Mapeia plug-in_modified_date para o último campo modificado.
plug-in_publication_date	date_published	Mapeia plug-in_publication_date para a data de publicação.
has_patch	remediation_type	Mapeia o tipo de correção do valor has_patch.
sinopse	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__score	pontuação	Mapeia a pontuação base do CVSS (Common Vulnerability Score System, sistema de pontuação comum) para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
exploit_available	exploração	Mapeia exploit_available fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9–10 – Crítico • 7–9 – Alto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		• 4–7 – Médio • 0–4 - Baixo
vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
vpr.drivers.ameaça_recency	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
cvss_temporal_score	cvss_temporal_score	Mapeia a pontuação temporal do CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mapeia a pontuação temporal do CVSS v3.
risk_factor	source_severity	Mapeia para a gravidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para nomear na tabela de entrada de terceiros.
stig_severity	stig_severity	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se as mesmas Vulnerabilidades e exposições comuns (CVE) na tabela de entrada de NVD (sn_vul_nvd_entry) forem encontradas, ele associará a vulnerabilidade atual à entrada NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
lance	A lista de bugs traqs é adicionada como referência.
see_also	A lista de URLs é adicionada como referência.
refsCruzadas	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores na entrada de terceiros e verifica se a entrada de terceiros existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele pega a saída da integração de plug-ins do Tenable.io e a transforma em ServiceNow AI Platform entradas de vulnerabilidade de terceiros. Qualquer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mudança nesta inclusão de script pode alterar a transformação dos dados de plug-ins do Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades do Tenable.io

O mapa de transformação de item vulnerável do Tenable.io é usado para transformar informações de vulnerabilidades abertas e corrigidas importadas do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades do Tenable são processados.

O mesmo mapa de transformação é usado para a Integração de vulnerabilidades fixas do Tenable.io e a Integração de vulnerabilidades abertas do Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE Mapa de transformação de item vulnerável do Tenable.io .

Campo de origem	Campo de destino	Descrição
u_asset.uuid	id	O UUID é mapeado para o campo ID do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo ipv4 é mapeado para o campo Endereço ip do registro cmdb_ci.
u_asset.last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação de autenticação do registro cmdb_ci.
u_asset.mac_addess	mac_address	O endereço MAC é mapeado para o campo de endereço mac do host do registro cmdb_ci.
u_asset.netbios_name	netbios	NetBIOS é mapeado para o campo netbios do registro cmdb_ci.
u._plug-in.cvss3_base_score	v3_base_score	A pontuação de base do CVSS v3 é mapeada para a pontuação de base v3 do registro de entrada de terceiros.
u._plug-in.cvss3_temporal_score	v3_temporal_score	A pontuação temporal CVSS v3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u._plug-in.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u._plug-in.cvss_temporal_score	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_plug-in.family	categoria	Mapeia a família de plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plug-in.modified_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_plug-in.publication_date	date_published	A data de publicação é mapeada para o campo Data de publicação do registro de entrada de terceiros.
u_plug-in.risk_factor	source_severity	O fator de risco é mapeado para o campo source_severity do registro de entrada de terceiros.
u_plug-in.solution	solução	A solução é mapeada para o campo de solução do registro de entrada de terceiros.
u_plug-in.synopsis	ameaça	A sinopse é mapeada para o campo Ameaça do registro de entrada de terceiros.
u_severity_id	prioridade	A prioridade é mapeada para o ID de gravidade da carga. O valor padrão é 5.
u_plug-in.exploit_available	exploração	Mapeia exploit_available fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		• 9–10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_plug-in.vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_sources_last28	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_intensity_last28	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_recency	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plug-in.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plug-in.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.
u_plug-in.family_id	Family_id	Mapeia o ID da família de plug-in para a coluna family_id na tabela de entrada de terceiros.
porta	porta	A porta é mapeada para o campo de porta do registro do item vulnerável.
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro do item vulnerável.
u_first_found	first_found	Primeiro encontrado é mapeado para o primeiro campo encontrado do registro de item vulnerável.
u_last_found	last_found	Encontrado pela última vez é mapeado para o último campo encontrado do registro de item vulnerável.
u_state	estado	O estado é mapeado para o campo Estado no registro de item vulnerável
[script]	origem	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integration_instance	Integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para nomear na tabela de entrada de terceiros.
u_plug-in.stig_severity	stig_severity	Mapeia a severidade do stig do plug-in para a coluna Severidade do stig na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se o mesmo CVE na tabela de entrada de NVD (sn_vul_nvd_entry) for

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
	encontrado, ele associará a vulnerabilidade atual à entrada de NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
lance	A lista de bugs traqs é adicionada como referência.
see_also	A lista de URLs é adicionada como referência.
refsCruzadas	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	TTriggers Tenable IO Vulnerabilities Processador que importa dados do Tenable.io usando o conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela Itens vulneráveis e na tabela de vulnerabilidades de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Verifica se a entrada e as detecções de terceiros existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Não é este script é para uso interno, e modificá-lo ou excluí-lo não é recomendado.
OnComplete (quando um conjunto de importação conclui a transformação).	Atualiza a contagem de ICs, Vits e detecções conforme importados do Tenable.io. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Importação de ativos do Tenable.sc

Os dados do ativo importados do Tenable.sc são carregados primeiro na tabela Importação de ativos do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos do Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de Ativo do Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE Transformação de ativo do Tenable.sc .

Campo de origem	Campo de destino	Descrição
u_uuid	id	O uuid não é preenchido a partir da API Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo uuid exclusivo para ativos e mapeá-lo para o registro cmdb_ci.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_ip	ip_address	Mapeia o campo ip da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço mac da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.
u_netbiosname	netbios	Mapeia o campo netbios da API para o campo netbios no registro cmdb_ci.
u_oscpe	os	As informações do SO são extraídas do atributo oscpe na carga e as mapeiam para o campo SO no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.
u_lastauthrun e u_lastunauthrun	last_scan_date	O lastauthrun é extraído da API Tenable ou lastunauthrun. O campo last_scan_date no registro do item descoberto é preenchido com base no valor que aparece na carga.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores no host e verifica se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Importação de plug-ins do Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela Importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plug-in_import). O Mapa de transformação do plug-in Tenable.sc é usado para transformar as informações de plug-ins que foram importadas. As mudanças nesta transformação alteram como os dados da importação do plug-in Tenable são processados. Para acessar este mapa

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar Mapa de transformação do plug-in Tenable.sc .

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será DEZ-12345.
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	O TPE importado desta integração tem o Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
u_family	categoria	Mapeia o campo de nome no objeto da família do plug-in para a coluna de categoria.
u_plug-in_modified_date	last_modified	Mapeia plug-in_modified_date para o último campo modificado.
u_plug-in_publication_date	date_published	Mapeia plug-in_publication_date para a data de publicação.
u_has_patch	Remediation_type	Mapeia o tipo de correção do valor has_patch.
u_synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_base_score	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solution	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_temporal_score	cvss_temporal_score	Mapeia a pontuação temporal do CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mapeia a pontuação temporal do CVSS v3.
u_risk_factor	gravidade da origem	Mapeia para a gravidade de origem na tabela de entrada de terceiros.
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia o exploitAvailable fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
u_vpr_score	source_risk_score	Mapeia a pontuação de VPR do scanner para a pontuação de risco

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9–10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_vpr_context	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id:"threat_sources_last_28"]	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
u_vpr_context[id:"threat_intensity_last_28"]	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_vpr_context	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceira parte.
u_vpr_context	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stig_severity	stig_severity	Mapeia o campo stig_severity no plug-in para stig_severity na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_family.id	family_id	Mapeia o plug-in family_id para family_id na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como referência.
u_see_also	A lista de URLs é adicionada como referência.
u_exploit_frameworks	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele pega a saída da integração de plug-ins do Tenable.sc e a transforma em ServiceNow entradas de vulnerabilidade de terceiros. Qualquer mudança nesta inclusão de script pode alterar a transformação dos dados de plug-ins do Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades do Tenable.sc

O Mapa de transformação de vulnerabilidades abertas do Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades abertas do Tenable.sc, e o mapa de transformação de vulnerabilidades fixas do Tenable.sc é usado para transformar dados importados da Integração de vulnerabilidades fixas do Tenable.sc.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/abertas do Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e fixas do Tenable.sc, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Instâncias de Integração** > **Integração de vulnerabilidades fixas/abertas do Tenable.sc** > **Fontes de dados** > **Vulnerabilidades abertas/corrigidas do Tenable.sc** > **Transformações**.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada de terceiros.
u_riskfactor	source_severity	Este campo é mapeado para source_severity no registro de entrada de terceiros.
u_severity	prioridade	O campo Prioridade é mapeado com a severidade. O valor padrão é 5.
u_hasbemitigado	estado	Foi mitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os VIS estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo ip do host da tabela cmdb_ci.
u_port	porta	A porta é mapeada para o campo de porta do registro do item vulnerável.
u_protocol	protocolo	O protocolo é mapeado para o campo de porta do registro do item vulnerável.
u_firstSeen	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro VI.
u_lastSeen	last_found	O último valor visto é mapeado para o último campo encontrado do registro VI.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo Exploit no registro de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_synopsis	ameaça	A sinopse é mapeada para o campo Ameaça no registro de entrada de terceiros.
u_description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_solution	solução	A solução é mapeada para o campo de solução no registro de entrada de terceiros.
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada de terceiros.
Pontuação u_temporal	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_cvssv3basecore	v3_base_score	Cvssv3basescocore é mapeado para a pontuação de base v3 no registro de entrada de terceiros.
pontuação u_cvsstemporalscore	v3_temporal_score	A pontuação temporal Cvssv3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u_pluginpublidata	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosName	netbios	NetbiosName é mapeado para o campo NETBIOS do registro cmdb_ci.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_ip	ip	O IP é mapeado para o campo IP do registro cmdb_ci.
exclusividadeHost	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o uuid do host.
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugintext	prova	O texto do plug-in é mapeado para prova no registro tpe.
[script]	origem	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm Tenable.sc como origem.
[script]	integration_instance	Integration_instance é o nome da instância da qual o item vulnerável é importado.
u_vpr_score	source_risk_score	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_vpr_context	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		na tabela de entrada de terceiros.
u_vpr_context	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id:"threat_sources_last_28]	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
u_vpr_context[id:"threat_intensity_last_28]	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_vpr_context	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceira parte.
u_vpr_context	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stigseverity	stig_severity	Mapeia o campo stig_severity no plug-in para stig_severity na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	family_id	Mapeia o plug-in family.id para family_id na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela third_party_entry é preenchida com base em exploit_available e v3_attack_vector das colunas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
u_cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se o mesmo CVE na tabela de entrada de NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada de NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.
u_bid	A lista de bugs traqs é adicionada como referência.
u_cpe	A lista de CPEs é adicionada como referência.
u_seealso	A lista de URLs é adicionada como referência.
u_xrefs	A lista de X-refs é adicionada como referência.
u_exploitframeworks	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Função usada para atualizar os valores na vulnerabilidade e verificar se ela existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de novos VIS criados e de VIS que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Importação de ativo de contêiner

Os dados de ativos importados são carregados primeiro no Tenable.cs Importação de ativos de contêiner [sn_vul_tenable_cs_container_asset_import].

. Tenable.cs O mapa de transformação de ativo de contêiner é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação do ativo do contêiner é processada. Para acessar este Mapa de transformação, navegue até Conjuntos para importação do sistema > Mapas de transformação. Pesquisar Tenable.cs Transformação de ativo de contêiner.

As tabelas a seguir listam os campos do mapa de transformação por integração.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos do mapa de transformação de ativo de contêiner

Campo de origem	Campo de destino	Descrição
u_digest	Image_id	A Tenable fornece um resumo exclusivo para os ativos do contêiner e mapeia para a imagem do contêiner descoberto e o registro de imagem do docker e é usado para pesquisa de IC.
u_digest	Image_digest	A Tenable fornece um resumo exclusivo para os ativos do contêiner e mapeia para a imagem do contêiner descoberto e o registro de imagem do docker e é usado para pesquisa de IC.
u_name	nome	Mapeia para o campo de nome do registro de imagem do docker.
u_positoryuri	nome	Mapeia para o registro do repositório de contêiner
u_positoryuri	reposição	Mapeia para o registro de imagem do contêiner descoberto.
u_virtualmachines	host_list	Mapeia para o registro de imagem do contêiner descoberto
u_labels	Image_labels	Mapeia o primeiro valor do SO para o campo SO do registro do item descoberto.
u_clusters	image_cluster	Mapeia para o registro de imagem do contêiner descoberto
u_imagetags	marcadores	Mapeia para o registro de imagem do contêiner descoberto
u_cloudprovider	cloud_providers	Mapeia para o registro de imagem do contêiner descoberto
u_accountid	cloud_account_ids	Mapeia para o registro de imagem do contêiner descoberto
u_region	cloud_regions	Mapeia para o registro de imagem do contêiner descoberto
u_operatingsystem	os	Mapeia para o registro de imagem do contêiner descoberto
u_scantime	last_scan_date	Mapeia para o registro de imagem do contêiner descoberto

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Tempo e finalidade do script do mapa de transformação de ativos do contêiner

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Uma função usada para atualizar valores no host e verificar se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Importação de vulnerabilidade do contêiner

Os dados de vulnerabilidade do contêiner importados são carregados primeiro no Tenable.cs Tabela de importação de vulnerabilidade de contêiner [sn_vul_tenable_cs_container_vuln_import].

. Tenable.cs O mapa de transformação de vuln do contêiner é usado para transformar as informações de vulnerabilidade do contêiner importado. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação de vulnerabilidade do contêiner é processada. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar Tenable.cs Transformação de vuln do contêiner.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
[script]	Image_id	O resumo é extraído do campo Resource.ID da API e mapeado para o campo image_id da imagem do contêiner descoberto e do registro de imagem do docker.
[script]	Image_digest	O Digest é extraído do campo Resource.ID da API e mapeado para o campo image_digest da imagem do contêiner descoberto e do registro de imagem do docker.
[script]	nome	As informações do repositório são extraídas do campo de nome e mapeadas para a imagem do docker e o registro do repositório de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
[script]	reposição	As informações do repositório são extraídas do campo de nome e mapeadas para o registro de imagem do contêiner Discover.
Rótulos.u_resource.Rótulos	Image_labels	Mapeia para o registro de imagem do contêiner descoberto
u_resource.CloudProvider	cloud_providers	Mapeia para o registro de imagem do contêiner descoberto
u_resource. AccountId	cloud_account_ids	Mapeia para o registro de imagem do contêiner descoberto
u_resource.Region	cloud_regions	Mapeia para o registro de imagem do contêiner descoberto
u_vulnerability. Id	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de entrada de terceiros será DEZ-12345.
u_vulnerability. ID da descrição	sumaryid	Mapeia para o registro de entrada de terceiros. Ou registro CVE.
u_vulnerability.severity	v4_base_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprScore	source_risk_score	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprSeverity	source_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.AttackVector	v4_attack_vector	Mapeia para o registro de entrada de terceiros.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Mapeia para o registro de entrada de terceiros.
[script]	origem	A origem do TPE importado é Tenable.cs.
u_vulnerability.ID	nome	Mapeia para o registro de referências de vulnerabilidade
u_vulnerability. Links	URL	Mapeia para o registro de referências de vulnerabilidade
	vulnerabilidade	Referência de TPE ou CVE no registro de referências de vulnerabilidade
u_software.Name	nome	Mapeia para o registro do pacote de imagem do contêiner
u_software.Versão	versão	Mapeia para o registro do pacote de imagem do contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_software.Type	package_type	Mapeia para o registro do pacote de imagem do contêiner
u_softwarepaths	caminho	Mapeia para o registro do pacote de imagem do contêiner
u_resolvido	status	Mapeia para o registro de descoberta da imagem do contêiner
u_firstscantime	first_found	Mapeia para o registro de descoberta da imagem do contêiner
u_resource.ScanTime	last_found	Mapeia para o registro de descoberta da imagem do contêiner
u_vulnerability.Description	prova	Mapeia para o registro de descoberta da imagem do contêiner
u_resolvido	estado	Mapeia para o registro de item vulnerável do contêiner
u_firstscantime	first_found	Mapeia para o registro de item vulnerável do contêiner
u_resource.ScanTime	last_found	Mapeia para o registro de item vulnerável do contêiner
[script]	origem	A origem do registro de item vulnerável do contêiner é Tenable.cs.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tenable.cs Tempo e finalidade do script de mapa de transformação de vuln do contêiner

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Aciona o Processador de vulnerabilidades de contêiner TenableCS que importa dados do Tenable.cs O uso do conjunto de importação e carrega cada registro na tabela IC do CMDB, na tabela Item vulnerável, na tabela Entrada de vulnerabilidade de terceiros, na tabela de referência de vulnerabilidade, no pacote de imagens do contêiner, na descoberta de imagens do contêiner e no item vulnerável do contêiner. Não é recomendável modificar ou excluir.
Antes de um conjunto de importação concluir a transformação)	Verifica se a entrada de terceiros e as descobertas de imagem existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação)	Atualiza a contagem de ICs, Vits e descobertas conforme importados de Tenable.cs. Este script é

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Tempo e finalidade do script de mapa de transformação de vuln do contêiner

Quando o script é executado	Finalidade
	para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Importação de Vulnerabilidade de Computação

Os dados de vulnerabilidade do host importados são carregados primeiro no Tenable.cs Tabela de importação de vulnerabilidade de computação [sn_vul_tenable_cs_compute_vuln_import].

. Tenable.cs O mapa de transformação de vuln de computação é usado para transformar as informações de vulnerabilidade do host importado. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação de vulnerabilidade de computação é processada. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Conjuntos para importação do sistema**. Pesquisar Tenable.cs Transformação de vuln de computação.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_resource.ID	object_id	Mapeia para o registro de IC do CMDB.
u_resource.Name	nome	Mapeia para o registro de IC do CMDB.
	asset_category	A nuvem é mapeada como Categoria de ativo no registro de item descoberto.
U_resource.CloudProvider	cloud_service_provider	Mapeia para o registro do item descoberto
u_resource.Region	cloud_region	Mapeia para o registro do item descoberto
u_resource.AccountId	cloud_account	Mapeia para o registro do item descoberto
u_resource. CloudProvider	cloud_resource_type	Mapeia para o registro do item descoberto
u_resource.ID	resource_id	Mapeia para o registro do item descoberto
u_resource.Name	resource_name	Mapeia para o registro do item descoberto
u_vulnerability.ID	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de entrada de terceiros será DEZ-12345.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
		Mapeia o ID para CVEs também.
u_vulnerability. Descrição	resumo	Mapeia para o registro de entrada de terceiros.
u_vulnerability.severity	v4_base_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprScore	source_risk_score	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprSeverity	source_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.AttackVector	v4_attack_vector	Mapeia para o registro de entrada de terceiros.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Mapeia para o registro de entrada de terceiros.
[script]	origem	A origem do TPE importado é Tenable.cs.
u_vulnerability.ID	nome	Mapeia para o registro de referências de vulnerabilidade
u_vulnerability.links	URL	Mapeia para o registro de referências de vulnerabilidade
	vulnerabilidade	Referência de TPE ou CVE no registro de referências de vulnerabilidade
u_resolvido	status	Mapeia para o registro de detecção de item vulnerável
u_firstscantime	first_found	Mapeia para o registro de detecção de item vulnerável
u_resource.ScanTime	last_found	Mapeia para o registro de detecção de item vulnerável
u_softwarepaths	prova	Mapeia para o registro de detecção de item vulnerável
u_softwareresoluçãoversões	solution_summary	Mapeia para o registro de detecção de item vulnerável
u_resolvido	estado	Mapeia para o registro de item vulnerável
u_firstscantime	first_found	Mapeia para o registro de item vulnerável
u_resource.ScanTime	last_found	Mapeia para o registro de item vulnerável
[script]	origem	A origem do registro de item vulnerável é Tenable.cs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tenable.cs Calcular tempo e finalidade do script de mapa de transformação de vuln

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Aciona o processador de vulnerabilidades de computação do Tenable CS que importa dados do Tenable.cs O uso do conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de vulnerabilidades de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Verifica se a entrada e as detecções de terceiros existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Atualiza a contagem de ICs, Vits e detecções conforme importados de Tenable.cs. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_digest	Image_id	Um resumo exclusivo fornecido pela Tenable para os ativos do contêiner. Mapeia para a imagem do contêiner descoberta e o registro de imagem do docker e é usado para pesquisa de IC.
u_name	nome	Mapeia para o campo de nome do registro de imagem do docker.

Defina parâmetros de filtro adicionais para Tenable.io importações

Personalize os parâmetros de filtragem para suas consultas programadas com Integrações de vulnerabilidade da Tenable para ajudar você a refinar ainda mais os dados de vulnerabilidade importados com Tenable.io produto.

Antes de Iniciar

Casos de uso: Como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você deseja exibir vulnerabilidades importadas que são filtradas por `cidr_range`, `num_assets`, `indexed_at`e `plugin_family`. Ou, digamos que você deseja executar um Tenable.io integração de forma que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudar você a coletar esses dados, você pode adicionar parâmetros compatíveis com o Tenable para ajudar a importar os detalhes de vulnerabilidade específicos necessários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite personalizar as informações da solicitação HTTP com parâmetros do Tenable em seu ServiceNow AI Platform. A seguir Tenable.io As integrações oferecem suporte à filtragem fornecendo conteúdo JSON no corpo da solicitação:

- Integração de ativos
- Integração de Vulnerabilidade Corrigida
- Integração de vulnerabilidades em aberto

Você deve saber como usar JSON cadeias de caracteres para este recurso.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Localize os parâmetros compatíveis com Tenable.io produto no site do desenvolvedor que você deseja usar para filtragem.

   Parâmetros e valores inseridos no Tenable.io os produtos são compatíveis somente no nível da instância de integração.

2. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
3. Na página de lista Integrações do Tenable, clique no registro do Tenable.io integração que você deseja abrir.
4. Com a guia Métodos REST do Tenable selecionada, clique no ícone de informações (I) do método REST seguido por **Registro em aberto** .
5. Selecione **Solicitação HTTP** guia.
6. Para editar o registro, na parte superior da página, clique no link em, para editar o registro, clique em **aqui** .
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON desejado como parte do corpo da solicitação.

   Como exemplo, você pode definir o parâmetro de severidade para vulnerabilidades importadas como, `{"filters": {"severity": ["critical"]}}`para Tenable.io Integração de ativos para importar somente vulnerabilidades críticas (pontuação CVSS de 10,0).

   Se você quiser inserir mais de um parâmetro, consulte Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Emissão de relatórios de Integração de vulnerabilidades do Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis no Resposta a vulnerabilidades painéis.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

trabalho, Explorar o. Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Versões anteriores de Resposta a vulnerabilidades

O painel de visão geral da Resposta a vulnerabilidades (Gestão de vulnerabilidades) fornece uma visão executiva das vulnerabilidades e itens vulneráveis, ajudando o administrador de vulnerabilidades a identificar áreas de preocupação rapidamente. O painel Correção de resposta a vulnerabilidades (Correção de vulnerabilidades) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando o padrão Resposta a vulnerabilidades painéis.

Função necessária: Responsável pela correção.

As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

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

para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão Geral da Correção**.

Gráfico de status de execução de integração para a Integração de vulnerabilidade do Tenable

O módulo Status de execução de integração do Tenable fornece uma exibição gráfica do status das execuções de integração do Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer peça no gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: Administrador de vulnerabilidades.

As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

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

Para exibir os dados, navegue até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Status da Execução da Integração**.

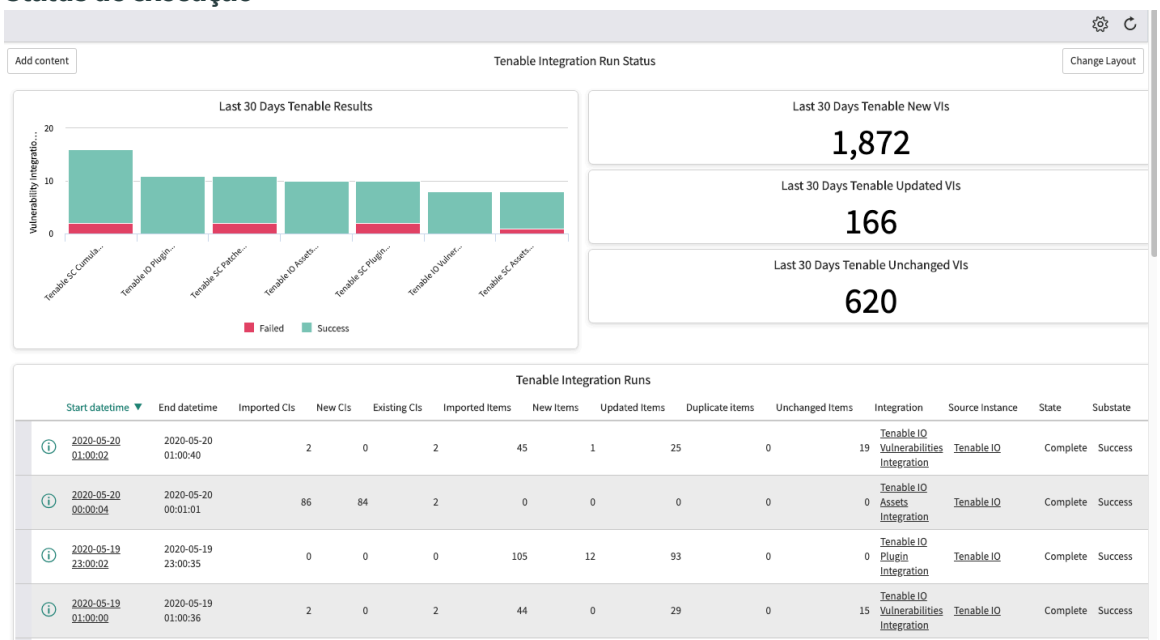
A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Status de execução



Relatórios de gráfico de status de execução da integração do Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução exibida como uma barra no gráfico.
VIs novos da Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs da Tenable atualizados nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções da integração com Tenable	Os registros de execução de integração em uma lista. **Nota: V16.1:** Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no `sn_vul_detection`tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.

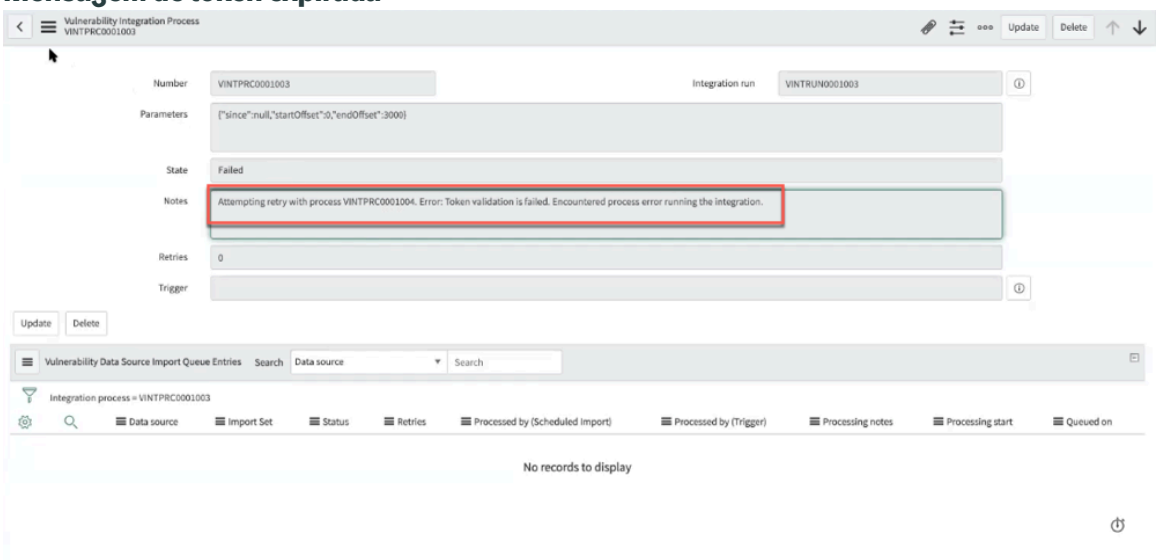
Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do Processo de integração de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de token expirada



Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidades no registro Processo de integração de vulnerabilidades.

Iniciar uma nova verificação para Tenable.sc integração

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas varreduras na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Tenable.sc produto do seu ServiceNow AI Platform® instância.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota: Tenable.sc o não oferece suporte para iniciar uma nova verificação em máquinas baseadas em agente.

Antes de começar, verifique se o scanner está ativado. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

Para iniciar uma nova varredura nos espaços de trabalho, consulte Nova verificação Tenable.io e. Tenable.sc itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidades, ou os gerentes de vulnerabilidades podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas varreduras de itens vulneráveis (VI), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de itens descobertos do seu ServiceNow AI Platform instância.

Permitir novamente seu responsáveis pela correção e analistas de vulnerabilidades Para verificar se suas atividades de correção, patches e outras ações corrigiram com sucesso vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o seu ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Tenable.sc itens vulneráveis.

Nota: Ao solicitar uma nova verificação do seu ServiceNow AI Platform® instância, selecionando Integração de Resposta a vulnerabilidades com Tenable as credenciais são opcionais. . ServiceNow® Tenable.sc A integração de credenciais de verificação importa e atualiza as credenciais do scanner do Tenable.sc produto em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais do Tenable.

Observe que esses dados importados não incluem senhas do Tenable ou outras informações confidenciais da conta do Tenable. . ServiceNow® Tenable.sc A integração de credenciais de verificação está habilitada (Ativo Automaticamente de dentro do Assistente de configuração na sua instância quando você configura o. Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades em aberto e corrigido).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário no seu ServiceNow AI Platform instância:

- Credenciais criadas com Tenable.sc a função de usuário administrador está disponível para usuários em todas as suas organizações.
- Credenciais criadas com Tenable.sc a função usuários organizacionais só está disponível para usuários dessa organização. Essas credenciais não são importadas para ServiceNow AI Platform para usuários fora da organização do criador, a menos que eles sejam compartilhados com a conta do usuário que está sendo usada para se conectar à instância.

Consulte Tenable.sc site de documentação para obter mais informações.

Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração para obter mais informações sobre como configurar o. Tenable.sc aplicação. Para exibir mais informações sobre a Integração de credenciais de verificação, navegue até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Integrações** > **Integração de credenciais de verificação do Tenable.sc**.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas varreduras para VIS com Tenable.sc como a origem. Verificar Tenable.scé exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se a coluna Origem não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique em **Personalizar lista** (Ícone de engrenagem) e use o Slushbucket para mover **Origem** de **Disponível** . **Selecionado** .

3. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve ser do Tenable.sc produto e em qualquer estado diferente de **Encerrado** . Para vários registros de VI, todos os VIS devem ser do produto Tenable.sc e estar em qualquer estado diferente de **Encerrado** .
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ser do Tenable.sc produto.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do Tenable.sc produto em qualquer estado diferente de **Encerrado** .

4. No canto superior direito do registro, clique em **Nova verificação** .
   Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Estas são as credenciais importadas pelo Tenable.sc Integração de credenciais de verificação.
5. Na caixa de diálogo, selecione os filtros e os tipos de credencial desejados.
6. Clique em **Verificação de solicitação** .

   É exibida uma mensagem indicando que sua verificação está sendo processada. O status de todas as novas varreduras pode ser encontrado a qualquer momento nas listas relacionadas de Varredura nos registros VI, RT, TPE que você usou para iniciar as novas varreduras. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e exibir todas as outras novas verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida. Todos os VIS que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** São importados com a próxima importação programada da Integração de vulnerabilidades fixas do Tenable.sc.

Iniciar uma nova verificação para Tenable.io integração

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Tenable.io produto do seu ServiceNow AI Platform® instância.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Antes de começar, verifique se o scanner está ativado. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade e. Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI Para iniciar uma nova verificação nos espaços de trabalho de Resposta a vulnerabilidades.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota: Tenable.io o não oferece suporte para iniciar uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, como responsável pela correção, especialista EM TI, analista de vulnerabilidades ou gerente de vulnerabilidades, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas varreduras de registros de item vulnerável (VI), tarefas de correção (VUL), entrada de terceiros (TPE) ou item descoberto (SDI) do seu ServiceNow AI Platform instância. Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao solicitar uma nova verificação do seu ServiceNow AI Platform® instância, selecionando Integração de Resposta a vulnerabilidades com Tenable as credenciais são opcionais. . ServiceNow® Tenable.io A integração de credenciais de verificação importa e atualiza as credenciais do scanner do Tenable.io produto em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais do Tenable.

Observe que esses dados importados não incluem senhas do Tenable ou outras informações confidenciais da conta do Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário no seu ServiceNow AI Platform instância:

- Credenciais criadas com Tenable.io a função de usuário administrador está disponível para usuários em todas as suas organizações.
- Credenciais criadas com Tenable.io a função usuários organizacionais só está disponível para usuários dessa organização. Essas credenciais não são importadas para ServiceNow AI Platform para usuários fora da organização do criador, a menos que eles sejam compartilhados com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte Tenable.io site de documentação para obter mais informações.

- . Tenable.io Integração de modelo e Tenable.io A integração de credenciais de verificação deve ser ativada antes de iniciar novas verificações. Para exibir mais informações sobre a Integração de credenciais de verificação, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Integrações** > **Integração de credencial de verificação do Tenable.io**.

  Por padrão, as Integrações de credencial de modelo e verificação estão desativadas. Quando você insere suas credenciais para Tenable.io. todos Tenable.io as integrações são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize Tenable.io registros de integração desejados.
  3. Abra cada registro e selecione **Ativo** caixa de seleção para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com a configuração do Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração para obter mais informações sobre como configurar o. Tenable.io e. Tenable.sc produtos.

Todo o seu ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Tenable.io itens vulneráveis.

Você pode exibir resultados atualizados nos registros a partir dos quais você iniciou as verificações após a próxima importação programada da Integração de vulnerabilidades fixas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Se você estiver usando Tenable.io Scanner, você só pode iniciar novas varreduras para VIS com Tenable.io como a origem. Verificar Tenable.ioé exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se a coluna Origem não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique em **Personalizar lista** (Ícone de engrenagem) e use o Slushbucket para mover **Origem** de **Disponível** . **Selecionado** .

3. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve estar em qualquer estado diferente de **Encerrado** . Para vários registros de VI, todos os VIS devem ser de Tenable.io produto e em qualquer estado diferente de **Encerrado** .
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os VIS associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como a origem.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do Tenable.io produto em qualquer estado diferente de **Encerrado** .
   - Em registros de itens descobertos, o registro deve ter pelo menos um registro VI associado do Tenable.io produto em qualquer estado diferente de **Encerrado** .

Tradução automática

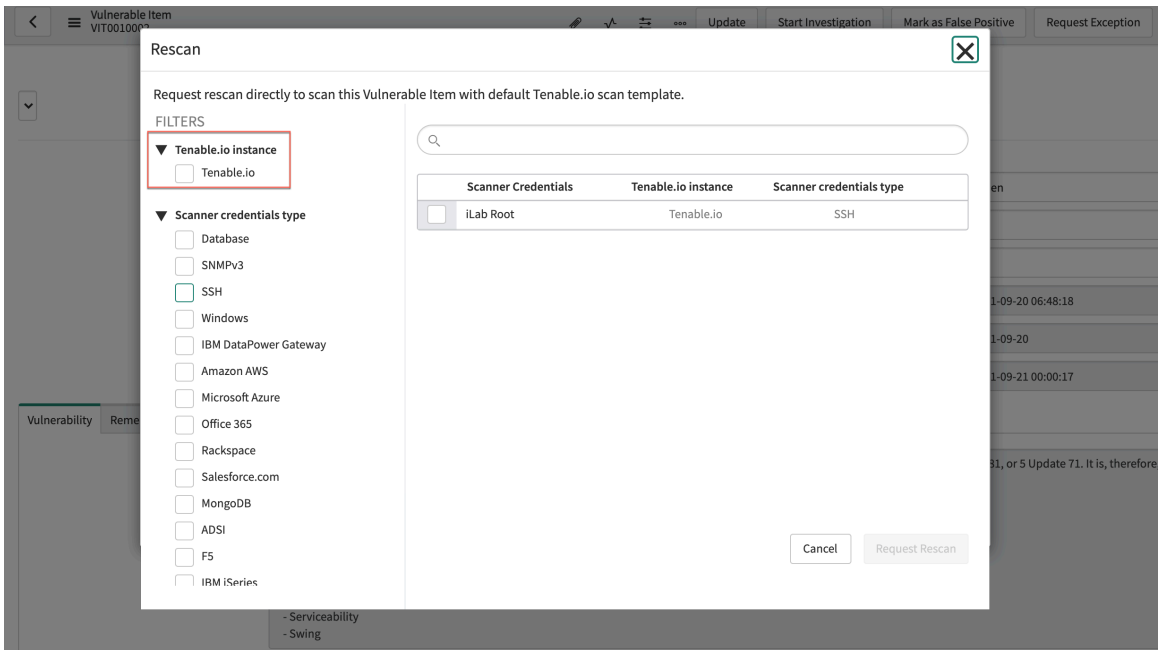
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Nova verificação** .
   Você será solicitado a escolher a instância ou instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pelo Tenable.io Integração de credenciais de verificação.

5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, Tenable.io é exibido. Se você tiver mais de um Tenable.io todos eles são exibidos em Tenable.io seção no formulário.



Campo	Descrição
Instância da Tenable.io	Escolha um Tenable.io instância de integração da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io são exibidos. Se existir uma VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar. **Nota:** Se você optar por verificar novamente o VIS de um registro de tarefa de correção para uma única instância de integração, somente os VIS ativos associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas, serão verificados.
Filtro de tipo de credenciais do scanner	Use este filtro para exibir credenciais por tipo.
Painel com credenciais do scanner, Tenable.io Tipo de credenciais do scanner	Estas são as credenciais do scanner disponíveis importadas do Tenable.io produtos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Escolha uma ou mais credenciais para usar na verificação.

6. Clique em **Solicitar nova verificação** .

   É exibida uma mensagem indicando que sua verificação está sendo processada e um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas à verificação nos registros VI, tarefa de correção, TPE e SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e exibir todas as outras novas verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode oferecer suporte é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida. Todos os VIS que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação programada do Tenable.io Integração de vulnerabilidades corrigidas.

   Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

   Você pode exibir resultados atualizados nos registros a partir dos quais você iniciou as verificações após a próxima importação programada da Integração de vulnerabilidades fixas.

Atualize itens de configuração com o identificador de partição de rede para Integrações de vulnerabilidade da Tenable

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão em Resposta a vulnerabilidades Uma maneira de identificar seus ativos é pelo endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (ICs) em seu ambiente podem compartilhar endereços IP, mas têm ids exclusivos de rede e repositório. No entanto, por padrão, esses ativos geralmente são identificados e armazenados como um único IC (IC 1) Durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para poder identificá-los como ativos distintos. A partir de uma importação de dados nova, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para Ativos e Integrações de vulnerabilidades fixas e abertas para Tenable.io e. Tenable.sc No Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o Identificador de partição de rede [network_partition_identifier] aos registros de IC existentes de dados importados. ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar seus dados existentes.

Quando você faz upgrade começando com v14.0 de Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable, os Modelos de classe de IC do CMDB (1,0.21.) é compatível. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de IRE (Identificação e reconciliação).

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados existentes do Tenable são criados ou atualizados para incluir a granularidade do identificador da partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são atualizados com os novos ICs.
Aguarde as importações de dados atualizados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo

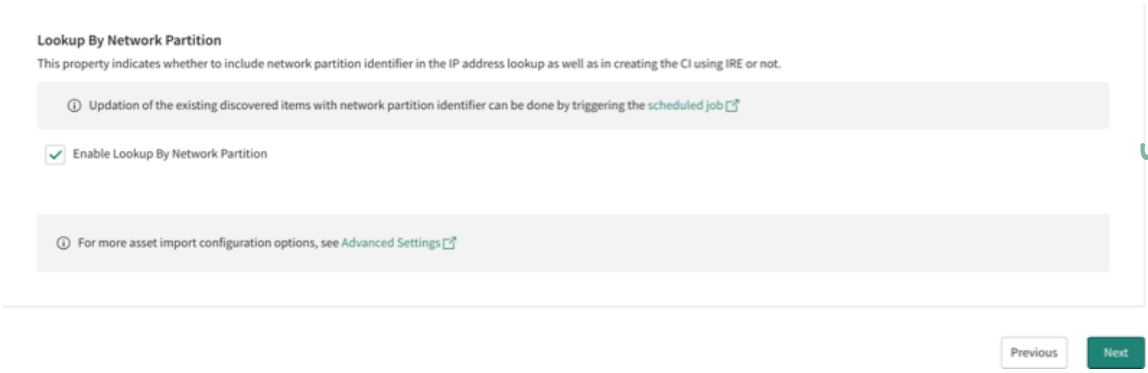
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	trabalho agendado. IC, item vulnerável e registros de detecção são atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Editar** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

Os identificadores de partição de rede NETWORK_ID e REPOSITÓRIO _ID são incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho agendado.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho agendado, as regras de pesquisa de identificação de endereço IP e de IC de endereço IP incompleto incluem o atributo identificador de partição de rede automaticamente para uma importação de dados das Integrações de ativos e vulnerabilidades fixas e abertas para Tenable.io e. Tenable.sc produtos.

Depois de habilitar a propriedade do sistema e salvar os registros, você também pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos agendados sob demanda.

Importar modificações para a Integração de vulnerabilidades do Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação do Tenable Vulnerabilities no ServiceNow® Integração de vulnerabilidades do Tenable.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação e conhecimento avançado sobre ServiceNow AI Platform.

Siga estas etapas para criar importações separadas por domínio para as Integrações do Tenable Vulnerabilities. O exemplo a seguir é para a integração Open Vulnerabilities do Tenable.io, mas este conteúdo é aplicável a outras integrações do Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio que você criar, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado run_as para o domínio no Tenable.io.

3. Integração de vulnerabilidades em aberto.
   O usuário é equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Considere este usuário como específico para esta função. O usuário não deve ter outra finalidade

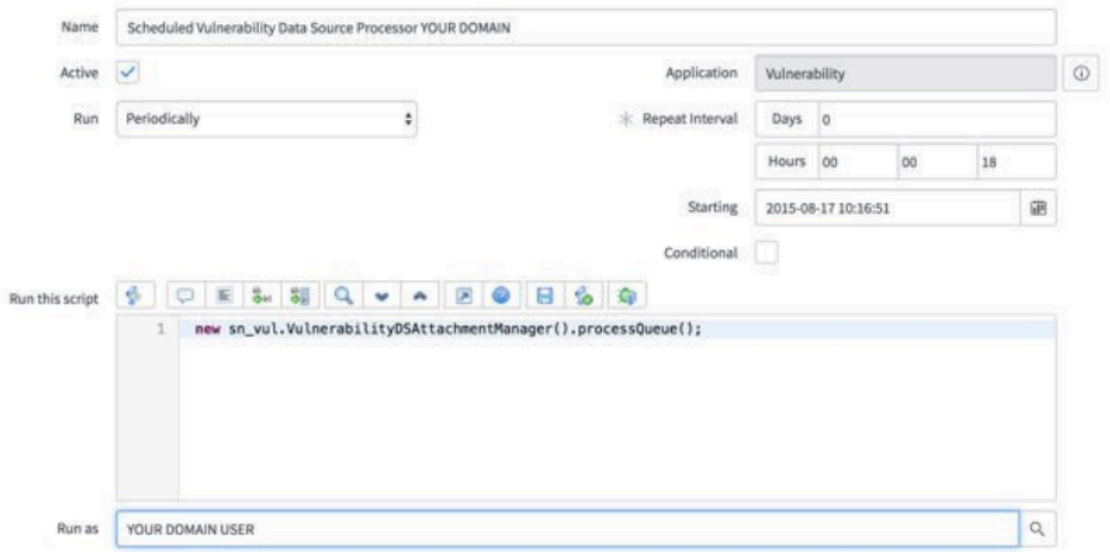
4. Em cada domínio, crie um trabalho agendado copiando o Processador da fonte de dados de vulnerabilidade programada encontrado em **Definição do Sistema** > **Trabalhos agendados**.
5. Anexe o domínio ao nome para identificar o trabalho agendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Mude o usuário run_as para o usuário que você criou na etapa anterior.

Nota: Edite a ação de IU a seguir para que a integração seja executada no domínio do usuário run_as.



7. Edite a ação Executar IU do Now na Integração de vulnerabilidades abertas do Tenable.io para adicionar este bloco de código à parte superior do arquivo.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Nota: Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

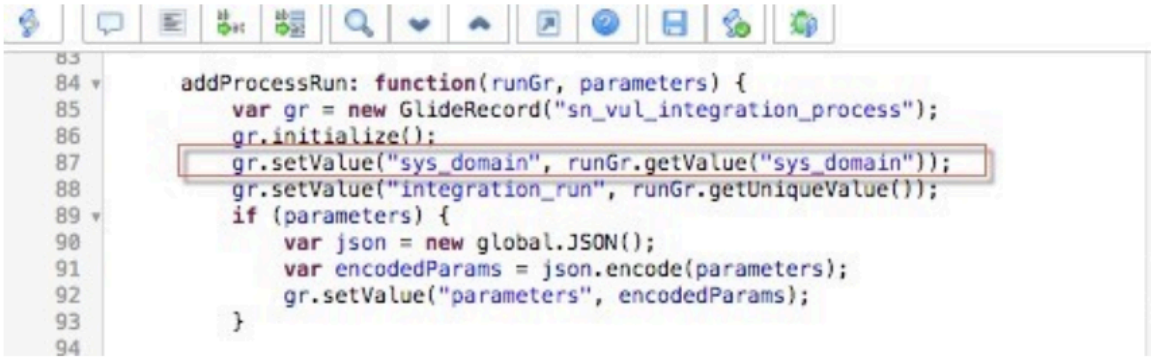
8. Edite o script VulnerabilityIntegrationUtils include método addIntegrationRun para adicionar o código realçado.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o script VulnerabilityIntegrationUtils include método addProcessRun para adicionar o código realçado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Edite o método de inclusão de script DataSourceVulnReportRefresProcessor _processFromDataSourceGroups para mudar este código original: Código _processFromDataSourcesGroups original para o código _processFromDataSourcesGroups editado.
11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem para adicionar os blocos de código realçados a seguir queueItem, _getNext, _processQueueEntry.

    Você está pronto para importações de detecção de host separadas por domínio.

    Desabilite as calculadoras antes da importação

    Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de todas as outras que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e podem afetar o desempenho da instância.

    Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Calculadoras de Vulnerabilidade**.
13. Abra o grupo Impacto da vulnerabilidade.
14. Abra a calculadora de Pontuação e Impacto baseado no serviço.
15. Desmarque o campo Ativo para desativar a calculadora.
16. Clique em Atualizar.

    Você desabilitou a calculadora padrão.

    Desabilite regras de negócios baseadas em notificação antes da importação inicial

    Siga estas etapas para desabilitar Desabilitar regras de negócios relacionadas a notificações antes da importação inicial de registro. Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desabilitá-las durante a importação.

    A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.
18. PESQUISE notificações de ic afetadas.
19. Abra a regra de negócio e insira a seguinte condição: `current.sys_class_name != “sn_vul_vulnerable_item"`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócios:
    - Notificações do centro de custos afetado
    - Notificações de grupo afetado
    - Notificações de local afetado

    Nota: Após a conclusão da importação de registro inicial, você tem a opção de reativar essas regras de negócios. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

    Modifique uma data de início inicial

    Siga estas etapas para Modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações do Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde esse momento sejam detectadas.

    Se você configurou a Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente três meses antes da data de hoje e, posteriormente, até a data de hoje. Observação: Considere definir o valor como um máximo de um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da Tenable API, bem como acione tempos limite de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. **Opcional:** Clique em **Executar agora** para executar imediatamente.

Divida detecções do Tenable com base na instância de vulnerabilidade para dividir itens vulneráveis

ServiceNow® A Resposta a vulnerabilidades permite a divisão de detecções de scanners do Tenable, permitindo a criação de um item vulnerável exclusivo (VIT) para cada instância de vulnerabilidade detectada. Essa divisão permite a atribuição de Vits a várias equipes de correção, aprimorando o gerenciamento e o acompanhamento de vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A carga útil do scanner do Tenable contém dados de detecção, com cada caminho na prova usado para dividir as detecções. O marcador de saída na carga identifica o local da vulnerabilidade, facilitando a identificação e o gerenciamento precisos de vulnerabilidades de acordo com seus caminhos específicos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na tabela Integrações de terceiros [sn_sec_int_integration], defina **Incluir prova na chave vi** valor da coluna como verdadeiro para Tenable.io, Tenable.sc e Tenable.cs.
2. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.
3. Para Tenable.cs produto, navegue até **Configuração da chave de detecção** tabela [sn_vul_detection_key_config], selecione Tenable.cs registrar e atualizar,
4. No formulário Incluir porta, selecione **Incluir porta** e selecione **clique aqui** Link (aplica-se somente a Tenable.io e Tenable.sc).
5. Na lista Adicionar prova às chaves VI, selecione **Novo** .
6. No formulário Adicionar prova à chave VI - Novo registro, em **Vulnerabilidade** Adicione o ID da Tenable para o qual você deseja incluir a prova.

   Nota: Você pode dividir as detecções com base exclusivamente nas informações de caminho ou combinando detalhes de caminho e versão. Para obter detalhes adicionais, consulte a seção "Divisão de detecções de scanners Tenable" nesta página.

7. Em **Expressão regular para Dividir Vits do Tenable** campo:
   - Divida a detecção com base somente no caminho inserindo Caminho
   - Divida a detecção com base no caminho e nas versões instaladas e fixas inserindo Path:
8. Selecione **Enviar**.

Example: Dividindo detecções de scanners Tenable

A detecção a seguir de um scanner do Tenable mostra uma prova no marcador de saída que inclui informações de caminho e versão.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",

               "tracked": true
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
"output": "In C: 11 Program Files (x86) \ \Common Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed version
Path
"plugin":
"bid":
123456

"checks_for_default_account": false,
"checks_for malware": false,

"coe":
"cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"

"cvSs3_base_score": 7.8,
"cvss3 temporal score": 7.0,

"cvss3_temporal_vector": {
"exploitability": "Proof-of-Concept",
"remediation level": "Official Fix",
"report_confidence": "Confirmed",
"raw": "E: P/RL:0/RC: C"
```


Noções básicas do Atlassian Jira integração com Resposta a vulnerabilidades

. Atlassian Jira integração com Resposta a vulnerabilidades permite que você aproveite diferentes ferramentas de acompanhamento de problemas e gestão ágil para rastrear esforços de correção de vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

ServiceNow® Resposta a vulnerabilidades está integrado ao Atlassian Jira para criar problemas correspondentes a vulnerabilidades e sincronizar a entidade do problema em Jira e a entidade do item de vulnerabilidade em Resposta a vulnerabilidades bidirecional para refletir as atualizações mais recentes. Os gerentes de vulnerabilidades exigem itens de vulnerabilidade presentes em ServiceNow Resposta a vulnerabilidades a ser criado e atribuído a usuários de correção (desenvolvedores, no caso de Resposta a vulnerabilidades de aplicações em seu sistema preferencial de ferramenta de gestão de registros e problemas, como Atlassian Jira. Qualquer andamento realizado nas vulnerabilidades na ferramenta de gestão de problemas deve ser atualizado em ServiceNow Resposta a vulnerabilidades Para visibilidade para gerentes de vulnerabilidades. Além disso, todas as atualizações feitas pelos gerentes de vulnerabilidades em Resposta a vulnerabilidades para itens de vulnerabilidade também devem ser passados para a ferramenta de gestão de problemas para visibilidade para os usuários de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis

Versão de lançamento	Notas da versão
Resposta a vulnerabilidades	Notas da versão da Integração de Resposta a vulnerabilidades
Resposta a vulnerabilidades e Conformidade de configuração para contêiner	Notas da versão do Resposta a vulnerabilidades do contêiner
Jira Spoke	Notas da versão do spoke do JIRA

Jira Integrações de vulnerabilidades

Para exibir o. Jira Integração de vulnerabilidades, navegue até **Tudo** > **Gestão do Agile para VR** > **Configurar ferramentas Agile** .

As integrações a seguir estão incluídas no sistema de base. Essas integrações não estão todas ativas por padrão.

Todos os dias, os trabalhos agendados são encadeados para executar as integrações automaticamente em ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Preparando para Jira Resposta a vulnerabilidades integração

Bem-sucedida Jira A integração de vulnerabilidades requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Jira Resposta a vulnerabilidades a integração pressupõe que você esteja familiarizado com Jira Produto e API.

Componentes instalados com o Agile Integration para Resposta a vulnerabilidades e. Jira Integração do Vulnerability Response

Vários tipos de componentes são instalados com a ativação do plug-in Agile Integration for Vulnerability Response e Jira Integration for Vulnerability Response, incluindo tabelas e funções de usuário.

Funções instaladas

Função [name]	Descrição
Administrador da ferramenta ágil [sn_vul_agile.agile_tool_admin]	Permite que você crie uma regra de configuração para o Agile Management criar ou atualizar problemas. Crie configurações de regra para Gestão ágil.
Administrador do JIRA [sn_vul_jira.admin]	Permite selecionar a ferramenta Agile para criar problemas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Função [name]	Descrição
	para a tabela de entidade selecionada.

Tabelas instaladas

Tabela	Descrição
Configuração da ferramenta ágil [sn_vul_agile_tool_rule_config]	Contém regras de configuração para criar problemas na plataforma Agile.
Mapeamento de campo da ferramenta ágil [sn_vul_agile_tool_field_mapping]	Contém o mapeamento de campo da regra de configuração.
Mapeamento de estado da ferramenta ágil [sn_vul_agile_tool_state_mapping]	Contém o mapeamento de estado do status do problema do Jira com o Item vulnerável da aplicação, Item vulnerável do contêiner, Tarefa de correção da aplicação e estado da Tarefa de correção do contêiner.
Manifesto da ferramenta ágil [sn_vul_agile_tool_manifest]	Contém carga para criação de problemas.
Recurso de dados da ferramenta ágil [sn_vul_agile_tool_data_resource]	Contém as informações sobre o problema do Jira criado.
Administrador do JIRA [sn_vul_jira.admin]	Permite selecionar a ferramenta Agile para criar problemas para a tabela de entidade selecionada.

Instale a Integração de resposta a vulnerabilidades com Jira

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Jira o produto se integra corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	• O JIRA Integration for Vulnerability Response requer a aplicação Vulnerability Response. • Para obter a versão mais atual do Jira Integration for Vulnerability Response, verifique se você tem a versão mais atual do Vulnerability Response instalada. Consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão . • Se a aplicação não estiver instalada e ativada, consulte, Instale o Vulnerability Response .
Verifique se o plug-in do Integration Hub está instalado.	• O spoke do JIRA requer o Integration Hub. • Consulte KB1112383 Para instalação do hub de integração. • Para obter mais informações, consulte Cronogramas jurídicos - Visão geral do IntegrationHub .
Verifique se a versão mais recente de Jira Spoke instalado.	Consulte KB0792632 Para instalação do Jira Spoke.
Verifique se a Integração de resposta a vulnerabilidades com o Agile Management está instalada.	A integração do Vulnerability Response com o Atlassian Jira requer esta integração.

Procedimento

1. Faça login na instância em que você deseja instalar Jira Resposta a vulnerabilidades integração em.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Resposta a vulnerabilidades integração com Jira aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Localize a aplicação, selecione-a e clique em **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

Configure regras na configuração da ferramenta ágil

Jira os problemas são criados no Jira Plataforma se os registros criados em Item vulnerável da aplicação, Item vulnerável do contêiner, Tarefa de correção da aplicação e Tarefa de correção do contêiner corresponderem às regras criadas na configuração da ferramenta ágil.

Antes de Iniciar

Funções necessárias: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin.

Procedimento

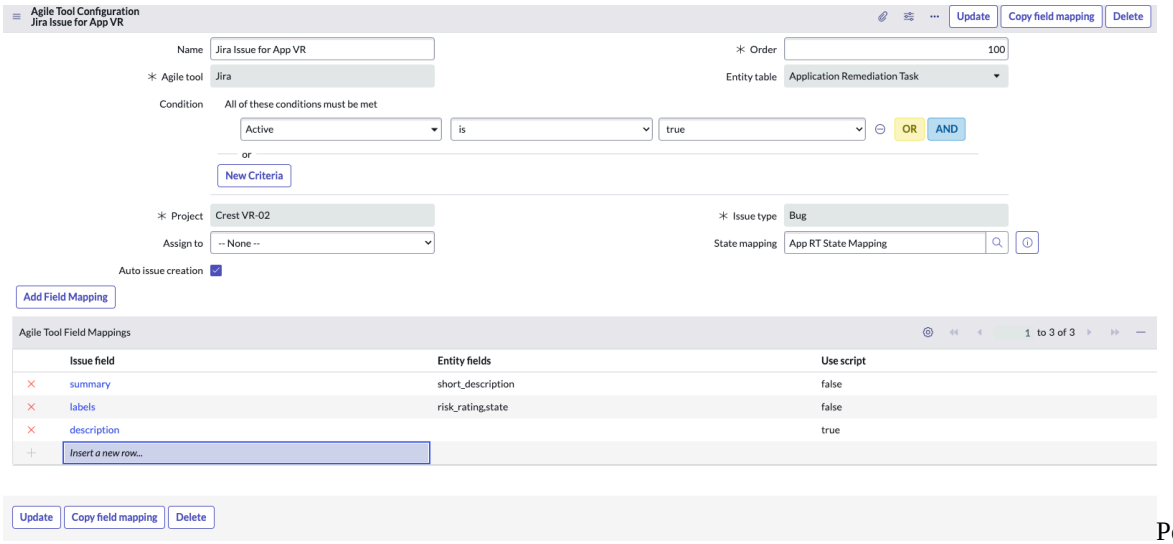
1. Navegar até **Tudo** > **Gestão do Agile para VR** > **Configurar ferramentas Agile**.
2. Para criar uma nova regra de configuração na Configuração da ferramenta Agile, selecione **Novo** .
3. No formulário, preencha os campos.

Formulário de configuração da ferramenta ágil

Campo	Descrição
Nome	Nome da configuração da ferramenta ágil.
Ordem	Configuração da ferramenta ágil.
Ferramenta Agile	A ferramenta ágil para criar problemas na plataforma ágil específica.
Tabela da entidade	Tabela na qual a regra de configuração será aplicada.
Condição	Condição de filtro na tabela Entidade selecionada para criar problemas na plataforma Agile.
Criação automática de problemas	A regra de configuração será consultada quando qualquer novo registro for criado na tabela Entidade selecionada, somente se a caixa de seleção estiver marcada. **Nota:** O usuário deve usar a ação de lista para criar problemas para registros de entidade existentes.
Projeto	O projeto no qual o problema do Jira será criado.
Tipo de ocorrência	O tipo de problema a ser criado em um projeto específico.
Atribuir a	O designado a quem o problema deve ser atribuído após a criação do problema. Para manter os problemas criados como não atribuídos, selecione "Nenhum".
Mapeamento de Estado	Os mapeamentos de estado existentes da tabela Mapeamento de estado da ferramenta ágil ou criam um novo mapeamento de estado entre o status do problema na plataforma ágil e o. ServiceNow estados da tabela de entidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, quando a aplicação é instalada Tarefa de correção de aplicação e Tarefa de correção de contêiner são exibidas no campo Tabela de entidade no formulário Configuração da ferramenta ágil.

4. Para adicionar o Item vulnerável à aplicação e o Item vulnerável ao contêiner na lista de seleção Tabela de entidade, navegue até **Propriedades do sistema** > **sn_vul_agile.tablesToShow** E adicione tudo no campo Valor.

Formulário Propriedade do sistema

Campo	Descrição
Escolhas	Valores separados por vírgula para uma lista de seleção.
Valor	Defina o valor desejado para a propriedade. Todos os valores de propriedade são armazenados como cadeias de caracteres. Ao recuperar propriedades por meio do método gs.getProperty (), trate os resultados como cadeias de caracteres. Por exemplo, uma propriedade verdadeiro|falso retorna 'verdadeiro' ou 'falso' (cadeias de caracteres), não o equivalente booliano.

5. Selecione o registro de mapeamento de estado existente ou crie um novo mapeamento de estado no Mapeamento de estado da ferramenta Agile.

Formulário Mapeamento de estado da ferramenta ágil

Campo	Descrição
Nome	Insira o nome exclusivo do Mapeamento de estado.
Ferramenta Agile	Selecione a ferramenta ágil.
Tabela da entidade	Selecione a tabela de origem na qual o mapeamento de estado será criado.
Projeto	Selecione o projeto no qual o estado será mapeado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado da entidade da ServiceNow	Selecione o estado que você deseja mapear com o status da ferramenta ágil.
Status da ferramenta Agile	Selecione o estado que você deseja mapear a partir dos estados de item de vulnerabilidade.

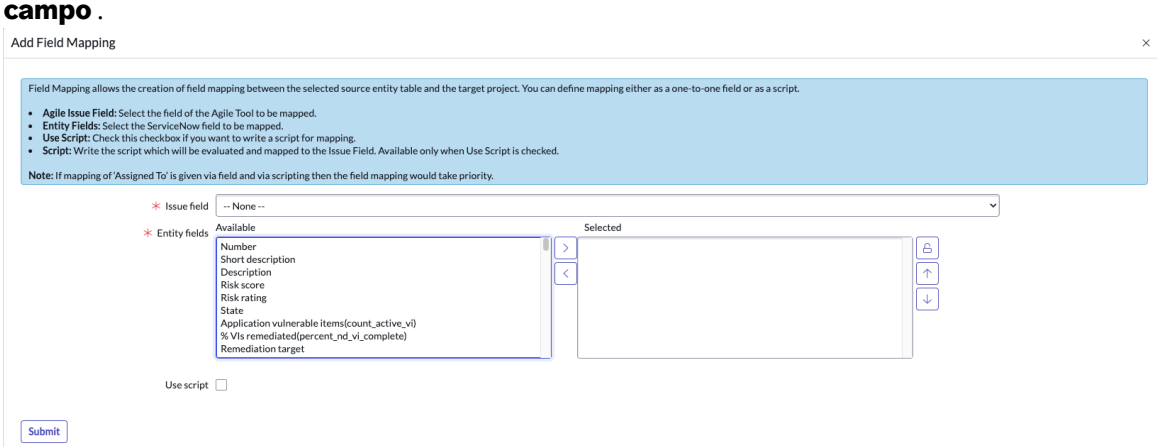
6. Clique em **Salvar e buscar projetos** Para buscar os projetos na regra de configuração do campo Projeto e validar as credenciais da ferramenta Agile.

   Dica: Você pode definir a propriedade do sistema **ProjectsPageSize** para buscar um número específico de projetos por página.

7. Navegue até **Propriedades do sistema** > **sn_vul_jira.projectsPageSize** E adicione o número de projetos a serem obtidos por página no campo Valor do Jira Cloud.
8. Selecione Projeto, Tipo de problema e Atribuir a na regra Configuração depois que os projetos forem obtidos.

   O mapeamento de campo padrão será preenchido na lista integrada de Mapeamentos de campo da ferramenta ágil. Por padrão, os campos Resumo e Descrição dos problemas são mapeados.

9. Para mapear outros campos de problema com ServiceNow, clique em **Adicionar mapeamento de campo** .



Nota:

- Mapeie campos Cadeia de caracteres e Tipo de opção somente.
- Todos os campos de problema obrigatórios da ferramenta Agile precisam estar mapeados corretamente com o campo de entidade.

Formulário Mapeamento de estado da ferramenta ágil

Campo	Descrição
Campo do problema	Contém os campos de problema do projeto selecionado no momento e o tipo de problema na Regra de configuração.
Campos da entidade	Contém os campos da tabela Entidade selecionada na Regra de configuração.
Use o Script	Selecione para usar o script para mapear os campos de problema com campos de entidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Script	Script para mapear o campo de problema com campos de entidade.

10. Clique em **Enviar** No modal do Glide para enviar o registro de mapeamento de campo na tabela Mapeamentos de campo da ferramenta ágil.

    Nota: Se você não mapear os campos obrigatórios, os problemas não serão criados para essa regra de configuração.

    Os campos obrigatórios são exibidos na parte superior do formulário Configuração da ferramenta ágil. Todo o mapeamento de campo para uma regra de configuração específica é exibido na lista integrada da tabela Mapeamento de campo da ferramenta ágil na tabela Configuração da ferramenta ágil.

11. Clique com o botão direito do mouse no cabeçalho para salvar suas mudanças.
    O registro salvo está visível na tabela Configuração da ferramenta ágil. Se algum registro for criado no Item vulnerável da aplicação, Item vulnerável do contêiner, Tarefa de correção da aplicação e Tarefa de correção do contêiner corresponderem a qualquer regra de configuração, o problema será criado para o registro de acordo com o mapeamento na regra de configuração.

12. Navegue até **Propriedades do sistema** > **sn_vul_jira.cloudBulkSize** E defina o número de problemas a serem criados por lote no campo Valor.

    Nota: O número máximo de problemas que podem ser criados por lote na nuvem do Jira é 50).

    Você pode definir o tamanho do lote para criar problemas no Jira Server.

13. Navegue até **Propriedades do sistema** > **sn_vul_jira.onPremIssue** e definir o número de problemas a serem criados por lote no **Valor** campo.
    Você também pode definir a contagem de erros no campo Valor na propriedade do sistema para processar os registros na tabela de manifesto para criar problemas Jira até uma contagem de erros específica.

14. Navegue até **Propriedades do sistema** > **sn_vul_agile.ManifestErrorCount** e definem o número máximo de vezes até que o manifesto com erro deve ser processado.

Crie um problema ágil manualmente usando a ação de lista

Quando uma ação de lista: Criar problema do Jira é acionada, os registros que correspondem aos critérios de configuração da regra devem ser considerados para "Criar problema do Jira" e esses registros devem ser ingeridos na tabela sn_vul_agile_tool_manifest com o mapeamento selecionado na regra de configuração.

Antes de Iniciar

Função necessária: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/Itens vulneráveis à aplicação/Itens vulneráveis ao contêiner**.

2. Selecione vários registros para criar problemas do Jira e clique em **Criar problema do Jira** .
   Os registros selecionados devem considerar o mapeamento de campo e o mapeamento de estado da ferramenta Agile associada.
   Os registros selecionados que atendem à condição da regra de configuração devem ser qualificados para a criação de problemas do Jira e esses registros devem ser adicionados ao `sn_vul_agile_tool_manifest`tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um problema ágil manualmente usando a ação de formulário

Crie um problema ágil manualmente usando a ação de formulário. Se o registro corresponder a qualquer condição de regra de configuração, uma caixa pop-up será preenchida com os valores selecionados na regra de configuração e, se não corresponder a nenhum critério, o usuário poderá selecionar valores para campos predefinidos.

Antes de Iniciar

Certifique-se de que todos os campos de problema obrigatórios da ferramenta Agile estejam mapeados corretamente com o campo Entidade.

Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/Itens vulneráveis à aplicação/Itens vulneráveis ao contêiner**.
2. Selecione qualquer registro para criar um problema ágil manualmente.
3. Selecione **Criar problema ágil** .
4. Insira detalhes válidos para os campos mencionados.

   Se o registro atender à condição de qualquer regra de configuração, os campos abaixo deverão ser preenchidos com o valor configurado e o usuário poderá modificar os valores do campo.

Campo	Descrição
Projeto	Selecione o projeto no qual o problema do Jira será criado.
Tipo de ocorrência	Selecione o tipo de problema a ser criado em um projeto específico.
Atribuir a	Selecione o designado a quem o problema deve ser atribuído após a criação do problema.
Mapeamento de Campos	Selecione os campos de tipo de problema da ferramenta ágil e insira os valores diretos para o campo selecionado.

5. Selecione **Criar problema ágil** para enviar o registro.
   Depois de enviar o registro, a entrada do registro será criada na tabela sn_vul_agile_tool_manifest.

Sincronizar manualmente o status do Jira problema

Atualize o estado do registro único clicando em **Sincronizar status do Agile** botão do menu de contexto do formulário e atualize os estados de vários registros clicando na ação de lista **Sincronizar status do Agile** Da tabela Item vulnerável à aplicação, Item vulnerável ao contêiner e Tarefa de correção no Espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O estado é sincronizado de ServiceNow para a ferramenta ágil se o estado da entidade for encerrado em ServiceNow Ou se alguma entidade for reaberta (ou seja, o Estado é Aberto). Todos os outros estados serão refletidos da ferramenta Agile para ServiceNow. O usuário não terá permissão para sincronizar o estado dos registros cuja regra configurada associada não tem mapeamento de estado ou os problemas criados diretamente a partir da ação de formulário.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/Itens vulneráveis à aplicação/Itens vulneráveis ao contêiner**.
2. Selecione vários registros para criar problemas do Jira e clique em **Sincronizar status do Agile** .
   Os estados dos registros para os quais os problemas já foram criados serão atualizados se o registro não estiver no estado Encerrado e o mapeamento de estado existir para os registros selecionados na regra de configuração.
3. Abra um registro e **Sincronizar status do Agile** fica visível no menu de contexto do formulário se as seguintes condições forem atendidas.
   - O problema é criado para o registro e o registro não está no estado Encerrado
   - O mapeamento de estado existe para o registro
4. Clique em **Sincronizar status do Agile** para sincronizar o status ágil com o estado mapeado.
   Você pode definir a propriedade do sistema para definir o tamanho do lote para buscar o status do problema do Jira.
5. Navegar até **Propriedade do sistema** > **sn_vul_jira.bulkIssueStatusSize** .
   - Para o Jira Server, o número máximo de problemas a serem retornados (o padrão é 50). O valor máximo permitido é ditado pela propriedade Jira 'jira.search.views.default.max'. Se você especificar um valor maior do que este número, os resultados da pesquisa serão truncados.
   - Se o problema for criado a partir da ação do formulário ou a regra configurada não tiver nenhum mapeamento de estado, esses registros não serão considerados para sincronização de estado.

Configure o agendador para criar problemas automaticamente

Configure o agendador para executar e criar automaticamente o. Jira problemas para os registros que foram criados na tabela sn_vul_agile_tool_manifest.

Antes de Iniciar

Função necessária: administrador ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa

Todos os registros do Item vulnerável à aplicação, Item vulnerável ao contêiner, Tarefa de correção da aplicação e Correção do contêiner criados na tabela sn_vul_agile_manifest serão considerados para Jira criação de problemas.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Trabalhos agendados** > **Criar problemas do Jira**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no script programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Execução agendada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado: ○ Diariamente - é executado diariamente, em um horário designado. ○ Semanalmente - Executa semanalmente, em um horário e dia designados. ○ Mensal - Executa mensalmente, em um horário e dia designados do mês. ○ Executado periodicamente - em um intervalo de repetição designado. ○ Uma vez – é executado somente para uma única ocorrência. ○ Sob demanda - é executado imediatamente sob demanda. ○ Calendário comercial: Início da entrada - é executado nas datas de entrada inicial do calendário comercial selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ○ Calendário comercial: Término da entrada - Executa a data de término do calendário comercial selecionado no campo. Esta seleção é executada da mesma maneira que Calendário comercial: Início da entrada, mas para as datas de término das entradas de calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: Início da entrada ou Calendário comercial: Término da entrada, você pode aplicar um fator de deslocamento para programar a execução do trabalho antes ou depois do intervalo de tempo do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Desvio. Para saber mais sobre como criar e usar calendários comerciais e definir entradas de calendário comercial, consulte Crie um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	calendário comercial e. Defina entradas de calendário comercial .
Dia	Dia em que o trabalho agendado deve ser executado. ○ Se Executar estiver definido como Semanal, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanal no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ○ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele deve ser repetido em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo de hora quando você especifica a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ○ **Nenhum** : Use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado é executado às 04:45 horas, horário dos EUA/Pacífico, se for o fuso horário atribuído ao usuário, e você insere 16:45 no campo Hora.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Usar Fuso horário do sistema** : Use o fuso horário padrão do sistema especificado para a instância em que ele é executado. Por exemplo, o trabalho agendado será executado às 10:15 horas, horário de Londres, se Europa/Londres for o fuso horário padrão do sistema para a instância, e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho agendado é executado às 1:30 na EUA Fuso horário do leste se você selecionar EUA/Leste e inserir 13:30 no campo Hora.
run_as	Por padrão, run_ as valor do campo deve estar vazio. O usuário pode definir o valor como valor de usuário do domínio para criar problema para um domínio específico.

Configure o agendador para atualizar problemas automaticamente

Configure o agendador para atualizar o. Jira problemas automaticamente para os registros que foram adicionados à tabela sn_vul_agile_tool_manifest.

Antes de Iniciar

Função necessária: administrador ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa

Todos os registros do Item vulnerável à aplicação, Item vulnerável ao contêiner, tarefa de correção da aplicação e correção do contêiner criados na tabela sn_vul_agile_manifest são considerados para Jira atualização do problema. Se o registro for encerrado e comentários forem adicionados, esses valores também deverão ser atualizados para o associado Jira problema.

Nota:

- O trabalho agendado "atualizar problemas" não atualizará Jira estado se o fluxo de trabalho do projeto de problema ágil escolhido restringir qualquer usuário de mudar diretamente o estado de outro estado.
- Se você fechar qualquer registro de entidade com comentários adicionais, somente o último comentário será considerado no momento da atualização e, para a próxima atualização, todos os comentários serão adicionados ao associado Jira.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Trabalhos agendados** > **Atualizar problemas do Jira**.
2. Você pode modificar **Executar** , **Fuso horário** e **Hora** Campos no script programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Execução agendada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado: ○ Diariamente: É executado diariamente, em um horário designado. ○ Semanalmente: É executado semanalmente, em um horário e dia designados. ○ Mensal: É executado mensalmente, em um horário e dia designados do mês. ○ Executado em um intervalo de repetição designado. ○ Uma vez: É executado somente para uma única ocorrência. ○ Sob demanda: É executado imediatamente sob demanda. ○ Calendário comercial: Início da entrada: É executado nas datas de entrada inicial do calendário comercial selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ○ Fim da entrada: É executado para a data de término do calendário comercial selecionado no campo. Esta seleção é executada da mesma maneira que Calendário comercial: Início da entrada, mas para as datas de término das entradas de calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: Início da entrada ou Calendário comercial: Término da entrada, você pode aplicar um fator de deslocamento para programar a execução do trabalho antes ou depois do intervalo de tempo do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Desvio. Para saber mais sobre como criar e usar calendários comerciais e como definir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	entradas de calendário comercial, consulte e. Crie um calendário comercial Defina entradas de calendário comercial .
Dia	Dia em que o trabalho agendado deve ser executado. ○ Se Executar estiver definido como Semanal, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanal no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ○ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele deve ser repetido em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo de hora quando você especifica a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ○ Nenhum: Use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado é executado às 04:45 horas. Horário DOS EUA/Pacífico se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Hora.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Usar Fuso horário do sistema: Use o fuso horário padrão do sistema especificado para a instância em que ele é executado. Por exemplo, o trabalho agendado será executado às 10:15 horário de Londres se Europa/Londres for o fuso horário padrão do sistema para a instância e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho agendado será executado às 1:30 no fuso horário da Leste dos EUA se você selecionar EUA/Leste e inserir 13:30 no campo Hora.
run_as	Por padrão, o **executar_ como** o valor do campo está vazio. Você pode definir o valor como um usuário de domínio para criar um problema para um domínio específico.

Configure o agendador para sincronizar o. Jira status para ServiceNow® automaticamente

Configure o agendador para sincronizar o estado de Jira itens de vulnerabilidade da aplicação, itens de vulnerabilidade do contêiner e tarefas na tabela sn_vul_agile_manifest.

Antes de Iniciar

Função necessária: Schedule_admin ou admin

Por Que e Quando Desempenhar Esta Tarefa

O programador é executado automaticamente de acordo com a programação configurada. O estado dos registros criados na tabela Item vulnerável à aplicação, Item vulnerável ao contêiner, Tarefa de correção da aplicação e Tarefa de correção do contêiner que têm problemas criados em Jiraé atualizado de acordo com o status atual do problema em Jira Plataforma baseada no mapeamento de estado na regra de configuração.

Todos os registros de item vulnerável à aplicação, item vulnerável ao contêiner, tarefa de correção da aplicação e correção do contêiner criados na tabela sn_vul_agile_manifest serão considerados para Jira criação de problemas.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Trabalhos agendados** > **Status da sincronização**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no script programado.

Formulário Execução agendada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Diariamente: É executado diariamente, em um horário designado. ○ Semanalmente: É executado semanalmente, em um horário e dia designados. ○ Mensal: É executado mensalmente, em um horário e dia designados do mês. ○ Executado em um intervalo de repetição designado. ○ Uma vez: É executado somente para uma única ocorrência. ○ Sob demanda: É executado imediatamente sob demanda. ○ Calendário comercial: Início da entrada: É executado nas datas de entrada inicial do calendário comercial selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ○ Fim da entrada: É executado para a data de término do calendário comercial selecionado no campo. Esta seleção é executada da mesma maneira que Calendário comercial: Início da entrada, mas para as datas de término das entradas de calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: Início da entrada ou Calendário comercial: Término da entrada, você pode aplicar um fator de deslocamento para programar a execução do trabalho antes ou depois do intervalo de tempo do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Desvio. Para saber mais sobre como criar e usar calendários comerciais e definir entradas de calendário comercial, consulte Crie um calendário comercial e. Defina entradas de calendário comercial .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Dia	Dia em que o trabalho agendado deve ser executado. ○ Se Executar estiver definido como Semanal, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanal no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ○ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele deve ser repetido em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo de hora quando você especifica a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ○ -Nenhum-: Use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado é executado às 04:45 horas, horário dos EUA/Pacífico, se for o fuso horário atribuído ao usuário, e você insere 16:45 no campo Hora. ○ Usar Fuso horário do sistema: Use o fuso horário padrão do sistema especificado para a instância em que ele

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	é executado. Por exemplo, o trabalho agendado será executado às 10:15 horário de Londres se Europa/Londres for o fuso horário padrão do sistema para a instância e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho agendado será executado às 1:30 no fuso horário da Leste dos EUA se você selecionar EUA/Leste e inserir 13:30 no campo Hora.
run_as	Por padrão, o valor do campo run_ as está vazio. Você pode definir o valor como o valor do usuário do domínio necessário para criar um problema para um domínio específico.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integração

A integração do Prisma Cloud Compute permite verificar hosts para detectar vulnerabilidades.

A partir da versão 24.02.0 do Resposta a vulnerabilidades, Você pode usar o Prisma Cloud Compute Integration para importar vulnerabilidades nos hosts em execução. As APIs do host Prisma permitem a recuperação de informações abrangentes de vulnerabilidade para um host específico e também fornecem um snapshot das vulnerabilidades do host em um momento específico. Esta API permite a sincronização regular entre a instância Prisma e a ServiceNow. Como o Prisma é oferecido como software como serviço (SaaS) e solução no local, é necessário usar um MID Server para invocar APIs Prisma da instância da ServiceNow. Você precisa usar um MID Server. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute e seu ServiceNow AI Platform as instâncias não estão no mesmo ambiente. Para obter mais informações, consulte Requisitos do sistema DO MID Server .

Você também pode exibir relatórios sobre vulnerabilidades e itens vulneráveis no Resposta a vulnerabilidades painéis. Essas vulnerabilidades podem ser priorizadas e corrigidas.

Exibindo as integrações

Você pode exibir as integrações que fazem parte do Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Para exibir as integrações, navegue até **Tudo** > **Integração do Prisma Cloud Compute** > **Integrações**.

As integrações a seguir estão disponíveis.

Sequência de execução	Agendamento	Integração	Descrição
1	Diariamente	Prisma Cloud Compute Hosts Integration	Recupera vulnerabilidades de hosts e cria Vits, detecções e itens descobertos para hosts.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se o plug-in Resposta de vulnerabilidade do contêiner estiver instalado, você também poderá exibir as integrações relacionadas ao Resposta de vulnerabilidade do contêiner.

Integração do Prisma processo

. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud ComputeÉ executado, ele verifica se existe uma CVE (Common Vulnerability and Exposure, vulnerabilidade comum) na tabela NVD (National Vulnerability Database, banco de dados nacional de vulnerabilidades). Se já estiver presente, as informações existentes serão usadas. No entanto, se o CVE não for encontrado, registros de espaço reservado serão gerados na tabela NVD. Ao criar esses registros NVD de espaço reservado, inicialmente somente o CVE e seu nome são preenchidos. Outros detalhes não são preenchidos com a suposição de que a integração NVD preenche esses detalhes posteriormente. Se o parâmetro de instância de integração *update_nvd*Definido como verdadeiro, ele atualiza os registros NVD de espaço reservado. Por padrão, o parâmetro de instância é definido como falso. No entanto, pelo menos até que a integração do NVD seja executada e preencha esses detalhes, é necessária alguma compreensão do CVE, como sua gravidade ou algumas informações básicas sobre o problema. Para atender a este requisito, use os campos **Existe uma exploração** e. **Anotações de correção** São preenchidos com os detalhes obtidos do Prisma. Essa configuração é personalizável, permitindo que você especifique quaisquer outros campos que deseja preencher na entrada NVD com base nas informações fornecidas pelo Prisma.

Preparando para Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Você pode se preparar para Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute executando tarefas de configuração.

Antes de começar

Para instalar e configurar o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute, você pode imprimir a seguinte check-list. Verifique se os itens listados estão concluídos antes de instalar a aplicação e importar os dados de vulnerabilidade para seu ServiceNow AI Platform® instância.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL de base da API • Nome de usuário e senha. Essas credenciais são usadas para extrair as vulnerabilidades da integração do Prisma Cloud Compute. Para obter mais informações, consulte https://pan.dev/compute/api/ . **Nota:** MID Server é opcional. A credencial do usuário usada para a integração do Prisma Cloud Compute precisa de permissão para monitorar as imagens. Consulte o seguinte código: `{"permission":"monitorImages","saas":true,"self-hosted":true}`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Se ainda não estiver instalado e ativado, instale o. Resposta a vulnerabilidades aplicação antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,1 de Resposta a vulnerabilidades ou posterior.
☐	Obtenha direitos e baixe o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação em seu ServiceNow AI Platform® instância.
☐	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com ServiceNow Suporte técnico.
☐	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir os itens vulneráveis: **administrador** Instale o aplicativo Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade do contêiner (sn_vul_container.vulnerability_admin) e outras funções. **sn_vul_container.vulnerability_admin** Conclui a configuração da integração do Prisma Cloud Compute. Esta função tem acesso completo ao Contêiner de Resposta a vulnerabilidades(CVR) e seus registros. Este administrador configura integrações e regras em Contêiner de Resposta a vulnerabilidades. **Grupo de resposta a vulnerabilidades** Por padrão, o grupo Resposta a vulnerabilidades está disponível. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam sn_vul.read_all, sn_vul_container.read_all. **Grupo do responsável pela correção do contêiner** Por padrão, o grupo Proprietário de correção de contêiner está disponível. Os usuários atribuídos a este grupo herdam sn_vul_container.remediation_owner. O responsável pela correção do contêiner corrige as vulnerabilidades do contêiner atribuídas a ele ou a um grupo ao qual ele pertence. **Analista de vulnerabilidades** Os usuários atribuídos ao grupo Analista de vulnerabilidades de contêiner herdam sn_vul.vulnerability_analyst. O analista de vulnerabilidades monitora a correção de todos os itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
	Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância. Para obter mais informações, consulte Crie um grupo de usuários .
☐	Instale o. Resposta a vulnerabilidades Integração com NVD e execute a API de integração do banco de dados nacional de vulnerabilidades do NIST - (somente CVE).

Você está pronto para Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.

Instalar o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que o produto Prisma Cloud Compute se integre corretamente com Resposta a vulnerabilidades e. Contêiner de Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Leia **Outros requisitos** e. **Dependências** seções, se necessário.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.
7. Atualize o. **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .

Resultado
Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois
Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute para o seu ambiente. Consulte Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.

Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação

Instale e configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Aplicação para importar dados do Prisma Cloud Compute. Você pode usar os dados importados para priorizar e corrigir vulnerabilidades para seus hosts.

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Abra o e-mail de ServiceNow que você recebeu sobre a integração.
2. Faça login em sua instância como administrador.
3. Siga as instruções no e-mail para obter Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navegar até **Tudo** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.
   No formulário Configuração de computação em nuvem do Prisma, preencha os campos. Para obter mais informações, consulte Formulário de configuração de computação em nuvem do Prisma.
5. Na lista Projetos, selecione qualquer um **Todos os projetos** ou **Projetos específicos** para configurar todos os projetos ou projetos selecionados, respectivamente.
   Se você selecionar **Projetos específicos** , Você pode selecionar os projetos na lista Disponível.
6. Conclua a configuração selecionando qualquer um **Concluir** ou **Salvar e testar credenciais** .
   - Se você configurou um projeto, selecione **Concluir** .
   - Se você não configurou um projeto, selecione **Salvar e testar credenciais**
7. Exiba a instância recém-criada navegando até **Integração do Prisma Cloud Compute** > **Administração** > **Instâncias de Integração**.
8. Exiba os projetos que você configurou anteriormente selecionando **Parâmetros da instância de integração** .
9. Execute a instância de integração recém-criada para importar os itens vulneráveis.
   Os Vits são criados com base na granularidade.
10. Configure a granularidade de um item vulnerável.
    a. Navegar até **Integração do Prisma Cloud Compute** > **Configurar chaves de vulnerabilidade de imagem**
    b. Configure a granularidade dos Vits marcando as caixas de seleção necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os itens vulneráveis são criados com base nas chaves selecionadas durante a próxima importação.

Nota: Por padrão, um VIT é criado para uma combinação de Repositório de imagens,] Vulnerabilidade e marcador de imagem. Você pode adicionar componentes à chave para obter granularidade adicional. Por exemplo, você pode criar um CVIT para uma combinação de Repositório de imagens, Vulnerabilidade, Marcador de imagem e Cluster. Quando os itens vulneráveis ou as descobertas de itens vulneráveis são criados, as caixas de seleção não são mais editáveis.

Gráfico de status de execução de integração para integração de computação em nuvem Prisma

O módulo Status de execução da integração de computação em nuvem do Prisma fornece uma exibição gráfica do status das execuções da integração de computação em nuvem do Prisma.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer peça no gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: Administrador de vulnerabilidades

As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

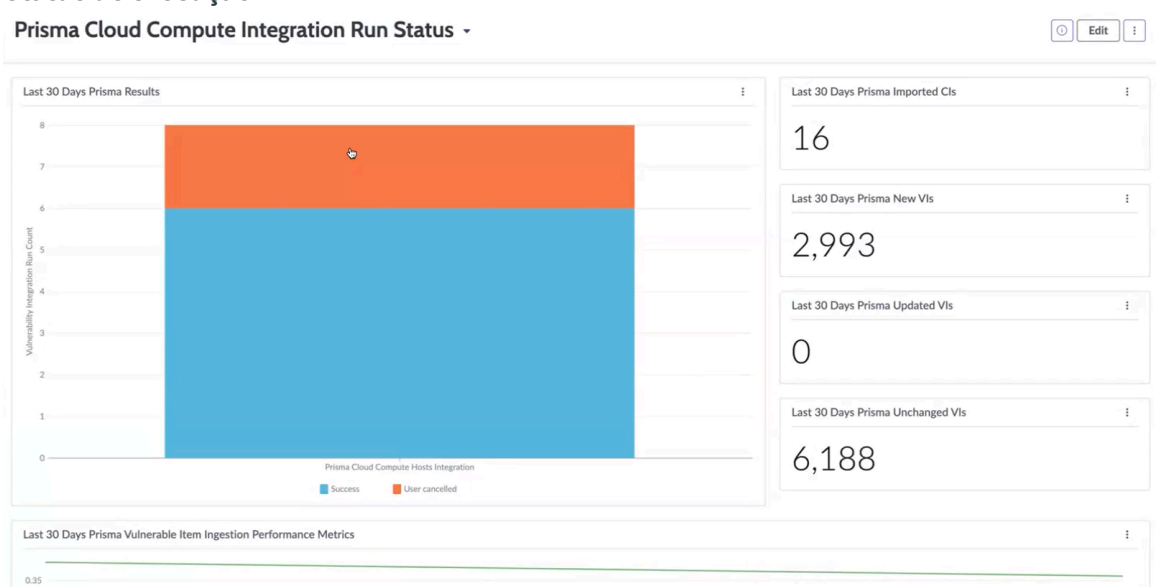
Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Para exibir os dados, navegue até **Tudo** > **Integração do Prisma Cloud Compute** > **Status da Execução da Integração**.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração do Prisma Cloud Compute executa relatórios de gráfico de status

Nome	Descrição
Resultados do Prisma dos últimos 30 dias	O número de execuções de integração concluídas para a integração. Mostra execuções bem-sucedidas e com falha. Cada execução exibida como uma barra no gráfico.
Prisma importou ICs nos últimos 30 dias	O número de itens de configuração (ICs) importados pelo Prisma nos últimos 30 dias. Mostrado como um número inteiro.
Prisma New VIS nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
Prisma atualizado nos últimos 30 dias	O número de itens vulneráveis (VIS) atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Prisma inalterada nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Métricas de desempenho de ingestão de item vulnerável do Prisma nos últimos 30 dias	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.

Noções básicas do Wiz Resposta a vulnerabilidades Integração

Importar dados de vulnerabilidade e conformidade do Wiz scanners em seu ServiceNow® Instância da plataforma de IA para ajudar você a obter informações mais detalhadas sobre os riscos da infraestrutura em nuvem. Essas integrações fornecem uma avaliação abrangente de sua postura geral de segurança na nuvem e ajudam a conduzir ações de correção diretamente da sua instância.

Integrações incluídas com Resposta a vulnerabilidades Integração com Wiz

. Resposta a vulnerabilidades Integração com Wiz inclui as seguintes integrações que importam dados de vulnerabilidade e conformidade:

- Wiz Integração de vulnerabilidade do host
- Wiz Contêiner de Resposta a vulnerabilidades Integração
- Wiz Conformidade de configurações (Resultados do teste) Integração e integração de problemas

Benefícios e usuários para as integrações

Benefício	Wiz Integração	Usuários
Importe e avalie detecções antecipadas de vulnerabilidades de host e vulnerabilidades em hosts em execução. A integração de vulnerabilidade do host importa descobertas relacionadas a máquinas virtuais e ativos sem servidor em seu ambiente de nuvem. Essas descobertas são mapeadas para Itens vulneráveis ao host (Vits) em Resposta a vulnerabilidades	Wiz Integração de vulnerabilidade do host.	Gerentes de vulnerabilidades, analistas e equipes de segurança na nuvem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Benefício	Wiz Integração	Usuários
aplicação para oferecer suporte a fluxos de trabalho de correção.		
Importe e avalie dados de vulnerabilidade da imagem do contêiner para ativos vulneráveis e fora de conformidade em sua infraestrutura de nuvem. As descobertas são mapeadas para Itens vulneráveis ao contêiner (CVITs) para oferecer suporte à triagem, priorização de risco e fluxos de trabalho de correção direcionados para cargas de trabalho baseadas em contêiner.	Wiz Integração de vulnerabilidade do contêiner.	Gerentes de vulnerabilidades, analistas e equipes de segurança na nuvem
Importar e avaliar resultados de teste de configuração de Wiz para detectar configurações de nuvem fora de conformidade. As descobertas são mapeadas para resultados de teste de nuvem (CTRs) no Conformidade de configurações aplicação para ajudar você a impor políticas e padrões de segurança em seu ambiente de nuvem. **Nota:** Configurações de host de Wiz não são importados.	Wiz Conformidade de configurações Integração (Wiz Resultados do teste).	Gerentes de vulnerabilidades, analistas e equipes de segurança na nuvem
Importação Wiz Problemas que identificam ativos envolvidos em combinações tóxicas de vulnerabilidades e configurações incorretas. Essas descobertas são mapeadas para CTRs e rotuladas com Problemas do Wiz como a origem para ajudar você a rastrear e corrigir ativos que podem representar riscos complexos e multivetoriais.	Wiz Integração de problemas.	Gerentes de vulnerabilidades, analistas e equipes de segurança na nuvem
Aplique etapas de correção em itens vulneráveis do host (Vits), itens vulneráveis do contêiner (CVTs), resultados de teste de nuvem (CTRs) e CTRs rotulados Problemas do Wiz .	Resposta a vulnerabilidades, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações aplicações.	Responsáveis pela correção

O que explorar a seguir

Para obter mais informações sobre como instalar, configurar e exibir dados importados com Wiz Integração de Resposta a vulnerabilidades, consulte:

- Ative o. Wiz Resposta a vulnerabilidades Aplicação de integração
- Configure o. Wiz Resposta a vulnerabilidades Integração
- Definir filtragem para Wiz Integração de vulnerabilidades do host
- Definir filtragem para Wiz Integração de vulnerabilidades de contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Definir filtragem para Wiz Integração de resultados de teste
- Definir filtragem para Wiz Integração de problemas
- Mapeamento de campo para Wiz Integrações de Resposta a vulnerabilidades

Ative o. Wiz Resposta a vulnerabilidades Aplicação de integração

Ative a aplicação necessária.

Antes de Iniciar

Verifique se você revisou as check-lists e instalou o seguinte ServiceNow® aplicações:

- Instalação de Resposta a vulnerabilidades e aplicações compatíveis Que incluem a integração NVD, Resposta a vulnerabilidades Integração com CISA e o trabalho agendado do CWE.
- Vulnerability Response e Configuration Compliance para contêineres.
- Conformidade de configurações.

Esses aplicativos estão disponíveis como assinaturas separadas. Consulte Instale um ServiceNow Store aplicação Para obter mais informações sobre como instalar aplicações da Store.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis**.
2. Localize Wiz Resposta a vulnerabilidades Aplicação de integração .
3. Selecione o cartão para abri-lo e selecione **Instalar** .
   Consulte Instale um ServiceNow Store aplicação Para obter mais informações sobre como instalar aplicações da Store.
   A caixa de diálogo de check-list de dependências é exibida. Selecione Qualquer **(Precisa ser instalado)** links para instalar dependências necessárias que você ainda não tenha instalado.
4. Selecione **Instalar** Na caixa de diálogo Instalação da aplicação.
   Uma mensagem é exibida depois que a aplicação é instalada com sucesso. Você está pronto para Configure o. Wiz Resposta a vulnerabilidades Integração.
5. Navegar até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Integrações**.
6. Verifique se as integrações com as quais você deseja importar dados estão ativadas (Coluna ativa definida como verdadeiro).
7. Selecione um registro para abri-lo e ativar ou desativar as integrações.

Configure o. Wiz Resposta a vulnerabilidades Integração

Configure a integração no seu Wiz conta de serviço e atribuir funções em seu ServiceNow Instância da plataforma de IA.

Antes de Iniciar

Você deve configurar o bloco de integração em seu Wiz conta que foi criada para esta integração com as permissões pré-selecionadas. Consulte Wiz documentação do produto para obter mais informações.

Função necessária:

- administrador para atribuir funções em seu ServiceNow Instância da plataforma de IA.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Atribua funções aos usuários para Wiz integração e para as aplicações que oferecem suporte ao na integração em seu ServiceNow Instância da plataforma de IA.

   a. Navegar até **Administração de usuários** > **Usuários**

   b. Atribua as seguintes funções.

   - sn_vul.vulnerability_admin para configurar o. Resposta a vulnerabilidades e. Contêiner de Resposta a vulnerabilidades aplicações.
   - sn_vulc.admin
   - sn_vul_wiz.configure_integration para configurar a integração.
   - sn_vul_wiz.read_integration para os usuários em sua organização que você deseja exibir dados e registros para esta integração.

   c. Consulte Administração de usuários para obter mais informações sobre como criar usuários e gerenciar funções.

2. Como um usuário com a função sn_vul_wiz.configure_integration, navegue até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configuração** em sua instância.
3. Preencha os campos.

Campo	Descrição
Instância de integração	Integração de Resposta a vulnerabilidades com Wiz.
URL de autenticação	URL de autenticação que você inseriu em Wiz ambiente.
URL da API	URL da API que você inseriu em Wiz ambiente.
ID de cliente	ID do cliente que você deseja usar para esta integração que você inseriu em Wiz ambiente.
Segredo do cliente	Segredo do cliente que você deseja usar para esta integração que você inseriu em Wiz ambiente.

4. **Selecione Salvar e testar** .
   Uma mensagem será exibida se as credenciais tiverem sido salvas e validadas com sucesso. Você pode selecionar a filtragem para as importações de integração.

Definir filtragem para Wiz Integração de vulnerabilidades do host

Defina os valores de filtragem para importar os dados de vulnerabilidade do host desejados.

Antes de Iniciar

Função necessária: sn_vul_wiz.configure_integration

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configuração**.
2. Se ainda não estiver selecionado, selecione **Configuração de vulnerabilidades do host** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos.
   Esses campos exibidos fornecem filtros para importar dados básicos de vulnerabilidade do host. Para exibir mais opções de filtragem, selecione **Avançado** e consulte a próxima tabela para obter mais informações.

Campo	Descrição
Primeiro	Paginação. Insira um valor. Você pode preferir começar com 1000.
Gravidade	Gravidade da descoberta. Nenhum é o padrão. Se selecionado, isso indica que você não deseja importar dados para este campo. Você pode especificar vários valores: ○ NENHUM - Retorna ativos sem valores de gravidade disponíveis. ○ BAIXO ○ MÉDIO ○ ALTO ○ CRÍTICO
Status do recurso	Retorna somente descobertas de vulnerabilidade para ativos com esses status. Você pode especificar vários valores: ○ Nenhum (padrão) - Se selecionado, indica que você não deseja importar dados para este campo. ○ Ativo ○ Erro ○ Inativo
Tipo de recurso	Filtre nesses tipos de objeto. Você pode especificar ambos os valores: ○ Nenhum (padrão) - Se selecionado, indica que você não deseja importar dados para este campo. ○ VIRTUAL_MACHINE ○ SEM SERVIDOR

4. Marque a caixa de seleção Avançado para exibir mais opções de filtragem.

   Para a maioria dos campos, você pode especificar vários valores. --Nenhum-- (padrão). Se --Nenhum-- permanece selecionado para um campo, nenhum dado é importado para este campo.

Campo	Descrição
Status	Filtrar por status da descoberta:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ ABERTO ○ REJEITADO ○ RESOLVIDO
Método de detecção	Filtre as descobertas de vulnerabilidade encontradas por estes métodos de detecção: ○ PACOTE ○ DEFAULT_PACKAGE ○ BIBLIOTECA ○ SO ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ FILE_PATH
Gravidade do problema relacionado	○ CRÍTICO ○ ALTO ○ INFORMATIVO ○ BAIXO ○ MÉDIO
Vulnerabilidade	Filtre as descobertas de vulnerabilidade com IDs externos correspondentes inseridos, por exemplo, CVE-1234-5678,CVE-9110-26117.
Tem exploração pública	Filtre as descobertas de vulnerabilidade para vulnerabilidades com uma exploração disponível: (Verdadeiro/falso).
ID do projeto	Filtre descobertas de vulnerabilidade com cadeias de caracteres que você insere para os projetos fornecidos.
Tem correção	Filtre as descobertas de vulnerabilidade para vulnerabilidades com uma correção disponível (verdadeiro/falso).
Recurso	Filtre um recurso inserido.
O recurso tem privilégios de administrador	Filtre descobertas de vulnerabilidade para ativos que têm privilégios de administrador (verdadeiro/falso).
Assinatura	Importe descobertas das seguintes cadeias de caracteres para assinaturas externas: (Conta da AWS, assinatura do Azure, projeto do GCP e compartimento do OCI). Você pode especificar vários valores em uma matriz. Se você não fornecer um valor, todas as assinaturas serão retornadas.
Tem exploração de KEV do CISA	Filtre descobertas de vulnerabilidade para vulnerabilidades com uma exploração de CISA KEV disponível (verdadeiro/falso).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
O recurso tem altos privilégios	Filtre descobertas de vulnerabilidade para ativos que têm privilégios altos (verdadeiro/falso).
O recurso tem ampla exposição na Internet	Filtre descobertas de vulnerabilidade para ativos que têm alta exposição à Internet (verdadeiro/falso).
O recurso tem exposição limitada na Internet	Filtre descobertas de vulnerabilidade para ativos com baixa exposição à Internet (verdadeiro/falso).
Visto pela primeira vez em (depois)	Filtre por ativos vistos a partir de uma data selecionada.
Resolvida em (após)	Filtre por ativos com vulnerabilidades que foram resolvidas a partir de uma data selecionada.
Atualizado em (após)	Filtre por ativos que foram atualizados a partir de uma data selecionada.

5. **Selecione Salvar e testar** .
   Se as credenciais tiverem sido salvas e validadas com sucesso, uma mensagem será exibida. Você pode selecionar a filtragem para outra importação de integração.

Definir filtragem para Wiz Integração de vulnerabilidades de contêiner

Defina os valores de filtragem para importar os dados de vulnerabilidade do contêiner desejados.

Antes de Iniciar

Função necessária: sn_vul_wiz.configure_integration

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configuração**.
2. Selecione **Configuração de vulnerabilidades de contêiner** guia.
3. Preencha os campos.

   Para alguns campos, você pode especificar vários valores. --Nenhum-- (padrão). Se --Nenhum-- permanece selecionado para um campo, nenhum dado é importado para este campo.

Campo	Descrição
Primeiro	Paginação. Insira um valor. Você pode preferir começar com 1000.
Tem exploração pública	Filtre as descobertas de vulnerabilidade para vulnerabilidades com uma exploração disponível: (Verdadeiro/falso).
Assinatura	Importe descobertas das seguintes cadeias de caracteres para IDs de assinatura externa: (Conta da AWS, assinatura do Azure, projeto do GCP e compartimento do OCI). Se você não fornecer um valor, todas as assinaturas serão retornadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tem correção	Importe descobertas de vulnerabilidade para vulnerabilidades com uma correção disponível (verdadeiro/falso).
Vulnerabilidade	Importe descobertas de vulnerabilidade com IDs externos correspondentes, por exemplo, CVE-1234-5678, CVE-9110-26117.
Tem exploração de KEV do CISA	Importe somente descobertas de vulnerabilidade para vulnerabilidades com uma exploração de CISA KEV disponível (verdadeiro/falso).
ID do projeto	Importe somente descobertas de vulnerabilidade para os projetos fornecidos (cadeias de caracteres).
O recurso tem altos privilégios	Retorna somente descobertas de vulnerabilidade que tenham privilégios altos (verdadeiro/falso).
Status do recurso	Retornar somente descobertas com estes status. Você pode especificar vários valores: ○ Ativo ○ Erro ○ Inativo
O recurso tem privilégios de administrador	Retorna somente descobertas de vulnerabilidade que tenham privilégios de administrador. (verdadeiro/falso)
Método de detecção	Filtre as descobertas de vulnerabilidade encontradas por estes métodos de detecção: ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ BIBLIOTECA ○ SO ○ PACOTE
O recurso tem exposição limitada na Internet	Filtre descobertas de vulnerabilidade que tenham baixa exposição à Internet (verdadeiro/falso).
Severidade da Vulnerabilidade	Filtrar descobertas por gravidade da vulnerabilidade: ○ CRÍTICO ○ ALTO ○ BAIXO ○ MÉDIO
Status	Filtrar descobertas por status: ○ ABERTO ○ RESOLVIDO

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Selecione Salvar e testar** .
   Se as credenciais tiverem sido salvas e validadas com sucesso, uma mensagem será exibida. Você pode selecionar a filtragem para outra importação de integração.
5. **Opcional:** Configure a granularidade dos itens vulneráveis ao contêiner (CVITs) especificando a combinação de chaves.

   (Optional) Um CVIT é criado por padrão combinando o repositório de imagens, a vulnerabilidade e a imagem. Você pode adicionar componentes à chave para obter granularidade adicional. Por exemplo, Criar um CVIT é para uma combinação de repositório de imagens, vulnerabilidade, imagem e cluster.

   Para configurar a granularidade, navegue até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configurar granularidade de IV baseada em CVR**.

   Selecione as chaves que você deseja adicionar. Se os dados forem importados, as chaves serão consideradas e as CVITs serão criadas.

Definir filtragem para Wiz Integração de resultados de teste

Defina os valores de filtragem para importar os dados de resultados de teste de nuvem desejados.

Antes de Iniciar
Função necessária: sn_vul_wiz.configure_integration

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configuração**.
2. Selecione **Configuração dos resultados do teste** guia.
3. Preencha os campos.

   Para alguns campos, você pode especificar vários valores. --Nenhum-- (padrão). Se --Nenhum-- permanece selecionado para um campo, nenhum dado é importado para este campo.

   Nota: Configurações de host de Wiz não são importados.

Campo	Descrição
Gravidade	Escolha um para filtragem de gravidade: ○ BAIXO ○ MÉDIO ○ ALTO ○ CRÍTICO ○ NENHUM - Retorna descobertas sem valores de gravidade disponíveis. Você pode preferir começar com ALTO ou CRÍTICO para limitar sua importação a descobertas de importância crítica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID do projeto	Especifique somente descobertas de configuração de nuvem para projetos, por exemplo, Nomeado "ID do projeto" .
Plataforma de nuvem	Descobertas da configuração por plataforma em nuvem. Você pode especificar vários valores, por exemplo, AWS, GitHub, terraform, OPENAI, GKE, OKE, EKS, AKS.
ID de Assinatura	Especifique inserindo o ID de assinatura. Você pode especificar vários valores em uma matriz.
Status do recurso	Especificar por status: ○ Ativo ○ Erro ○ Inativo
Categoria de estrutura	Insira estruturas de segurança, subcategorias de segurança ou categorias de segurança. Você pode especificar vários valores.
Tipo de recurso	Tipos de entidade. Você pode especificar vários valores, por exemplo, BUCKET, BANCO DE DADOS
Tipo nativo	Especifique descobertas com base no tipo nativo do recurso de nuvem, por exemplo, bucket .
Tem correção	Especifique descobertas com (VERDADEIRO ou sem (FALSO instruções de correção.
Primeiro	Paginação. Insira um valor. Você pode preferir começar com 1000.
Analisado após	Filtre descobertas que foram analisadas a partir de uma data selecionada.
Status	Filtrar por status: ○ ABERTO ○ RESOLVIDO

Tradução automática

4. **Selecione Salvar e testar** .
   Se as credenciais tiverem sido salvas e validadas com sucesso, uma mensagem será exibida. Você pode selecionar a filtragem para outra importação de integração.

Definir filtragem para Wiz Integração de problemas

Defina os valores de filtragem a serem importados Wiz Problemas que identificam ativos envolvidos em combinações tóxicas de vulnerabilidades e configurações incorretas.

Antes de Iniciar
Função necessária: sn_vul_wiz.configure_integration

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade do Wiz** > **Administração** > **Configuração**.
2. Selecione **Configuração de problemas** guia.
3. Preencha os campos.

   Para alguns campos, você pode especificar vários valores. --Nenhum-- (padrão). Se --Nenhum-- permanece selecionado para um campo, nenhum dado é importado para este campo.

Campo	Descrição
Gravidade	Filtre por gravidade da descoberta. ○ BAIXO ○ MÉDIO ○ ALTO ○ CRÍTICO ○ INFORMATIVO
ID do projeto	Importe somente descobertas para os projetos fornecidos (cadeias de caracteres).
Tipo de ocorrência	Problemas pelo tipo de regra pelo qual eles são gerados. ○ CLOUD_CONFIGURATION ○ THREAT_DETECTION ○ TOXIC_COMBINATION
ID de Assinatura	Especifique as descobertas inserindo um ID de assinatura. Você pode especificar vários valores em uma matriz.
Plataforma de nuvem	Descobertas da configuração por plataforma em nuvem. Você pode especificar vários valores, por exemplo, AWS, GitHub, terraform, OPENAI, GKE, OKE, EKS, AKS.
Categoria de estrutura	Insira estruturas de segurança, subcategorias de segurança ou categorias de segurança. Você pode especificar vários valores.
Tipo nativo	Problemas baseados no tipo nativo do recurso de nuvem, por exemplo, bucket .
Primeiro	Paginação. Insira um valor. Você pode preferir começar com 1000.
Status	Filtrar por status: ○ ABERTO ○ EM ANDAMENTO ○ RESOLVIDO

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Selecione Salvar e testar** .
   Se as credenciais tiverem sido salvas e validadas com sucesso, uma mensagem será exibida. Você pode selecionar a filtragem para outra importação de integração.

Mapeamento de campo para Wiz Integrações de Resposta a vulnerabilidades

Revise os campos de origem e de destino e exiba dados importados em tabelas e registros em seu ServiceNow Instância da IA da Now Platform.

Mapeamento de campo de integração de vulnerabilidade do host

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
descrição	sn_vul_detection	prova
status	sn_vul_detection	source_status
LastDetectedAt	sn_vul_detection	last_found
FirstDetecteAt	sn_vul_detection	first_found
vulnerableAsset.name	sn_vul_detection	dns
correção	sn_vul_detection	solution_summary
VulnerableAsset.ipAddresses[0]	sn_vul_detection	ip_address
VendorSeveridade	sn_vul_detection	source_severity
FixedVersion	sn_vul_detection	fixed_version
status	sn_vul_detection	_ignorado
status	sn_vul_detection	status
nome	sn_vul_nvd_entry	id
pontuação	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	resumo
VendorSeveridade	sn_vul_nvd_entry	source_severity
Cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
Cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
Cvssv3.ConfidentialityImpacto	sn_vul_nvd_entry	v3_confidential_impact
Cvssv3.privilegesNecessário	sn_vul_nvd_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
TemExploit	sn_vul_nvd_entry	exploração
TemCisaKevExploit	sn_vul_nvd_entry	cisa_exists
VulnerableAsset.tags	sn_sec_cmn_src_ci	host_tag
vulnerableAsset.id	sn_sec_cmn_src_ci	source_id
vulnerableAsset.name	sn_sec_cmn_src_ci	nome
VulnerableAsset.region	sn_sec_cmn_src_ci	cloud_region

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
vulnerableAsset.providerUniqueId	sn_sec_cmn_src_ci	resource_id
VulnerableAsset.cloudPlatform	sn_sec_cmn_src_ci	cloud_service_provider
VulnerableAsset.type	sn_sec_cmn_src_ci	assetType
RelatedIssueAnalytics	sn_sec_cmn_src_ci	source_data
VulnerableAsset.nativeType	sn_sec_cmn_src_ci	cloud_resource_type
VulnerableAsset.subscriptionExternalId	sn_sec_cmn_src_ci	cloud_account
vulnerableAsset.name	sn_sec_cmn_src_ci	resource_name
VulnerableAsset.imageName	sn_sec_cmn_src_ci	image_id
VulnerableAtivo.*	sn_sec_cmn_src_ci	source_data
LastDetectedAt	sn_sec_cmn_src_ci	source_data

Mapeamento de campo de integração de vulnerabilidade do contêiner

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
ImageId	sn_vul_container_image	image_id
vulnerableAsset.name	sn_vul_container_image	image_name
VulnerableAsset.repositório.externalId após o nº	sn_vul_container_image	registro
VulnerableAsset.repositório.externalId antes do nº	sn_vul_container_image	reposição
VulnerableAsset.tags	sn_vul_container_image	image_labels
projetos	sn_vul_container_image	image_projects
VulnerableAsset.region	sn_vul_container_image	cloud_regions
VulnerableAsset.cloudPlatform	sn_vul_container_image	cloud_providers
VulnerableAsset.subscriptionExternalId	sn_vul_container_image	cloud_account_ids
vulnerableAsset.executionControllersAncestorContainer	sn_vul_container_image	image_namespace
vulnerableAsset.executionControllersAncestorContainer	sn_vul_container_image	image_clusters
vulnerableAsset.executionControllersAncestorContainer	sn_vul_container_image_vulnerable_item	image_clusters
vulnerableAsset.executionControllersAncestorContainer	sn_vul_container_image_vulnerable_item	image_namespace
VulnerableAsset.repositório.externalId antes do nº	sn_vul_container_image_vulnerable_item	image_repositório
LayerMetadata.isBaseLayer	sn_vul_container_image_findings	_base_image
FirstDetecteAt	sn_vul_container_image_findings	first_found
LastDetectedAt	sn_vul_container_image_findings	last_found
DetailedName	sn_vul_container_image_package	nome
versão	sn_vul_container_image_package	versão
LocationPath	sn_vul_container_image_package	caminho

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
nome	sn_vul_nvd_entry	id
pontuação	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	resumo
vendorseveridade	sn_vul_nvd_entry	source_severity
Cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
Cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
Cvssv3.ConfidentialityImpacto	sn_vul_nvd_entry	v3_confidential_impact
Cvssv3.privilegesNecessário	sn_vul_nvd_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
TemExploit	sn_vul_nvd_entry	TemExploit
LayerMetadata.isBaseLayer	sn_vul_container_image_layer	Camada de base
layerMetadata.details	sn_vul_container_image_layer	instrução
layerMetadata.id	sn_vul_container_image_layer	id
status	sn_vul_container_image_findings	_ignorado
validate_at_runtime	sn_vul_container_image_findings	validate_at_runtime
id	sn_vul_container_image_findings	unique_key

Conformidade de configurações mapeamento do campo de integração de resultados de teste

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
rule.id	sn_vulc_test	source_id
rule.name	sn_vulc_test	short_description
Rule.remediationInstrutions	sn_vulc_test	correção
rule.description	sn_vulc_test	descrição
severidade	sn_vulc_test	source_criticality
status	sn_vulc_result	resultado
id	sn_vulc_result	source_id
AnalizadoAt	sn_vulc_result	last_seen
PristSeenAt	sn_vulc_result	first_seen
Rule.remediationInstrutions	sn_vulc_result	correção
Resource.nativeType	sn_sec_cmn_src_ci	source_data
resource.type	sn_sec_cmn_src_ci	source_data
id	sn_vulc_result	descrição
id	sn_vulc_result	source_id

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
securitySubCategories.category.framework.id	sn_vulc_auth_src	source_id
securitySubCategories.category.framework.name	sn_vulc_auth_src	short_description
securitySubCategories.category.framework.description	sn_vulc_auth_src	descrição
securitySubCategories.id	sn_vulc_citation	seção
SecuritySubCategories.title	sn_vulc_citation	section_name
resource.projects	sn_sec_cmn_src_ci	projetos
status	sn_vulc_result	_ignorado

Mapeamento de campo de integração de problemas

Nota: Os dados mapeados para os problemas Integração com resultados de teste de nuvem (CTRs) são rotulados com Problemas do Wiz Como a origem para ajudar você a diferenciar esses CTRs dos CTRs de integração de resultados de teste.

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
sourceRule.id	sn_vulc_test	source_id
sourceRule.name	sn_vulc_test	short_description
SourceRule.ResolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_test	correção
sourceRule.description	sn_vulc_test	descrição
severidade	sn_vulc_test	source_criticality
createdAt	sn_vulc_result	first_seen
updatedAt	sn_vulc_result	last_seen
status	sn_vulc_result	resultado
id	sn_vulc_result	source_id
SourceRule.ResolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_result	correção
SourceRule.controlDescription	sn_vulc_result	descrição
EntitySnapshot.nativeType	sn_sec_cmn_src_ci	source_data
EntitySnapshot.type	sn_sec_cmn_src_ci	source_data
Problema do Wiz'	sn_vulc_result	result_type
id	sn_vulc_result	descrição
severidade	sn_vulc_test	source_criticality
id	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.id	sn_vulc_auth_src	source_id
sourcerule.securitySubCategories.category.framework.name	sn_vulc_auth_src	short_description
sourcerule.securitySubCategories.category.framework.description	sn_vulc_auth_src	descrição
sourcerule.securitySubCategories.id	sn_vulc_citation	seção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Wiz	ServiceNow coluna da tabela	ServiceNow coluna de campo
sourcerule.securitySubCategories.title	sn_vulc_citation	section_name
projetos	sn_sec_cmn_src_ci	projetos
status	sn_vulc_result	_ignorado

Mapeamento para itens vulneráveis e registros de resultado de teste

- As descobertas de vulnerabilidade do host são mapeadas para Itens vulneráveis do host (Vits).
- As descobertas de vulnerabilidade do contêiner são mapeadas para Itens vulneráveis ao contêiner (CVITs).
- As descobertas dos resultados do teste de configuração são mapeadas para Registros de resultados de testes em nuvem (CTRs) no Conformidade de configurações aplicação.
- As descobertas de problemas são mapeadas para registros de resultados de testes em nuvem (CTRs) no Conformidade de configurações aplicação.

Criar manualmente uma integração de vulnerabilidade

As integrações de vulnerabilidades permitem que clientes e fornecedores enriqueçam os dados de vulnerabilidade em sua instância recuperando dados de sistemas e fornecedores externos. Essa capacidade pode simplificar o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Para obter instruções detalhadas sobre como criar integrações, consulte Defina uma nova integração de vulnerabilidade.

Defina uma nova integração de vulnerabilidade

Uma integração de vulnerabilidade extrai dados de relatório de um sistema de terceiros, geralmente para recuperar dados de vulnerabilidade e processar esses dados de relatório usando fontes de dados ou um processador personalizado.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Integrações**.
2. Clique em **Nova**.
3. Preencha os campos, conforme necessário.

Integração da vulnerabilidade

Campo	Descrição
Nome	Um nome descritivo para a integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Se a integração está ativa. Se você não quiser que ele seja executado por um período específico, configure os parâmetros que deseja usar e desative o trabalho.
Executar	A frequência que você deseja que a integração execute, Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos ou não com base em sua configuração neste campo.
Dia	O dia em que você deseja que a integração seja executada. ○ Se você selecionou **Semanalmente** em **Executar** este campo exibe os dias da semana. ○ Se você selecionou **Mensal** em **Executar** este campo exibe os dias do mês.
Hora	A hora em que você deseja que a integração comece. Este campo aparecerá somente se você selecionou **Diariamente** , **Semanalmente** ou **Mensal** em **Executar** campo.
Aplicação	[Somente leitura] O nome da aplicação para a qual esta integração foi criada.
Intervalo de repetição	Se você selecionou **Periodicamente** em **Executar** este campo exibe o número de dias e horas antes que a integração seja executada novamente.
Iniciando	Se você selecionou **Periodicamente** em **Executar** este campo exibe as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Se quiser adicionar parâmetros condicionais, selecione este campo.
Condição	Se você selecionou **Condicional** insira as condições aqui.
Detalhes de Integração	
Script de integração	Selecione a inclusão de script que estende VulnerabilityIntegrationBase a ser executada quando a integração for executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Insira um script que defina como construir a inclusão de script selecionada para **Script de integração** . Para obter mais informações, consulte Campos de script de fábrica de integração. **Nota:** Os scripts exigem ambos ServiceNow e. Resposta a vulnerabilidades experiência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estratégia do processador de relatórios	Selecione a estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração for executada. ○ Selecione **Anexo de fonte de dados** se você quiser processar dados usando uma fonte de dados. ○ Selecione **Processador de relatório personalizado** para selecionar um processador personalizado.
Processador de relatórios	Se você selecionou **Processador de relatório personalizado** em **Estratégia do processador de relatório** Selecione a inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase a ser executada quando a integração for executada. Este script define como processar os dados retornados pelo script de integração.
Script de fábrica do processador	Insira um script que defina como construir a inclusão de script selecionada para **Processador de relatório** .

4. Clique em **Enviar**.

Tópicos relacionados

Script de integração de vulnerabilidades

Estratégias do processador de relatórios

Campos de script de fábrica de integração

Executar manualmente uma integração de vulnerabilidade

Script de integração de vulnerabilidades

No formulário Integração de vulnerabilidades, o script de integração é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityIntegrationBase.

A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController para gerenciar os meios pelos quais os dados são recuperados de uma fonte de dados externa. Cada subclasse de VulnerabilityIntegrationBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- IntegrationGr: Um GlideRecord do registro de integração de vulnerabilidade que solicitou a execução da integração.
- IntegrationProcessGr - GlideRecord que fornece informações contextuais para o processo atual de uma integração.

O processo de vulnerabilidade contém parâmetros especiais a serem usados em uma integração, geralmente para fins de paginação. Cada execução de uma integração de vulnerabilidade (chamada Execução de integração de vulnerabilidade) tem pelo menos um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

processo de integração de vulnerabilidade associado. Para integrações de várias chamadas, há um ou mais registros de processo de integração de vulnerabilidades para cada Execução de integração de vulnerabilidades.

A inclusão de script deve fornecer uma implementação para `RetrieveData()` e retornam um objeto que é processado pelo script do processador de relatório. O objeto retornado por retrieveData é um objeto simples com propriedades para conteúdo, contentType e extensão.

Esta é uma captura de tela de VulnerabilityIntegrationBase.retrieveData():

IntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

A lógica no `RetrieveData()` depende da interface necessária para recuperar os dados. Por exemplo, se a origem dos dados que estão sendo extraídos tiver uma REST API, o corpo desse método poderá estar chamando o endpoint REST, provavelmente por meio de RESTMessageV2. A resposta da chamada pode ser analisada ou colocada em um anexo, e os detalhes podem ser usados para construir o objeto de retorno.

Integrações de chamada única

Scripts de integração de chamada única (página única) são os tipos mais simples de integrações. Eles exigem uma chamada, geralmente para uma fonte externa de dados, para recuperar dados. Apenas o retrieveData() precisa ser implementado para integrações de página única/chamada única.

Uma amostra que demonstra um script simples de integração de chamada única é a seguir. Ele cria um RESTMessageV2 e o executa. Em seguida, ele retorna um objeto usando o corpo da resposta como o conteúdo, junto com um contentType e uma extensão presumidos.

Script de integração de chamada única

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de várias chamadas

Scripts de integração de várias chamadas (ou várias páginas) são um pouco mais complicados. Eles exigem várias chamadas para uma fonte de dados para recuperar dados.

Como uma integração de chamada única, uma integração de chamada múltipla também deve ter retrieveData() implementado. No corpo de retrieveData(), a integração usa os métodos hasMoreData() e setNextRunParameters() fornecidos pelo VulnerabilityIntegrationBase.

O método hasMoreData() aceita um único booliano que instrui o VulnerabilityIntegrationController a inserir mais processos para extrair mais dados. Ao passar verdadeiro para hasMoreData(), uma chamada para setNextRunParameters() é feita para fornecer contexto para o próximo processo.

O método setNextRunParameters() aceita um único objeto que fornece informações de contexto a serem usadas pela próxima chamada para retrieveData(). Este objeto é usado para passar estado para chamadas subsequentes para retrieveData(). Um exemplo de caso de uso é passar um objeto que indica o número da página atual e o tamanho da página para um serviço web.

Para integrações de várias chamadas, cada chamada de retrieveData() verifica primeiro os parâmetros do processo atual. O método _getProcessParameters() é fornecido a todas as VulnerabilityIntegrationBase como uma conveniência para obter os parâmetros definidos pelo processo anterior. Se não houver parâmetros, isso indicaria que é o primeiro processo.

Uma captura de tela de um exemplo de script de integração de várias chamadas é exibida a seguir. Estendendo o exemplo de integração de chamada única, este script demonstra como fazer chamadas para um endpoint REST que tem suporte a paginação básica. Ele mostra como você pode obter uma única página de dados, reconhecer que há mais dados para recuperar e informar ao próximo processo qual página recuperar.

Script de integração de várias chamadas

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anexos como RetrieveData() valores de retorno

Às vezes, é preferível retornar um anexo de retrieveData(). A lógica para criar e/ou recuperar um anexo é específica da implementação, mas depois que o anexo é conhecido, suas informações podem ser retornadas.

Para fornecer um anexo, retrieveData() retorna um objeto como:

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

Um exemplo que se estende no exemplo anterior , Mas salva o corpo da resposta da mensagem REST no registro do processo de integração a seguir. Em seguida, ele retorna esse identificador de anexo como o conteúdo do objeto de retorno.

Retornar anexo de retrieveData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Estratégias do processador de relatórios

. **Estratégia do processador de relatório** O campo no formulário Integração de vulnerabilidades é usado para selecionar o método para processar os dados retornados pelo script de integração de vulnerabilidades quando o processo de integração de vulnerabilidades é executado.

O valor padrão é **Anexo de fonte de dados** . Este método é a implementação de linha de base que usa os dados recuperados e os passa para uma fonte de dados para serem importados para o sistema. Selecionando **Processador de relatório personalizado** permite selecionar um script de processador personalizado para processar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use a estratégia do processador de relatório de anexo da fonte de dados

A estratégia do processador de relatório de anexo de fonte de dados é usada para passar dados recuperados pelo script de integração para fontes de dados configuradas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Integrações** e. crie uma nova integração .
2. Em **Estratégia do processador de relatório** campo, selecione **Anexo de fonte de dados** .
3. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
4. Em **Fontes de dados de integração de vulnerabilidades** lista relacionada, clique em **Novo** .
5. Defina a fonte de dados a ser usada.
6. Clique em **Enviar**.
7. Repita as etapas 4 a 6 se precisar de fontes de dados adicionais.
   Especifique a ordem em que as várias fontes de dados enviam informações no **Pedido** campo.
8. Clique em **Atualizar**.

Sobre scripts de processador de relatório personalizados

No formulário Integração de vulnerabilidades, o Processador de relatório é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase. A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController e define os meios pelos quais os dados retornados pelo script de integração são processados.

Cada subclasse de VulnerabilityReportProcessorBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- IntegrationGr - um GlideRecord do registro de Integração de vulnerabilidades que solicitou a execução da integração.
- IntegrationProcessGr - GlideRecord do processo de vulnerabilidade que fornece informações contextuais para o processo atual de uma integração.

A inclusão de script deve fornecer uma implementação para `ProcessReport()` método. O objeto passado para processReport() é o objeto retornado por retrieveData e, como tal, é um objeto simples com propriedades para content, contentType e extension. A lógica real em processReport() é específica da implementação e depende dos dados do relatório fornecidos.

Aqui está uma captura de tela do VulnerabilityReportProcessorBase.processReport():

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Script do processador de relatório personalizado

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Campos de script de fábrica de integração

O formulário Integração de vulnerabilidades contém o script de fábrica de integração e, quando **Processador de relatório personalizado** A estratégia do processador de relatório está selecionada, o script de fábrica do processador. Esses campos são usados para fornecer a lógica para realmente instanciar o objeto definido pelos campos de referência de inclusão de script, script de integração e processador de relatório, respectivamente.

Quando a inclusão de script é selecionada, ambos os campos são preenchidos previamente com uma chamada de construtor sem argumento. Isso é suficiente, mas pode haver ocasiões em que mais lógica é necessária para instanciar o objeto de script.

O registro integrationProcessGr é exposto aos campos de script de fábrica para que informações específicas do processo possam ser usadas, conforme necessário.

Executar manualmente uma integração de vulnerabilidade

Integrações de vulnerabilidades para Resposta a vulnerabilidades e. Resposta a vulnerabilidades de aplicações são configurados para serem executados em uma base programada. No entanto, você pode executá-los manualmente quando necessário.

Antes de Iniciar
Funções necessárias:

- sn_vul.read_integrations (Resposta a vulnerabilidades)
- sn_vul.app_read_integrations (Resposta a vulnerabilidades de aplicações)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa
Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
2. Abra o registro da integração que você deseja executar.
3. Clique em **Executar Agora**.

Ingestão manual de vulnerabilidades

Ingerir manualmente vulnerabilidades no Resposta a vulnerabilidades para que você possa corrigi-los rapidamente sem precisar esperar os resultados do scanner.

Scanners de terceiros, como Rapid7 importar dados de vulnerabilidade para Resposta a vulnerabilidades e processam os dados para relatar as descobertas. Com a integração de ingestão manual, você pode ingerir proativamente as vulnerabilidades e corrigi-las em vez de esperar que os scanners relatem os ativos que estão em risco. A ingestão manual de vulnerabilidades protege efetivamente os ativos contra ameaças desconhecidas, como explorações de dia zero.

Ingestão manual de vulnerabilidades

Você pode importar os dados da vulnerabilidade carregando um modelo nos seguintes formatos de arquivo:

- Excel
- Valor separado por vírgulas (CSV)

Para acessar e baixar o modelo, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Carregar IU de arquivo**.

Siga estes pontos principais ao preencher os registros no modelo:

- Não faça erros de digitação nos registros da coluna Severidade/Estado. Se houver um erro de digitação, o registro será ignorado.
- Não mude os nomes das colunas.
- Não coloque nomes de coluna em nenhuma linha, exceto na primeira linha.
- Não altere a ordem das folhas no Microsoft Excelmodelo. Os dados de vulnerabilidades devem estar sempre presentes na segunda planilha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Não coloque detalhes de vulnerabilidades em nenhuma planilha, exceto na planilha Detecções manuais de entrada.
- Não use caracteres, exceto caracteres alfanuméricos e especiais, como hífen (-), ponto (.), mais (

Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.

A partir da v24.0.6 de Resposta a vulnerabilidades você também pode criar colunas adicionais no Microsoft Excel modelo. Para obter mais informações, consulte KB1646630 .

Integrações de ingestão manual

A integração é acionada quando um arquivo é carregado. Com base no tipo de arquivo carregado, a integração relacionada é acionada.

Para exibir as integrações, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Integrações**.

As seguintes integrações de ingestão manual do sistema de base estão disponíveis por padrão.

Integrações

Tipos de integração	Descrição
Integração do Excel de ingestão manual	Recupera dados buscando o mais recente Microsoft ExcelArquivo carregado da tabela Fila de push de ingestão de vulnerabilidades e copia o anexo para a respectiva execução de integração.
Integração CSV de ingestão manual	Recupera dados buscando o arquivo CSV mais recente carregado da tabela Fila de push de ingestão de vulnerabilidades e copia o anexo para a respectiva execução de integração.

A integração de terceiros de ingestão manual cria uma instância de integração, por padrão, com os dois seguintes parâmetros de instância de integração:

- max_input_records: Define o número de registros que podem ser criados no modelo. Se você adicionar mais registros do que o especificado neste parâmetro, os registros adicionais serão ignorados. O número de registros pode ser atualizado na coluna Valor. O número recomendado de criações de registro no modelo é 1000. Qualquer valor acima desse valor pode representar desafios de desempenho.
- Insert_fixed: Importa detecções de vulnerabilidade corrigidas.

Para exibir os parâmetros da instância de integração, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Integrações** e clique na instância de origem de qualquer integração. Como alternativa, você pode navegar até **Tudo** > **Resposta a vulnerabilidades** > **Instâncias de Integração** e clique em **Ingestão manual** .

Ingerir vulnerabilidades manualmente

Ingerir vulnerabilidades manualmente carregando um modelo com dados de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique nos links Excel ou CSV e baixe o modelo no respectivo formato.
3. No modelo, insira os dados da vulnerabilidade nos registros.
   Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.
4. Clique em **Arquivo de importação** e carregue o modelo atualizado.
5. Clique em **Enviar**.
   A página Filas de push de integração de vulnerabilidades é exibida. Você pode exibir a lista de instâncias de integração, o status das execuções de integração e as anotações de log após a conclusão da execução da integração.

O que Fazer Depois

Depois de carregar o arquivo, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Integrações**. Verifique se a execução da integração foi bem-sucedida.

Verifique a execução da integração manual

Verifique se a execução da integração foi bem-sucedida. Exiba o número de detecções individuais e os itens vulneráveis (VIS) criados ou atualizados devido à execução da integração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Integrações**.
2. Clique no nome da integração com base no tipo de arquivo carregado.
3. Clique em **Execuções de Integração de vulnerabilidades** guia.
4. Clique no número de execução de integração.
5. Clique em **Itens** guia.
6. Revise as informações em **Itens** guia.

Guia Itens

Guia/Campo	Descrição
Guia Itens	Exibe o número total de VIS importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
Novos itens	Exibe o número de itens vulneráveis criados a partir desta execução de integração.
Itens importados	Exibe a soma de todos os campos nesta seção.
Itens duplicados	Exibe itens duplicados. Este campo não está mais preenchido.
Itens atualizados	Exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução da integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia/Campo	Descrição
	Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
Itens inalterados	Exibe itens vulneráveis encontrados durante a execução da integração que existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

O que Fazer Depois

Depois de verificar se a execução da integração foi bem-sucedida, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**. Verifique se há registros com falha nas Anotações.

Configurar detecções manuais de fechamento automático

Habilite o fechamento automático de detecções manuais para fechar detecções manuais obsoletas automaticamente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique em **Configuração de fechamento automático** .
3. Clique em **Detecções manuais** guia.
4. Certifique-se de **Detecções manuais de fechamento automático** a caixa de seleção está marcada.
5. Em **Detecções manuais encontradas pela última vez (dias atrás)** insira o número de dias após os quais as detecções manuais devem ser encerradas.
   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias.

Verifique o status do carregamento

Verifique se a execução da integração de vulnerabilidade foi bem-sucedida, parcialmente bem-sucedida ou uma falha.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**.
2. Na tabela Filas de push de integração de vulnerabilidades, verifique a hora do carregamento e o status do carregamento nas colunas Criado e Estado, respectivamente.
3. **Opcional:** Em **Anotações** exiba o motivo da falha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo para ingestão manual de vulnerabilidades

O modelo fornece colunas que devem ser preenchidas com dados de vulnerabilidade e item de configuração (IC). Depois que o modelo é preenchido e carregado, os dados são processados.

Instruções para preencher o modelo

Para inserir os detalhes no modelo, siga as instruções fornecidas na tabela a seguir.

Instruções do modelo

Coluna	Obrigatório/ Opcional?	Comprimento da cadeia de caracteres (máximo)/ Valores válidos	Descrição
ID do ativo	Opcional	255	Identificador universal exclusivo (UUID) ou ID do ativo. Pode ser o valor gerado por um scanner.
Insira informações em pelo menos uma das cinco colunas a seguir:			
Endereço MAC	Necessários	24	Host ou informações do ativo. A combinação de todos os valores fornecida deve ser exclusiva para um ativo.
FQDN	Necessários	255	
NETBIOS	Necessários	255	
Endereço IP	Necessários	255	
Nome do Host	Necessários	255	
As colunas restantes não dependem umas das outras.			
ID de vulnerabilidade	Necessários	255	Representa uma vulnerabilidade no National Vulnerability Database (NVD) ou um ID retornado de um scanner de terceiros.
Resumo de vulnerabilidade	Opcional	512	Breve descrição da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID da vulnerabilidade está indisponível.
Gravidade	Opcional	crítico, alto, médio, baixo, nenhum	Gravidade da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID da vulnerabilidade está indisponível. Se o registro estiver vazio, por padrão, ele será considerado crítico.
Porta	Opcional	Não aplicável	Porta da qual a vulnerabilidade é detectada. O valor deve ser um número inteiro válido. Se houver uma entrada inválida, o registro será ignorado.
Protocolo	Opcional	40	Tipo de protocolo de rede usado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instruções do modelo

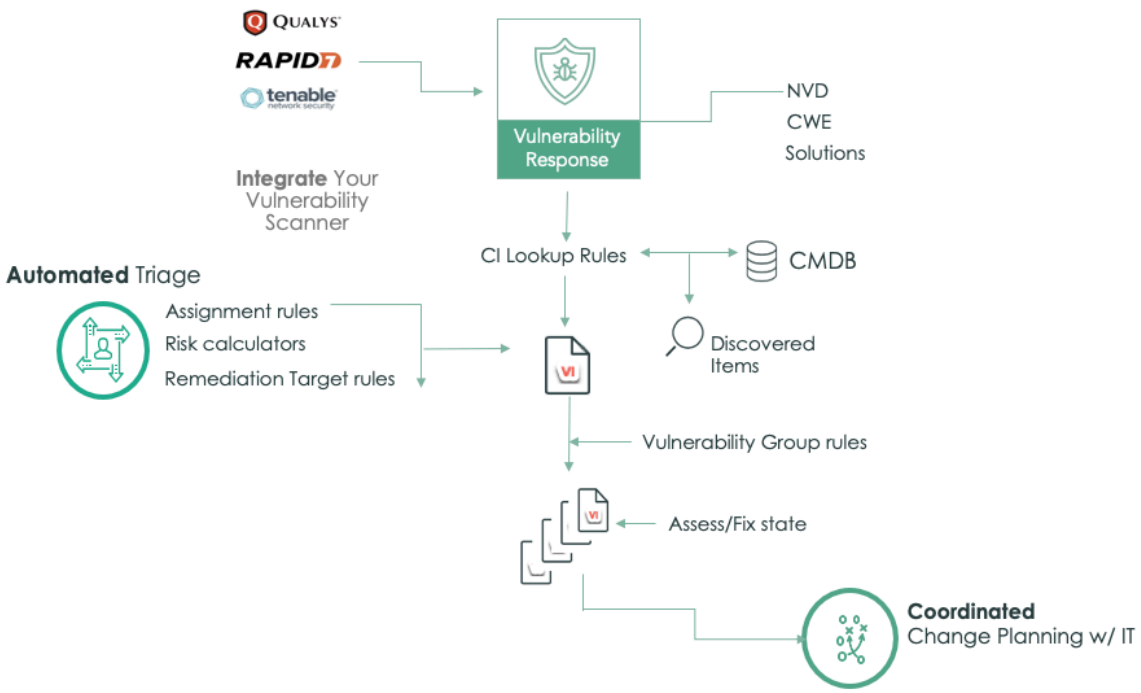
Coluna	Obrigatório/ Opcional?	Comprimento da cadeia de caracteres (máximo)/ Valores válidos	Descrição
Prova	Opcional	4000	Representa o local ou o caminho do sistema da vulnerabilidade.
Estado	Opcional	aberto, fixo	Status da detecção. Se o registro estiver vazio, por padrão, ele será considerado aberto.

Resposta a vulnerabilidades visão geral da correção

Resposta a vulnerabilidades a correção é um processo em fases que consiste em verificar a conclusão da importação, fazer a triagem de novas vulnerabilidades e monitorar o andamento até a conclusão. Abordado dessa forma, a correção se torna gerenciável, oportuna e, de muitas maneiras, automatizada.

Entender sua postura de segurança nos ativos da empresa ajuda a identificar as vulnerabilidades mais críticas para correção. Este processo de correção requer isso Resposta a vulnerabilidades e uma integração de terceiros, como Qualys Vulnerability Integration instalados e configurados.

Fluxo do processo de integração do Resposta a vulnerabilidades



Verifique a conclusão bem-sucedida das importações de integração de terceiros

A primeira fase deste processo é garantir que tudo esteja funcionando corretamente. Resposta a vulnerabilidades Está predefinido para baixar vulnerabilidades do National Vulnerability Database (NVD) e do Common Enumeration Weakness (CWE). As importações de terceiros fornecem os dados necessários para criar itens vulneráveis e tarefas de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correção. A correção bem-sucedida depende da importação consistente e bem-sucedida de vulnerabilidades e itens vulneráveis.

Durante a importação, as regras de pesquisa de IC correspondem ativos de terceiros aos ativos no Configuration Management Database (CMDB). Todos os ativos são armazenados no módulo Itens descobertos. As informações de IC são essenciais para a implementação da solução.

Nota: Depois que uma integração de terceiros é instalada e configurada, há algumas instâncias em que uma importação pode falhar, por exemplo, se o fornecedor de terceiros limitar suas chamadas de API. Quando as importações falham, elas exigem atenção imediata.

Os relatórios de execução de status de integração para as integrações de terceiros compatíveis são enviados com as aplicações para fornecer uma visão geral gráfica de suas importações. Use este relatório ou crie o seu próprio relatório para determinar facilmente se a importação mais recente foi bem-sucedida. Para obter mais informações sobre integrações compatíveis, consulte Integrações do Resposta a vulnerabilidades.

Revise e faça a triagem de vulnerabilidades e itens vulneráveis

A próxima fase de correção exige a revisão de novas vulnerabilidades e itens vulneráveis. Um item vulnerável (VI) é uma combinação detectada de vulnerabilidade e item de configuração (IC). À medida que os itens vulneráveis são formados, várias regras são executadas que atribuem VIS, determinam o risco que representam e definem metas de correção. Ajuste todas as regras, conforme necessário, para garantir que os itens vulneráveis tenham sido triados com sucesso.

Monitore o andamento da correção de vulnerabilidade existente

A fase final da correção consiste em monitorar seu andamento.

- Revise o status das importações de implementações de patch que não foram exibidas e acompanhe as operações de TI.
- Rastreie o andamento das obrigações de conformidade regulatória e garanta sua conclusão.
- Revise o status do item adiado e revise ou implemente correções.
- Monitore os painéis da Gestão de vulnerabilidades. Para revisar tendências, exibir relatórios em tempo real e usar métricas que rastreiam suas taxas de realização da meta de correção, você pode preferir monitorar seus processos com o. Performance Analytics para Resposta a vulnerabilidades aplicação.
- Fechando detecções obsoletas em Resposta a vulnerabilidades.

Verifique a conclusão bem-sucedida de Resposta a vulnerabilidades importações de integração

A maneira mais fácil de determinar se suas importações foram bem-sucedidas é usar um painel Status de execução de integração. O painel Status de execução de integração fornece um exemplo de exibição gráfica do status das execuções de integração de terceiros.

. Qualys e. Rapid7 as integrações de vulnerabilidades têm um painel de status de execução de integração. Consulte Qualys gráfico de status de execução de integração ou Integração com Rapid7 Vulnerability executar gráfico de status para obter informações detalhadas sobre o conteúdo do gráfico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Gráficos, para integrações não fornecidas por ServiceNow®, pode ser criado a partir de relatórios em um painel, mas pode exigir ServiceNow experiência. Para obter mais informações sobre como criar relatórios e painéis, consulte Introdução aos relatórios e. Painéis .

Exibir Resposta a vulnerabilidades dados de detecção de item vulnerável

Os dados completos coletados pelas integrações de scanner de terceiros com Resposta a vulnerabilidades São exibidos nas guias Detecções e Detecções iniciais nos registros de item vulnerável (VIT). Ele também é exibido nos registros de detecção na lista de detecção de item vulnerável em seu ServiceNow AI Platform® instância.

Antes de Iniciar

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

Função necessária:

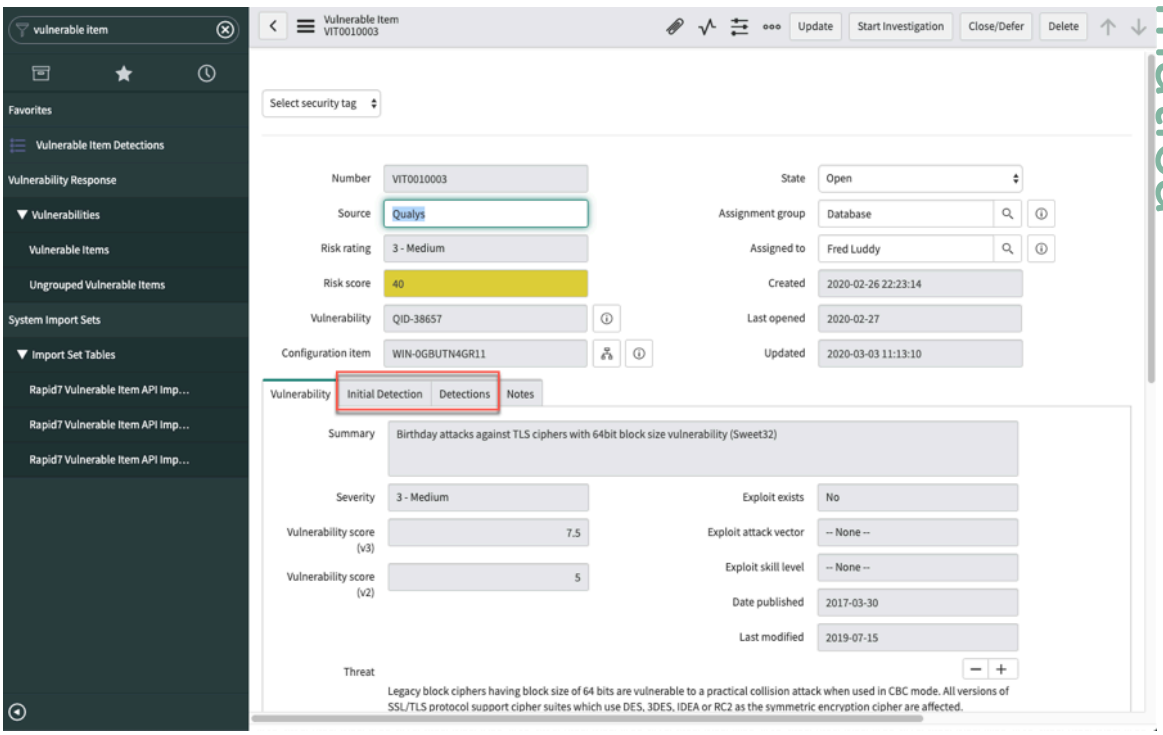
- sn_vuln.admin inicia execuções de integração e exibe os dados de detecção de item vulnerável.
- sn_vul.remediation_owner recebe itens vulneráveis criados a partir de detecções de itens vulneráveis e exibe dados em registros de VI.

Procedimento

1. Para exibir os dados de detecção de item vulnerável, navegue até um registro de item vulnerável e abra-o.

   O registro é exibido com as guias Detecções iniciais e Detecções.

   Nota: Os dados exibidos anteriormente na guia Detalhes da configuração são exibidos junto com outros dados de detecção nas guias Detecção inicial e Detecções.

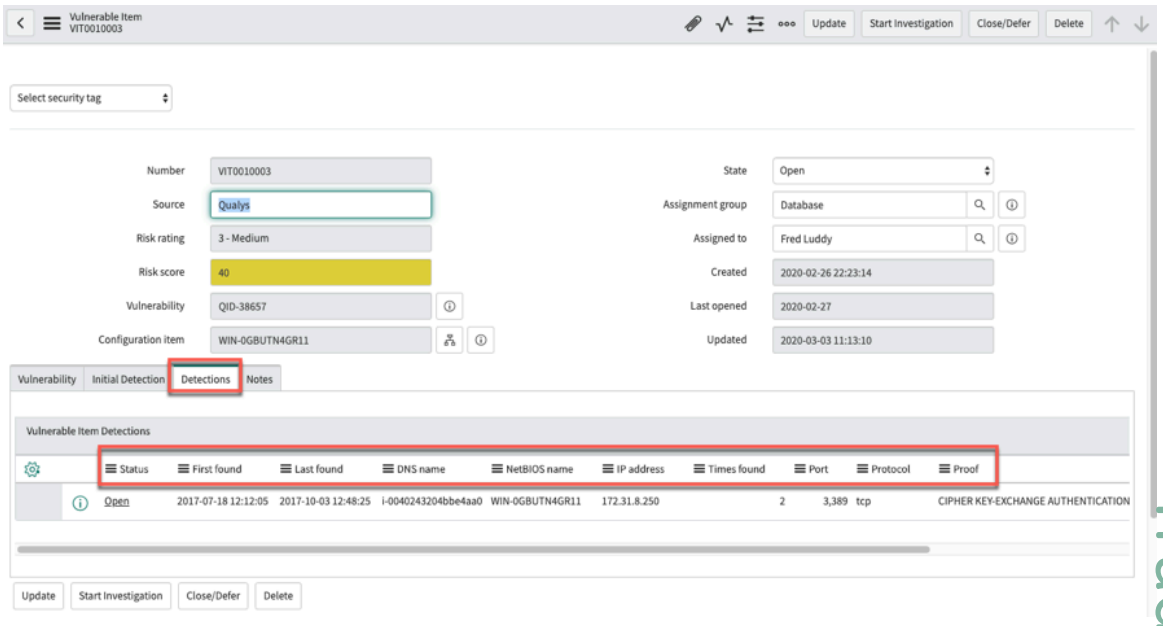


2. Clique em **Detecções** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando um item vulnerável é criado a partir dos resultados de uma verificação de terceiros, os dados da verificação são exibidos no registro de detecção, conforme mostrado na figura a seguir.



Cada linha na seção Detecções de item vulnerável representa dados de uma detecção distinta. Na primeira coluna Encontrado, a data em que o item vulnerável foi detectado pela primeira vez pelo scanner é exibida. Na coluna Mais recente encontrada, a data da detecção mais atual é exibida. O campo Origem exibe o scanner que recuperou os dados.

Nota: Para Qualys, Com detecções de item vulnerável, os seguintes campos são descontinuados no registro VI e não são mais preenchidos:

- Qualys gravidade
- Última atualização por origem

Também para Qualys, Conforme mostrado na figura anterior, quando um VI é criado a partir de uma verificação, o valor da verificação de resultados é exibido na coluna Prova no registro de detecção. No entanto, este valor não é exibido na parte superior do registro VI.

Para o Rapid7, quando um VI é criado a partir de uma verificação, o valor da prova da verificação pode ser exibido na coluna Prova no registro de detecção e na parte superior do registro VI, mas não por padrão. Para exibir este valor na parte superior do registro VI, selecione o campo Prova no layout do formulário.

3. **Opcional:** Para configurar o layout da guia Detecções no registro, siga estas etapas.

   a. Por padrão, as colunas a seguir são exibidas na guia Detecções.

   - Status
   - Primeiro encontrado (dados)
   - Encontrado pela última vez (data)
   - Nome DNS
   - BIOSname líquido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço IP
- Horas encontradas
- Porta
- Protocolo
- Prova
- SSL

Nota:

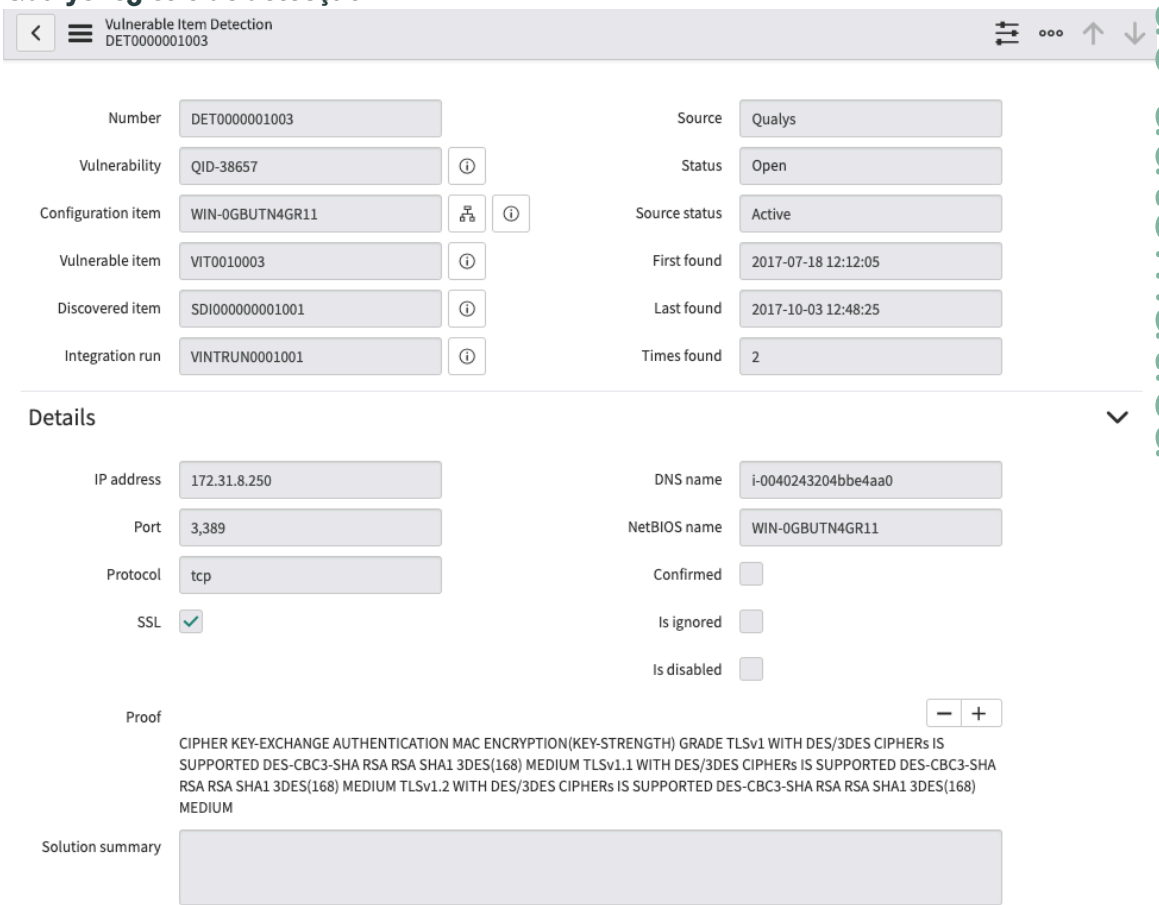
Observação: Se não houver nenhum valor em uma coluna, os dados desse campo não foram detectados pelo scanner.

b. Clique no ícone de engrenagem ( ) para personalizar sua exibição.

c. Selecione as colunas da caixa de listagem para exibir dados específicos e clique em **OK** .

4. Com a guia Detecções selecionada, na coluna Status, clique em um item para abrir o registro de detecção e exibir os detalhes associados a esse item vulnerável, incluindo um resumo da solução (somente integração do Rapid7 InsightVM).

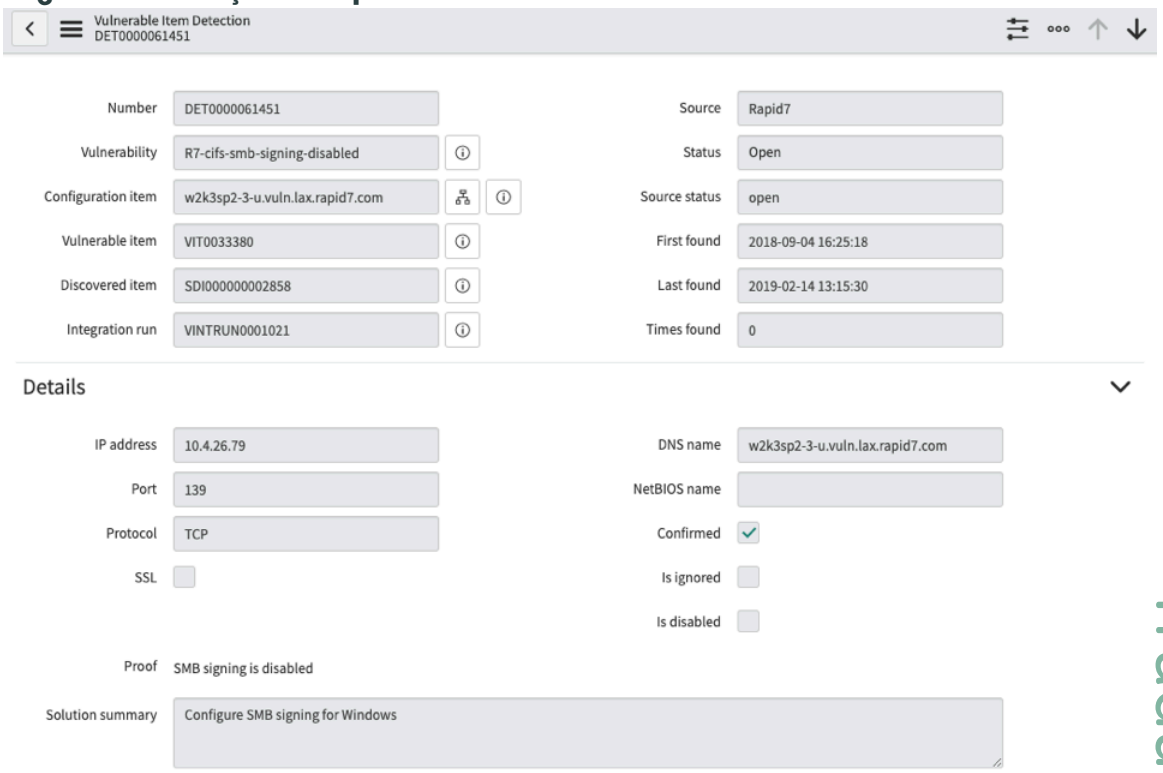
Qualys registro de detecção



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de detecção do Rapid7

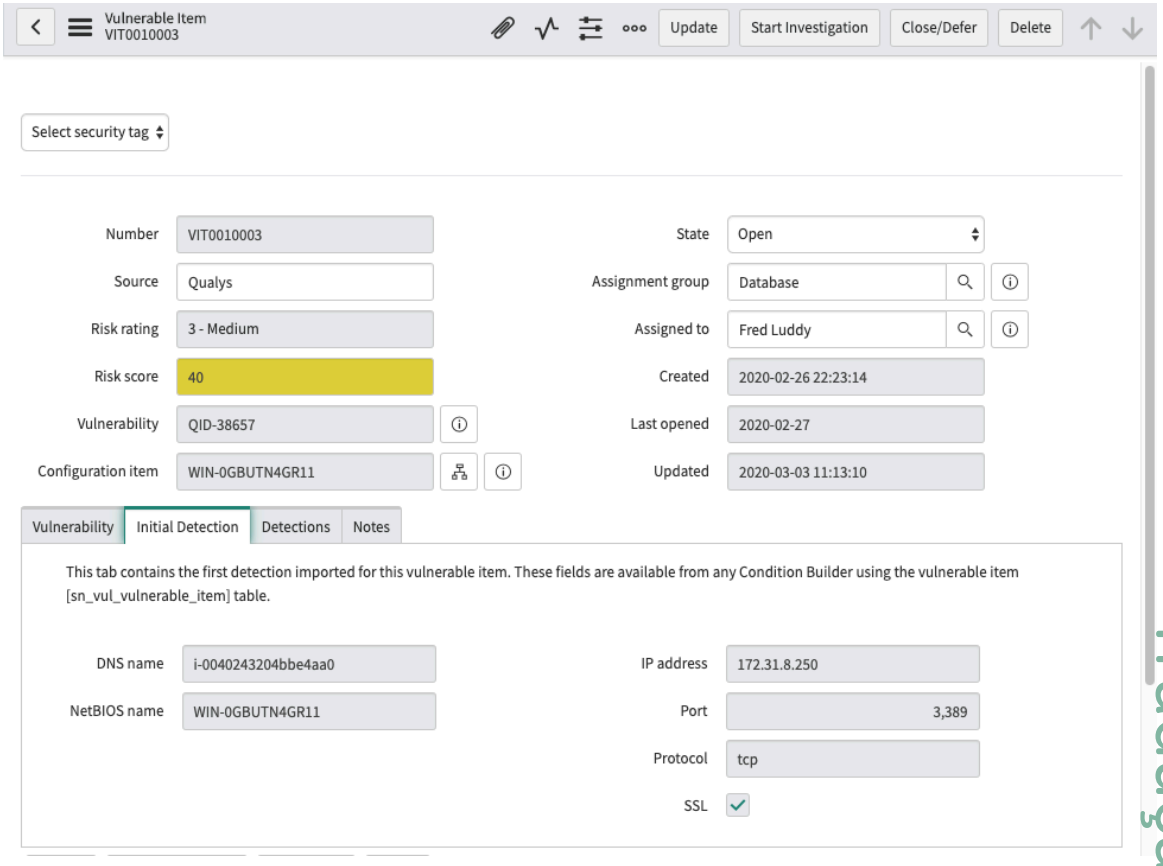


5. Retorne ao registro e selecione a guia Detecção inicial.

A guia Detecções iniciais exibe os dados importados do scanner de terceiros na primeira ocorrência da detecção. Essas informações na guia Detecção inicial não mudam conforme os dados de detecção são atualizados.

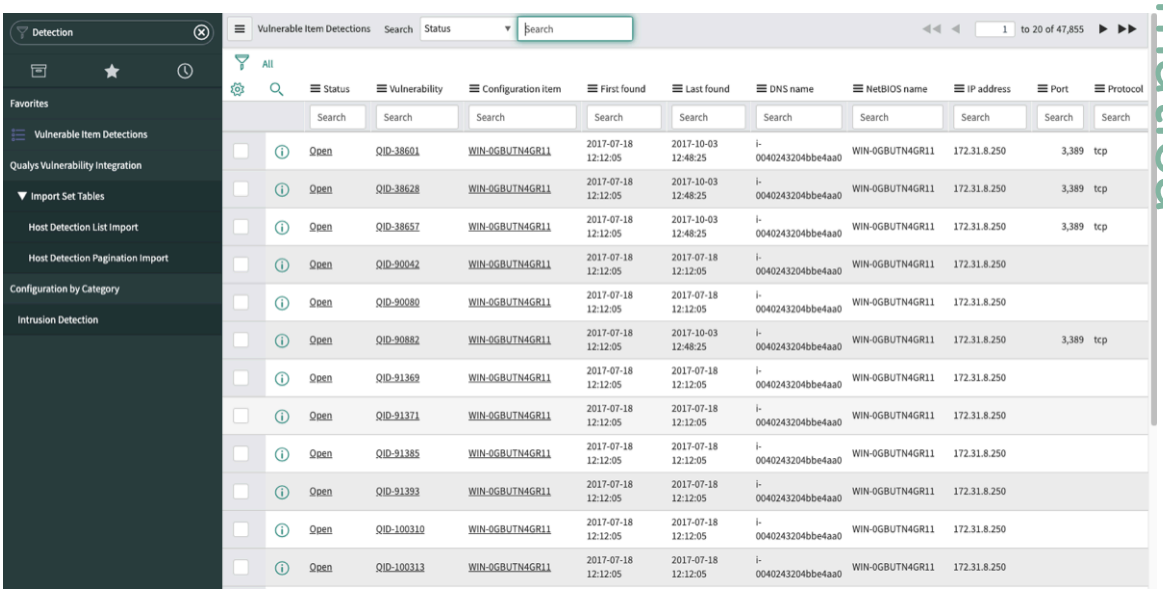
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. **Opcional:** Navegue até Detecções de item vulnerável para exibir a Lista de detecção de item vulnerável.

(Optional) A lista de detecção de item vulnerável é exibida. Cada linha na lista de detecções de itens vulneráveis representa uma detecção distinta. As colunas exibem os mesmos dados que o registro VI.



As detecções são abertas ou fechadas somente por dados encontrados por um scanner, elas não rolam do VIS. À medida que as detecções são importadas, elas são usadas para criar VIS e atualizar os estados de VIs . Se todas as detecções forem encerradas para um item vulnerável, esse item vulnerável será encerrado. No registro VI, o estado é encerrado e o subestado é corrigido .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Os erros são registrados em log enquanto:

- Processando anexos recuperados do scanner.
- Criando ou atualizando detecções ou itens vulneráveis.

Para obter informações sobre como lidar com erros de detecção, consulte Tratamento de erros para detecções.

Quando todos os VIS são encerrados para uma tarefa de correção, a tarefa de correção é encerrada.

Fechado VIS com um subestado de **corrigido** ou **obsoleto** São reabertos se uma nova detecção for criada e o VIS puder ser correspondido à nova vulnerabilidade.

Itens vulneráveis definidos como **Resolvido** em sua instância, mas não fez a transição para **Encerrado/Corrigido** as execuções de integração subsequentes serão reabertas se forem detectadas durante novas verificações.

Quando todos os VIS são encerrados para uma tarefa de correção, o registro é encerrado.

Itens vulneráveis definidos como "Resolvido" em sua instância, mas não transferidos para "Encerrado/Corrigido" pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Para Rapid7 Detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir os VIS resolvidos por idade. Vis definido como **Resolvido** então não fez a transição para **Encerrado/Corrigido** pelas verificações subsequentes, retorne para **Aberto** após o número de dias inserido.

Para Qualys Se o scanner continuar a encontrar Vs que foram definidos como "Resolvido", mas não foram transferidos para **Encerrado/Corrigido** Por verificações subsequentes, esses VIS retornam para **Aberto** Quando a data da última descoberta é posterior à data de resolução.

O que Fazer Depois

Para exibir mais dados, incluindo contagens de itens e detecção, você pode Verificar Resposta a vulnerabilidades Dados de detecção de item vulnerável em registros de execução de integração (VINTRUN).

Verificar Resposta a vulnerabilidades Dados de detecção de item vulnerável em registros de execução de integração (VINTRUN)

De registros de execução de integração em seu ServiceNow AI Platform®, você pode localizar dados de detecção de item vulnerável da integração de terceiros com base na data e na hora das verificações. Verifique se a verificação foi concluída com sucesso, exiba o número (contagens) de detecções individuais, bem como todos os itens vulneráveis (VIS) criados ou atualizados diretamente como resultado das verificações.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode preferir que as informações de execução da integração, data e hora da verificação, ou o número do registro de execução da integração (nº VINTRUN) do item vulnerável ou registros de detecção para ajudá-lo a localizar registros específicos das listas a seguir.

Procedimento

1. Escolha um para continuar.

Integração	Descrição
Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**	Na lista Integrações do Rapid7, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção. **a.** Depósito de dados do Rapid7: ▪ Integração de item vulnerável do Rapid7 ▪ Integração de resolução de item vulnerável do Rapid7 ▪ Integração abrangente de item vulnerável do Rapid7 **b.** ☒Integração de resolução de item vulnerável do Rapid7 (InsightVM) ▪ Integração de item vulnerável do Rapid7 - API ▪ Integração abrangente de item vulnerável do Rapid7 - API
Navegar até **Qualys** > **Integração de vulnerabilidades da Qualys** > **Integrações Primárias**	Na lista Integrações da Qualys, escolha: ○ Integração do Qualys Host Detection ○ Integração abrangente de detecção de host da Qualys
Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**	Na lista Integrações do Tenable, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção.
Navegar até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integrações**	Na lista Integrações do Microsoft TVM, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção.

2. Na parte inferior da página exibida, clique em **Execuções de Integração de vulnerabilidades** guia .

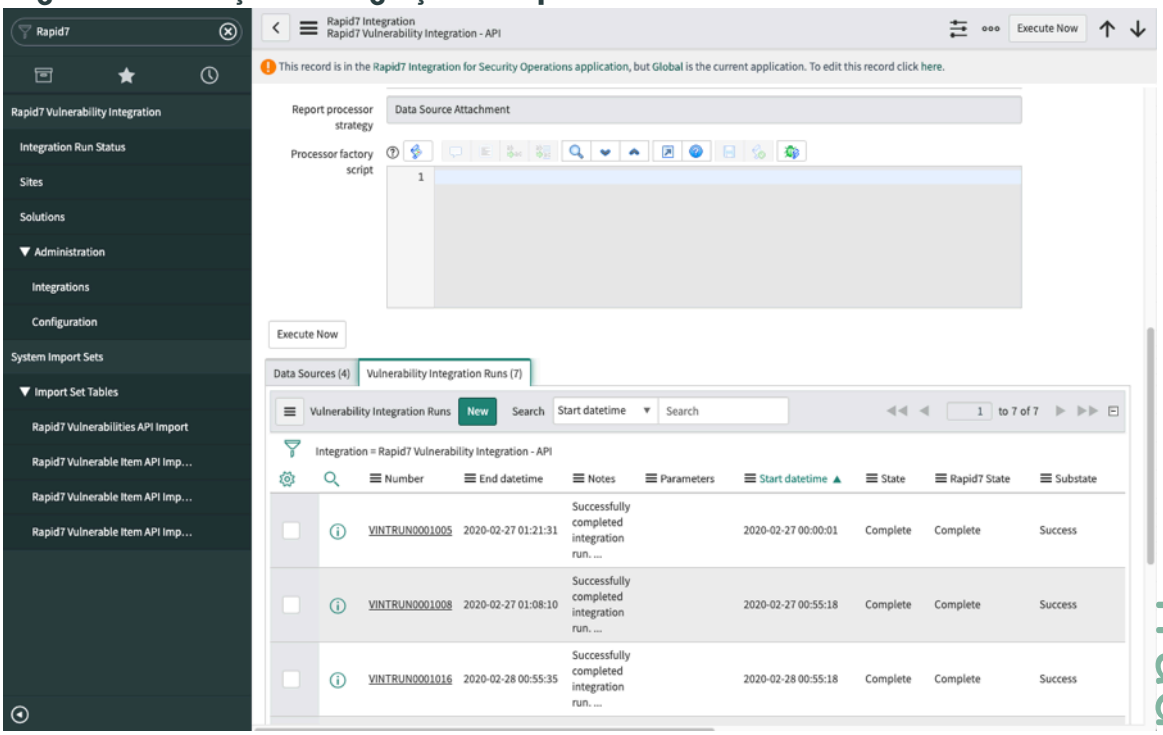
3. Clique em um item nas colunas Número ou Origem de importação para abrir um registro.

O registro de execução de integração é exibido.

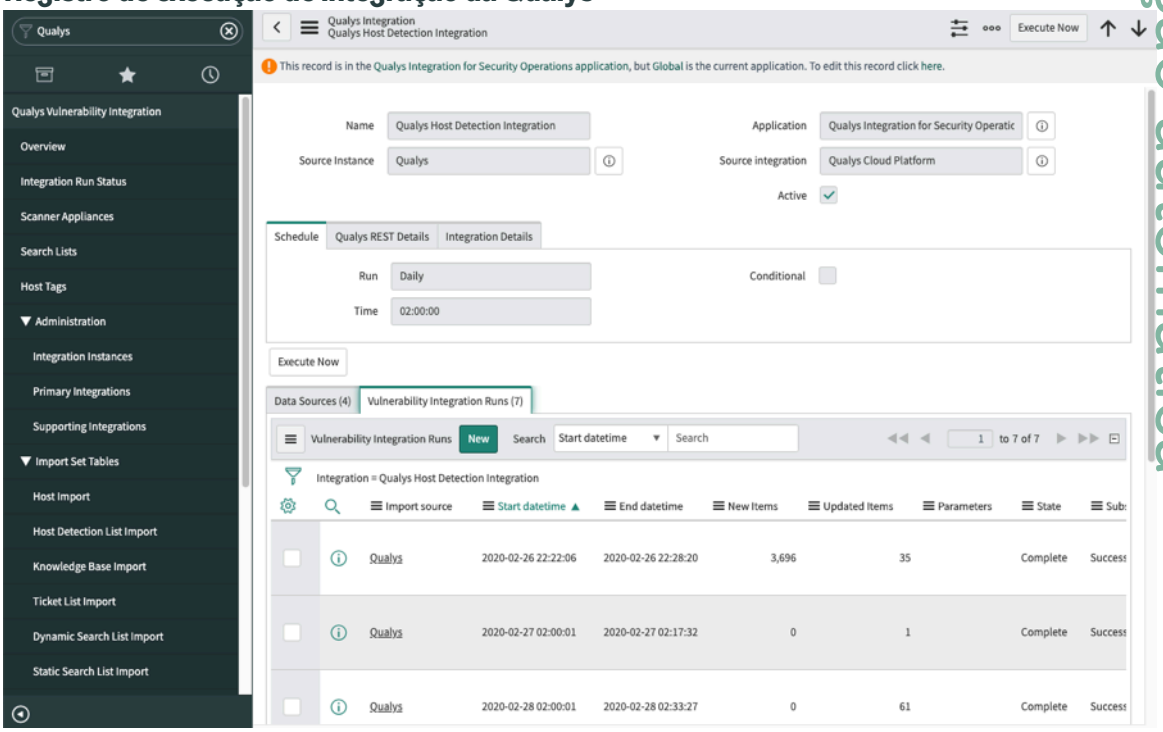
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de execução da integração do Rapid7



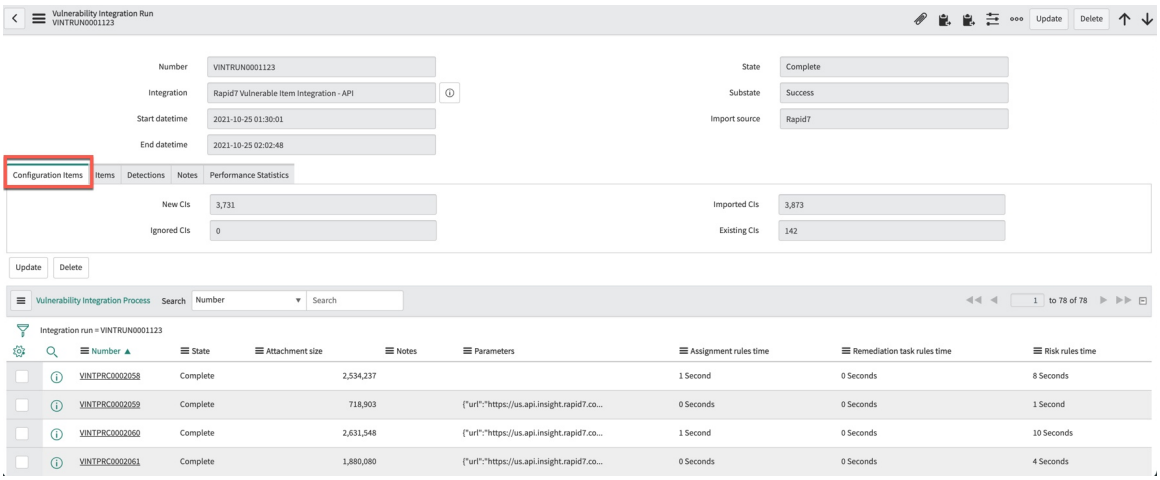
Registro de execução de integração da Qualys



O registro de execução de integração é exibido. Você pode verificar no campo Estado se a integração foi executada com sucesso. Selecione **Itens de configuração** guia.

Tradução automática

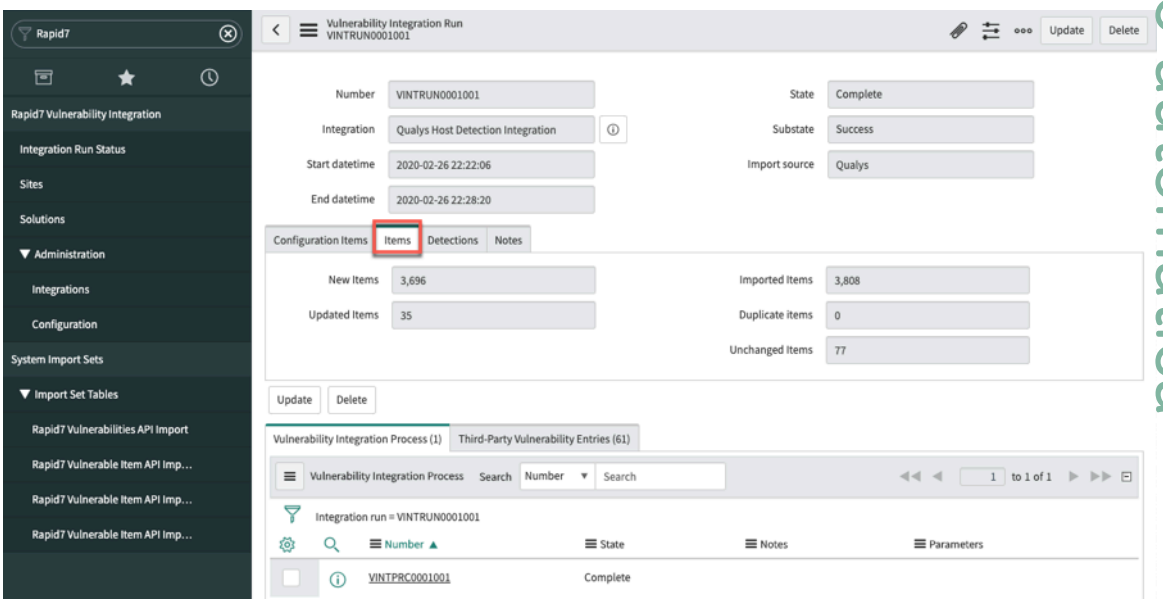
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia Itens de configuração exibe as seguintes informações:

- A guia Itens de configuração exibe o número total de itens de configuração importados.
- O campo Novos ICs exibe o número de ICs criados como parte desta execução de integração.
- O campo ICs importados exibe a soma de todos os ICs nesta seção.
- O valor do campo ICs ignorados é sempre 0 para Resposta a vulnerabilidadesintegrações.
- O campo ICs existentes exibe o número total de ICs que já existem.

Clique em **Itens** guia.



A guia Itens exibe as seguintes informações:

- A guia Itens exibe o número total de VIS importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
- O campo Novos itens exibe o número de itens vulneráveis criados a partir desta execução de integração.
- O campo Itens importados exibe a soma de todos os campos nesta seção.
- O campo Itens duplicados não está mais preenchido.

Tradução automática

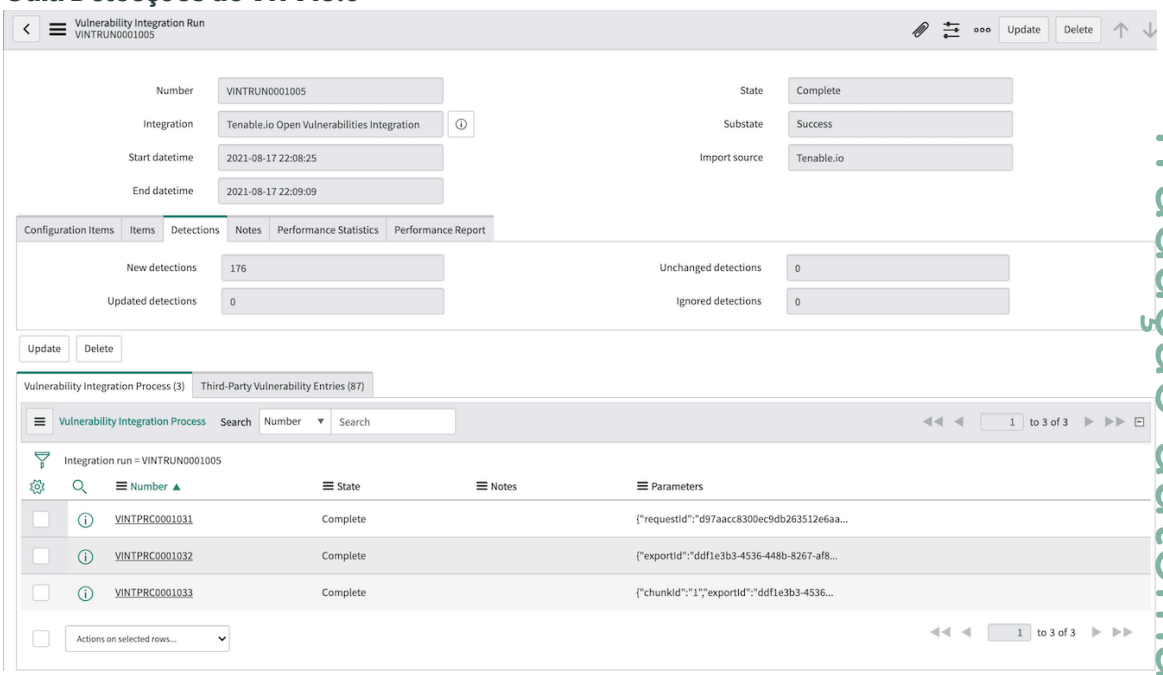
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O campo Itens atualizados exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução da integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
- O campo Itens inalterados exibe itens vulneráveis encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

4. Clique em **Detecções** guia.

   Esta guia só será exibida se a execução de integração tiver detecções. Você pode verificar o total de detecções importadas adicionando os números listados.

Guia Detecções de VR v15.0



Nota: Antes da v15.0, não havia campo para detecções ignoradas.

A guia Detecções exibe as seguintes informações:

- A partir da v15, um novo campo Detecções ignoradas foi adicionado para rastrear as detecções, que foram ignoradas anteriormente. Com esta implementação, a contagem de detecções importadas e a contagem rastreada nos registros de execução de integração se tornam consistentes. Esta funcionalidade foi implementada para todos os scanners, ou seja, Qualys Vulnerability Integration, Integração com Rapid7 Vulnerability, Integrações de vulnerabilidade da Tenable e. Microsoft TVM.
- O campo Novas detecções exibe as novas detecções criadas durante esta execução de integração.
- O campo Detecções inalteradas exibe detecções encontradas durante a execução da integração que já existem no banco de dados, mas não foram atualizadas, porque nenhum dos valores de campo relevantes foi alterado.
- O campo Detecções atualizadas exibe o número de vezes que as detecções são atualizadas durante esta execução da integração. Este valor não é o número de detecções exclusivas atualizadas. Se, por exemplo, uma detecção for atualizada duas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vezes como parte da execução da integração, ela será contada duas vezes e exibida como 2 detecções atualizadas.

Nota: Detecções que não são exibidas nessas contagens são detecções que estão em um estado fechado (fixo), porque registros fixos são usados para atualizar os VIS existentes. Se você quiser mais visibilidade desses registros de detecção, poderá exibir os VIS fechados que são criados quando não há um VI correspondente existente em um estado aberto. Para obter mais informações sobre vulnerabilidades no estado fixo que você pode habilitar no Assistente de configuração para a integração da Qualys, consulte Configurando Resposta a vulnerabilidades Usando o Assistente de configuração.

5. Clique em um item nas colunas Número ou Origem de importação para abrir um registro.

Exibição de dados de patch e programação de patches em Resposta a vulnerabilidades

A partir da v16.1 de Resposta a vulnerabilidades, você pode programar patches e exibir dados de patch junto com a solução e outras informações de vulnerabilidade em registros no ambiente clássico e no Resposta a vulnerabilidades Espaços de trabalho em seu ServiceNow AI Platform instância.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para importar seus patches para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades e Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.
- Exibição de dados de orquestração de patches no Resposta a vulnerabilidades painéis no ambiente clássico.
- Exibir dados em cartões de pontuação no Resposta a vulnerabilidades Espaços de trabalho.

Patches de programação

Você pode programar patches a partir dos seguintes registros:

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

Dados de patch no ambiente clássico

Do ambiente clássico em Resposta a vulnerabilidades aplicação:

- Para exibir registros de Atualização de patch, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Patches**.
- Para exibir Soluções, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Soluções**.
- Para exibir os VIS atribuídos a você que têm patches, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para exibir tarefas de correção, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**
- Para exibir registros de itens descobertos, navegue até **Tudo** > **Operações de segurança** > **Itens descobertos**.

Dados de patch e rollup de estado para orquestração de patches em Resposta a vulnerabilidades

A partir da v16.1 de Resposta a vulnerabilidades Os dados e os estados do patch são acumulados para Atualização de patch e outros registros no Resposta a vulnerabilidades aplicação.

Registros de atualização de patch nos espaços de trabalho no ambiente clássico em Resposta a vulnerabilidades

As informações sobre patches, soluções de vulnerabilidade e vulnerabilidades estão todas conectadas no Resposta a vulnerabilidades aplicação.

Os dados do patch e os dados e status do rollup de patch são exibidos nos registros em sua instância. Os registros de patch estão incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exiba registros de Patch (VPU) nos Espaços de resposta a vulnerabilidades na exibição de lista no Espaço de correção de TI. Os registros de atualização de patch na exibição clássica e nos espaços de resposta a vulnerabilidades incluem os seguintes dados:

- Dados e informações da solução de vulnerabilidade de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos com atualizações ausentes.
- Status de correção que inclui % de VIS corrigidos e o total de VIS que têm um patch como patch preferencial.
- Dispositivos associados, Itens vulneráveis, Implantações de patch e Solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos Espaços de resposta a vulnerabilidades.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades e Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.
- Exibição de dados de orquestração de patches no Resposta a vulnerabilidades painéis no ambiente clássico.
- Exibir dados em cartões de pontuação no Resposta a vulnerabilidades Espaços de trabalho.

Tradução automática

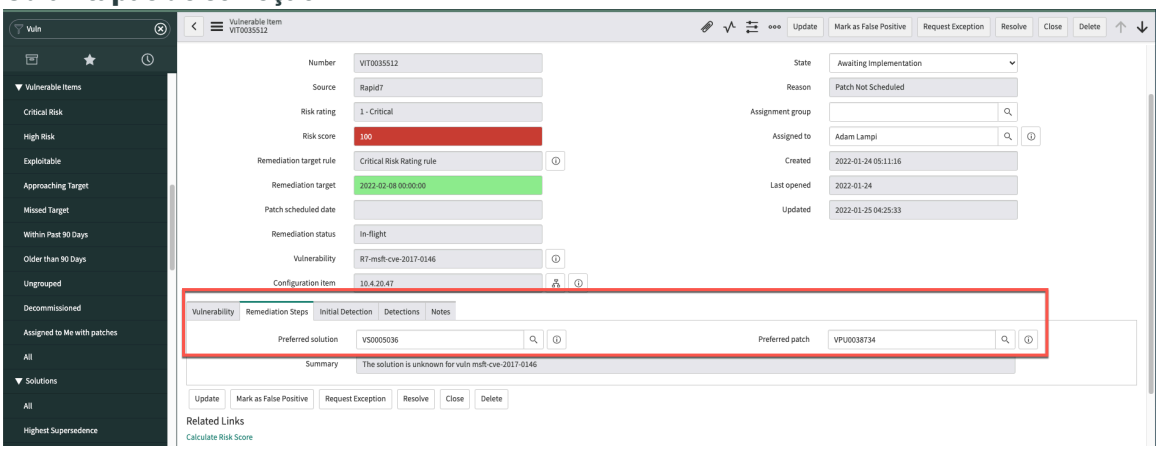
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dados de patch e acúmulo de estado

Para exibir os itens vulneráveis que têm patches e que estão atribuídos a você no ambiente clássico, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**.

Se um registro de item vulnerável for preenchido com um patch preferencial, ele fará a transição automaticamente para **Aguardando implementação** Somente se o estado do VI não for **Encerrado** , **Resolvido** , **Adiado** ou **Em Revisão** . Para detalhar os dados para exibir a solução preferencial e outros dados, clique em **Correção** No registro VI.

Guia Etapas de correção



Uma VI com um patch preferencial faz transições para **Aguardando implementação** nos seguintes casos:

- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção e o IC tiver um VI associado, o motivo é o VI **Aguardando implementação** . **Patch programado** .
- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção, e o IC tiver uma VI associada e a data de destino de correção (prazo) posterior à data da Hora de correção (TTR), o estado da VI será **Aguardando implementação** com o motivo como **Patch programado (data de destino ausente)** .
- Se um patch não estiver programado para implantação em um IC que faz parte de uma importação de coleção, o estado do VI será **Aguardando implementação** , com o motivo como **Patch não programado** .

Clique em **Patch preferencial** Ícone de informações para abrir as atualizações de patch e exibir as seguintes informações nos links relacionados:

Itens vulneráveis

Itens vulneráveis associados a este patch.

Dispositivos associados

Dispositivos que têm atualizações e aqueles que não têm atualizações.

Implantações de patch

Implantações programadas para este patch em máquinas individuais (ativos) ou em grupos de ativos.

Solicitações de patches

Uma lista de solicitações de patch que foram enviadas para aprovação antes de serem programadas para implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Patches em potencial

Patches que podem lidar com uma vulnerabilidade.

Clique em **Informações de patch preferenciais** Ícone para abrir o registro e exibir as informações listadas anteriormente, além dos seguintes dados de Atualização de patch:

Status de correção da fonte

O total de dispositivos que exigem este patch e todos os dispositivos que estão sem o patch.

Status da Correção

O status (total de VIS, % corrigido, VIS adiado) dos VIS que têm este patch preferencial.

Patches e soluções preferenciais

Quando uma vulnerabilidade importada corresponde a um ativo em seu Configuration Management Database (CMDB) Um item vulnerável (VI) é criado em Resposta a vulnerabilidades. Se o item de configuração (IC) associado a este VI também for importado de um fornecedor de patch de terceiros e for mostrado como ausente um patch para a mesma vulnerabilidade, um patch preferencial será listado e acumulado para suas soluções. Essas informações permitem que você saiba que um ativo (IC) tem uma correção de um patch disponível que é a melhor correspondência para sua vulnerabilidade.

Exibição de patches sem soluções

Após uma importação, se não houver dados de solução de vulnerabilidade disponíveis, o **Solução de vulnerabilidade** O campo no registro de Atualização de patch é deixado em branco. Para obter mais informações sobre como exibir informações para esses tipos de patches, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Exibir patches sem soluções em Resposta a vulnerabilidades

A partir da v16.0 de Resposta a vulnerabilidades Para patches que não têm soluções após uma importação, o sistema pesquisa IDs de patch nos dados de referência de vulnerabilidade para que você possa exibir esses patches em registros de vulnerabilidade.

Patches sem soluções

Função necessária: sn_vul.vulnerability_admin.

Os dados importados das aplicações de solução de vulnerabilidade e orquestração de patches, bem como as integrações do verificador de patches, são processados, conectados e exibidos no Resposta a vulnerabilidades Aplicação em registros de atualização de patch.

Quando existe uma solução para uma vulnerabilidade, as informações relacionadas são correlacionadas em sua instância e são acumuladas dos patches, às soluções de vulnerabilidade e às vulnerabilidades. Para exibir essas informações, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Patches** > **Tudo**.

Após uma importação, se não houver dados de solução de vulnerabilidade disponíveis, o **Solução de vulnerabilidade** O campo no registro de Atualização de patch é deixado em branco. Para que você possa ver as informações de solução relacionadas a esses patches, uma propriedade do sistema, [**sn_vul_patch_orch.no_solution_patch_rollup**], é ativado por padrão em sua instância. Esta propriedade pesquisa IDs de boletim e IDs de artigo nos dados de referência de vulnerabilidade das importações do scanner. Se uma correspondência for encontrada, os dados associados serão preenchidos na tabela Patches potenciais e essas informações serão exibidas nas listas relacionadas de registros de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você tiver um grande número de vulnerabilidades ou o trabalho agendado de rollup estiver demorando muito para ser concluído, convém desativar esta propriedade do sistema para evitar possíveis problemas de desempenho. No entanto, observe que, se você desativar esta propriedade do sistema, os dados de solução importados não serão pesquisados nem acumulados para suas vulnerabilidades sem soluções.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema, siga estas etapas:

1. Navegar até **sys.properties.list**.
2. Localizar **sn_vul_patch_orch.no_solution_patch_rollup** e clique nele para abrir o registro.
3. No campo Valor, digite `falso` .
4. Clique em **Atualizar**.

Exibição de dados de orquestração de patches no Resposta a vulnerabilidades painéis

A partir da v16.1, você pode exibir dados de atualização de patch no ambiente clássico nos painéis incluídos com Resposta a vulnerabilidades aplicação.

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Para obter mais informações, consulte Espaço do gerente de vulnerabilidade e Explorar o. Espaço de correção de problemas de TI.

Você também pode exibir esses dados nos painéis de CISO e Gestão de vulnerabilidades (PA) se tiver uma assinatura do Performance Analytics.

Você também pode exibir dados de patch no ambiente clássico. Para obter mais informações sobre as funções necessárias e como exibir dados no Resposta a vulnerabilidades painéis no ambiente clássico que estão incluídos com Resposta a vulnerabilidades e aqueles que exigem uma assinatura separada, consulte Usando o padrão Resposta a vulnerabilidades painéis.

Exibir uma solução

Exiba todas as soluções, soluções com maior substituição e soluções associadas a itens vulneráveis para informar suas atividades de correção.

Antes de Iniciar

Função necessária: sn_vul.read, sn_vul.vulnerability_admin ou sn_vul.remediation_owner

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como analista de vulnerabilidades ou responsável pela correção, você pode exibir diferentes conjuntos de soluções relacionados a itens vulneráveis.

Nota: Os registros de solução são somente leitura, exceto em **Anotações** em **Anotações internas** seção ou soluções criadas pelo usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Soluções**.
2. Escolha uma lista de soluções.

   Nota: Você pode filtrar uma lista de soluções usando caracteres curinga para o nome do produto.

3. Para revisar, clique em cada item.
4. **Opcional:** Insira anotações em **Anotações** e clique com o botão direito do mouse **Salvar** para permanecer na página ou clique em **Atualização** para salvar e retornar ao **Soluções de vulnerabilidades** lista.

   Nota: Se você tiver apenas a função sn_vul.read, não poderá executar esta etapa.

Crie uma solução de vulnerabilidade

Crie uma solução de vulnerabilidade para que você possa rastrear soluções de vulnerabilidade que não são cobertas pelo conteúdo de solução de terceiros.

Antes de Iniciar

Função necessária: admin, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou vulnerability.write

Solução de gestão de vulnerabilidadeé um recurso disponível no Resposta a vulnerabilidades aplicação.

Solução de gestão de vulnerabilidade requer uma assinatura separada.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar uma solução a partir de qualquer uma das listas de soluções. Você deve instalar a aplicação Gestão de soluções de vulnerabilidade antes de criar uma solução.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Soluções**.
2. Escolha uma lista de soluções: **Todos** , **Maior substituição** ou **Com itens vulneráveis** .
3. Clique em **Nova**.
4. Preencha os campos editáveis no formulário, conforme apropriado.
   Qualquer campo não utilizado pode ser deixado em branco. Para obter mais informações sobre campos individuais, consulte Campos de formulário de solução.
5. Clique com o botão direito do mouse **Salvar** no cabeçalho.
   O registro de solução é adicionado e aparece em **Todos** e. **Maior substituição** listas, por padrão.
6. As listas relacionadas são exibidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode associar esta solução às seguintes listas relacionadas: **Itens vulneráveis** , **Vulnerabilidades de terceiros** , **CVEs** , **Soluções de substituição** e. **Soluções anteriores** . Escolha uma vulnerabilidade ou solução e clique em **Enviar** .

Nota:

Solução de gestão de vulnerabilidade associa automaticamente itens vulneráveis e tarefas de correção a soluções quando os registros de vulnerabilidade são associados manualmente a soluções.

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

Se você quiser excluir o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque ela não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente, consulte Exclua manualmente soluções de registros de terceiros ou vice-versa.

Exclua manualmente soluções de registros de terceiros ou vice-versa

Exclua o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque ela não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente. Exclua manualmente soluções usando uma vulnerabilidade de terceiros ou um registro de solução.

Antes de Iniciar

Função necessária:

- sn_vul.write
- sn_vul.remediation_owner

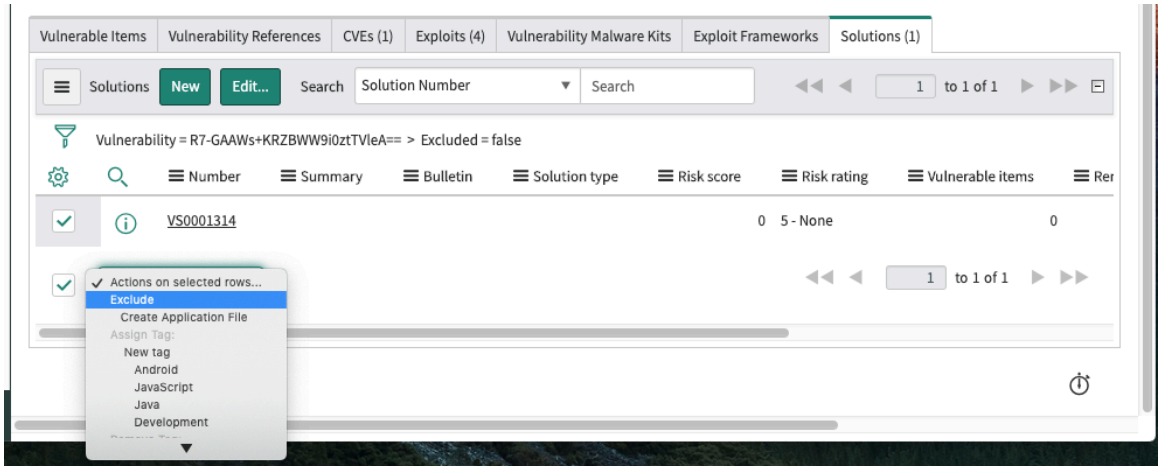
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** ou **Resposta a vulnerabilidades** > **Todas as soluções**
2. Abra um registro de vulnerabilidade ou solução de terceiros.
   a. Para um registro de terceiros: Selecione **Soluções** guia relacionada.
   b. Para um registro de solução: Selecione **Vulnerabilidades de terceiros** guia relacionada.
3. Marque a caixa ao lado de cada registro de vulnerabilidade ou solução que você deseja excluir.
4. Em **Ações nas linhas selecionadas** menu suspenso, escolha **Excluir** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro de solução ou de terceiros não aparece mais na guia Relacionado.

Relacionamentos de vulnerabilidade de terceiros com soluções também são excluídos quando as soluções são atualizadas ou se o trabalho noturno estiver habilitado.

Relacionamentos de vulnerabilidade de terceiros com soluções são excluídos durante o trabalho programado noturno .

Excluir vulnerabilidades de terceiros significa que a solução não é mais um fator para qualquer avaliação de solução preferencial. Impactos da exclusão:

- Tudo conta para soluções, já que a vulnerabilidade de terceiros, os itens vulneráveis (VIS) e os itens de configuração (ICs) anexados à vulnerabilidade de terceiros não contam mais para a solução.
- Determinar a solução preferencial para a vulnerabilidade de terceiros e, por extensão, a solução preferencial de todos os VIS anexados e tarefas de correção que contenham o VI

Fazer a triagem de vulnerabilidades automaticamente

Analisar e fazer a triagem de novas vulnerabilidades é necessário para garantir a correção bem-sucedida. Transforme importações de vulnerabilidades em tarefas de correção com atribuição automatizada de item vulnerável (VI), cálculo de risco, metas de correção e agrupamento de VI.

Começando com vulnerabilidades importadas, reconcilie os ativos não encontrados no CMDB, priorize os resultados, converta isso em atividades de correção atribuídas automaticamente, orquestre o processo de correção e confirme a conclusão com uma verificação de validação.

Novos itens vulneráveis geralmente são classificados em tarefas de correção após a importação, com base nas regras de tarefas de correção. Às vezes, os itens vulneráveis não podem ser agrupados ou não contêm um item de configuração reconhecido.

Uma visão geral do processo de triagem de vulnerabilidades:

- Faça login na sua instância Resposta a vulnerabilidades.
- Valide se suas regras (Pesquisa de IC, Atribuição) para item vulnerável estão funcionando conforme o esperado. Para obter informações sobre como revisar regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros. Para obter informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Devido ao grande volume nas importações de dados, é necessário ter cuidado com a atribuição automatizada de itens vulneráveis.

- Valide se seus destinos de correção estão corretos. Consulte Resposta a vulnerabilidades regras de destino de correção para obter informações sobre como funcionam as regras de destino de correção e como revisá-las.
- Exibir itens vulneráveis não agrupados .
  - Olhando os itens vulneráveis não agrupados, considere revisar as regras de grupo e executar uma nova verificação. Para obter mais informações, consulte Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção.
  - Agrupar manualmente os itens vulneráveis. Crie manualmente uma tarefa de correção em Resposta a vulnerabilidades para obter mais informações.
  - Revise as pontuações de risco dos itens vulneráveis em suas tarefas de correção. Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
  - Feche itens vulneráveis mais antigos não detectados recentemente por suas integrações de terceiros. Para obter mais informações, consulte Fechamento automático de itens vulneráveis e detecções.
- Exibir e reclassificar itens de configuração incompatíveis.
- PESQUISE o que precisa ser feito para correção.

  Esta etapa pode incluir:

  - Determine com o que lidar agora e o que você pode adiar. Essa determinação geralmente é baseada na pontuação de risco, nos sistemas afetados e nos patches com janelas de mudança.

    Nota: As regras de destino de correção pertencem a itens vulneráveis. Essas regras são executadas quando o item vulnerável é importado. Essas regras foram criadas anteriormente no Assistente de configuração.

  - Atualizar itens vulneráveis , se necessário, e. Exiba o status de destino de correção de um Resposta a vulnerabilidades item vulnerável.
  - Crie um **Solicitação de mudança** E atribuem a tarefa de correção a um grupo de atribuição (operações DE TI) para correção.

    Nota: Se a vulnerabilidade constituir um incidente de segurança e o Resposta a incidentes de segurança o plug-in (com.snc.security_incident) está ativado, você pode criar registros de incidentes de segurança a partir das tarefas de correção.

  - Depois de enviar uma ou mais solicitações de mudança, mova o estado do grupo para Em investigação.

Edite itens vulneráveis em massa em Resposta a vulnerabilidades

Edite itens vulneráveis em massa para economizar tempo selecionando campos e executando um trabalho assíncrono de edição em massa em segundo plano.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Importante: O recurso Edição em massa está disponível para itens vulneráveis do host no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Usando a edição em massa no Espaço do gerente de vulnerabilidade.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Selecione os itens vulneráveis executando uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . #unique_154_Connect_42_entry-be-record-selection campo.
   - Aplique filtros se quiser usar **Todos os itens vulneráveis que correspondem ao filtro** . #unique_154_Connect_42_entry-be-record-selection campo.
3. Selecione **Edição em massa** botão.
4. No modal Edição em massa, preencha os campos.

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente Itens vulneráveis selecionados ○ Todos os itens vulneráveis que correspondem ao filtro ○ Tarefa de correção ○ Entrada de vulnerabilidade
Estado	Mudança para **Estado** no item vulnerável. As opções são: ○ Não atualizar ○ Aberto ○ Sob Investigação ○ Aguardando Implementação ○ Adiado **Nota:** ▪ Quando você seleciona esta opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Ao adiar Vits, uma tarefa de correção é criada e esta tarefa é enviada para aprovação. ○ Encerrado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ▪ Quando você seleciona esta opção para marcar os registros como falso-positivo, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você marca os registros como falso-positivo, uma tarefa de correção é criada e esta tarefa é enviada para aprovação. ○ Resolvido
Solução preferencial	Solução destinada a corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para **Solução preferencial** Item vulnerável (Vits). As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os Vits selecionados. **Nota:** ○ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os Vits selecionados. ○ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** Para uma edição em massa, todos os Vits da vulnerabilidade . ser definido para a solução preferencial selecionada. **Nota:** Esta operação não define **Solução preferencial** no nível de entrada da vulnerabilidade. Definindo o. **Solução preferencial** no nível de entrada de vulnerabilidade, definiria o. **Solução preferencial** Para todos os novos Vits daqui para frente. A edição em massa modifica somente o conjunto atual de Vits. ○ Vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione Vits com critérios diferentes para definir o. **Solução preferencial** . ○ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição da lista de itens vulneráveis.
Preferencial patch	Patch destinado a corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar a Orquestração de patches para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os patches potenciais em todos os Vits selecionados. ◦ Vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione Vits com critérios diferentes para definir o. **Patch preferencial** . ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro Motivo para fechar registros: ◦ Falso Positivo **Nota:** ▪ Quando você seleciona esta opção, os campos Descrição resumida, Até,e Informações adicionais são exibidos. ▪ Uma tarefa de correção é criada quando você marca os registros como falso-positivo e esta tarefa é enviada para aprovação. ◦ Cancelado(a) ◦ Fixo **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve anotação descrevendo o motivo das solicitações de adiamento e encerradas-falso-positivo. Essas informações são refletidas no campo Descrição da tarefa de correção que é criada para solicitações adiadas e encerradas-falso-positivas. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-Positivo.
Até	Data até a qual o registro permanece adiado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo aparece quando você seleciona o Estado como Adiado.
Informações adicionais	Qualquer outra informação necessária. Essas informações são refletidas no campo Informações adicionais na guia Visão geral. Se sua solicitação de adiamento for aprovada, essas informações adicionais serão exibidas como anotações de adiamento na VIT e na tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-Positivo.
Cancelar atribuição	Todos os itens selecionados não têm atribuição atribuída ao grupo de atribuição e ao responsável pela correção. Para obter mais informações sobre como um responsável pela correção pode remover as atribuições de itens vulneráveis, consulte Remova atribuições de itens vulneráveis para você ou seus grupos . **Nota:** ○ Este campo aparece quando você seleciona o Estado como Não atualizar. ○ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e esta tarefa é enviada para aprovação.
Grupo de atribuição	Grupo de atribuição para o VIT. Selecione Manualmente ou Usar recomendações de atribuição, se estiver habilitado. **Nota:** Este campo é desabilitado quando você seleciona **Cancelar atribuição** caixa de seleção.
Anotações de trabalho	Texto inserido para descrever as mudanças.

5. Selecione **OK**.
   Um trabalho assíncrono de edição em massa atualiza os registros selecionados. O número do trabalho com um link é exibido na página Itens vulneráveis, onde você pode exibir seu status. Uma tarefa de correção é criada com os itens vulneráveis selecionados quando você adia, cancela a atribuição ou fecha itens vulneráveis (falso-positivo) em massa. E esta tarefa de correção é enviada para aprovação.

Desagrupado Resposta a vulnerabilidades itens vulneráveis

Itens vulneráveis são atribuídos automaticamente a uma tarefa de correção quando são importados. No entanto, às vezes, se um item vulnerável (VI) for criado manualmente, por exemplo, o VI poderá se tornar órfão. . **Desagrupado** o módulo de item vulnerável lista esses itens vulneráveis sem um grupo.

Nota: Os processos automatizados de integração não criam órfãos, portanto, espera-se que este caso de uso seja pequeno.

O desagrupamento ocorre se um item vulnerável foi criado sem uma vulnerabilidade ou se não houver uma regra de tarefa de correção que atribua o VI a um grupo.

Nesse caso, revise a lista de itens vulneráveis não agrupados navegando até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Desagrupado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a revisão, suas escolhas são as seguintes:

- Você pode Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção para capturar todos os itens que aparecem nesta lista.
- Você pode Crie manualmente uma tarefa de correção em Resposta a vulnerabilidades e adicionar manualmente itens desta lista ao grupo ou definir uma condição que corresponda a esses itens.
- Você pode abrir uma tarefa de correção existente e. adicione todos os itens vulneráveis relevantes ao grupo Desde que esteja no estado Aberto ou Em investigação.

Nota: Itens vulneráveis adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições de grupo.

Para obter mais informações sobre como as tarefas de correção e as regras de tarefa se comportam, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção.

Exibição desagrupada Resposta a vulnerabilidades itens vulneráveis

Itens vulneráveis que não são atribuídos a um grupo são colocados em uma lista visível.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis desagrupados**.
2. Revise os itens vulneráveis na lista.
3. Clique em cada item vulnerável para exibir e determinar como incluir em um grupo.

Adicione manualmente um item vulnerável a uma tarefa de correção

Se um item vulnerável for deixado desagrupado, você poderá adicioná-lo a uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Registre o número vulnerável.
2. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
3. Escolha uma tarefa de correção (VUL) para o item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Editar** no canto inferior direito.
5. Insira **item vulnerável** Número no campo de pesquisa da Coleção.
6. Selecione o item vulnerável na coleção e adicione à lista.
7. Clique em **Salvar**.

Remova atribuições de itens vulneráveis e tarefas de correção

Limpe **Atribuído a.** e. **Grupo de atribuição** campos em registros de item vulnerável no Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações e Contêiner de Resposta a vulnerabilidades aplicações.

Antes de Iniciar

Funções necessárias:

- sn_vul.remediation_owner ou sn_vul.vulnerability_analyst para itens vulneráveis (Vits) e tarefas de correção (VULs).
- sn_vul.app_sec_manager para Resposta a vulnerabilidades de aplicações Itens vulneráveis (AVITs) e tarefas de correção (AVULs).
- sn_vul_container.remediation_owner ou sn_vul_container.vulnerability_analyst para itens vulneráveis do contêiner (CVITs) e tarefas de correção (CVULs).

Por Que e Quando Desempenhar Esta Tarefa

. **Cancelar atribuição** A ação de IU é compatível com o ambiente clássico e os espaços de trabalho para os seguintes registros em qualquer estado diferente de Encerrado ou Resolvido:

- Tarefas de correção (VULs, AVULs e CVULs). Se uma tarefa de correção for atualizada com este recurso, o **Atribuído a.** e. **Grupo de atribuição** Os campos em todos os seus Vits associados que têm o mesmo grupo de atribuição também são limpos.
- Itens vulneráveis (Vits).
- Itens vulneráveis à aplicação (AVITs).
- Itens vulneráveis do contêiner (CVITs).

Importante: Você pode cancelar a atribuição de itens vulneráveis do host em massa no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Usando a edição em massa no Espaço do gerente de vulnerabilidade.

Procedimento

1. No ambiente clássico ou no Espaço do responsável de correção de TI, navegue até um registro de item vulnerável (VIT) atribuído a você e que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar **Atribuído a.** e. **Grupo de atribuição** na exibição clássica, na parte superior do registro, selecione **Cancelar atribuição** .
3. Como alternativa, navegue até um registro de item vulnerável (VIT, AVIT ou CVIT) no espaço de correção de TI atribuído a você ou aos seus grupos e clique em **Cancelar atribuição** No menu Mais opções () para limpar os campos de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para registros de tarefa de correção no espaço atribuídos a você ou aos seus grupos, abra uma seleção de registro **Cancelar atribuição** No menu Mais opções () para limpar os campos de atribuição.
5. Na caixa de diálogo Cancelar atribuição para itens vulneráveis e tarefas de correção, forneça anotações de trabalho e selecione **Enviar** .
   A solicitação de aprovação de mudança de estado é enviada para aprovação.

   Nota: Para tarefas de correção, você será notificado de que **Atribuído a.** e. **Grupo de atribuição** Os campos em todos os Vits associados a uma tarefa de correção também são limpos.

   Depois que a solicitação para limpar os campos é aprovada para uma tarefa de correção, todos os **Atribuído a.** e. **Grupo de atribuição** os campos em seus itens vulneráveis que têm o mesmo grupo de atribuição também não são atribuídos. Se algum item vulnerável tiver um grupo de atribuição diferente da tarefa de correção associada, ele não terá atribuição cancelada. Na maioria dos casos, esses itens vulneráveis foram atribuídos manualmente.
6. Exiba as seguintes informações:
   - As anotações de trabalho fornecidas são exibidas na seção Anotações.
   - Em **Aprovação de mudança de estado** , o registro de aprovação de mudança de estado é exibido com o estado Em revisão, o que ajuda a rastrear o fluxo de trabalho de aprovação.
   - Em **Aprovações solicitadas** Sua solicitação para remoção de você ou do seu grupo de atribuição é exibida no estado Solicitado.

Resultado

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades.

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada farão a transição para o estado Aprovado. Você e seus grupos serão removidos do **Atribuído a.** e. **Grupo de atribuição** campos. Não atribuído é exibido em **Tipo de atribuição** E a tarefa de correção e os Vits são exibidos na lista do módulo Não atribuído de cada produto.

  As notificações de que registros não são atribuídos são enviadas automaticamente para gerentes ou analistas de vulnerabilidades no grupo de notificação Cancelar atribuição. Para configurar o sinalizador de aprovação, as notificações e o grupo de atribuição padrão, consulte Removendo atribuições de itens vulneráveis e tarefas de correção .

- Se sua solicitação for rejeitada, o estado do registro de aprovação de mudança e do registro de aprovação solicitada farão a transição para o estado Rejeitado.

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

O que Fazer Depois

Navegue até os Módulos não atribuídos para Resposta a vulnerabilidades e. Resposta a vulnerabilidades de aplicações Contêiner de Resposta a vulnerabilidades monitoram todos os registros

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

não atribuídos para itens que podem se enquadrar no seu escopo e reatribua-os a você mesmo.

Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades

Aprove solicitações para a remoção de itens vulneráveis de um grupo de atribuição ou de um usuário individual no Resposta a vulnerabilidades aplicação.

Antes de Iniciar

Função necessária: Para aprovações de cancelamento de atribuição, um aprovador é necessário no grupo Aprovador - Nível 1.

- sn_vul.unassign_approver para AVITs e Vits
- sn_vul_container.unassign_approver para CVITs

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação de cancelamento de atribuição é criado. Os usuários do grupo Não atribuir aprovador - Nível 1 podem aprovar a solicitação. Por padrão, este grupo contém uma função de aprovador de cancelamento de atribuição, sn_vul.unassign_approver. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar uma regra de aprovação, selecione qualquer uma das seguintes regras de aprovação no módulo Regras de aprovação e navegue até a configuração de aprovação no **Configurações de aprovação** guia:

- *`Vulnerable item field change request`* para um item vulnerável.
- *`Vulnerability field change request`* para uma tarefa de correção.
- *`Application vulnerability field change request`* Para um item vulnerável à aplicação (AVIT).
- *`Approval for container management`* Para um item vulnerável de contêiner (CVIT).

Para obter mais informações sobre regras e configurações de aprovação, consulte Configurações do fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição.

Importante: Você pode aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade. .

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Minhas aprovações** Para Vits e AVITs. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações** Para CVITs.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação adicionando os comentários apropriados.

Fechamento automático de itens vulneráveis e detecções

Você pode fechar automaticamente detecções obsoletas e itens vulneráveis (VIS) associados a ICs desativados usando o módulo Regras de fechamento automático.

Você pode fechar automaticamente detecções obsoletas e VIS nos seguintes cenários:

- Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades
- Fechar automaticamente itens vulneráveis relacionados a ICs desativados

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Trabalhar com itens de configuração desativados e. Criar regras de fechamento automático.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhar com itens de configuração desativados

Itens de configuração desativados (ICs) são movidos para o estado desativado, arquivado ou excluído em Configuration Management Database (CMDB). Resposta a vulnerabilidades Contém itens vulneráveis (VIS) compostos por ICs. Quando o estado de um IC é atualizado para desativado, os VIS associados são encerrados com o subestado "IC desativado".

Nota: A partir da v25.0.3 de Resposta a vulnerabilidades Uma nova regra de fechamento automático "IC desativado" é introduzida para fechar os itens vulneráveis e as detecções relacionadas a ICs desativados.

Se o CMDB mudar o status da fase do ciclo de vida de um IC para desativado, você poderá optar por fechar automaticamente o VIS associado. Para obter mais informações sobre como fechar automaticamente o VIS associado, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O IC descontinuado é arquivado ou excluído permanentemente do CMDB.

Impacto de descontinuar os ICs:

- **Impacto nos itens descobertos:** Quando o IC é descontinuado, o item descoberto (DI) relacionado é marcado como "IC desativado".
- **Impacto nos itens vulneráveis:** Quando o estado de um DI é atualizado para "IC desativado", o VI associado é encerrado e a seção Anotações é atualizada automaticamente.

  Nota: O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de uma VI é atualizado para Encerrado somente quando **VIS de fechamento automático vinculado a ICs descontinuados** a opção está habilitada. Para obter mais informações sobre como fechar automaticamente o VIS associado, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O trabalho agendado *Close detections/VIs for decommissioned CIs*É executado diariamente para o DIS atualizado. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará o DI que contém um IC desativado e fechará o VI relacionado com o subestado "IC desativado". Se todos os VIS em uma tarefa de correção estiverem encerrados e seu subestado for IC desativado, a tarefa de correção também será encerrada com o subestado "Cancelado". Para exibir o VIS desativado, navegue até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Desativado**.

Nota: Se um IC voltar para o estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os VIS são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente itens vulneráveis relacionados a ICs desativados

. Configuration Management Database (CMDB) Muda o status da fase do ciclo de vida de um item de configuração (IC) para desativado. Você pode optar por fechar automaticamente os itens vulneráveis (VIS) e as detecções associados.

Antes de Iniciar

Função necessária: sn_vul.admin

Por Que e Quando Desempenhar Esta Tarefa

A partir da v22.0 de Resposta a vulnerabilidades, Para fechar automaticamente os VIS e as detecções associadas, você deve habilitar a propriedade do sistema *sn_vul_cmn.auto_close_vis_linked_retired_cis*Para fechar automaticamente os VIS

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

associados a ICs descontinuados. Para habilitar a opção, defina o campo Valor como "1". Por outro lado, para desabilitar a opção, defina o campo Valor como "0".

Durante um upgrade se a propriedade do sistema *sn_vul_cmn.auto_close_vis_linked_retired_cis*está selecionado na v21.0 de Resposta a vulnerabilidades, em seguida, o valor permanece como "1". Quando esta opção está habilitada, todos os VIS e detecções novos ou existentes relatados para o mesmo IC são criados ou atualizados automaticamente com um status "Encerrado". Isso é baseado no ID do ativo na carga do scanner e no status da entrada de itens descobertos. Para obter mais informações sobre o impacto de ICs descontinuados, consulte Trabalhar com itens de configuração desativados

.

Nota:

- O estado de um DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de uma VI é atualizado para Encerrado somente quando **VIS de fechamento automático vinculado a ICs descontinuados** a opção está habilitada.
- As informações fornecidas no procedimento a seguir só se aplicam a versões anteriores à v2.0de Resposta a vulnerabilidades. A partir da v22.0 de Resposta a vulnerabilidades, você tem a opção de configurar opções de pesquisa adicionais. Para obter mais informações, consulte Criar regras de fechamento automático.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Configuração de fechamento automático** > **Ciclo de vida do item de configuração**.
2. Para fechar automaticamente os itens vulneráveis associados aos ICs desativados, selecione **VIS de fechamento automático vinculado a ICs descontinuados** caixa de seleção.
3. Selecione **Atualizar**.

Nota: Se um IC já tiver sido descontinuado antes de **VIS de fechamento automático vinculado a ICs descontinuados** A opção está habilitada, os VIS são criados somente para novas detecções de scanners. O estado desses VIS é Encerrado e o subestado é IC desativado.

Você não pode reabrir manualmente o VIS cujo estado é IC desativado, usando **Reabrir** ou **Edição em massa** opções.

Os VIS encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e o VIS puder ser correspondido à nova vulnerabilidade. Para obter mais informações, consulte Detecções, tarefas de correção e estados de itens vulneráveis.

Fechando detecções obsoletas em Resposta a vulnerabilidades

O módulo Encerramento automático de detecções obsoletas ajuda a limpar automaticamente detecções vulneráveis mais antigas e obsoletas não encontradas recentemente por suas integrações de terceiros. Mover essas detecções para Encerradas reduz o número de itens vulneráveis ativos e tarefas de correção em seu ServiceNow AI Platform E ajudam a reconciliar ativos no CMDB.

Visão geral e termos principais

Para acumular dados de detecção com mais precisão para seus itens vulneráveis, o módulo Fechar detecções obsoletas ajuda a limpar detecções de itens vulneráveis mais antigas e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obsoletas que não foram encontradas recentemente por suas integrações de terceiros. Para obter mais informações sobre esse recurso, consulte o caso de uso abaixo.

Em versões anteriores de Resposta a vulnerabilidades, O módulo Fechar itens vulneráveis automaticamente fez a transição automática de itens vulneráveis não encontrados recentemente ou atualizados por suas integrações de scanner de terceiros para Encerrado - obsoleto.

Antes de habilitar o recurso Encerrar detecções obsoletas automaticamente, revise os termos a seguir, como os estados se acumulam em itens vulneráveis e tarefas de correção e os pré-requisitos para suas integrações de terceiros que importam dados de detecção.

Para habilitar o recurso, consulte Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades.

Termos principais

Detecções obsoletas

Refere-se a detecções associadas a itens vulneráveis em seu ServiceNow AI Platform® instâncias que estão envelhecidas e não foram encontradas, atualizadas ou detectadas por verificações de integração de terceiros por um período significativo.

Últimas detecções encontradas

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais ou mais recentes em que as detecções foram encontradas novamente pelo scanner.

Ativos verificados pela última vez

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros, e suas detecções associadas não são atualizadas por detecções de itens vulneráveis. Como resultado, as detecções e seus itens vulneráveis relacionados não são atualizados no Resposta a vulnerabilidades e eles se tornam inativos (obsoletos).

Para fechar essas detecções antigas que têm dados de item vulnerável inalterados e reduzir o número de tarefas de correção (RTS) e VIS ativas, habilite Encerramento automático de detecções obsoletas. Este recurso fecha automaticamente as detecções de item vulnerável que não foram recentemente encontradas ou atualizadas por suas integrações de scanner de terceiros com base nos critérios de pesquisa e em uma idade em número de dias que você definiu.

Por exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado em uma detecção de um scanner de terceiros nos últimos 90 dias. Este recurso fecha automaticamente esta detecção que não tem novos dados de vulnerabilidade para que o VI associado possa ser encerrado.

Como uma VI pode ter mais de uma detecção associada a ela, esse recurso só faz a transição das detecções determinadas como obsoletas pelos parâmetros definidos. Por exemplo, se uma VI tiver quatro detecções associadas a ela e duas detecções estiverem obsoletas, ou seja, nenhum novo dado de vulnerabilidade tiver sido importado nos últimos 90 dias, este recurso fechará somente as detecções obsoletas. Antes que o VI possa ser fechado, você deve primeiro corrigir as outras duas detecções em aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acúmulo de estados de detecção para VIS

Para diferenciar as detecções encerradas automaticamente das detecções encerradas por scanners de terceiros, um novo valor para o campo Status, obsoleto, foi adicionado. Os valores possíveis para este campo são Aberto, Encerrado e obsoleto. Obsoleto indica que uma detecção foi encerrada pelo recurso de detecção de fechamento automático.

Precedência de estado: Aberto > Encerrado > obsoleto.

1. Se alguma detecção estiver aberta, o estado de VI associado permanecerá aberto.
2. Se nenhuma detecção estiver aberta, algumas estiverem encerradas e outras obsoletas, o estado do VI associado mudará para Encerrado - Corrigido.
3. Se todas as detecções estiverem obsoletas, o estado de VI associado será transferido para Encerrado - obsoleto.

   Começando com Resposta a vulnerabilidades20,0, Se a detecção estiver obsoleta e seu VI associado estiver no estado Encerrado, o estado do VI não fará a transição para Encerrado - obsoleto. Evitar que o VI seja reaberto quando uma nova detecção for identificada, para que você possa evitar passar por todo o processo de solicitação e aprovação de falso-positivo. Para reverter esse comportamento, desmarque **Ignorar detecções obsoletas para VIS encerrados** Caixa de seleção no formulário Configuração de fechamento automático. Para obter mais informações, consulte Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades.

Acúmulo de estados de VI para tarefas de correção (VUL)

Precedência de estado: Aberto > Encerrado - Fixo > Encerrado - obsoleto.

1. Se algum VIS em um VUL (tarefa de correção) estiver aberto, o estado DO VUL não será alterado.
2. Se pelo menos um VI estiver encerrado - fixo e o restante estiver encerrado - obsoleto, o estado VUL mudará para Encerrado - fixo.
3. Se todos os VIS em um VUL estiverem encerrados - obsoletos, o estado do VUL mudará para Encerrado - Cancelado.
4. Se algum VIS for fechado como Encerrado - Falso positivo, o VUL não fechará automaticamente.

Para obter mais informações sobre cenários de rollup e rolldown de estado, consulte, Cenários de roll-up e roll-down de estado.

Detecções de fechamento automático e requisitos de integração de terceiros

Usuários do Microsoft TVM e Fechamento automático de detecções obsoletas

Item de check-list	Descrição
Microsoft TVM Vulnerability Integration	Com o Microsoft TVM Vulnerability Integration, se você selecionar **Detecções encontradas pela última vez** Para basear sua pesquisa, este recurso requer uma execução bem-sucedida da Integração de vulnerabilidades de máquina do Microsoft TVM (importação completa) nos últimos sete dias. Esta integração é executada semanalmente. Se as detecções obsoletas de Fechamento automático estiverem habilitadas e configuradas para **Detecções**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	encontradas pela última vez E a Integração de vulnerabilidades de máquina do Microsoft TVM estiver desabilitada ou uma importação de dados não for concluída com sucesso nos últimos sete dias, o trabalho agendado para fechar detecções ainda será executado diariamente, mas algumas detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Ativos verificados pela última vez** Para basear sua pesquisa, a execução de Integração de vulnerabilidades de máquina do Microsoft TVM não é necessária. Para ativar esta integração: 1. Navegar até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integração**. 2. Localize e habilite o. **Microsoft TVM Machine Vulnerabilities Integration (importação completa)** .
(Opcional) Implemente várias instâncias das integrações do Microsoft TVM em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações em seu ambiente. O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. Detecções obsoletas são transferidas automaticamente para obsoletas em instâncias que concluíram execuções de integração com sucesso. Se o Fechamento automático de detecções obsoletas estiver habilitado e você desabilitar as integrações executadas semanalmente em uma instância, o trabalho agendado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não passar para obsoletas automaticamente conforme o esperado.

Qualys Itens vulneráveis obsoletos e Fechamento automático

- Ativado Qualys integrações de terceiros que recuperam dados de detecção podem ser executadas com este módulo. Não há específico Qualys aplicações necessárias.
- Opcionalmente, você pode implantar várias instâncias do Qualys integrações em seu ambiente.
- O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. Detecções obsoletas são transferidas automaticamente para obsoletas em todas as instâncias.

Rapid7 Usuários e Fechamento automático de detecções obsoletas

Item de check-list	Descrição
. Rapid7 Integração de vulnerabilidades	Se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso requer uma execução bem-sucedida de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	um dos Rapid7 Integrações abrangentes de itens vulneráveis nos últimos sete dias. Estas integrações abrangentes são executadas semanalmente: • Para Rapid7 Nexpose depósito de dados, uma execução bem-sucedida do Rapid7 A integração abrangente de item vulnerável é necessária. • Para Rapid7 InsightVM, uma execução bem-sucedida do Rapid7 Integração abrangente de item vulnerável - A API é necessária. Se Fechar detecções obsoletas automaticamente estiver habilitado e configurado para **Detecções encontradas pela última vez** e Rapid7 As Integrações abrangentes de item vulnerável estão desabilitadas ou uma importação de dados não foi concluída com sucesso nos últimos sete dias, o trabalho agendado para fechar detecções ainda é executado diariamente, mas algumas detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Ativos verificados pela última vez** para basear sua pesquisa, não abrangente Rapid7 a execução de integração é necessária. Para ativar estas integrações: **1.** Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integração**. **2.** Localize e habilite o. Rapid7 Integração abrangente de item vulnerável de que você precisa. **Nota:** Além dessas integrações que são executadas semanalmente, Rapid7 Nexpose e. Rapid7 InsightVM Cada um tem integrações de VI que são executadas diariamente, a integração de item vulnerável do Rapid7 e a API de integração de item vulnerável do Rapid7. Diariamente e semanalmente Rapid7 as integrações estão habilitadas, somente uma integração é executada por vez. Se um desses trabalhos de integração estiver em execução, o trabalho da outra integração será ignorado até o próximo trabalho agendado.
(Opcional) Implanta várias instâncias do Rapid7 integrações em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações abrangentes em seu ambiente. O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. Detecções obsoletas são transferidas automaticamente para obsoletas em instâncias que concluíram execuções de integração com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	Se Fechar detecções obsoletas automaticamente estiver habilitado e você desabilitar as integrações executadas semanalmente em uma instância, o trabalho agendado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não fazer a transição para obsoletas automaticamente conforme o esperado.

Usuários do Tenable Vulnerability Integration e fechamento automático de itens vulneráveis obsoletos

- Quaisquer integrações ativadas da Integração de vulnerabilidades do Tenable que recuperam dados de detecção podem ser executadas com este módulo. Não há integrações de vulnerabilidade específicas do Tenable necessárias.
- Opcionalmente, você pode implantar várias instâncias da Integração de vulnerabilidades do Tenable em seu ambiente.
- O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. Detecções obsoletas são transferidas automaticamente para **Obsoleto** em todas as instâncias.

Depois de verificar se suas integrações estão configuradas corretamente, consulte Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades para habilitar o recurso.

Atualize as informações de Fechar automaticamente itens vulneráveis obsoletos para Fechar automaticamente detecções obsoletas

Para o módulo Fechar detecções obsoletas automaticamente, se você usou anteriormente Fechar itens vulneráveis obsoletos automaticamente:

- O valor do número de dias que você inseriu para **Ativos verificados pela última vez** A opção de Fechar itens vulneráveis obsoletos automaticamente é preservada automaticamente para **Ativos verificados pela última vez** Em Fechamento automático de detecções obsoletas.
- O valor do número de dias que você inseriu para **Itens vulneráveis encontrados pela última vez** A opção de Fechar itens vulneráveis obsoletos automaticamente é preservada automaticamente para **Detecções encontradas pela última vez** Em Fechamento automático de detecções obsoletas.
- Detecções em aberto existentes com itens vulneráveis como encerrados - obsoletos serão transferidas para obsoletos de acordo com as definições de configuração de fechamento automático quando *`Auto-Close Stale Detections`*o trabalho agendado é executado após o upgrade.

Acúmulo de informações

- Se um item vulnerável foi encerrado - obsoleto antes do upgrade e todas as detecções forem marcadas como obsoleto após o upgrade, o estado VI permanecerá encerrado - obsoleto.
- Se um item vulnerável foi encerrado - obsoleto antes do upgrade, e somente algumas de suas detecções estiverem marcadas como obsoletas após o upgrade e o restante tiver sido encerrado pelo scanner, o item vulnerável será transferido para Encerrado - corrigido de acordo com a lógica de rollup.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades

Habilite Fechar detecções obsoletas automaticamente para fechar automaticamente detecções vulneráveis obsoletas não encontradas recentemente por suas integrações de terceiros.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (descontinuado) ou um gerenciador de vulnerabilidades com a função granular sn_vul.manage_auto_close_stale_vi.

Para obter mais informações sobre esse recurso, termos principais e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de detecção, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades para obter mais informações.

Nota: As informações fornecidas no procedimento a seguir só se aplicam a versões anteriores à v2.0de Resposta a vulnerabilidades. A partir da v22.0 de Resposta a vulnerabilidades, você tem a opção de configurar opções de pesquisa adicionais. Para obter mais informações, consulte Criar regras de fechamento automático.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Configuração de fechamento automático** > **Detecções obsoletas**.
   O formulário Fechar configuração obsoleta automaticamente é exibido.
2. Preencha os campos.
3. Para **Fechamento automático de detecções obsoletas com base em** escolha uma opção para sua pesquisa.

   Ambas as pesquisas correspondem à idade das detecções mais antigas e obsoletas em número de dias até uma data fornecida pelo scanner.

   Nota: A partir da v22.0 de Resposta a vulnerabilidades, as opções **Detecções encontradas pela última vez** e. **Ativos verificados pela última vez** são criados como uma lista.

   - **Detecções encontradas pela última vez** . Esta opção pesquisa a data mais atual ou mais recente em que as detecções foram encontradas novamente pelo scanner.

     Nota: Para Rapid7 e. Microsoft Usuários de TVM, uma mensagem de aviso é exibida sobre a necessidade de informações de detecção atuais.

     Se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso requer uma execução de integração bem-sucedida de um dos Rapid7 Integrações abrangentes de itens vulneráveis nos últimos sete dias.

     Se você selecionar **Detecções encontradas pela última vez** Para basear sua pesquisa, este recurso requer uma execução de integração bem-sucedida da Integração de vulnerabilidades de máquina do Microsoft TVM (importação completa) nos últimos sete dias.

   - **Ativos verificados pela última vez** . Esta opção pesquisa a data mais atual em que um ativo foi verificado pela última vez por um scanner de terceiros.
4. Para Rapid7 e. Microsoft Somente usuários de TVM, verifique se todas as integrações necessárias estão habilitadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Noções básicas do Integração com Rapid7 Vulnerability e Noções básicas sobre a integração de vulnerabilidades do Microsoft Threat and Vulnerability Management.

5. Para habilitar o módulo, clique na caixa de seleção Ativo para selecioná-lo.
6. Em **Detecções encontradas pela última vez (dias atrás)** insira a idade das detecções antigas e obsoletas no número de dias.

   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias. Este valor é usado para corresponder a uma data fornecida pelo scanner. Com 90 e. **Detecções encontradas pela última vez** exibidas, todas as detecções não encontradas nos últimos 90 dias serão encerradas automaticamente. Com 90 e. **Ativos verificados pela última vez** exibidas, todas as detecções associadas a ativos não verificados nos últimos 90 dias são encerradas automaticamente.

   Nota:

   Há um relacionamento entre **Últimas detecções encontradas/ativos verificados pela última vez (dias atrás)** campo para este recurso e **Importar desde** No Rapid7 Comprehensive Vulnerable Item Integration - API e na integração Microsoft TVM Machine Vulnerabilities.

   Para essas integrações, o **Importar desde** o campo nas páginas de configuração está vazio por padrão.

   Se você não inserir um valor ou o campo não tiver valor, os dados do número de dias configurados no **Últimas detecções encontradas/ativos verificados pela última vez (dias atrás)** o campo é usado.

   Por exemplo, se o número de dias definido no formulário de configuração de fechamento automático for 90 e **Importar desde** o campo está vazio nas páginas de configuração de integração e a primeira execução de integração importa os dados dos últimos 90 dias. . **Importar desde** campos para Rapid7 Integração abrangente de item vulnerável - API e a integração Microsoft TVM Machine Vulnerabilities são editáveis, para que você também possa fornecer os valores desejados. O valor de 90 dias será fornecido como padrão se o campo permanecer vazio para que o recurso de fechamento automático não feche os falsos positivos.

   Este relacionamento entre esses campos se aplica somente à primeira execução de integração. Depois disso, mude **Últimas detecções encontradas/ativos verificados pela última vez (dias atrás)** O campo no formulário Fechar automaticamente detecções vulneráveis obsoletas não afeta **Importar desde** campo nas páginas de configuração de integração. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta.

7. **Opcional:** Selecione **Ignorar detecções obsoletas para VIS adiados** Caixa de seleção para ignorar detecções obsoletas que são mapeadas para VIS adiado ou para VIS atualmente em revisão para adiamento.

   (Optional) Se você deixar esta opção desabilitada, todas as detecções que corresponderem aos seus critérios serão encerradas e mapeadas para VIS adiados ou para VIS que estão em revisão para adiamento. Os VIS adiados, ou VIS que estão em revisão que correspondem a essas detecções, também são encerrados automaticamente com base na lógica de acúmulo. Para obter mais informações sobre lógica de acúmulo, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades e. Cenários de roll-up e roll-down de estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar esta opção, todas as detecções que corresponderem aos seus critérios mapeadas para VIS adiados ou para VIS que estão em revisão para adiamento serão ignoradas durante o fechamento automático.

8. **Opcional:** Desmarque **Ignorar detecções obsoletas para VIS encerrados** caixa de seleção.

   (Optional) Por padrão, esta caixa de seleção é marcada para que o VI encerrado não seja reaberto quando uma nova detecção relacionada a este VI encerrado for identificada. Para obter mais informações sobre a lógica de acúmulo, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades e. Cenários de roll-up e roll-down de estado.

9. Clique em **Atualizar** para salvar suas mudanças.

   . *`Auto-Close Stale Detections`*o trabalho agendado é executado diariamente. O trabalho determina se você selecionou a data em que as detecções foram encontradas pela última vez ou a data em que os ativos foram verificados pela última vez. Em seguida, ele faz a transição das detecções correspondentes para o estado obsoleto. É importante observar que o recurso Encerrar detecção obsoleta automaticamente fecha detecções obsoletas somente para instâncias de integração ativas. Detecções e itens vulneráveis associados a instâncias de integração ativas são encerrados. A partir da v22.0 de Resposta a vulnerabilidades o trabalho agendado foi modificado para levar em conta a tabela comum [sn_vul_cmn_auto_close_rule].

   Depois que as detecções forem marcadas como obsoletas, se o scanner relatar que descobriu essa detecção novamente, o campo Status das detecções será aberto. Os itens vulneráveis correspondentes da detecção também são reabertos.

   Além disso, se a detecção estiver marcada como obsoleta e o scanner descobrir que ela está corrigida, a detecção mudará para Encerrada. O estado também é acumulado para o VIS.

Criar regras de fechamento automático

Use regras de fechamento automático para fechar detecções mais antigas automaticamente com base nas condições de filtro definidas.

Antes de Iniciar

Função necessária: sn_vul.manage_auto_close_stale_vi

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de fechamento automático**.

   O sistema de base fornece as seguintes regras de fechamento automático:

   - **Ativos verificados pela última vez** Detecções associadas a ativos que não foram verificados nos últimos 90 dias são transferidas para **Obsoleto** estado.
   - **Detecções manuais encontradas pela última vez** Detecções manuais que não foram encontradas nos últimos 90 dias. Se você ativar **Detecções encontradas pela última vez** , este recurso requer uma execução de integração bem-sucedida de Rapid7 Integrações abrangentes de item vulnerável e integração de vulnerabilidades de máquina do Microsoft TVM (importação completa) nos últimos sete dias.
   - **Detecções encontradas pela última vez** Detecções que não foram encontradas nos últimos 90 dias.

2. Selecione **Novo** para criar uma nova regra de fechamento automático.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário, preencha os campos.

Campo	Valor
Nome	Nome da regra de fechamento automático.
Ativo	Opção para ativar a regra. Se ativado, ele fecha automaticamente todas as detecções que correspondam aos critérios de filtro.
Ignorar itens adiados	Se selecionado, todas as detecções mapeadas para **Em revisão** ou **Adiado** os estados são ignorados e não encerrados. Se você desmarcar esta opção, todas as detecções que corresponderem aos seus critérios serão encerradas.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.

. `Auto-Close Stale Detections`o trabalho agendado é executado diariamente. Identifica detecções com base nas condições especificadas e faz a transição das correspondentes para **Obsoleto** estado. O trabalho lida com os seguintes cenários:

- Se todas as detecções em um item vulnerável (VIT) estiverem marcadas como obsoletas, a VIT será fechada com o subestado definido como "obsoleto".
- Se houver pelo menos uma detecção que permanecer aberta em uma VIT, enquanto outras estiverem no status obsoleto, a VIT permanecerá aberta.
- Nos casos em que há detecções com status "Encerrado" e "obsoleto" em uma VIT, a VIT é fechada com o subestado definido como "Fixo".

Quando você faz upgrade para a versão mais recente de Resposta a vulnerabilidades, as condições definidas em suas regras de fechamento automático também são atualizadas de acordo. Além disso, se as regras estiverem associadas a domínios diferentes, as regras serão criadas especificamente nesses domínios.

Reclassificar hardware não classificado

Reclassifique o hardware não classificado atualizando as regras de pesquisa de IC.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa

A tabela Mapa de importação de host [sn_sec_cmn_src_cmdb_map] exibe as variáveis de entrada da carga e suas atribuições correspondentes na tabela Itens descobertos. Ocasionalmente, discrepâncias nas convenções de nomenclatura entre o scanner e a Descoberta podem fazer com que o hardware fique sem classificação. Ao criar um novo IC de hardware não classificado, certifique-se de que o nome na carga contenha somente o Nome do host. Mais tarde, quando a Descoberta identifica o ativo, ele pode ser reclassificado na classe de IC apropriada. Se necessário, um script pode ser gravado para gerar um valor derivado que se alinhe ao nome dos ICs na Descoberta e no Configuration Management Database (CMDB).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o mecanismo de Identificação e reconciliação (IRE) estiver ativado, a opção Reclassificar de itens descobertos não será compatível.

Procedimento

1. Navegue até a tabela Mapas de importação de host [sn_sec_cmn_src_cmdb_map].
2. Selecione uma origem.
3. Na lista Campo de destino, selecione **Nome** .
   . **Usar script** a caixa de seleção se torna visível.

   Nota:

   - O script estará disponível somente se **Nome** É selecionado na lista Campo de destino.
   - Para adicionar um script para outras opções na lista de campos de destino, você deve desabilitar a política de IU da seguinte forma:
     - Desabilitando "Definir uso de script falso".
     - Desabilitando "Mostrar ou ocultar usar script".
     - Removendo a condição "O campo de destino é o nome" em "Mostrar ou ocultar política de script".
   - A tabela Mapas de importação de host é atualizada com duas novas colunas: Script e Usar script.

4. Selecione **Usar script** caixa de seleção.
   . **Script** o campo exibe o script padrão, mas você tem uma opção para criar um personalizado. Neste campo, você pode especificar a origem e os valores derivados para alinhar com a convenção de nomenclatura do banco de dados. O valor gerado pelo script é armazenado em sourcePayload['DERIVADO'] [rule.source_field]. Certifique-se de que as regras de pesquisa de IC sejam ajustadas para utilizar a carga de origem, os valores de atributo derivado e de destino ao fazer check-in das tabelas correspondentes.
5. Para aplicar o script a registros duplicados mais antigos, faça o seguinte:

   a. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens descobertos**.

   b. Selecione os registros duplicados.

   c. Na lista Ação nas linhas selecionadas, selecione **Reaplicar regras de Pesquisa de IC** .
   Mostra uma correspondência com um ativo existente.

6. Para aplicar o script Tenable.io, faça o seguinte:

   a. Navegar até **Resposta a vulnerabilidades Mapas de importação do host** .

   b. Selecione o script para a linha com NetBIOS, NOMES DE HOST e nome de FQDNS como **Origem** campo.

   c. Atualize o script para cada elemento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para Tenable.io, O scanner retorna uma matriz para NetBIOS, NOMES DE HOST e nome de FQDNS, para a qual o script não funciona conforme o esperado.

Porque o Mapa de importação de host para Tenable.io contém **netbios_name** em **Origem** , você deve escrever um script. Outro campo de origem durante a pesquisa **NETBIOS** é usado, que tem uma matriz de valores. Uma nova linha é adicionada à tabela e a mesma lógica deve ser gravada em um loop no script. Da mesma forma, para **FQDNS** e. **NOMES DE HOST** .

7. Para aplicar o script Rapid7, faça o seguinte:
   a. Navegar até **Tudo** > **Resposta a vulnerabilidades Mapas de importação do host** .
   b. Para Rapid7 Linhas com FQDN e nome de host, atualize o Método de pesquisa para Script.

Nota: Para Rapid7, O Método de pesquisa de IC é definido como Correspondência de campo para FQDN e Nome de host, o que ajuda a impedir que ele use o script.

Crie manualmente uma tarefa de correção em Resposta a vulnerabilidades

A criação de uma tarefa de correção manualmente é feita quando você deseja agrupar itens vulneráveis por algo diferente dos critérios de regras da tarefa de correção. Por exemplo, você pode criar tarefas para um gerente específico ou para novas explorações ativas, como ransomware que incluem vulnerabilidades diferentes. Você também pode usá-lo para agrupar itens vulneráveis não agrupados.

Importante: Você pode criar tarefas de correção de host em:

- Espaço do gerente de vulnerabilidade como um usuário com sn_vul.vulnerability_analyst, ou função sn_vul.vulnerability_admin.
- Espaço de correção de problemas de TI como um usuário com a função sn_vul.remediation_owner.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.

   As regras de tarefa de correção funcionam da mesma forma que as regras de tarefa de correção funcionavam anteriormente e ainda estão disponíveis para você. No entanto, você pode preferir deixar as regras de tarefa de correção inativas à medida que se acostuma com os recursos disponíveis para seus gerentes de segurança e equipes DE TI nos espaços de trabalho.

2. Selecione uma das categorias de tarefas para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.
   Para obter informações sobre campos específicos, consulte Campos do formulário de tarefa de correção.
5. Clique em **Enviar**.
   Quando a tarefa é criada, usando **Condição** ou **Grupo de filtros** tipo de filtro **Item vulnerável** a lista relacionada pesquisa e exibe todos os itens vulneráveis correspondentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar o Link relacionado, **Verificar vulnerabilidades novamente** para acionar manualmente um ServiceNow®- verificação iniciada. Para obter informações sobre como configurar um verificador de vulnerabilidades, consulte Configurar e gerenciar Qualys verificações e verificações de vulnerabilidades.

Para uma Integração de vulnerabilidades da Qualys, um scanner padrão é pré-instalado no **Scanners de vulnerabilidades** módulo. Este scanner está desativado por padrão. Selecione **Ativo** e. **Padrão** Caixas de seleção para ativar o scanner da Qualys para trabalhar usando o. **Verificar vulnerabilidades** link relacionado nos formulários tarefa de correção e item vulnerável.

. **Atualizar status** o link relacionado exibe a data e a hora da última atualização. Acumula informações do VIS na tarefa de correção. Para obter mais informações, consulte Campos do formulário de tarefa de correção. Quando uma tarefa é formada com base em uma vulnerabilidade específica, essa vulnerabilidade é listada no formulário de tarefa de correção.

Se você abrir um item vulnerável associado, todas as entradas de tarefa de correção associadas serão exibidas em **Tarefa de correção** guia lista relacionada.

Adicione usuários ao grupo Resposta a vulnerabilidades

Quando o recurso Fechar/Adiar é usado para adiar ou fechar um item vulnerável sem exigir uma verificação, o. Resposta a vulnerabilidades o grupo é notificado para aprovar ou rejeitar a solicitação. Você pode atribuir os usuários apropriados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.
2. Abra o. Resposta a vulnerabilidades grupo.
3. Clique em **Membros do grupo** lista relacionada e clique em **Editar** .
4. Selecione um ou mais nomes em **Coleção** lista.
5. Clique em **Adicionar**.
6. Clique em **Salvar**.

Tópicos relacionados

Criar um usuário

Gerencie itens vulneráveis individuais manualmente

Itens vulneráveis representam um item de configuração (IC) com uma determinada vulnerabilidade. Itens vulneráveis são importados de fontes de terceiros ou usando as informações SAM NVD (link) para comparar entradas de vulnerabilidade com registros de software recuperados do Software Gestão de ativos módulo.

Itens vulneráveis estão contidos em tarefas de correção definidas por regras de vulnerabilidade. Normalmente, as tarefas de correção são o local onde os grupos de itens vulneráveis são atribuídos e trabalhados.

Itens vulneráveis podem ser exibidos e editados em massa no **Itens vulneráveis** módulo. Os registros de itens vulneráveis exibem informações da vulnerabilidade no **Vulnerabilidade**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

guia. Esta guia pode indicar se há explorações públicas ou ativas para ela. Além disso, mostra se isso pode ser corrigido por meio de um patch, mudança de configuração ou combinação de ambos. Se houver endereços IP encontrados durante a desduplicação, eles serão exibidos em uma lista relacionada.

Se um IC for removido do CMDB, todos os itens vulneráveis associados também serão removidos.

Quando um item vulnerável é adicionado a uma tarefa de correção, o grupo aparece em **Tarefas de correção** Lista de itens vulneráveis.

Quando uma tarefa é criada que afeta um item vulnerável, a tarefa aparece em **Tarefas que afetam** Lista relacionada de itens vulneráveis.

Itens vulneráveis podem ser criados manualmente. Você pode criar incidentes de segurança ou solicitações de mudança e encerrá-los ou adiá-los manualmente. As regras de tarefa de correção podem ser aplicadas a itens vulneráveis criados manualmente.

As tarefas de correção e as regras de tarefa de correção foram aprimoradas para assumir a funcionalidade da tarefa. Itens vulneráveis não podem ser vinculados como uma tarefa primária.

Criar Resposta a vulnerabilidades itens vulneráveis

Vários métodos criam itens vulneráveis (VI). Mais comumente, uma integração a um scanner de vulnerabilidades é instalada e configurada para importar resultados todas as noites. Há casos, como vulnerabilidades de segurança física, em que você pode preferir adicionar manualmente registros de item vulnerável.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Por Que e Quando Desempenhar Esta Tarefa

Os VIS criados manualmente e criados automaticamente são adicionados e removidos automaticamente das tarefas de correção por regras de tarefa de correção e condições de grupo.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Selecione uma categoria para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.
   Para obter informações sobre os campos de Itens vulneráveis, consulte, Resposta a vulnerabilidades campos de formulário de item vulnerável.
5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .

   As regras da tarefa de correção avaliam o item vulnerável e o adicionam a uma tarefa existente ou criam uma nova tarefa. Se a avaliação falhar, o item vulnerável será adicionado a. **Itens vulneráveis não agrupados** lista.

   Quando você salva um novo item vulnerável, todos os calculadoras habilitadas executar.

   Nota: Apenas uma calculadora por **Campo de destino** está autorizado a estar ativo por vez. Quando você ativa um, todos os outros com o mesmo **Campo de destino** estão desativados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Você pode clicar em qualquer uma das listas relacionadas para exibir informações adicionais.

   Você pode usar o Link relacionado, **Verificar vulnerabilidades** para acionar manualmente um ServiceNow®- varredura iniciada. Para obter informações sobre como configurar um verificador de vulnerabilidades, consulte Configurar e gerenciar Qualys verificações e verificações de vulnerabilidades.

   Para uma Integração de vulnerabilidades da Qualys, um scanner padrão é pré-instalado no **Scanners de vulnerabilidades** módulo. Este scanner está desativado por padrão. Selecione **Ativo** e. **Padrão** Caixas de seleção para ativar o scanner da Qualys para trabalhar usando o. **Verificar vulnerabilidades** link relacionado nos formulários tarefa de correção e item vulnerável.

   As seguintes opções de edição e correção ficam disponíveis na barra de cabeçalho:

   - Atualizar: Salva as atualizações no formulário.
   - Criar incidente de segurança: Cria um incidente de segurança.
   - Fechar: Fecha o item. Se todos os itens do grupo estiverem encerrados, a tarefa de correção será fechada automaticamente.
   - Exceção de solicitação: Envia uma solicitação para adiar um item.
   - Resolver: Resolve o item.
   - Excluir: Remove o item vulnerável.

Tópicos relacionados

Edite itens vulneráveis em massa em Resposta a vulnerabilidades

Adie um item vulnerável

Se você determinar que o problema associado a um item vulnerável (VIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, poderá usar **Adiar** recurso.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho agendado é executado todos os dias verificando se há itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do VI for definido para expirar, o registro será reaberto.

Começando com Resposta a vulnerabilidades V20.0, antes de reabrir um VI adiado, o. Verifique a expiração do adiamento de itens vulneráveis e grupos O trabalho agendado verifica se alguma regra de exceção é aplicável em um VI adiado e atualiza o. **Motivo** e. **Até** campos de acordo com a regra de exceção. O estado do VI permanece adiado até a data de vencimento mais recente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item vulnerável.
3. Clique em **Exceção de solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado adiado expira e a tarefa de correção é reativada. **Nota:** A partir da versão 18,0 de Resposta a vulnerabilidades(VR), se um item vulnerável adiado for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do VIT será revertido para o estado adiado respeitando a janela de exceção ativa. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_vit_in_active_exception_window como verdadeiro. Além disso, a data Adiado até persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação. Se o registro for enviado, se notificações por e-mail são definidos, membros do Resposta a vulnerabilidades o grupo receberá um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.
   O grupo está marcado **Em Revisão** . . **Reabrir** o link relacionado é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho em **Aprovações de mudança de estado** guia.

Solicite uma extensão para um item vulnerável adiado

Solicite uma extensão para um item vulnerável adiado antes que ele atinja sua data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item vulnerável adiado.
3. Selecione **Extensão da solicitação** .

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até a qual o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Um e-mail é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Atualizar Resposta a vulnerabilidades itens vulneráveis

. **Atualizar status** o link relacionado é usado para que itens vulneráveis sejam inspecionados para ver se há itens vulneráveis adicionais que pertencem a uma tarefa de correção. Use-o se uma atualização for garantida fora do trabalho agendado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write ou, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

. **Atualizar status** o link relacionado só pode ser editado no formulário de tarefa de correção no **Aberto** ou **Em investigação** usando um grupo de filtros ou em que o tipo de filtro é condição. Esta inspeção é feita independentemente do status do **Atualizar itens vulneráveis automaticamente** caixa de seleção.

A partir da v22.0 de Resposta a vulnerabilidades. **Atualizar status** o botão está disponível na exibição de registro para tarefas de correção no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra qualquer registro no **Aberto** ou **Em investigação** estados.
3. Clique em **Atualizar status** link.
   Novos itens vulneráveis aparecem em **Itens vulneráveis** guia.

Identificar e escalar problemas de segurança em software de terceiros

Você pode exibir vulnerabilidades de software retornadas de entradas de terceiros para determinar a correção. Use essas informações para corresponder as entradas de software vulneráveis a um Software Gestão de ativos modelo da descoberta.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Bibliotecas** > **Terceiro**.
   Uma lista de softwares vulneráveis baixados é mostrada.
2. Clique em um registro de software para exibir informações de vulnerabilidade.
3. Clique nas listas relacionadas a seguir para obter mais informações para identificar vulnerabilidades.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração potencialmente vulnerável e software. Para obter mais informações sobre um emparelhamento, clique no ícone de informações ( ). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos do **Itens vulneráveis** lista relacionada.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando NVD

Quando os registros do identificador CVE-ID (Common Vulnerability and Exposures Identifier) são baixados do National Vulnerability Database (NVD), eles são comparados com o software na rede da sua empresa, conforme identificado pelo modelo de descoberta de Ativo de software. Quando um CVE-ID corresponde ao software vulnerável ou item de configuração em sua rede, um item vulnerável é criado. Você usa as informações no registro CVE-ID para decidir se o item vulnerável deve ser escalado para correção.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Bibliotecas** > **NVD**.
   Uma lista de IDs CVE que foram baixados do NVD é mostrada. As atualizações do NVD podem ser realizadas sob demanda e por execuções programadas nos registros de integração do banco de dados de vulnerabilidades nacional do NIST localizados em **Tudo** > **Administração** > **Integrações**.
2. Clique em um registro CVE para exibir as seguintes informações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um resumo do CVE-ID.
- Uma referência a uma entrada de enumeração de pontos fracos comuns (CWE), se aplicável.
- A pontuação de vulnerabilidade do CVE-ID no CVSS (Common Vulnerability Score System, sistema de pontuação de vulnerabilidade comum). Para obter mais informações sobre o CVSS, consulte Site do National Vulnerability Database .

3. Clique nas listas relacionadas para obter mais informações sobre vulnerabilidades.

Referências de vulnerabilidade

Nome, descrição e URL da vulnerabilidade fornecida e onde ela é referenciada.

Explorações

Detalhes.

Pontos fracos

Lista de pontos fracos do CWE.

4. Clique nas listas relacionadas a seguir para obter mais informações para identificar vulnerabilidades.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração potencialmente vulnerável e software. Para obter mais informações sobre um emparelhamento, clique no ícone de informações ( ). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos do **Itens vulneráveis** lista relacionada.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando o CWE

Exiba a biblioteca de registros de enumeração de pontos fracos comuns (CWE) do National Vulnerability Database (NVD) para entender como eles estão relacionados aos registros de Vulnerabilidade e exposição comuns (CVE). Em seguida, use essas informações para corresponder as entradas de software vulneráveis a um Software Gestão de ativos modelo da descoberta.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribuo. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Bibliotecas** > **CWE**.
   Uma lista de softwares vulneráveis baixados é mostrada.
2. Clique em um registro de software CWE para exibir informações de vulnerabilidade.
3. Clique nas listas relacionadas a seguir para obter mais informações para identificar vulnerabilidades.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração potencialmente vulnerável e software. Para obter mais informações sobre um emparelhamento, clique no ícone de informações ( ). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos do **Itens vulneráveis** lista relacionada.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Exiba o status de destino de correção de um Resposta a vulnerabilidades item vulnerável

Quando um item vulnerável quase atinge (ou passa) sua data de destino de correção, conforme definido por uma regra de destino de correção, o registro do item vulnerável é atualizado com um status. Essas informações podem ajudar o analista a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [somente leitura]

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

. trabalho agendado chamado **Avalie os destinos de correção** é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de destino de correção associada. Quando a data atual cai no número de dias antes do vencimento da correção, um status de correção é adicionado ao registro de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre regras de destino de correção, consulte Resposta a vulnerabilidades regras de destino de correção.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Itens vulneráveis**.
2. Clique no item vulnerável que você deseja revisar.
   . Se a data de correção do item vulnerável estiver dentro do intervalo das condições definidas na regra de destino de correção, o. **Status de destino de correção** a guia está visível.
3. Clique em **Status de destino de correção** guia.
4. Clique no registro de status de destino de correção para revisá-lo.

Nota: Para exibir o número de itens vulneráveis que estão se aproximando do destino, em trânsito e no destino passado, consulte Usando o padrão Resposta a vulnerabilidades painéis.

Tópicos relacionados

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Trabalhar com ICs incompatíveis

Como gerente e analista de vulnerabilidades, você pode exibir e reclassificar itens de configuração (ICs) incompatíveis, reconciliar itens descobertos incompatíveis, reaplicar regras de pesquisa de IC nos itens descobertos selecionados e desduplicar ICs existentes.

Exibir e reclassificar itens de configuração incompatíveis

Itens de configuração (ICs) que não são encontrados no Configuration Management Database (CMDB) são colocados em uma lista visível de itens descobertos. Esta lista oferece uma maneira conveniente de reclassificar ICs incompatíveis.

Antes de Iniciar

Função necessária:
sn_vul.read (mínimo para exibir ICs incompatíveis)

e

itil ou ativo (para reclassificar)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como analista de vulnerabilidades, você pode exibir ICs incompatíveis.

A ação Reclassificar está disponível somente em *sn_sec_cmn_unmatched_ci*ICs de classe, quando você tem as funções itil ou de ativo. Depois que um IC é reclassificado, ele não pode ser reclassificado usando a IU. Você pode reclassificar, no formulário de IC ou na exibição de lista de ICs, alterando **classe** valor.Para obter mais informações, consulte Reclassificar um IC .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Itens descobertos**.
2. Para revisar, clique em cada item.
3. Para fazer correções nas informações no **Item descoberto** campos de formulário, edite nesta página e clique com o botão direito do mouse **Salvar** .
   Quaisquer dados adicionados ou deixados nesses campos são transferidos para o resultante **Item de configuração** quando é reclassificado.
4. Se tudo parecer correto, clique em **Reclassificar** .
5. Na lista de seleção, selecione um **Nome da classe** e clique em **Enviar** .
   . **Item descoberto Classe** é atualizado, o. **Estado** O campo é alterado para reclassificado e todos os dados estão no CMDB.

Reconciliar itens descobertos sem correspondência

Crie um trabalho agendado para reconciliar itens descobertos incompatíveis.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Um item vulnerável (VI) consiste em uma vulnerabilidade e um item de configuração (IC). Quando uma VI é criada, o IC adicionado a ela no momento da criação pode estar desatualizado. As informações de IC incompatíveis não serão reconciliadas se as informações no CMDB mudarem. Para reconciliar, aplique regras de pesquisa de Item de configuração (IC) nos itens que estão em um estado incompatível quando o CMDB é atualizado com os ICs mais recentes.

Você pode executar uma demanda de trabalho programada para reaplicar a regra de correspondência de IC aos itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Detecções afetadas e itens vulneráveis também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação** .
3. No formulário, preencha os campos.

Nota: Você só pode editar o. **Parâmetros** campo.

Formulário Trabalho em segundo plano

Campo	Descrição
Número	Número de trabalho exclusivo.
Criada por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10 000 itens descobertos serão reconciliados. ○ FirstDiscovereditem: Primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação começará a partir do primeiro item descoberto.
Estado	Estado atual do trabalho em segundo plano.
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis** .
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total necessário para concluir o trabalho.
Subestado	Subestado do estado selecionado.
Anotações	Número de registros que foram processados.

4. Clique em **Enviar**.

Nota:

- Para parar a execução do trabalho, clique em **Cancelar** .
- Você não pode reconciliar ICs incompatíveis ou reaplicar regras de pesquisa de IC ao importar hosts ou itens vulneráveis.

5. Começando com Resposta a vulnerabilidades V26.0.11, você pode "Reaplicar regras de pesquisa" para itens selecionados ou filtrados na exibição da tabela Itens descobertos.

Nota: Na versão mencionada acima, o trabalho agendado Reconciliar itens descobertos incompatíveis foi descontinuado.

6. **Opcional:** Selecionar **Tudo** > **Operações de segurança >Reaplicar regras de pesquisa** para itens selecionados ou filtrados na tabela itens descobertos.

Nota: Se nenhum filtro for aplicado, a opção Reaplicar será desabilitada.

Depois de reaplicar, uma URL de trabalho em segundo plano ou uma mensagem de erro será exibida quando a integração estiver em execução.

Reaplicar regras de pesquisa de IC nos itens descobertos selecionados

Reaplique as regras de pesquisa de item de configuração (IC) nos itens descobertos selecionados nas ações de seleção de exibição da lista de itens descobertos. Se o IC mudar depois que você reaplicar as regras, os itens descobertos serão atualizados com o novo IC e as detecções afetadas. Itens vulneráveis também são atualizados.

Tradução automática

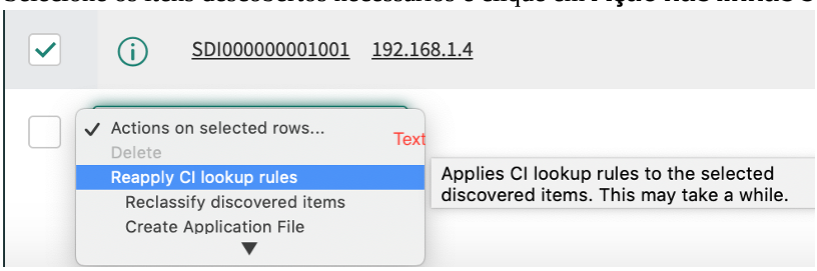
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para obter mais informações, consulte Mudanças de IC para itens descobertos.

Para obter mais informações sobre os conceitos de correspondência de IC e o CMDB, pesquisa de item descoberto, identificação baseada em regra e outras informações detalhadas sobre como funciona a correspondência de IC, consulte Correspondência de IC no artigo Resposta a vulnerabilidades [KB0998706] Na Base de conhecimento HI.

Procedimento
1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Itens descobertos**.
2. Selecione os itens descobertos necessários e clique em **Ação nas linhas selecionadas** .



3. Na lista, selecione **Reaplicar regras de pesquisa de IC** .

Nota:

Começando com Resposta a vulnerabilidades V24.0.6, você pode ignorar a reaplicação de regras de pesquisa de IC em itens descobertos com o subestado "IC desativado" habilitando a propriedade do sistema *sn_sec_cmn.skipItemsWithCIDecommissioned*.

As regras são reaplicadas nesses itens descobertos.

4. Clique em **Exibir status** na mensagem.

O status é exibido no formulário de trabalho em segundo plano.

Nota: Em **Anotações** . Itens descobertos não puderam ser processados devido à exceção Um atributo com um valor diferente de zero indica que há um erro ou exceção ao reaplicar uma regra de pesquisa de IC. Verifique os logs do sistema para obter mais detalhes.

5. Reaplicar se aplica somente a itens verificados nos últimos 90 dias com base em **last_scan_date, last_comp_scan_date, non_infra_last_scan_date, non_infra_last_comp_scan_date** coluna.

Propriedade do sistema ci_lifecycle_status_source adicionada para configurar colunas de status do ciclo de vida do IC (por exemplo, Status de instalação, Status operacional). Você pode configurar colunas adicionais para desativar ICs.

As colunas são adicionadas à exibição da lista de trabalhos em segundo plano:

- Tempo decorrido (ms): O tempo necessário para processar o trabalho em segundo plano.
- Itens processados: O número de itens processados até o momento.
- Total de itens a serem processados: O número total de itens restantes a serem processados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tempo até a conclusão (ms): O tempo restante até que o trabalho em segundo plano seja processado. Essas colunas fornecem visibilidade do andamento do trabalho. Essas colunas estão disponíveis para cada exibição de formulário para você adicionar de acordo com o requisito.

Reaplicar melhorias de regras de pesquisa de IC

Reaplique as regras de pesquisa de item de configuração (IC) em itens descobertos selecionados, como SO e netbios.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

- Os valores de SO e netbios presentes nos dados de origem devem ser preenchidos antes do item de configuração ao preencher esses campos no item descoberto.
- Em caso de valores vazios de SO e NETBIOS nos dados de origem, os valores são obtidos do item de configuração ao preencher esses campos na tabela Itens descobertos.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Itens descobertos**.
2. Selecione os itens descobertos necessários e clique em **Ação nas linhas selecionadas** .
3. Na lista, selecione **Reaplicar regras de pesquisa de IC** .

   As regras são reaplicadas nesses itens descobertos.

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

Tome medidas para ajudar a evitar registros duplicados ou órfãos resultantes da correspondência de (itens de configuração (ICs) em CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em tempos de processamento longos. Testes e depuração completos de scripts de processamento nas regras ajudam a aliviar o potencial de problemas posteriormente no processo.

Evitando registros duplicados ou órfãos

- Use pequenos subconjuntos de dados específicos para a regra de pesquisa de IC que está sendo testada.
  - Defina todas as regras de pesquisa de IC, exceto a que está sendo testada, como inativas.
  - Analise os ICs importados para garantir que você esteja observando o comportamento esperado e a correspondência esteja ocorrendo corretamente.
- Revise ICs correspondentes
  - Examine a contagem de ICs correspondentes versus incompatíveis. Certifique-se de que a porcentagem seja aceitável. Não olhe apenas para a primeira página, que é provavelmente a primeira inserida.
  - PESQUISE manualmente alguns ICs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Verifique se há problemas de nomenclatura ou campo (como pesquisar um domínio específico).

  Se parecer apropriado, adicione regras de correspondência adicionais.

- Revise ICs incompatíveis
  - Navegue até a tabela ICs incompatíveis.
  - Agrupar por classe de item de configuração.
  - Revise todas as classes que não parecem corretas (certificados, placas de rede, imagens).
    - Descubra por que eles não corresponderam ao IC correto?
    - A classe deve ser excluída?
    - A classe deve ser elevada a uma classe relacionada?
- Revise estados de IC, como **Descontinuado** .
- Remover dados de teste
  - Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, comece novamente.
  - Para começar novamente: Excluir os dados usados para testes: (Consulte **Excluindo dados de tabelas**)
    - Itens descobertos
    - Itens vulneráveis
    - Tarefas de correção
  - Executar novamente manualmente todas as regras de correspondência de IC.

Para obter mais informações sobre Regras de pesquisa de IC e Qualys, consulte KB0750656 artigo.

Para obter mais informações sobre Regras de pesquisa de IC e Rapid7, consulte KB0818096 .

Excluindo dados de tabelas

Às vezes, você importou dados e percebe que algo está errado. Se algo estiver errado em um ambiente de desenvolvimento ou desempenho, você poderá clonar novamente de um ambiente melhor, mas isso nem sempre é uma opção.

Nota: Executar essas ações requer ServiceNow experiência.

Há quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** ativado **Configuração da tabela** .
- Configure o. **Limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo **Limpeza automática** registro.
- Trunque gs.truncateTable usando um script em segundo plano.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando `truncateTable`é necessário desativar a caixa de seleção registro para rollback nos scripts em segundo plano. Caso contrário, uma cópia da tabela e das tabelas em cascata relacionadas será criada, levará muito tempo e provavelmente falhará.

Nota: Nunca use `truncateTable`em um ambiente de produção. Antes de executar exclusões grandes em ambientes de produção ou compartilhados, consulte seu representante de suporte.

Desduplicação de itens de configuração existentes

Sempre que itens de configuração (ICs) são atualizados por meio de uma tarefa de desduplicação, os itens descobertos (dis) relacionados a esses ICs também são atualizados. Itens vulneráveis (VIS) e detecções também são atualizados com o IC.

Para obter mais informações, consulte Mudanças de IC para itens descobertos.

Tópicos relacionados

Como corrigir uma tarefa de desduplicação

Resolver tarefas de correção

A flexibilidade inerente a Resposta a vulnerabilidades permite corrigir vulnerabilidades da forma que melhor se adapte à sua organização de segurança.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Depois de ser notificado de que uma solicitação de mudança foi resolvida, mova o estado da tarefa de correção para Resolvido e aguarde a próxima verificação. As novas varreduras são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.

Nota:

Se a sincronização de estado estiver ativada, as tarefas de correção serão movidas automaticamente para o estado Resolvido depois que uma solicitação de mudança associada a uma tarefa de correção (VUL) for implementada e estiver no estado Revisão. Consulte Gestão de mudanças para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído a mim**.
2. Clique em um registro que está no estado Aberto.

   O estado Aberto indica que o registro ainda não foi trabalhado. O formulário exibe:

   - Informações da tarefa de correção
   - Detalhes da configuração do grupo
   - Anotações
   - Itens vulneráveis associados
   - ANS de tarefas
   - Solicitações de mudança
3. Execute sua análise do grupo.
4. Quando você estiver pronto para começar a trabalhar no registro, escolha qualquer uma das seguintes opções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Se o item vulnerável representar um risco para o seu ambiente DE TI, crie um registro CHG e escale o problema para Gestão de mudanças equipe.	Atribua o grupo ao grupo ou indivíduo apropriado e clique em **Criar mudança** .
Se o item vulnerável representar um possível risco à segurança para sua organização, crie um registro de incidente de segurança e escale o problema para Resposta a incidentes de segurança equipe.	Clique em **Criar incidente de segurança** . Este botão é exibido somente quando Resposta a incidentes de segurança está ativado. Um cálculo de impacto nos negócios é aplicado, o incidente é atribuído e o incidente de segurança é criado.

Depois de criar uma solicitação de mudança, o registro apropriado aparece em **Solicitações de mudança** Lista relacionada no formulário Grupo de vulnerabilidades.

5. Se você determinar que o problema é de baixo risco e pode ser adiado, clique em **Exceção de solicitação** . Para obter mais informações sobre como adiar uma tarefa de correção, consulte Adie uma tarefa de correção.
6. Se você determinar que o problema pode ser encerrado imediatamente sem análise adicional, clique em **Fechar** .
   Para obter mais informações sobre como fechar uma tarefa de correção, consulte Feche uma tarefa de correção. A partir da v23.0 de Resposta a vulnerabilidades. **Fechar** o botão foi removido para uma tarefa de correção.

   Um trabalho agendado de integração de terceiros atualiza e verifica automaticamente os registros em um intervalo definido. Os itens vulneráveis são verificados na próxima data e hora programadas. Como alternativa, você pode iniciar manualmente uma verificação de vulnerabilidade usando **Verificar vulnerabilidades** link relacionado.

   Se a verificação encontrar novamente a vulnerabilidade no item de configuração e não a marcar como corrigida, o item vulnerável retornará ao estado Em investigação. Entre em contato com Operações DE TI para reabrir a solicitação de mudança.

   Se a verificação não encontrar a vulnerabilidade e retornar que o item vulnerável foi marcado como corrigido, o item vulnerável mudará para o estado Encerrado-corrigido e será encerrado durante a importação.

   Somente quando todos os itens vulneráveis em uma tarefa estão no estado Encerrado-fixo, a tarefa de correção é fechada automaticamente. Tarefas de correção com itens vulneráveis em estados Encerrado diferentes de Fixo devem ser encerradas manualmente.

Adie uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção (VUL) é de baixa prioridade e pode ser adiado imediatamente sem análise adicional, poderá usar **Exceção de solicitação** recurso.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você pode adiar uma tarefa de correção de um registro de tarefa de correção no Resposta a vulnerabilidades Espaços de trabalho. Depois de enviar a solicitação, ela será enviada para aprovação. Consulte Solicite uma exceção no Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um trabalho agendado é executado todos os dias verificando se há tarefas de correção adiadas que atingiram a data de reabertura. No dia em que o adiamento da tarefa for definido para expirar, a tarefa será reaberta.

Nota: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados Encerrado ou Adiado.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra um registro.
3. Clique em **Exceção de solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada. Se o registro for enviado, se notificações por e-mail são definidos, membros do Resposta a vulnerabilidades o grupo receberá um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, a tarefa de correção é definida novamente como **Aberto** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado em Revisão. . **Reabrir** o link relacionado é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho em **Aprovações de mudança de estado** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma extensão para uma tarefa de correção adiada

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Na aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis devem estar no estado Adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feche uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção pode ser encerrado imediatamente sem análise adicional, poderá usar **Fechar** recurso. A partir da v23.0 de Resposta a vulnerabilidades. **Fechar** o botão foi removido para uma tarefa de correção e o fechamento de uma tarefa de correção é orientado pelo scanner.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Em Resposta a vulnerabilidades Espaços de trabalho, uma tarefa de correção passa pelos mesmos estados de uma tarefa de correção anterior em versões anteriores de Resposta a vulnerabilidades. Quando todos os itens vulneráveis (Vits) em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado inativo.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção do Encerrado ou Adiado estados.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione **Encerrar/Adiar** botão.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione um estado. As opções são: ○ Adiado ○ Encerrado
Até	Disponível somente em **Adiar** estado pop-up. Selecione a data em que **Adiar** o estado expira e a tarefa de correção é reativada. Se o registro for enviado, se notificações por e-mail são definidos, membros do Resposta a vulnerabilidades o grupo receberá um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como **Aberto** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para encerrar o problema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informações adicionais	Insira outras informações relevantes.

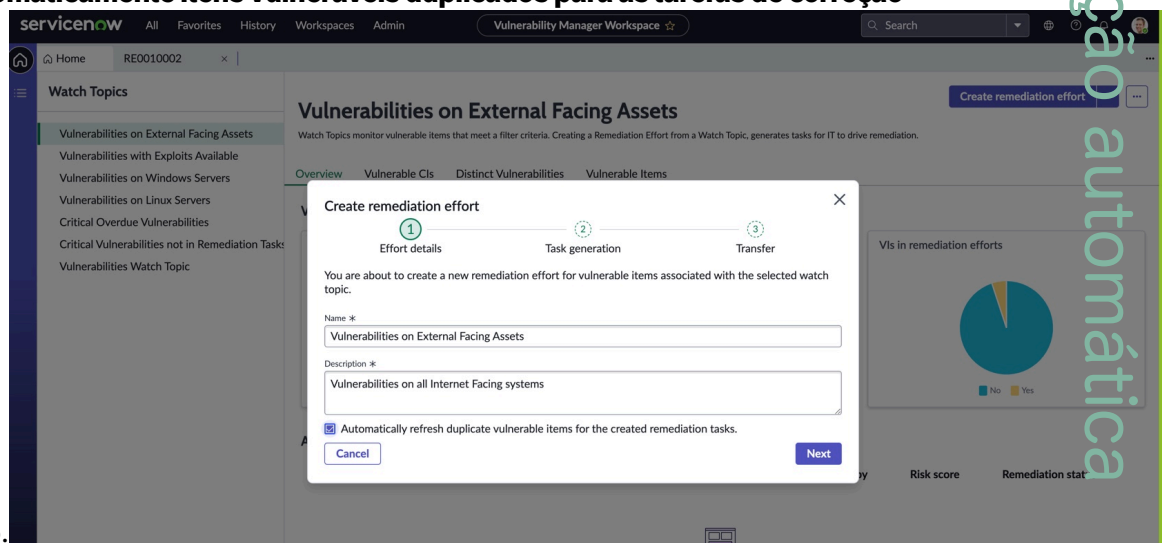
4. Selecione **Enviar**.
   A tarefa de correção é marcada **Encerrado** .

Identificar itens vulneráveis duplicados de vários scanners

Se você estiver usando vários scanners no mesmo ativo para detectar vulnerabilidades, vários itens vulneráveis (VIS) poderão ser criados. Você pode identificar esses VIS duplicados para garantir que as vulnerabilidades duplicadas não sejam atribuídas aos responsáveis pela correção.

Essa resolução só será possível se as mesmas vulnerabilidades, como as mesmas vulnerabilidades e exposições comuns (CVEs) forem detectadas. A combinação de vulnerabilidade depende dos scanners que estão sendo usados. Por exemplo, a Qualys e a Tenable têm seu próprio tipo de vulnerabilidade, ou seja, entradas de terceiros (TPEs) e outros scanners, como o Microsoft Defender para vulnerabilidades de detecção de endpoint com base em CVEs.

A partir da versão 17,1, ao criar um esforço de correção, você pode atualizar automaticamente itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar **Atualizar automaticamente itens vulneráveis duplicados para as tarefas de correção criadas**opção.



Mostrar VIS duplicados Identificar itens vulneráveis duplicados relatados por vários scanners no sistema. Você pode marcar o VI duplicado como resolvido. Para obter mais informações, consulte Resolva vulnerabilidades duplicadas automaticamente. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando CVEs. Para obter mais informações, consulte Tarefa de correção de resposta a vulnerabilidades e estados de item vulnerável.

Possíveis duplicatas são identificadas para as seguintes combinações de vulnerabilidade:

Combinação de scanner	Tipo de vulnerabilidade
Scanner 1 e Scanner 2	CVE
Scanner 1 e Scanner 2	CVE e TPE

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resolva vulnerabilidades duplicadas automaticamente

A partir de Resposta a vulnerabilidades(VR) v17.1, você pode resolver automaticamente quaisquer vulnerabilidades duplicadas em um ativo.

Quando um ativo é verificado com vários scanners, há uma chance de identificar a mesma vulnerabilidade como duplicatas pelos diferentes scanners. Por exemplo, se os scanners da Qualys e da Microsoft identificarem a mesma vulnerabilidade, você poderá optar por resolver automaticamente a duplicada.

Cenário de amostra

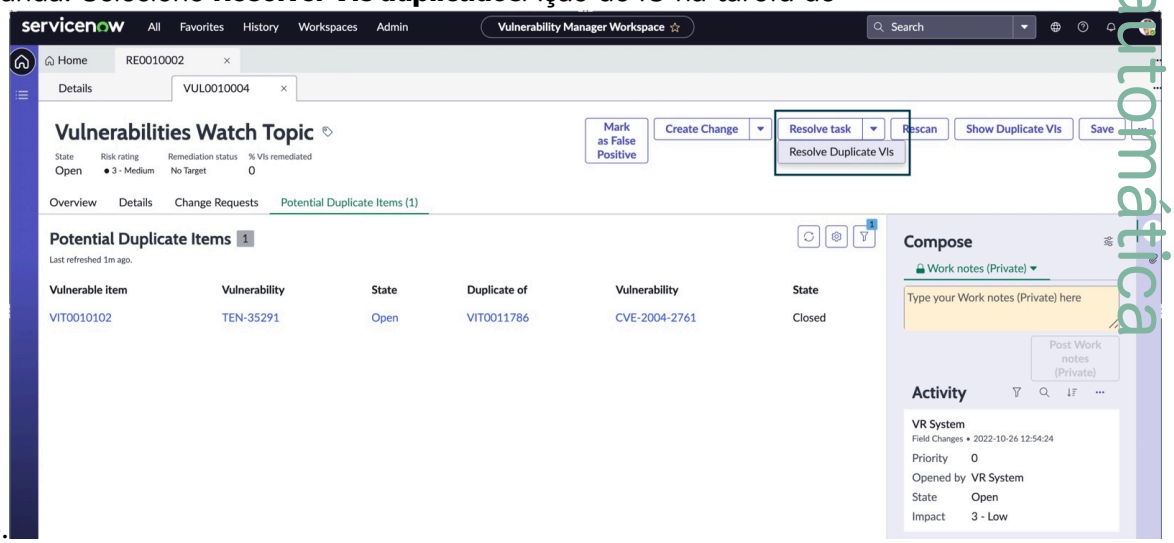
O VR cria um registro, VI1, para a vulnerabilidade 1 do verificador Microsoft Defender for Endpoint. Um segundo registro, VI2, é criado a partir do scanner da Qualys para a mesma vulnerabilidade. A equipe de correção aplica os patches que podem resolver os registros VI1 e VI2. Se você configurar a programação de verificação da Qualys além de um dia, nesse momento, o Microsoft Defender fornecerá as informações de vulnerabilidade fixa e o VR fechará o registro do VI1 como Encerrado/Corrigido.

Nesse cenário, o registro VI2 ainda está no estado Aberto e o VR aguarda os resultados da verificação da Qualys. Nesta situação, os registros de VI do segundo scanner permanecem no estado aberto, mesmo se o patch for aplicado e o VI for confirmado como corrigido pelo outro scanner.

Para lidar com essa situação, você pode considerar resolver o registro de vulnerabilidade duplicado com base na condição de que a vulnerabilidade é encerrada pelo primeiro scanner.

Resolva vulnerabilidades das seguintes maneiras:

- Sob demanda: Selecione **Resolver Vis duplicados**Ação de IU na tarefa de correção.



- Automatizado: Habilite a propriedade do sistema `sn_vul.auto_resolve_duplicate_vit` para resolver automaticamente itens vulneráveis duplicados. O trabalho agendado diário "Atualizar e resolver vits duplicados na tarefa de correção" atualiza automaticamente os itens duplicados.

Os VIS duplicados são marcados como resolvidos.

Nota: O registro do item de vulnerabilidade resolvida será reaberto se o scanner o identificar como **Não corrigido** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar e editar um grupo de classificação

Crie grupos para que as regras subjacentes desse grupo possam classificar os registros da tabela com base nas condições. As regras podem ser usadas para selecionar qualquer campo na tabela correspondente.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegue até a tabela Propriedades do sistema.
2. Em *sn_sec_cmn.classificationTables*propriedade do sistema, adicione o nome da tabela para a qual você deseja criar o grupo de classificação.
3. Crie uma nova regra de negócio adicionando o seguinte snippet de código à regra de negócio na tabela definida no grupo:
```
Var ClassificationCalculator: New
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','n_vul_classification_rule');
classificationCalc.calculate();
```
   Nota: As regras de negócio são fornecidas para executar a classificação durante a ingestão das tabelas Itens descobertos e Entrada de vulnerabilidade. Para outras tabelas, para ter as regras de classificação na ingestão, você deve adicionar as regras de negócio.
4. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de classificação**.
5. No menu de contexto Grupos de classificação, clique em **Novo** .
6. No formulário, preencha os campos.

Formulário Grupo de classificação de vulnerabilidades

Campo	Descrição
Nome	Nome do novo grupo de classificação.
Ativo	Opção para ativar o grupo.
Descrição	Descrição do novo grupo de classificação.
Tabela	Tabela baseada na qual as regras são executadas. **Nota:** O sistema de base de Resposta a vulnerabilidades inclui grupos de classificação para itens descobertos e vulnerabilidades.

Criar e editar uma regra de classificação

Crie regras para classificar automaticamente as vulnerabilidades de entrada para as equipes corretas para correção.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa
Quando criadas, essas regras classificam as vulnerabilidades como pertencentes a uma plataforma ou aplicação. Você pode configurar essas regras para substituir o valor de um campo específico na entrada de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use essas regras para mover o cálculo para cima para a tabela Entrada de vulnerabilidades de terceiros para habilitar a reutilização de conteúdo.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de classificação**.
2. Para exibir um grupo de classificação, clique nesse grupo.
3. No menu de contexto Regras de classificação, clique em **Novo** .
4. No formulário, preencha os campos.

Formulário Regra de classificação de vulnerabilidade

Campo	Descrição
Nome	Nome da nova regra de classificação.
Ativo	Opção para ativar a regra.
Descrição	Descrição da nova regra de classificação.
Ordem de execução	Ordem na qual a regra deve ser executada.
Exibição avançada	Opção para exibir campos adicionais nas seções com guias.
Quando esta condição for atendida	
Tipo de condição	Tipo de condição da regra. Estas são as opções: ○ **Filtro** Condições básicas de filtro para determinar se a regra deve ser usada ou não. ○ **Grupo de filtros** Conjunto de várias condições que são usadas juntas. A regra é avaliada com base nas condições definidas no grupo de filtros. ○ **Script** Condição de script usada para determinar quando aplicar esta regra. Este campo aparece somente quando **Exibição avançada** a opção está selecionada.
Condição	Condição da regra. Defina condições com base na coluna selecionada na coluna de entrada de vulnerabilidade necessária. Você pode adicionar várias condições para refinar a regra. Este campo aparece somente quando **Filtro** selecionado em **Tipo de condição** campo. **Nota:** Ao definir várias condições ou modelos, você pode selecionar somente de uma tabela primária e secundária. Não é possível selecionar entre duas ou mais tabelas secundárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de filtros	Grupo de filtros. O grupo é definido quando um conjunto de condições é usado repetidamente em vários lugares. Clique na pesquisa usando o ícone de lista ( ) para selecionar o grupo de filtros. Para obter mais informações, consulte Criar e definir grupos de filtros em Operações de segurança . Este campo aparece somente quando **Grupo de filtros** selecionado em **Tipo de condição** campo.
Script	Script avaliado para determinar quando aplicar esta regra. Você pode escrever seu código e definir a resposta como verdadeira ou falsa. Este campo aparece somente quando **Script** selecionado em **Tipo de condição** campo
Definir estes valores	
Classificação	Classificação da regra. Para selecionar uma opção, clique no ícone de lâmpada ( ). A lista exibe as opções para Plataforma e Aplicação. Como alternativa, você pode inserir sua própria classificação que não está na lista.
Tipo de classificação	Tipo de classificação. Este campo mostra a lista filtrada de tipos de classificação com base no valor selecionado para **Classificação** campo.
Tipo de valor	Tipo do valor atribuído usando esta regra. Estas são as opções: ○ **Modelo**: selecionar um modelo. Você pode usar um modelo obrigatório. ○ **Script** : Selecione um script pré-existente ou escreva seu próprio script personalizado. Este campo aparece somente quando **Exibição avançada** a opção está selecionada.
Modelo	Outra condição para a regra, além de **Classificação** e. **Tipo de classificação** campos. Selecione uma combinação de campos e valores que você deseja definir quando a regra for avaliada. Este campo aparece somente quando **Modelo** selecionado em **Tipo de valor** campo.
Valor do script	Script para definir valores no registro atual. Este campo define quais valores definir nos campos nas entradas de vulnerabilidade. Este campo aparece somente quando **Script** selecionado em **Tipo de valor** campo.

5. Para criar a nova regra, clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Use regras de classificação de VR para adicionar a lógica a tabelas ascendentes, como Vulnerabilidade e Itens descobertos, e calculá-la. Você pode reutilizar a saída várias vezes, melhorando o desempenho de regras, como regras de atribuição. Por exemplo, classifique a entrada de terceiros (TPE) como Java e reutilize a saída nas regras de atribuição várias vezes. Regra de atribuição de amostra:

```
VI.TPE.Classfication Type
        | IS | Java
```

Aplique uma regra a uma vulnerabilidade existente

Ao alterar uma regra de classificação, execute novamente todas as regras ativas em todas as entradas de vulnerabilidade. Você também pode adaptar as vulnerabilidades existentes, aplicando as regras de classificação recém-criadas às vulnerabilidades existentes.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidades**.
2. Para selecionar uma regra, marque a caixa de seleção ao lado da regra.
3. Clique em **Aplicar mudanças**.
4. Clique em **Reaplicar** .

Desative ou exclua uma regra de classificação

Desative ou exclua uma regra de classificação se ela não for mais necessária ou relevante.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa
Quando uma regra de classificação é desativada ou excluída, os dados que foram preenchidos em **Classificação** e. **Classification_type** os campos por essa regra excluída permanecem em suas respectivas tabelas.

Se você quiser limpar esses dados, crie uma regra com valores vazios em **Classificação** e. **Classification_type** e reaplique o grupo. Quando esta nova regra é reaplicada, as mudanças são refletidas em todos os registros aos quais esta regra é aplicável, com base nas condições da regra.

A partir da v24.0.6 de Resposta a vulnerabilidades se uma regra de classificação for excluída ou desativada, ela não será mais aplicada ao item descoberto ou à entrada de vulnerabilidade e aos dados no **Classificação** e. **Classification_type** os campos são limpos.

Procedimento

1. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidades**.
2. Para selecionar a regra que você deseja excluir, clique na caixa de seleção ao lado da regra.
3. Para excluir a regra, siga um destes procedimentos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na lista Ação nas linhas selecionadas, clique em **Excluir** .
- Selecione a regra e clique em **Excluir** botão.

4. Clique em **Aplicar mudanças**.

> **Nota:** Se você não clicar neste botão, a regra continuará a residir no sistema. As vulnerabilidades referenciadas pela regra continuam a fazer referência a elas.

Crie uma regra de exclusão

Crie uma regra para filtrar ou excluir detecções de serem convertidas em itens vulneráveis (Vits) durante a ingestão.

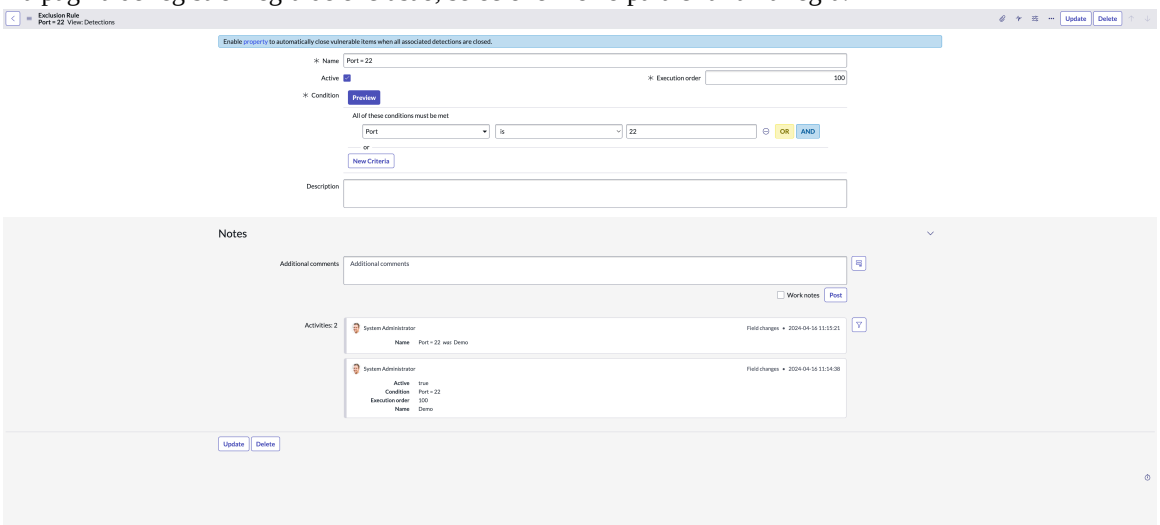
Antes de Iniciar

Função necessária: Administrador de vulnerabilidades

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Regras de exclusão**.
2. Na página de registro Regra de exclusão, selecione **Novo** para criar uma regra.



Uma mensagem dizendo "Habilitar propriedade para fechar automaticamente itens vulneráveis quando todas as detecções associadas forem encerradas" é exibida. Por padrão, a propriedade está inativa. Para habilitar, selecione o link de propriedade e insira o valor como verdadeiro em **Valor** campo.

3. No formulário, preencha os campos.

Formulário Regra de exclusão

Campo	Descrição
Nome	Nome da regra de exclusão.
Ativo	Opção para ativar a regra de exclusão.
Ordem de execução	Ordem exclusiva para cada regra de exclusão.
Condição	Condições de filtro para as detecções que podem ser definidas durante o processamento delas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Não é possível selecionar Regra de exclusão ou condições do campo Item de vulnerabilidade.
Descrição	Descrição da regra de exclusão.

4. Selecione **Enviar**.
   A atividade é registrada no sistema.

Nota: Quando uma regra de exclusão é criada, ela entra em vigor nas detecções a partir da ingestão subsequente.

Gestão de mudanças tarefas para Resposta a vulnerabilidades

Em Tarefas de correção (RTS), crie solicitações de mudança, associe RTS a solicitações de mudança existentes ou divida tarefas de correção em novas tarefas com subconjuntos de itens vulneráveis (VI).

Crie e gerencie solicitações de mudança diretamente de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro ajuda a investigar e resolver vulnerabilidades rapidamente.

Consulte Gestão de mudanças para Resposta a vulnerabilidades para obter uma visão geral de como a gestão de mudanças funciona com o. Resposta a vulnerabilidades e os requisitos do sistema.

Consulte os tópicos a seguir para saber como criar solicitações de mudança, associar tarefas de correção a solicitações de mudança existentes e dividir tarefas de correção. Consulte Sincronização de estado entre solicitações de mudança e tarefas de correção Para obter informações sobre como os campos de estado em solicitações de mudança (CHG) resolvem automaticamente as tarefas de correção.

Crie uma solicitação de mudança a partir de uma tarefa de correção

Como responsável pela correção DE TI, crie uma solicitação de mudança (CHG) diretamente de uma tarefa de correção (VUL) para todos os itens vulneráveis no grupo. Crie uma solicitação de mudança com informações preenchidas previamente que incluem a solução preferencial para agilizar sua investigação de vulnerabilidades que exigem intervenção manual.

Antes de Iniciar

Funções necessárias: Para criar uma solicitação de mudança: Qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Função necessária: Para aprovação de solicitações de mudança: Usuários com funções itil, admin, sn_change_write, change_manager.

Por Que e Quando Desempenhar Esta Tarefa

Para obter informações sobre como criar uma solicitação de mudança do Resposta a vulnerabilidades espaços, consulte Crie uma solicitação de mudança no Espaço de correção de problemas de TI.

Para criar uma solicitação de mudança no ambiente clássico, siga as etapas listadas abaixo.

Tradução automática

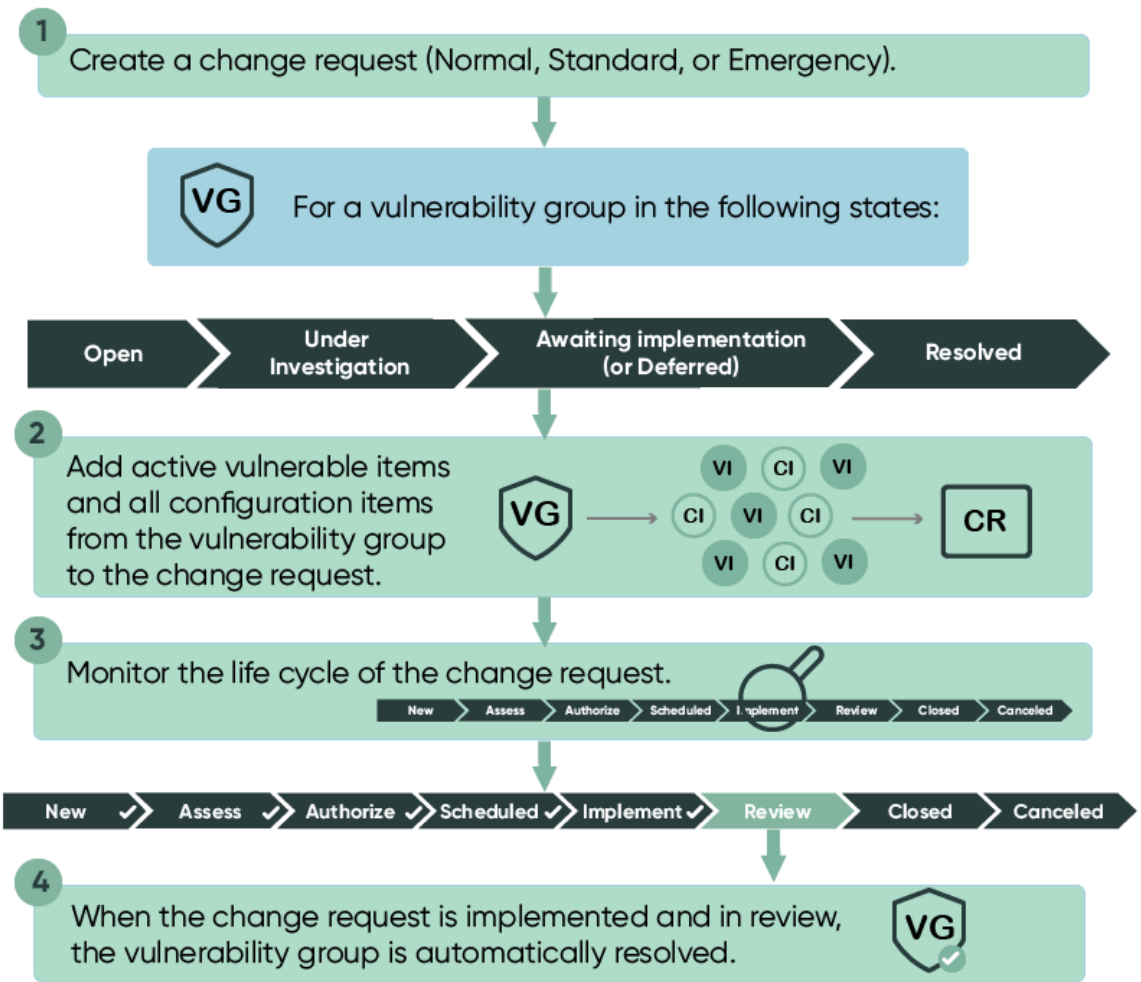
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente de uma tarefa de correção. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente a partir de uma tarefa de correção:

- Padrão. Uma mudança pré-autorizada que é de baixo risco, relativamente comum e segue um procedimento especificado ou instrução de trabalho.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de serem implementadas, revisadas e encerradas.
- Emergência. Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de um VUL (tarefa de correção). As etapas detalhadas deste fluxo seguem a imagem.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Em versões anteriores de Resposta a vulnerabilidades Tarefas de correção foram chamadas, grupos de vulnerabilidades (VG) Nas imagens a seguir, VG: Tarefa de correção ou um registro VUL.



Nota: Pontos principais sobre como criar novas solicitações de mudança:

- Você pode criar novas solicitações de mudança para qualquer tarefa de correção (VUL) em um estado diferente de Encerrado .
- Verifique se você tem um aprovador para solicitações de mudança diferente de Padrão (pré-aprovado) que você cria ou associa a um VUL. Mover o VUL para a resolução. Para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obter mais informações sobre como adicionar usuários, consulte Adicione usuários ao grupo Resposta a vulnerabilidades.

- Para que uma tarefa de correção possa ser resolvida, todas as tarefas em pelo menos um CHG associado ao VUL devem ser concluídas para que a solicitação de mudança possa ser implementada e movida para Revisão estado.

Procedimento

1. Para criar uma solicitação de mudança completa a partir de um registro de tarefa de correção existente, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**.
   A lista de tarefas de correção atribuídas ao seu grupo de atribuição é exibida.
2. **Opcional:** Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Visão Geral da Correção** Para exibir o painel Visão geral da correção e localizar um VUL atribuído a você ou ao seu grupo de atribuição.
3. Como alternativa, na coluna Número, clique em uma tarefa de correção para abrir o registro e exibir os detalhes.
   O registro é exibido.
4. Com o registro VUL exibido para o qual você deseja criar a solicitação de mudança, no canto superior direito do registro, clique em **Criar mudança** .
   O formulário Criar solicitação de mudança é exibido.
5. Preencha os campos.

   a. Na lista de seleção do campo Aplica-se a, escolha um para continuar.

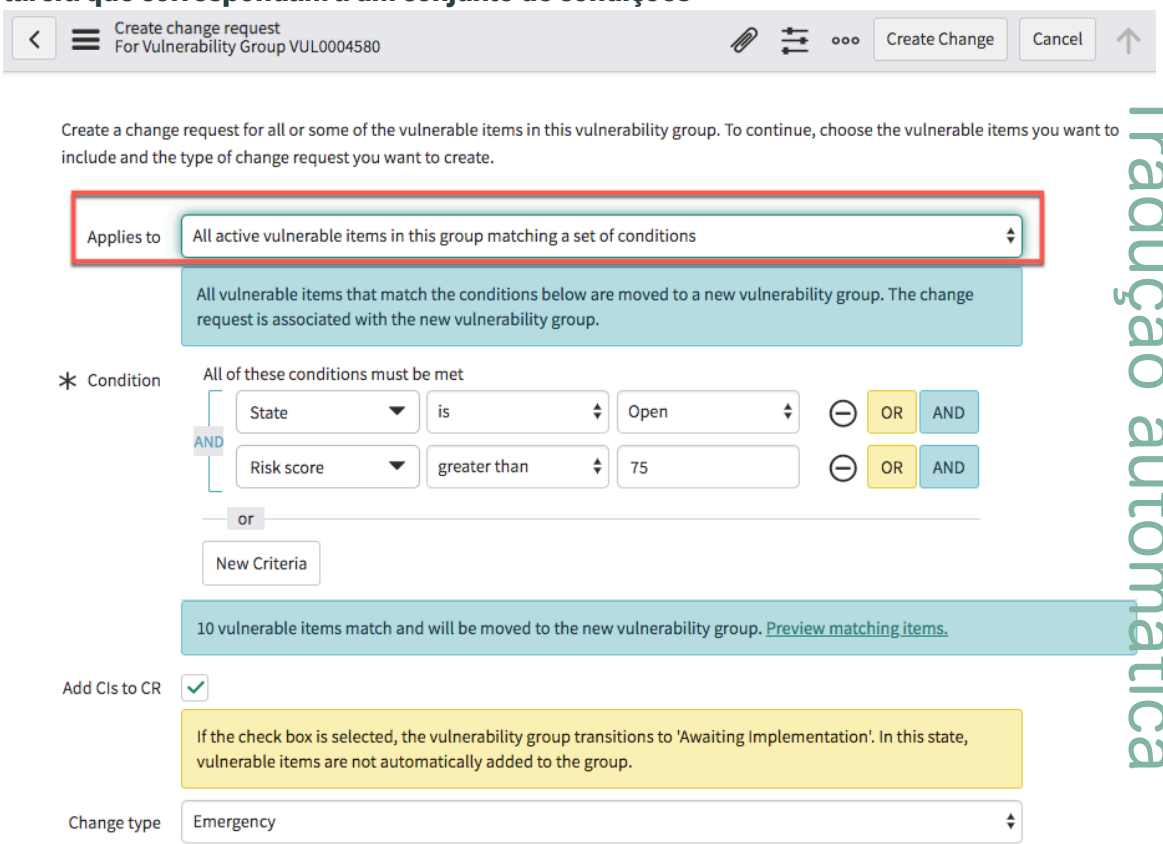
Opção	Descrição
Todos os itens vulneráveis ativos neste grupo	Se selecionado, todos os itens vulneráveis ativos desta tarefa de correção com um estado diferente de Encerrado serão adicionados automaticamente à solicitação de mudança depois que você clicar em **Criar mudança** .
Todos os itens vulneráveis neste grupo correspondem a um conjunto de condições	Se selecionado, o Construtor de condições será exibido conforme mostrado na segunda figura abaixo. Insira critérios de filtro para identificar os itens vulneráveis que você deseja para a nova solicitação de mudança. Um exemplo de filtro pode incluir somente itens vulneráveis que correspondam a critérios de pesquisa específicos: **Estado . Aberto** e. **Pontuação de risco maior que 75** . Depois de inserir suas condições, uma mensagem será exibida com o número de VIS que correspondem aos seus critérios (10). Um link (**Visualizar itens correspondentes** para visualizar os itens correspondentes é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Se nenhum item corresponder às condições do filtro, uma mensagem será exibida abaixo do construtor de condições instruindo você a ajustar o filtro. Depois de clicar em **Criar mudança** todos os itens vulneráveis que correspondem a este filtro de condição são movidos para uma nova tarefa de correção. Esta solicitação de mudança está associada à nova tarefa de correção.

Formulário Criar solicitação de mudança para itens vulneráveis em uma tarefa que correspondam a um conjunto de condições



Tradução automática

b. Opcional: Se for exibido no formulário, clique em **Visualizar itens correspondentes** Link para uma lista dos VIS que correspondem aos critérios de filtro.
A visualização da Lista de tarefas de correção é exibida. Você pode selecionar itens nesta lista de visualização e executar ações de IU neles, no entanto, essas ações também são realizadas no VUL. Por exemplo, se você excluir um VI da lista de visualização, esse VI também será excluído do VUL.

c. Depois de concluir a visualização, feche a janela do navegador para retornar o formulário de solicitação de mudança.

d. Na caixa de seleção Adicionar ICs à CR, escolha uma para continuar.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Caixa de seleção Adicionar ICs à CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem a itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. O VUL move automaticamente para Aguardando implementação estado.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos itens vulneráveis ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o VUL e o VUL permanece em seu estado atual.

e. Na lista de seleção do campo Tipo de mudança, escolha um para continuar.

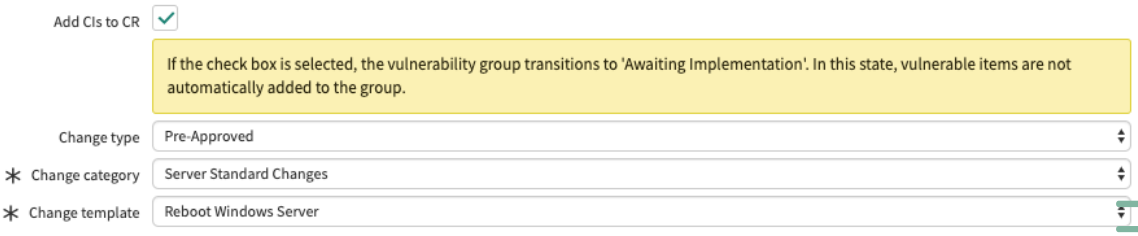
Tipo de mudança	Descrição
Emergência	Uma mudança para resolver um incidente grave.
Normal	Um tipo de mudança que é usado para implementar qualquer mudança em um serviço que não seja uma mudança padrão ou de emergência.
Padrão	Uma solicitação de mudança pré-autorizada e de baixo risco que é implementada com frequência. As solicitações de mudança padrão aprovadas podem ser predefinidas em um catálogo de modelos para tornar mais eficiente o acesso e a solicitação de uma mudança padrão. Se selecionado, dois campos serão exibidos conforme mostrado na figura a seguir. Selecione um de cada lista de seleção para preencher estes campos: ▪ Categoria de mudança: Selecione uma categoria para a mudança no catálogo existente, por exemplo, Hardware , Mudanças padrão do servidor , Software . Neste exemplo, Patches de mudanças padrão selecionado. ▪ Modelo de mudança: Selecione um modelo disponível para solicitações de mudança com tarefas de suporte predefinidas do seu catálogo. Neste exemplo, Ciclo de aplicação de patches mensal da Microsoft o modelo está selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de mudança	Descrição
	Para obter mais informações sobre categorias de solicitação de mudança do ITSM, modelos e tipos de mudança, consulte Tipos de mudança .

O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Change Management. Por exemplo, se você mudar o nome das solicitações de Mudança padrão no ITSM de `Padrão` . `Pré-aprovado` , Seu novo nome é exibido automaticamente na lista de seleção de tipo de mudança em Criar solicitação de mudança de, conforme mostrado na figura a seguir.



Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações do VUL. Se necessário, esses valores de campo podem ser editados. Por exemplo, revise os valores nos campos na figura a seguir:

Data de término planejada

Esta data (`2019-10-10`) É o mesmo valor exibido no campo Data de destino de correção do VUL. Este valor é derivado da data de destino de correção mais antiga dos itens vulneráveis que pertencem ao VUL. Se você estiver criando uma solicitação de mudança para um problema crítico que requer uma data de correção anterior, você pode preferir editar esse valor e o valor no campo Prioridade.

Justificativa

Este campo exibe o número de ICs adicionados ao CHG. Se você quiser adicionar informações adicionais, você pode preferir editar este texto. Por exemplo, você pode preferir adicionar uma anotação neste campo sobre o filtro usado para criar o novo VUL, por exemplo, `Pontuação de risco maior que 75` . Este texto pode ajudá-lo a localizar sua nova solicitação de mudança e tarefa de correção.

Plano de implementação

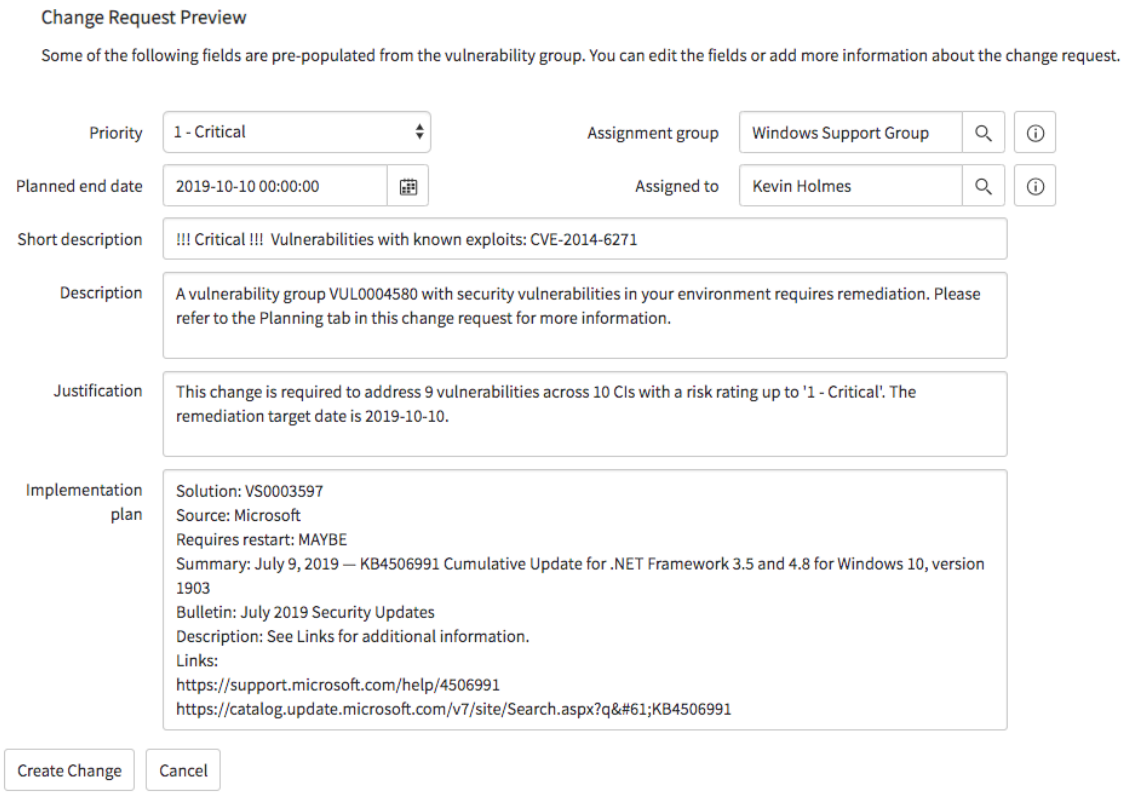
Este campo exibe a solução preferencial para a vulnerabilidade.

Grupo de atribuição e Atribuído a.

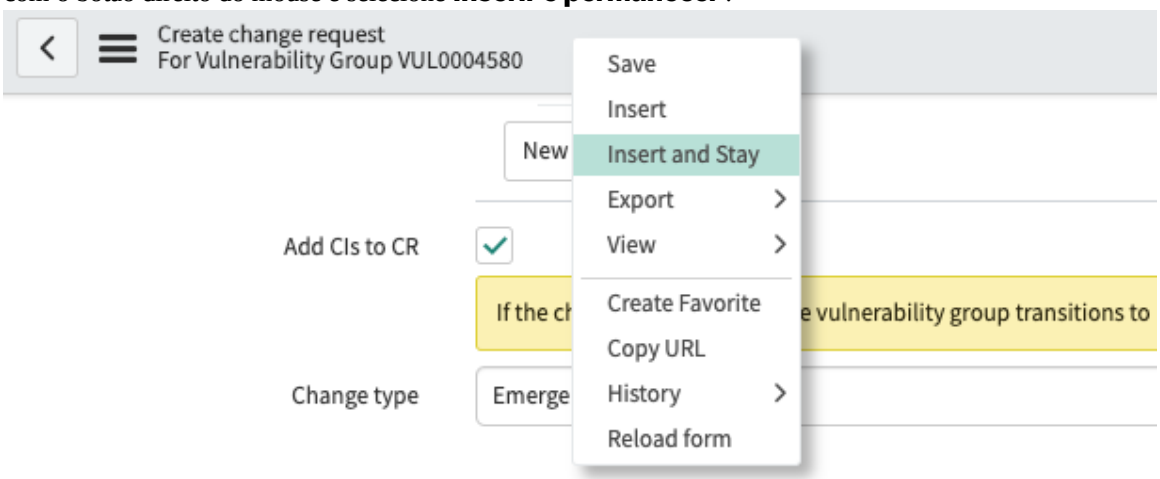
Edite esses campos para mudar o grupo de atribuição ou reatribuir esta solicitação de mudança a um usuário em um de seus grupos de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Continue a visualizar e editar os campos conforme necessário.
7. Para salvar suas mudanças e permanecer nesta página, na faixa cinza na parte superior do formulário, clique com o botão direito do mouse e selecione **Inserir e permanecer** .



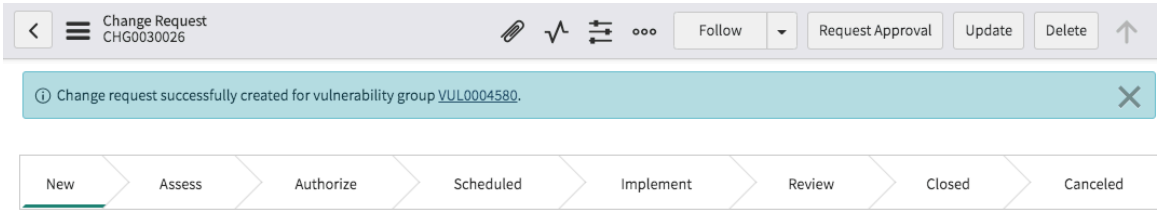
8. Depois de concluir suas edições, escolha uma para continuar.

Opção	Descrição
Criar mudança	Sua solicitação de mudança é criada e a nova solicitação de mudança é exibida em Novo estado. Na parte superior, são exibidas mensagens que indicam que a solicitação de mudança foi criada com sucesso com o número de itens vulneráveis que foram adicionados, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Se a sincronização de estado estiver habilitada e o VUL ainda não estiver em Em investigação , O VUL é movido automaticamente para Em investigação e uma anotação de trabalho é publicada.
Cancelar	A solicitação de mudança não foi criada e o VUL é exibido.



Nota:

Para uma tarefa de correção no Aberto estado Com os campos Grupo de atribuição e Atribuído a não atribuídos (vazio), o usuário conectado atual é atribuído automaticamente à tarefa depois que você clica em **Criar mudança** . Além disso, a caixa de seleção Adicionar ICs à CR deve ser marcada. Na parte superior do VUL, uma mensagem de confirmação azul é exibida indicando esta atribuição.

O que Fazer Depois

Monitore a solicitação de mudança e as tarefas de mudança para verificar se elas foram concluídas e se a solicitação de mudança foi implementada. Depois que este CHG é implementado e movido para Revisão estado, se a sincronização de estado estiver habilitada, o VUL será movido automaticamente para Resolvido . Para obter mais informações sobre sincronização de estado, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Associe uma tarefa de correção a uma solicitação de mudança existente

Como responsável pela correção DE TI, evite criar solicitações de mudança duplicadas (CHG) ao trabalhar para resolver suas tarefas de correção associando uma tarefa de correção (VUL) a uma solicitação de mudança que já esteja disponível em sua instância.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: Qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente a um usuário quando a função itil é atribuída.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Crie uma solicitação de mudança no Espaço de correção de problemas de TI.

Tradução automática

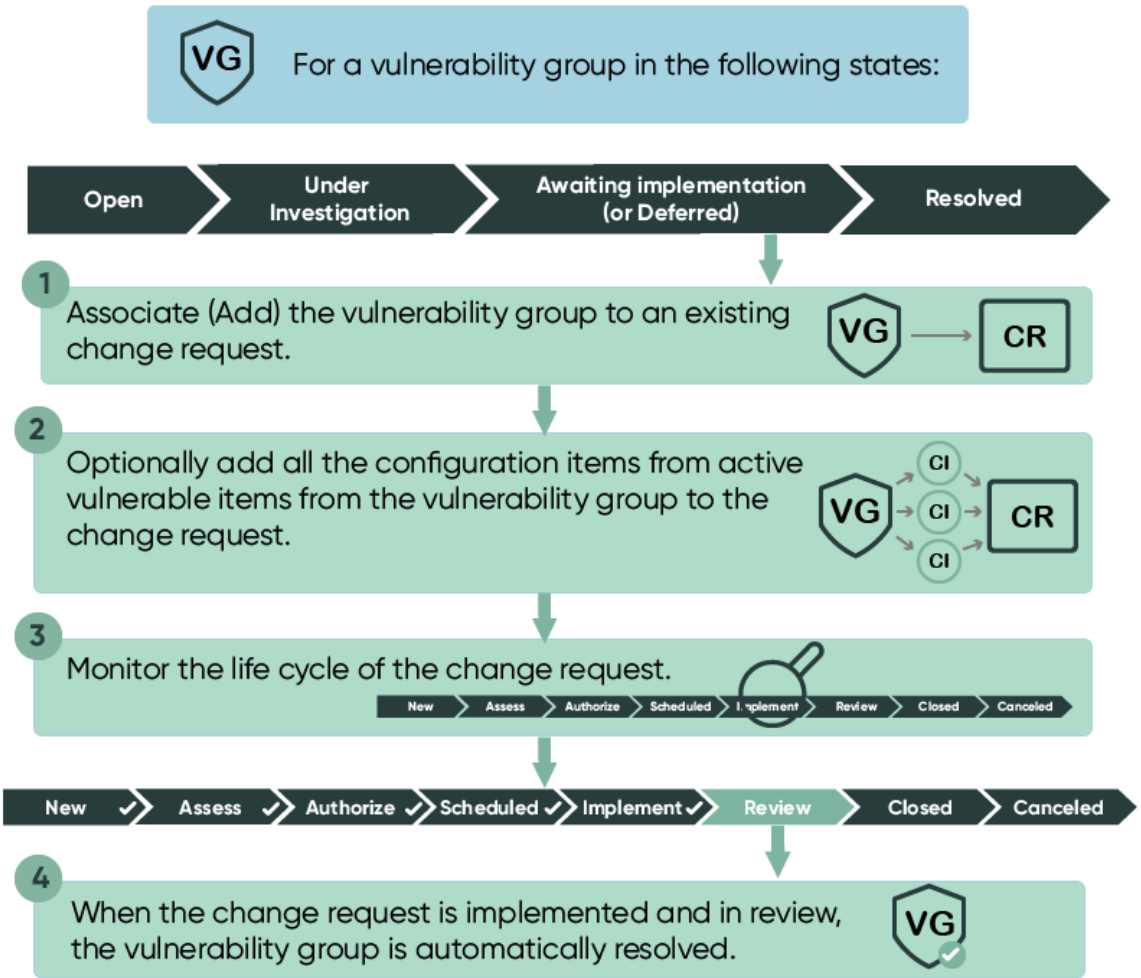
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Em versões anteriores de Resposta a vulnerabilidades Tarefas de correção foram chamadas, grupos de vulnerabilidade (VG). Nas imagens a seguir, VG: Tarefa de correção ou um registro VUL.

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Crie uma solicitação de mudança no Espaço de correção de problemas de TI.

Como responsável pela correção, você pode associar tarefas de correção atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros da tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança a um VUL (VG) existente. As etapas detalhadas deste fluxo seguem a imagem.

Fluxo de trabalho para associar uma tarefa de correção a uma solicitação de mudança existente



Nota: Você pode associar uma solicitação de mudança existente a um VUL em qualquer estado (Aberto, Em investigação, Aguardando implementação, Encerrado e Adiado). Quando você associa uma solicitação de mudança a um VUL existente, somente os VIS ativos são adicionados à solicitação de mudança.

Antes de começar, para evitar a criação de solicitações de mudança duplicadas, você pode preferir exibir todas as solicitações de mudança existentes já associadas a um VUL. Para rastrear facilmente o número de solicitações de mudança relacionadas a um VUL específico, consulte a coluna Contagem de CR na lista Tarefas de correção. Se não for

Tradução automática

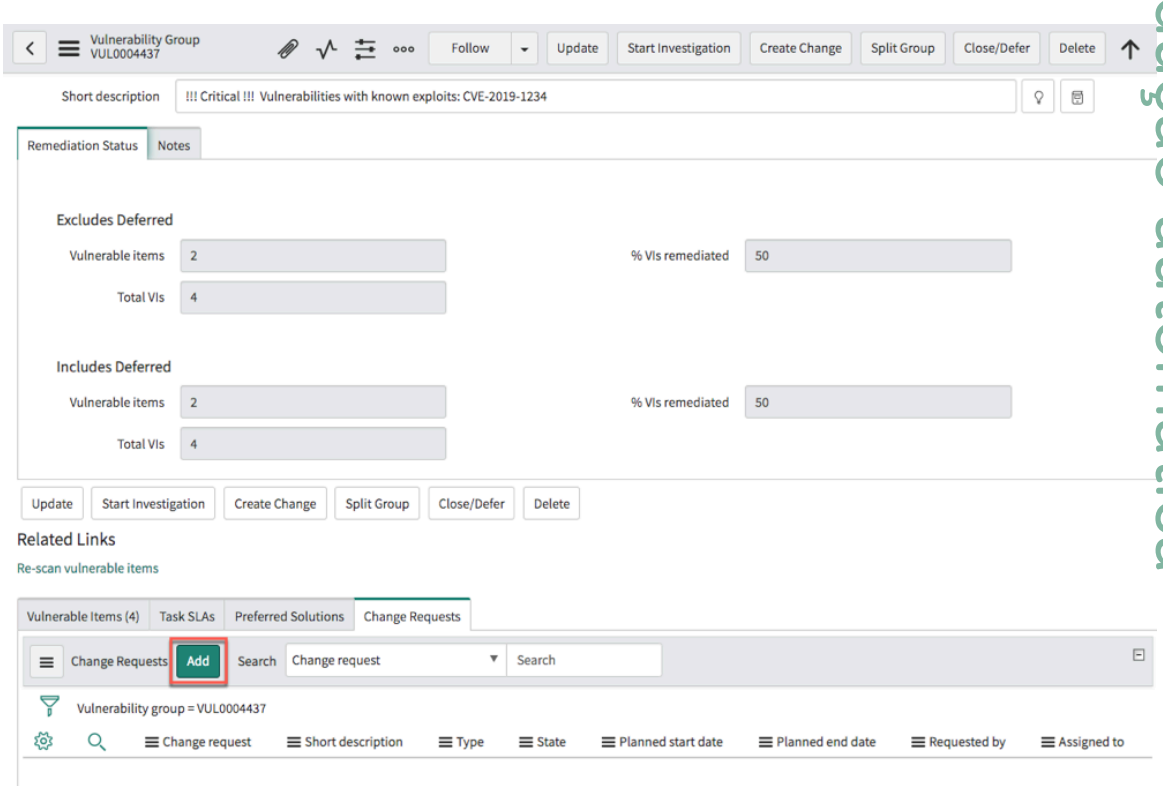
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exibido, clique no ícone de configurações ( ) no canto superior direito. Mova a coluna de contagem de CR de Disponível para Selecionado e clique em **OK** .

Para preencher automaticamente a nova coluna, para clientes com dados existentes nesta tabela, execute o trabalho agendado: Preencha a nova coluna Contagem de CR .

Procedimento

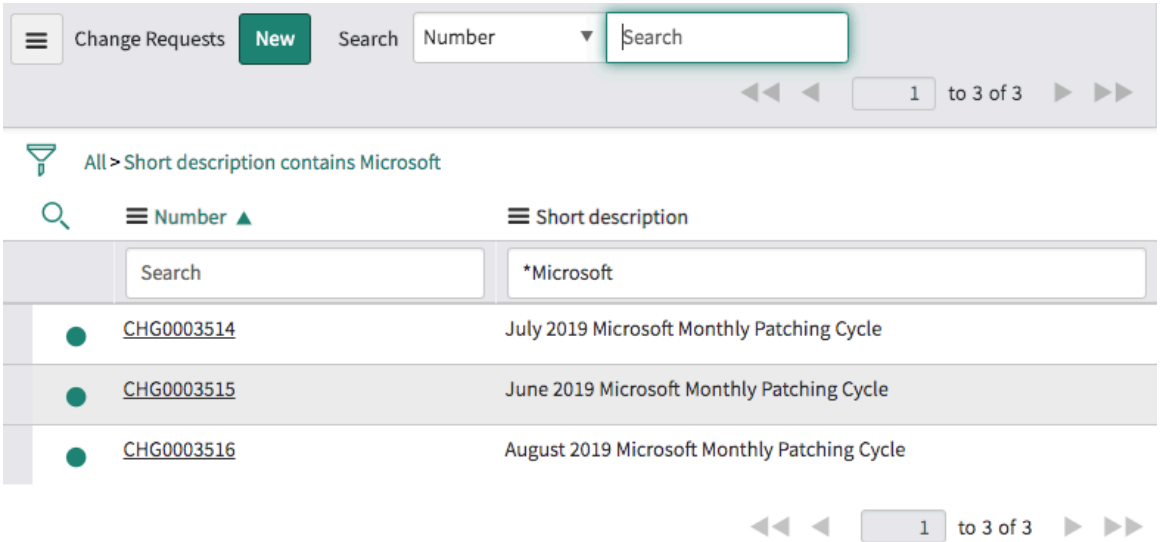
1. Para associar uma tarefa de correção a uma solicitação de mudança existente, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Localize a tarefa de correção com a qual você está trabalhando.
3. **Opcional:** Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Visão Geral da Correção** Para exibir o painel Visão geral da correção e localizar um VUL atribuído a você ou ao seu grupo de atribuição.
4. Na coluna Número, clique em um registro VUL para abri-lo.
   O registro VUL é exibido.
5. Com o registro em aberto exibido, se ainda não estiver sendo exibido, role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas ao VUL são exibidas junto com **Adicionar** botão. Na figura a seguir, não há solicitações de mudança já associadas a este VUL.



6. Para associar o VUL a um CHG existente, clique em **Adicionar** .
   O formulário Adicionar solicitação de mudança existente à tarefa de correção é exibido.
7. No formulário, clique no ícone de pesquisa.
   Uma exibição de lista de solicitações de mudança existentes é exibida em uma nova janela, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Selecione um item na lista exibida ou, como alternativa, clique no filtro ( ) e insira condições para limitar os resultados da pesquisa.
9. Na caixa de seleção Adicionar ICs à CR, escolha uma para continuar.

Nota: Esta caixa de seleção é exibida somente para solicitações de mudança existentes no Novo estado.

Opção	Descrição
Caixa de seleção Adicionar ICs à CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem a itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. Quando selecionado, o estado da solicitação de mudança é sincronizado com o VUL. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos itens vulneráveis ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o VUL e o VUL permanece em seu estado atual.

10. Com o número da solicitação de mudança que você deseja exibir no campo Pesquisar solicitação de mudança, clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O VUL é exibido. Na parte superior do registro, a mensagem de confirmação azul é exibida indicando que a solicitação de mudança selecionada foi associada com sucesso ao VUL.

Nota: Para um VUL no Aberto estado Com os campos Grupo de atribuição e Atribuído a não atribuídos (vazio), o usuário conectado atual é atribuído automaticamente ao VUL depois que você clica em **Adicionar** . Além disso, a caixa de seleção Adicionar ICs à CR deve ser marcada. Na parte superior do VUL, uma mensagem de confirmação azul é exibida indicando que o usuário atual está atribuído.

O que Fazer Depois

Revise o registro VUL. Na coluna Solicitação de mudança na lista relacionada Solicitações de mudança, clique no link para o novo CHG exibir o registro de CR. No registro CHG aberto, você pode monitorar o estado da solicitação de mudança. Os itens de configuração (ICs) afetados e as tarefas de correção são exibidos nas listas relacionadas de ICs afetados e tarefas de correção.

Divida uma tarefa de correção

Como responsável pela correção de TI, em uma tarefa de correção (VUL) existente, identifique um subconjunto de itens vulneráveis (VI) que você deseja mover para um novo grupo.

Antes de Iniciar

Nota:

Os casos de uso para dividir VIS de VULs existentes em novas tarefas de correção podem incluir os seguintes exemplos:

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para uma tarefa dividida.
- Quando você reatribui um grupo dividido a outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou exceção para uma tarefa dividida, porque sabe que algumas vulnerabilidades em itens de configuração (IC) específicos não podem ser corrigidas em um determinado intervalo de tempo.

Função necessária: Qualquer usuário com a função itil para dividir um VUL.

Nota: A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como dividir tarefas de correção no Resposta a vulnerabilidades espaços, consulte Divida uma tarefa de correção no Espaço de correção de problemas de TI.

Para dividir uma tarefa de correção no ambiente clássico ou para versões de Resposta a vulnerabilidades.

Você pode dividir tarefas de correção existentes com mais de um item vulnerável que estão em Aberto estados Em investigação ou Aguardando implementação. Ao criar um novo VUL com itens vulneráveis que correspondem a critérios específicos, você pode trabalhar com um grupo específico de itens vulneráveis sem afetar a tarefa de correção original.

Quando você especifica as condições para os itens vulneráveis que deseja mover para uma nova tarefa de correção com o construtor de condições, somente os VIS ativos que correspondem aos seus critérios são movidos para o novo grupo.

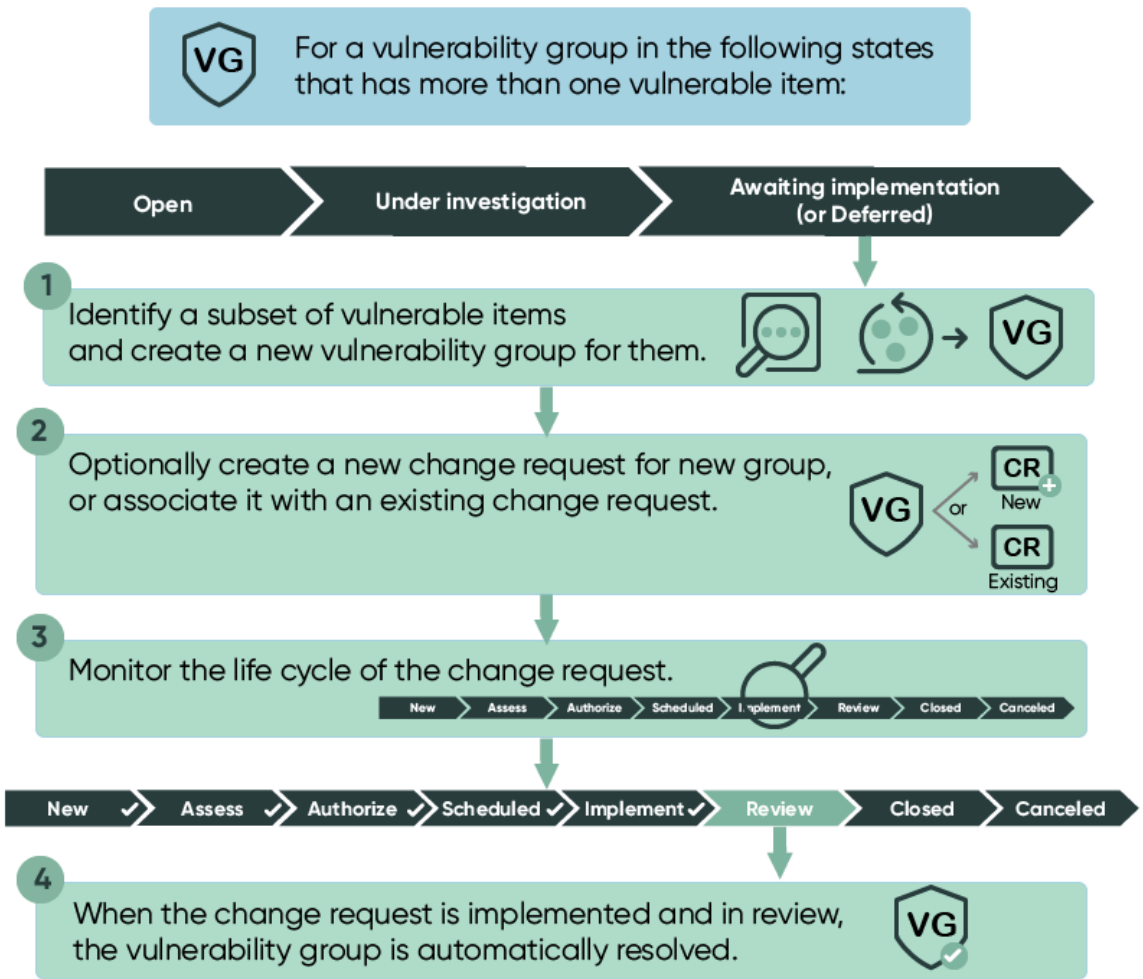
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você não precisa criar Solicitações de Mudança (CHG) ao dividir um VUL. Você tem a opção de dividir um VUL ao criar uma solicitação de mudança ou dividir um VUL sem criar uma solicitação de mudança. A imagem a seguir ilustra o fluxo básico para dividir uma tarefa de correção. As etapas detalhadas deste fluxo seguem a imagem.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Em versões anteriores de Resposta a vulnerabilidades Tarefas de correção foram chamadas, grupos de vulnerabilidade (VG). Nas imagens a seguir, VG: Tarefa de correção ou um registro VUL.

Fluxo de trabalho para dividir uma tarefa de correção

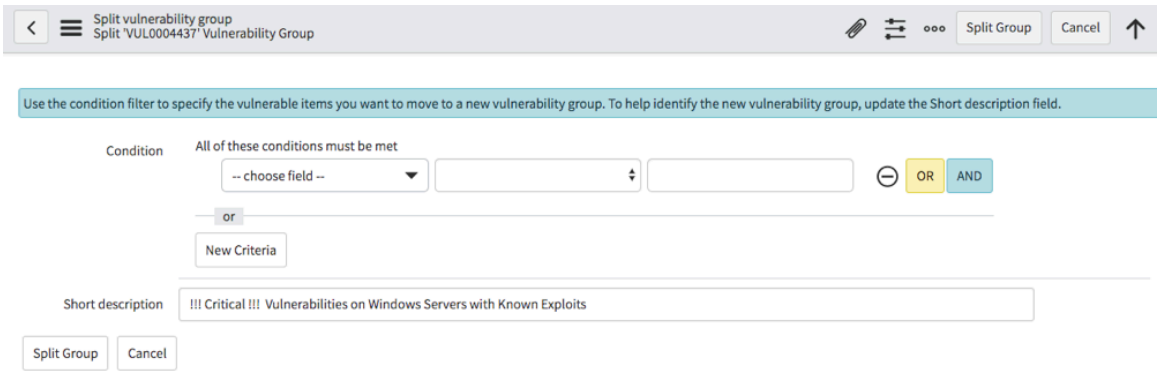


Tradução automática

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**.
   A lista Tarefas de correção é exibida.
2. Na coluna Número, clique em um registro para abri-lo.
   O registro é exibido.
3. No canto superior direito do VUL, clique em **Tarefa dividida** .
   O formulário Tarefa de correção dividida é exibido.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

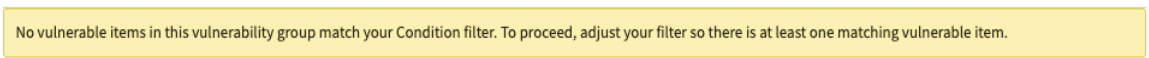


4. Com o filtro de condição exibido, especifique as condições dos itens vulneráveis que você deseja mover para uma nova tarefa.
   Por exemplo, você pode preferir filtrar somente itens vulneráveis que correspondam às seguintes condições:
   - Em Aberto estados.
   - Pontuações de risco maiores que 80 .
   - Itens de configuração que contêm ' WINSV '.
   - Localizado em San Diego.

   Por exemplo, para Condições, você pode inserir:
   - Estado - É - Aberto
   - Pontuação de risco - é maior que ou é - 80
   - Item de configuração . Nome - Contém - WINSV
   - Item de configuração . San Diego

   Se os itens vulneráveis corresponderem ao seu filtro depois que você inserir as condições, uma mensagem será exibida com o número de itens vulneráveis correspondentes.

   Nota: Se uma mensagem for exibida informando que nenhum item vulnerável corresponde ao seu filtro, ajuste as condições para que pelo menos um item vulnerável corresponda aos critérios de filtro.

5. **Opcional:** Ajuste o filtro conforme necessário.
6. **Opcional:** Para ajudá-lo a identificar o novo VUL após ele ser criado, você pode preferir atualizar o campo Descrição resumida.
   Se editado, use o campo Descrição resumida como critérios de pesquisa para o novo VUL para ajudá-lo a localizá-lo depois que ele for criado, por exemplo, LOCALIZADO EM SAN DIEGO .
7. **Opcional:** Para visualizar detalhes sobre os itens vulneráveis que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Tarefa dividida** Para criar o novo VUL.
   Esses detalhes incluem solicitações de mudança existentes que já estão associadas a este subconjunto e VULs com esses itens vulneráveis. Exibir essas informações na visualização pode impedir que você crie VULs duplicados.

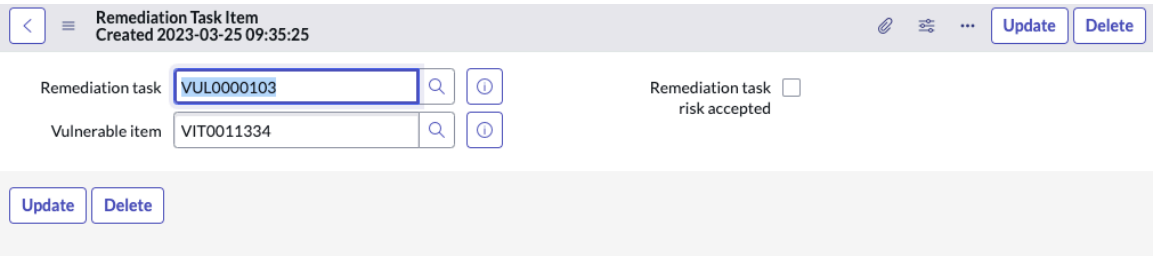
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na mensagem de confirmação azul no formulário Tarefa de correção dividida, clique em **Visualizar itens correspondentes** .
A lista Item da tarefa de correção é exibida em uma nova janela no navegador com uma lista de itens vulneráveis que correspondem às suas condições.

b. Na coluna Número, clique em um item para abrir o registro.

c. No registro exibido, à direita do grupo de vulnerabilidades ou dos campos de item de vulnerabilidade, clique no ícone de informações do item vulnerável para exibir os registros.



d. Na caixa de diálogo exibida, clique em **Registro em aberto** .
As informações sobre a data de destino de correção são exibidas. Na seção Listas relacionadas, clique em uma lista relacionada para exibir mais informações sobre o VI

8. Quando você estiver pronto para criar o novo VUL com as VI(s) que atendem às suas condições, feche a janela de visualização para retornar ao formulário de tarefa dividida na outra janela e, na parte superior do formulário, clique em **Tarefa dividida** .

Nota:

Para menos de 200 VIS, a operação de divisão é feita de forma síncrona.

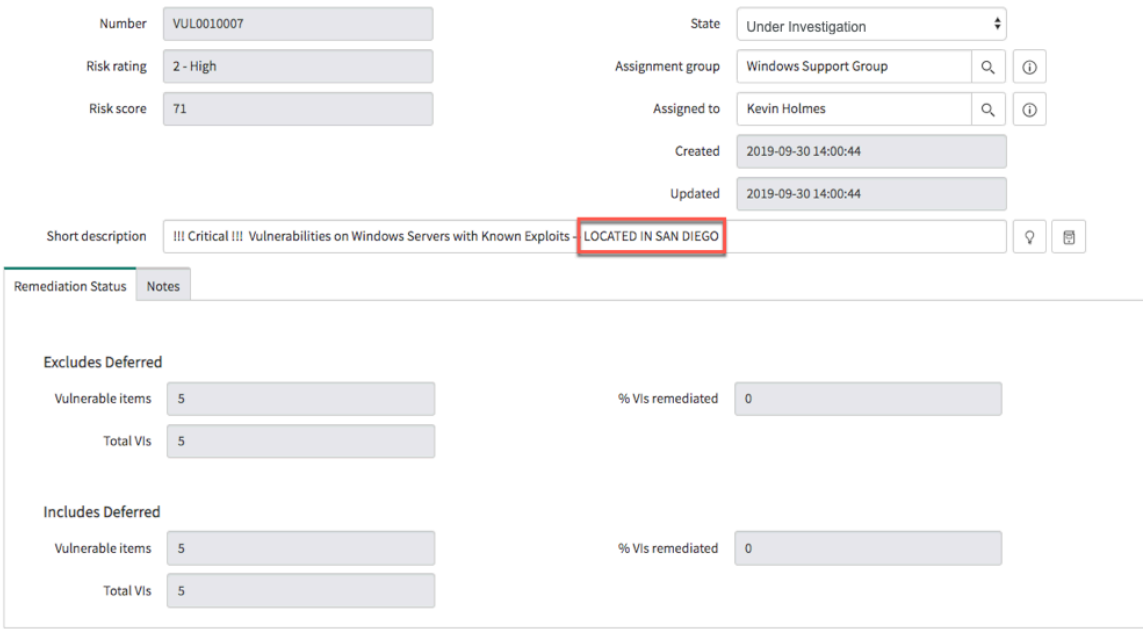
Para mais de 200 VIS, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que o VIS apareça no novo grupo.

É exibida uma mensagem de confirmação que mostra todos os VIS ativos que são movidos para o novo grupo. O novo número da tarefa de correção também é exibido. Se ainda não estiver sob investigação, o VUL será movido para Em investigação. Verifique o campo Descrição resumida do texto inserido para o novo VUL no (LOCALIZADO EM SAN DIEGO).

Os cálculos de acúmulo no novo grupo são realizados para calcular sua nova Pontuação de risco, Data de destino de correção e outros valores de campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os itens vulneráveis, as soluções preferenciais e as solicitações de mudança são exibidos nas listas relacionadas na parte inferior do registro. Processe e monitore esta nova tarefa como faria com qualquer tarefa de correção.

9. **Opcional:** Role até **Anotações** lista relacionada e clique para selecioná-la.
   Confirme se o número de itens vulneráveis da tarefa de correção original foi movido para o novo grupo no fluxo de atividades.
10. **Opcional:** No novo VUL, para selecionar e dividir o VIS da lista relacionada Itens vulneráveis mais uma vez, role até a parte inferior do registro da tarefa de correção e, com o VIS que você deseja mover selecionado na coluna Item vulnerável da lista relacionada Itens vulneráveis, na lista de seleção Ações nas linhas selecionadas, selecione **Tarefa dividida** .
    O formulário Tarefa de correção dividida é exibido.
11. Para dividir o grupo novamente e mover os itens selecionados para um novo grupo, clique em **Tarefa dividida** .
    Os VIS selecionados são movidos para outra tarefa de correção, a mensagem de confirmação é exibida e o novo grupo é exibido.
12. Escolha um para continuar sua investigação ou correção.

Opção	Descrição
Criar Incidente de segurança	Crie um incidente de segurança.
Criar mudança	Crie uma solicitação de mudança para esta tarefa de correção.
Dividir tarefa	Se o novo grupo tiver mais de um VI, divida esta tarefa de correção novamente para criar outro subconjunto de itens vulneráveis.
Aguardando Implementação	Se exibida, mova a tarefa de Em investigação para o estado Aguardando implementação.
Fechar ou solicitar exceção	Feche ou adie a tarefa de correção. Uma caixa de diálogo de confirmação é exibida com os seguintes campos obrigatórios:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Estado ○ Motivo ○ Informações adicionais Preencha os campos para fechar ou adiar o grupo e clique em **Enviar** .
Excluir	Exclua esta tarefa de correção.
Estado	Mova o registro para outro estado exibido na lista de seleção e clique em **Atualização** para salvar suas mudanças no registro. **Nota:** Você pode mover manualmente o novo VUL pelos estados de seu ciclo de vida. No entanto, se a sincronização de estado estiver habilitada e o sistema registrar que uma solicitação de mudança associada ao VUL mudou seu estado, ou você adicionar um CHG ou removê-lo do VUL, a sincronização de estado poderá substituir sua intervenção manual. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.
Grupo de atribuição	Reatribua o VUL a um grupo de atribuição e clique em **Atualização** para salvar suas mudanças no registro.
Atribuição a	Atribua o VUL a você mesmo ou a um usuário específico em outro grupo de atribuição e clique em **Atualização** para salvar suas mudanças no registro.

O que Fazer Depois

Monitore o estado do novo VUL para agilizar sua resolução.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos Estado de tarefas de correção (VULs) e os campos Estado de solicitações de mudança (CHG) no Resposta a vulnerabilidades produto. À medida que uma solicitação de mudança avança pelo ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente.

Sincronização de estado

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Em versões anteriores de Resposta a vulnerabilidades Tarefas de correção foram chamadas, grupos de vulnerabilidade (VG). Nas imagens a seguir, VG: Tarefa de correção ou um registro VUL.

A sincronização de estado é habilitada por uma propriedade do sistema (sn_vul.cr_state_synch) por padrão em sua instância quando você baixa o. Resposta a vulnerabilidades aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando a sincronização de estado está habilitada, o campo Estado de CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

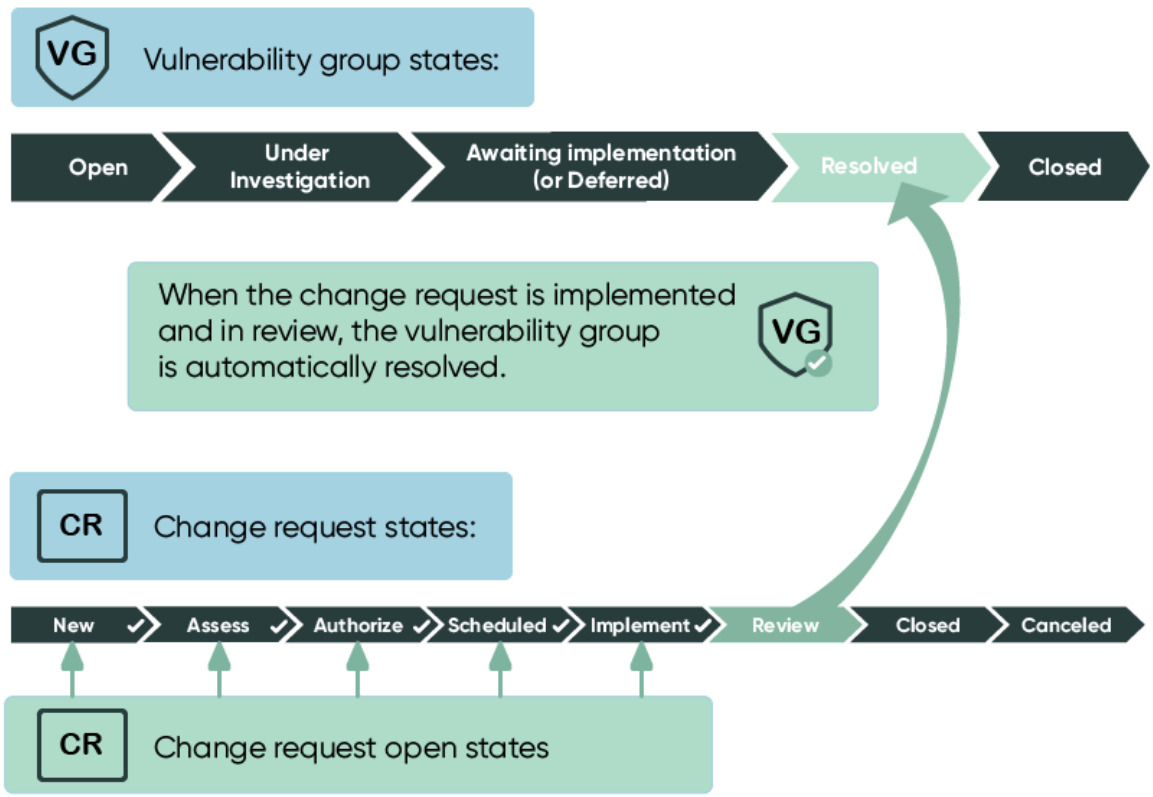
- Quando um novo CHG é criado para uma tarefa de correção (VUL), se não estiver em Aguardando implementação , O estado VUL avança para Aguardando implementação .
- Quando um CHG existente é associado a um VUL, se não estiver em Aguardando implementação , O estado VUL avança para Aguardando implementação .
- Depois que as tarefas em um CHG são concluídas (Implementado E o CHG é movido para Revisão estado, o VUL avança para Resolvido .

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

Nota: Você ainda pode mover manualmente CHGs e VULs pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado ou você adiciona um CHG ou o remove de um VUL, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente o VUL do Encerrado ou Adiado estados.

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados de CHG movem automaticamente estados de VUL em um ciclo de vida avançado, ou seja, de Aberto . Resolvido .



Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de Encerrado . A sincronização de estado move automaticamente o VUL bidirecional por meio do Aberto , Em investigação , Aguardando implementação e Resolvido estados. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (Adicionar ICs ao CR) é exibido em um formulário e você escolhe desmarcar a caixa de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O VUL não avança para Resolvido Quando um CHG está em seus estados abertos. Qualquer CHG nos estados anteriores a. Revisão em seu ciclo de vida, como, Novo , Avaliar , Autorizar , Programado ou Implementar Como mostrado na figura anterior, são considerados estados abertos para o CHG. os estados em aberto não movem o campo de estado no VUL, porque as investigações ou tarefas no CHG não foram concluídas. A sincronização de estado é invocada quando um CHG é criado ou associado ao VUL ou o estado de um relacionamento existente muda no CHG. Os estados CHG concluídos são Revisão e com sucesso Encerrado . Quando um CHG é encerrado com sucesso, seus códigos encerrados são: Bem-sucedido ou Problemas bem-sucedidos , Nesse caso, o VUL avança para Resolvido .

Sincronização de estado reverso

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Se o CHG for Cancelado ou Encerrado (com um código de fechamento de Malsucedido), o VUL retorna automaticamente para Em investigação . O VUL retorna para Em investigação porque não há plano ativo para corrigir a vulnerabilidade.

Se um VUL estiver em um Resolvido E você cria um novo CHG ou o associa a um CHG existente em um dos estados abertos iniciais, o VUL faz a transição automaticamente de volta para Aguardando implementação . O VUL retorna para este estado, porque mais trabalho agora está atribuído ao CHG.

VULs com mais de um CHG

Se um VUL estiver Aguardando implementação Tem mais de um CHG associado a ele, a sincronização de estado é baseada no status do CHG no estado mais antigo de seu ciclo de vida. Por exemplo, um VUL tem quatro CHGs associados a ele, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número de CHG	Estado de CHG
1	Implementar
2	Cancelado
3	Encerrado (código de fechamento de Malsucedido)
4	Encerrado (código de fechamento Bem-sucedido)

A sincronização de estado entre o CHG e o VUL, neste caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (Implementar). Nesse caso, o VUL permanece em Aguardando implementação .

Em outro exemplo, se um VUL estiver em Resolvido E tem um CHG existente que foi implementado e está em Revisão E um novo CHG é criado, o VUL retorna Resolvido . Aguardando implementação . A sincronização de estado é baseada no CHG no Novo estado, que é o CHG no estado mais antigo.

Número de CHG	Estado de CHG
1	Revisão
2	Novo(a)

Além disso, quando os VULs têm mais de um CHG, o estado do VUL faz a transição automaticamente nos seguintes casos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando um CHG avança para Revisão Se todos os outros CHGs associados ao VUL estiverem em Revisão ou Encerrado (Com um código de fechamento bem-sucedido),o VUL faz a transição automaticamente para Resolvido . Quaisquer outros CHGs relacionados que forem cancelados ou encerrados sem sucesso serão ignorados.
- Quando um CHG se move para Cancelado ou Encerrado (código de fechamento de Malsucedido Se todos os outros CHGs associados ao VUL estiverem no mesmo estado, o VUL retornará automaticamente para Em investigação .

Para obter mais informações sobre estados de tarefa de correção e o que você pode fazer em cada estado, consulte Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável.

Avalie sua exposição a software vulnerável

Você pode fornecer as informações do fornecedor e do produto no módulo Avaliação de exposição para avaliar sua exposição de dia zero (dia atual) de seus ativos a software vulnerável usando Gestão de ativos de software do ITSM Aplicação Foundation (SAM).

Importante: Você pode executar a avaliação de exposição por software e Vulnerabilidades e exposições comuns (CVE) para aproveitar os recursos adicionais no Espaço de avaliação de vulnerabilidades. Para obter mais informações, consulte Explorar o Espaço de avaliação de vulnerabilidade.

Antes de Iniciar

Função necessária: Administrador de vulnerabilidades (sn_vulnerability_write)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Tenha as seguintes informações disponíveis sobre o software vulnerável que você deseja avaliar:

- Fornecedor
- Versão
- Produto
- Edição

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre requisitos do sistema, consulte Configure o. Vulnerabilidade Avaliação de exposição.

Exiba o módulo de avaliação de exposição de software e crie e edite registros de avaliação de exposição sob demanda para software vulnerável em seu ServiceNow AI Platform® instância.

Você gerencia as atividades de resposta a vulnerabilidades de uma grande operação responsável por muitos ativos. O Centro de operações de segurança (SOC) em sua operação entra em contato com você sobre uma versão do software que eles descobriram ser vulnerável. Você descobre que uma verificação de seus ativos foi concluída recentemente e não encontrou esta vulnerabilidade. A equipe do SOC aprendeu sobre essa vulnerabilidade de uma fonte confiável fora do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou de outras bibliotecas de terceiros em sua

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

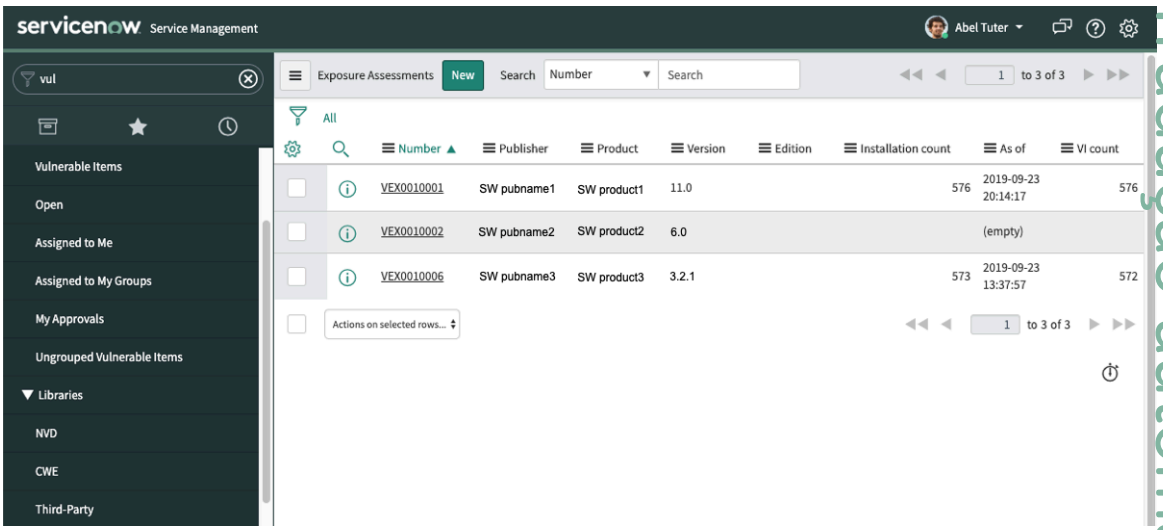
instância, e você está preocupado com o fato de que o verificador de vulnerabilidades ainda não adicionou o plug-in para ela.

Você tem certeza de que os dados dessa vulnerabilidade serão atualizados no NVD e importados em breve para que o scanner possa detectar essa vulnerabilidade na próxima verificação, mas, como você está preocupado com o escopo de sua possível exposição, você deseja determinar hoje se tem ativos em sua rede que têm este software instalado.

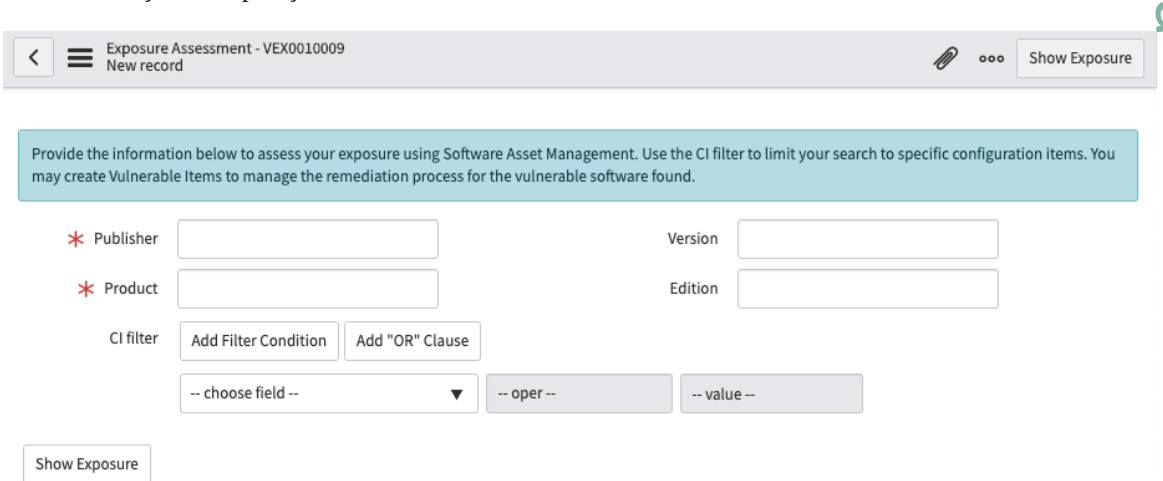
A partir da v23.0 de Resposta a vulnerabilidades Se você tiver a assinatura Pro ou Enterprise, será redirecionado para **Avaliação de exposição** Nos Espaços de trabalho com base em sua função ao selecionar o. **Avaliação de exposição** link no **Todos** menu. Para obter mais informações, consulte Configure o. Vulnerabilidade Avaliação de exposição.

Procedimento

1. Para criar uma nova avaliação de exposição, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Avaliação de Exposição**.
   A lista Avaliações de exposição é exibida.



2. Selecione **Novo**.
   O formulário Avaliação de exposição é exibido.



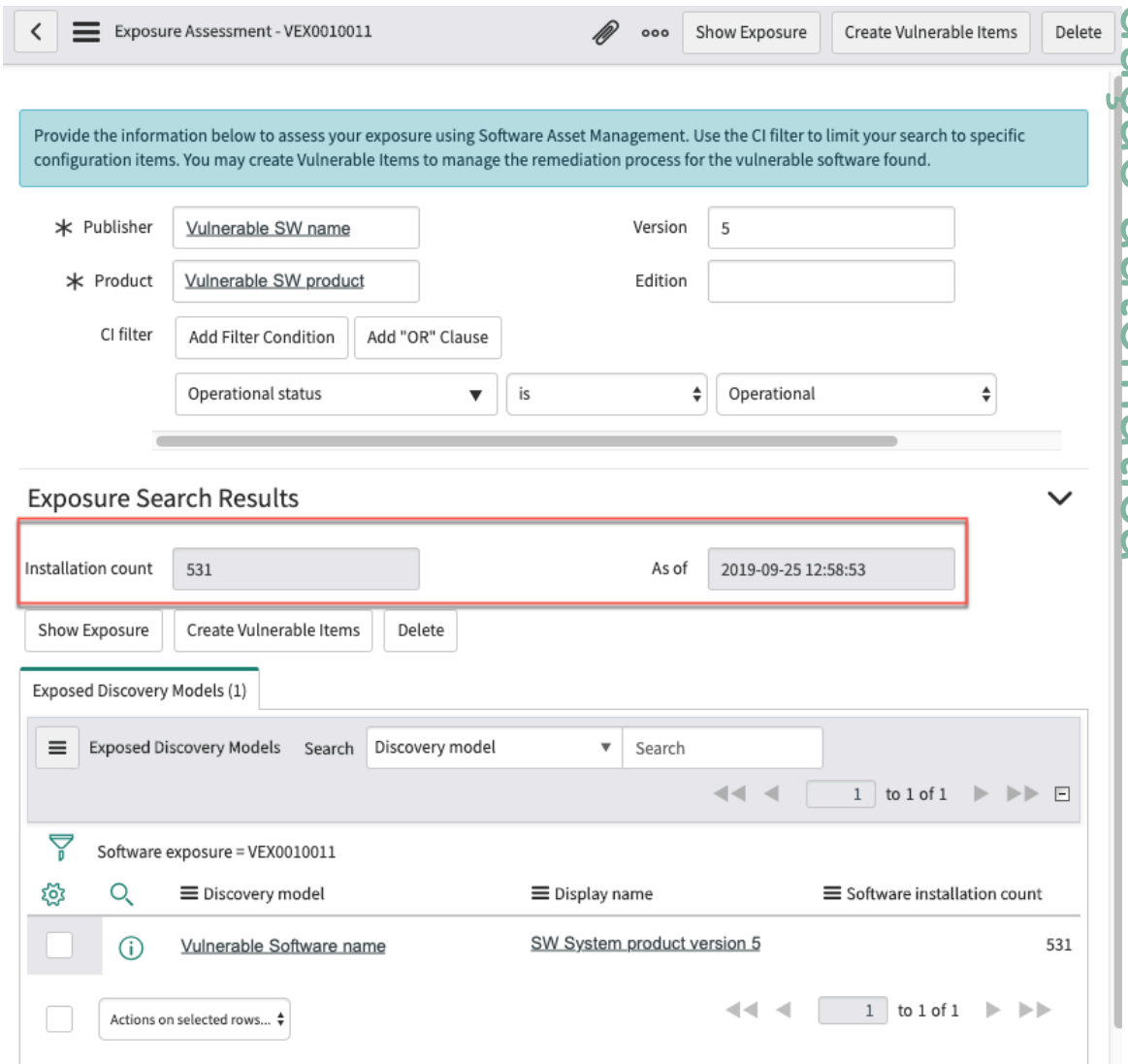
3. Preencha o formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fornecedor	Nome do fornecedor do software.
(Opcional) Versão	Insira o número da versão para ajudá-lo a restringir a pesquisa em seus ativos.
Produto	Nome do produto de software.
(Opcional) Edição	Insira a edição para ajudá-lo a restringir a pesquisa em seus ativos.
Filtro de IC	Use as listas de seleção do filtro Item de configuração (IC) para limitar sua pesquisa a itens de configuração específicos (ativos). Por exemplo, você pode enviar uma consulta somente para ativos ativos que podem ter este software instalado: O status operacional é Operacional

4. Selecione **Mostrar exposição** .
   O registro Avaliação de exposição com seu modelo de descoberta e a contagem de instalação de software em seus ativos a partir da data específica é exibido.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Escolha um para continuar.

Opção	Descrição
Mostrar Exposição	Adicione condições de filtro de IC adicionais e selecione **Mostrar exposição** para refinar ainda mais os resultados da pesquisa.
Criar Itens vulneráveis	Crie itens vulneráveis para os itens de configuração a partir dos resultados da pesquisa. Se os itens vulneráveis forem criados com sucesso, uma tarefa de correção será criada para todos os itens vulneráveis e exibida no registro de avaliação de exposição.
Excluir	Exclua este registro e retorne à lista Avaliações de exposição. Uma caixa de diálogo de confirmação é exibida.

6. **Opcional:** Crie um item vulnerável para o resultado da pesquisa.

Nota: Depois de criar itens vulneráveis, você não pode alterar os critérios de pesquisa para este registro de exposição.

7. Como alternativa, revise as condições de filtro e refine ainda mais os resultados da pesquisa.

8. Para criar itens vulneráveis, siga estas etapas:

a. Selecione **Criar itens vulneráveis** .
A caixa de diálogo Criar itens vulneráveis é exibida.

b. Preencha os campos.

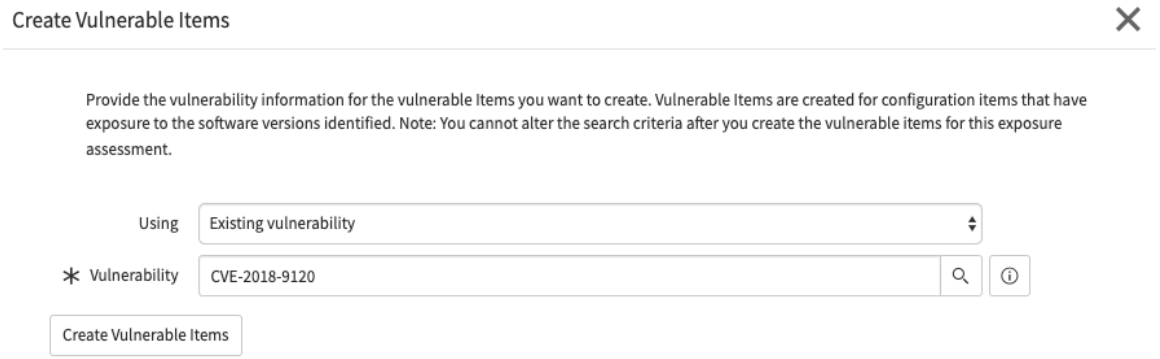
Campo	Descrição
Usando	Na lista de seleção, escolha uma para continuar. ▪ **Vulnerabilidade existente** . À direita do campo Vulnerabilidade, clique no ícone de pesquisa. Na lista exibida, selecione o CVE-ID ou insira os critérios de pesquisa para localizar o CVE-ID existente, por exemplo, CVE 2018-9120. **Nota:** Pode ser um CVE-ID de um banco de dados de vulnerabilidades diferente do NVD. ▪ **Nova vulnerabilidade** . Insira o CVE-ID da sua nova vulnerabilidade no formato xxxx-xxxx, xxxx-xxxxx ou xxxx-xxxxxxx.
Resumo da vulnerabilidade (somente para nova vulnerabilidade)	Insira um resumo para a nova vulnerabilidade, por exemplo, Um invasor pode executar script no navegador de um usuário desavisado .

As imagens a seguir mostram exemplos do formulário preenchido para uma vulnerabilidade existente e uma nova vulnerabilidade.

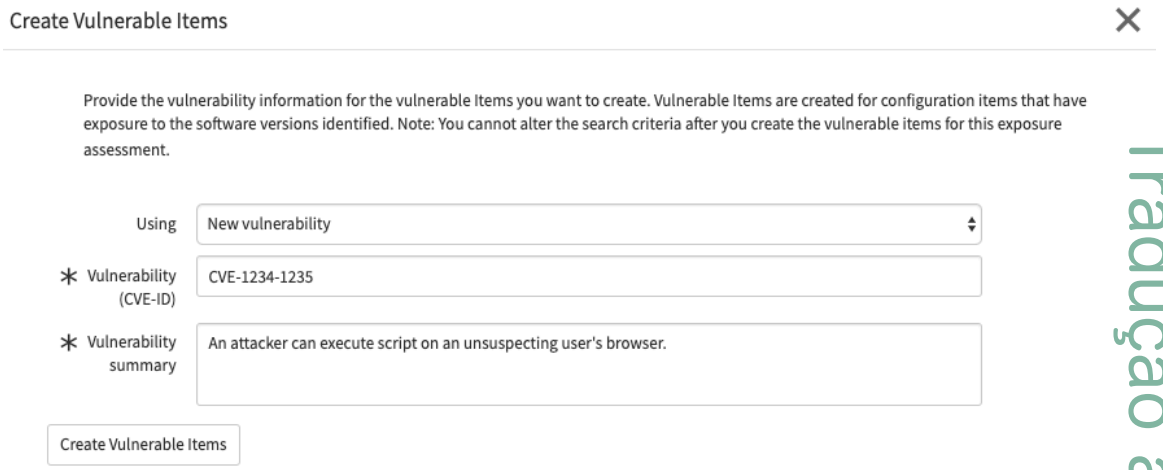
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidade Existente



Nova Vulnerabilidade



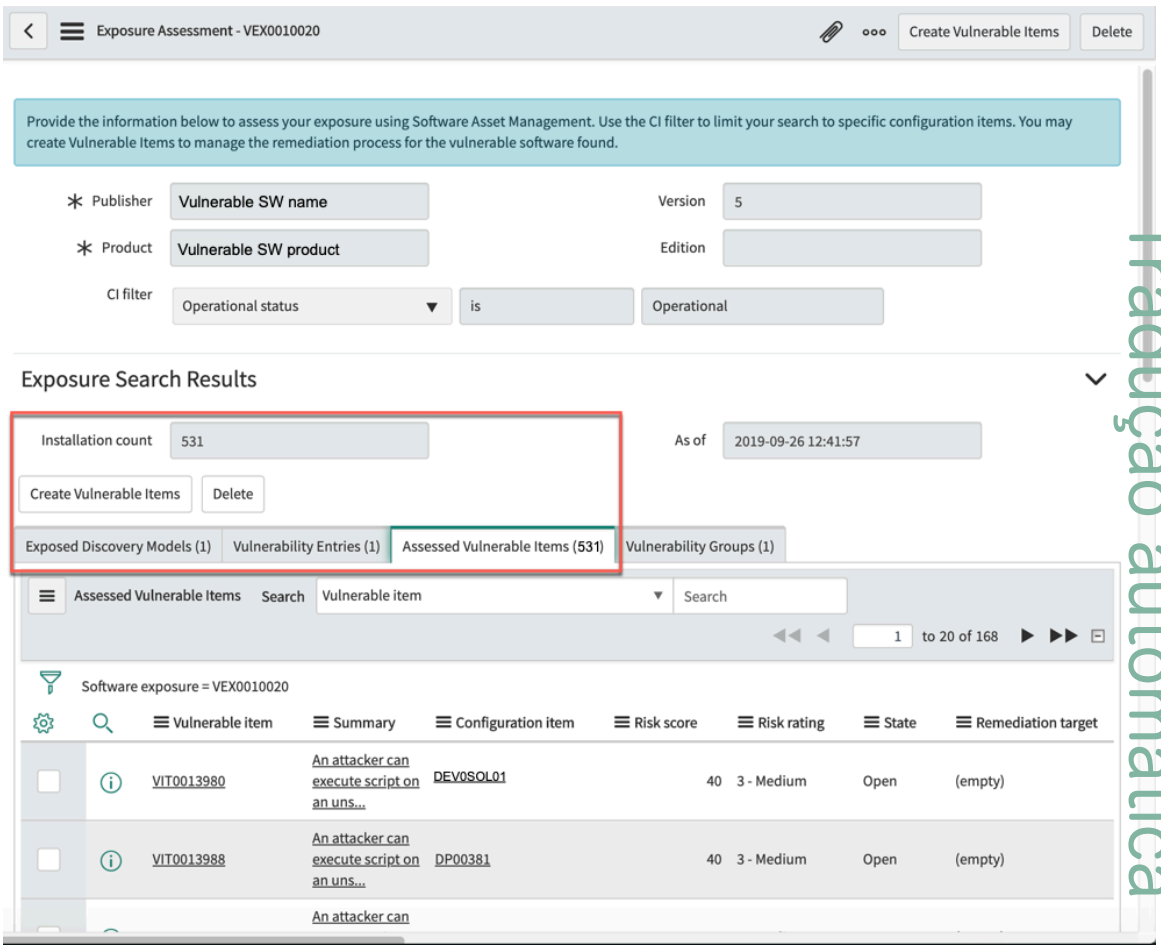
c. Selecione **Criar itens vulneráveis** .
O registro Avaliação de exposição é exibido com uma mensagem de status que indica que itens vulneráveis estão sendo criados.

d. Após alguns segundos, na parte superior do formulário, clique com o botão direito do mouse na faixa cinza para recarregar a página.
Os novos itens vulneráveis são exibidos conforme mostrado na figura a seguir na guia Itens vulneráveis avaliados (531). A nova tarefa de correção criada para esses itens vulneráveis é exibida na guia Tarefa de correção (1).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para este exemplo, uma tarefa de correção é criada de acordo com as regras e condições de grupo da regra de tarefa de correção chamada Vulnerabilidade. Esta regra de grupo é a regra de tarefa de correção padrão que é instalada com o produto Resposta a vulnerabilidades em seu ServiceNow AI Platform® instância. Neste exemplo, as condições desta regra de grupo colocaram todos os itens vulneráveis em uma única tarefa de correção. Se você preferir criar mais de uma tarefa de correção para os itens vulneráveis que correspondem aos resultados da pesquisa de avaliação de exposição, você pode preferir configurar regras de tarefa de correção adicionais. Criar mais tarefas de correção pode ajudar a impedir a criação de tarefas de correção com um grande número de itens vulneráveis. Para obter mais informações sobre regras de tarefa de correção, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção e. Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção.



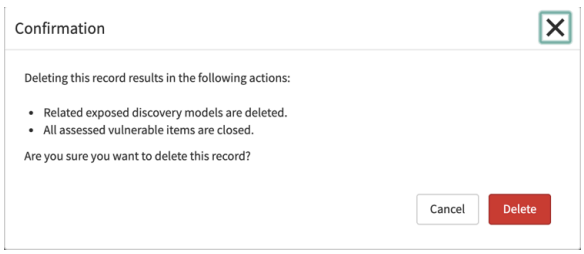
Tradução automática

9. Escolha um para continuar.

Opção	Descrição
Tarefas de correção	Com a guia Tarefas de correção selecionada, na coluna Número, clique para abrir o registro e revisar e atribuir a tarefa para correção. Para obter mais informações sobre grupos de atribuição, consulte Criando grupos .
Itens de vulnerabilidade avaliados	Com a guia Itens vulneráveis avaliados selecionada, na coluna Item vulnerável, clique para abrir os registros e revisar e atribuir itens vulneráveis individuais.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Excluir	Exclua o registro de avaliação de exposição. Uma caixa de diálogo de confirmação é exibida. **Nota:** Se você excluir o registro de exposição depois de criar itens de vulnerabilidade, todos os itens vulneráveis que você criar para este registro que não estejam relacionados a outro registro de exposição serão movidos automaticamente para Encerrado estado. O motivo do fechamento é Cancelado .



O que Fazer Depois

Responda a ameaças de dia zero (dia atual) com base em sua avaliação de exposição. Para obter mais informações sobre tarefas de correção e gestão de mudanças para Resposta a vulnerabilidades, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção e. Gestão de mudanças para Resposta a vulnerabilidades.

Exibindo recomendações de atribuição

Um grupo de atribuição geralmente é alocado a um item vulnerável usando regras de atribuição. Essas regras são configuradas pelo administrador de vulnerabilidades para alocar os grupos de atribuição corretos que são baseados nos dados recebidos de scanners de terceiros.

Para obter mais informações, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto, você poderá usar Recomendações de atribuição de vulnerabilidade para exibir grupos de atribuição alternativos.

Usar Recomendações de atribuição de vulnerabilidade para executar as seguintes ações:

- Solicitar recomendações de grupo de atribuição para um item vulnerável.
- Solicitar recomendações de grupo de atribuição para vários itens vulneráveis.
- Solicitar recomendações de grupo de atribuição para uma tarefa de correção.

Solicitar recomendações de grupo de atribuição para um item vulnerável

Solicitação Recomendações de atribuição de vulnerabilidade para que você possa exibir recomendações de grupo de atribuição. Você pode solicitar recomendações se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto para um item vulnerável (VI).

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** E abra um VI.
   O item deve estar no estado Aberto, Adiado, Em investigação ou Aguardando implementação.
2. Clique no ícone Recomendar ( ) ao lado de **Grupo de atribuição** Campo para sugestões de atribuição para esse VI.
3. Na caixa de diálogo Recomendações de grupo de atribuição, selecione uma recomendação baseada na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para o VI Para obter mais informações, consulte Soluções de aprendizado de máquina para Resposta a vulnerabilidades.
4. Clique em **Atribuir** .

Resultado

O grupo selecionado aparece em **Grupo de atribuição** E o Tipo de atribuição mudam para Recomendação.

Solicitar recomendações de grupo de atribuição para vários itens vulneráveis

Usar Recomendações de atribuição de vulnerabilidade Para exibir as recomendações do grupo de atribuição para vários itens vulneráveis (VIS) usando uma edição em massa. Quando vários VIS são selecionados, uma previsão é realizada em uma amostra aleatória dos VIS selecionados.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

As recomendações e suas pontuações de confiança podem diferir um pouco entre invocações, com base nas amostras coletadas do VIS selecionado. A pontuação de confiança avalia se o sistema está confiante de que o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade. Use `assignment_recommendation_batchsize` propriedade do sistema para definir o tamanho do lote quando você solicita Recomendações de atribuição de vulnerabilidade Para tarefas de correção (VULs) e VIS usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para desempenho de previsão ideal.

Nota: Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade para esses casos, pode mudar.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Item vulnerável** E selecione Vários VIS.
   Os itens devem estar no estado Aberto, Em investigação ou Aguardando implementação.
2. Clique em **Edição em massa** .
3. No formulário, preencha os campos.

Formulário Itens vulneráveis em massa

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição a ser definido para os itens vulneráveis selecionados. Para exibir os grupos de atribuição recomendados, clique no ícone Recomendar ( ) ao lado do campo. Selecione uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	recomendação baseada na pontuação de confiança e clique em **Atribuir** .
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.

Resultado
O grupo selecionado aparece em **Grupo de atribuição** E o Tipo de atribuição mudam para Recomendação para todos os VIS selecionados.

Solicitar recomendações de grupo de atribuição para uma tarefa de correção

Usar Recomendações de atribuição de vulnerabilidade Para exibir recomendações de grupo de atribuição para uma tarefa de correção (VUL).

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
Use `assignment_recommendation_batchsize` propriedade do sistema para definir o tamanho do lote quando você solicita Recomendações de atribuição de vulnerabilidade Para VULs e itens vulneráveis (VIS) usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para desempenho de previsão ideal.

Nota: Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade para esses casos, pode mudar.

Procedimento
1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** E selecione um VUL.
   O grupo deve estar no estado Aberto, Em investigação ou Aguardando implementação.
2. Clique no ícone Recomendar (ao lado de **Grupo de atribuição** Campo das recomendações do grupo de atribuição para o VUL selecionado.
   A caixa de diálogo Recomendações de grupo de atribuição exibe os grupos de atribuição recomendados com a pontuação de confiança média para todos os VIS nesse grupo.
3. Selecione uma recomendação na lista Grupo de atribuição com base na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para o VUL selecionado.
4. Clique em **Atribuir** .
   O grupo selecionado aparece em **Grupo de atribuição** campo.
5. Salve a tarefa de correção com as informações atualizadas.

Resultado
Todos os VIS com o mesmo grupo de atribuição que o VUL são atribuídos ao grupo de atribuição selecionado. O tipo de atribuição muda para Recomendação para o VUL, bem como todos os VIS modificados.

Solicitando e aprovando uma exceção

Você pode solicitar o adiamento da correção de um item vulnerável ou tarefa de correção por um período especificado. Por exemplo, como responsável pela correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode solicitar exceções do Resposta a vulnerabilidades Espaços de trabalho. Consulte Solicite uma exceção no Espaço de correção de problemas de TI.

- Solicite uma exceção para um item vulnerável
- Solicite uma exceção para uma tarefa de correção
- Solicite uma exceção em massa

Você também pode solicitar exceções de política usando GRC: Gestão de políticas e conformidade:

- Solicite uma exceção usando GRC: Gestão de políticas e conformidade
- Solicite uma exceção em massa usando GRC: Gestão de políticas e conformidade

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Solicite uma exceção para um item vulnerável

Solicite uma exceção para um item vulnerável (VI) que não pode ser corrigida imediatamente. Por exemplo, como responsável pela correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Importante: Você pode solicitar exceções do Gerenciador de vulnerabilidades e dos espaços de correção de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade e Solicite uma exceção no Espaço de correção de problemas de TI.

Você também pode solicitar exceções para VIS no ambiente clássico.

Nota:

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Tudo**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
3. No formulário Item vulnerável, clique em **Exceção de solicitação** .
4. Se Resposta a vulnerabilidades Estiver selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo reverte para o estado Aberto. **Nota:** A partir da versão 18,0 de Resposta a vulnerabilidades(VR), se um item vulnerável foi adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo scanner, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vul.auto_defer_vit_in_active_exception_win* verdadeiro. E adiado **Até** a data persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da solicitação. As opções são: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Redução do controle no local ○ Outro Para ver como adicionar novas opções de motivo, consulte Defina o mapeamento do motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser atualizado pelo responsável pela correção.

5. Envie a solicitação de exceção clicando em **Aprovação da solicitação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

O estado do item vulnerável muda para Em revisão. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicite uma exceção para uma tarefa de correção

Solicite uma exceção para adiar uma tarefa de correção por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Importante:

Você pode solicitar as exceções no Gerenciador de vulnerabilidades e nos espaços de correção de TI. Consulte Solicite uma exceção no Espaço de correção de problemas de TI.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções para tarefas de correção no ambiente clássico.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Tudo**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Em investigação ou Aguardando implementação.
3. No registro de tarefa de correção (VUL), selecione **Exceção de solicitação** .
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Solicite uma exceção em massa

Use a opção de edição em massa para solicitar uma exceção para vários itens vulneráveis (Vits) em vez de selecionar manualmente cada item.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Quando vários Vits são selecionados, uma tarefa de correção (VUL) é formada com esses itens. Consulte Edite itens vulneráveis em massa em Resposta a vulnerabilidades Para obter mais informações sobre como editar vários Vits.

Importante: Você pode solicitar uma exceção para:

- VIT do Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI. Para obter mais informações, consulte Solicite uma exceção no Espaço de correção de problemas de TI.
- Vários Vits do Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Tudo** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Em investigação ou Aguardando implementação.
2. Clique em **Edição em massa** .
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Motivo	Subestado para o Estado selecionado.
Descrição resumida	Nome da tarefa de correção que você está criando.
Até	Data de término especificada para sua solicitação de exceção.
Informações adicionais	Mais detalhes que você deseja mencionar para informar o aprovador sobre os motivos da sua solicitação.
Solução preferencial	Solução destinada a corrigir todos os itens vulneráveis que você selecionou para uma edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Você pode selecionar um grupo manualmente ou usar Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada contendo o VIS selecionado. Esta tarefa de correção foi enviada para aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma exceção usando GRC: Gestão de políticas e conformidade

Solicitar exceções de política usando GRC capacidade de gestão de exceções de política no Gestão de políticas e conformidade aplicação a partir de Resposta a vulnerabilidades.

Antes de Iniciar

Antes de usar a Integração de exceção de política para solicitar exceções de política, você deve baixar o. GRC: Gestão de políticas e conformidade aplicação do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** (ou **Tarefas de correção**)> **Todos** e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Exceção de solicitação** .
3. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começará. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e o estado do item vulnerável ou grupo muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** Que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

4. Clique em **Enviar**.
   Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma exceção em massa usando GRC: Gestão de políticas e conformidade

Selecione um grupo de itens vulneráveis e envie uma exceção em massa.

Antes de Iniciar

Antes de usar a Integração de exceção de política para solicitar exceções em massa, você deve baixar o. GRC: Gestão de políticas e conformidade aplicação do ServiceNow Store.

Nota: Para usar este recurso, você deve fazer upgrade GRC: Gestão de políticas e conformidade antes de atualizar Resposta a vulnerabilidades. Se você já fez upgrade Resposta a vulnerabilidades antes GRC: Gestão de políticas e conformidade e quiser usar este recurso, você deve executar os procedimentos de upgrade novamente na ordem correta.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções no ambiente clássico em Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Tudo** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Em investigação ou Aguardando implementação.
2. Clique em **Edição em massa** .
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Descrição resumida	Nome da tarefa que você está criando.
Solução preferencial	Solução que você está visando para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Você pode selecionar um grupo manualmente ou usar Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada com os itens vulneráveis selecionados.
5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começará. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e o estado do item vulnerável ou grupo muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** que você definiu para a política em GRC: Gestão de políticas e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

6. Clique em **Enviar**.
   Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Aprovar ou rejeitar uma solicitação de exceção em Resposta a vulnerabilidades

Aprove ou rejeite as solicitações de exceção para itens vulneráveis ou tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações de risco e aprová-las para adiamento até que possam ser corrigidas.

Importante:

Você pode aprovar ou rejeitar as solicitações de exceção no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Você também pode aprovar solicitações de exceção no ambiente clássico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Trabalhar com uma regra de exceção

Você pode solicitar uma exceção para vulnerabilidades, itens vulneráveis (VIS) ou itens de configuração (ICs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de VI, você pode adiar os VIS correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Crie uma regra de exceção
- Aprovar uma solicitação de regra de exceção
- Ativando uma regra de exceção
- Reabra uma regra de exceção
- Atualize uma regra de exceção aprovada
- Exclua uma regra de exceção

Nota:

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Crie uma regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica para um grupo de itens vulneráveis (VIS), como uma regra com uma condição baseada na gravidade da vulnerabilidade desses VIS. Com esta regra, você pode adiar os novos e existentes VIS automaticamente se eles corresponderem à condição de regra aprovada.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A regra é aplicada da data "Válido de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para este VUL é conhecido como regras de exceção. O VUL é criado no estado Adiado. Não é possível fechar, reabrir ou excluir este VUL. Vs novos e reabertos são adiados e adicionados a este VUL a partir da data "Válido de" até que o grupo expire na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Na página Novo registro de Regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário, preencha os campos.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.
Válida de	Data a partir da qual esta regra está ativa para adiar o VIS.
Válida até	Data a partir da qual a tarefa de correção para de aceitar novos VIS.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção que foi criada para rastrear o VIS adiado está atribuída.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição do filtro para o VIS que pode ser definido durante o processamento do VIS.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.
Estado	Estado da regra de exceção.
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando os VULs e VIS são adiados. Nesta data, o VUL criado é encerrado, todos os VIS são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	movidos para fora do grupo e as regras do grupo são reaplicadas.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.

Aprovar uma solicitação de regra de exceção

Avalie solicitações de regra de exceção de usuários para que você possa aprovar ou rejeitar essas solicitações.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Os membros do grupo de usuários de nível 1 do aprovador de exceção podem aprovar as solicitações de regra de exceção de nível 1. Da mesma forma, os membros do grupo de usuários de nível 2 do aprovador de exceção de nível podem aprovar as solicitações de regra de exceção de nível 2. Ambos os grupos de usuários herdam a função de aprovador de exceção por padrão.

Nota:

Se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com e explique por que você aprovou ou rejeitou a solicitação.
   Depois que uma regra de exceção é aprovada, uma tarefa de correção (RT) é criada no estado Adiado por padrão. A partir da data "Válido de", esta regra é executada em todos os VIS criados e também nos que são movidos do estado fechado para o estado aberto. Os VIS que correspondem às condições definidas são adicionados ao RT e adiados pelo período especificado.

   Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Ativando uma regra de exceção

Uma regra é ativada na data "Válido a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis (VIS).

A regra de exceção segue este ciclo de vida:

1. Os novos itens vulneráveis (VIS) que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar nos dados existentes ao executar a regra de exceção pela primeira vez, todos os VIS ativos e não adiados que

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correspondem à condição da regra de exceção serão movidos para a tarefa de correção (RT) recém-criada e seu estado será alterado para Adiado.

2. Se um VI recém-criado corresponder à condição da regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra de grupo não será executada nele.
3. Na data "Válido de", os VIS existentes serão adicionados se você habilitar a opção Executar nos dados existentes.
4. O RT para de aceitar novos VIS quando a regra expira na data "Válido até". O RT permanece existente até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Solicite uma extensão para uma regra de exceção

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até a qual a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas e itens vulneráveis. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.
- A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Reabra uma regra de exceção

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. Reabrir a regra a move para o estado Rascunho.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode atualizar e reenviar a regra para aprovação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Encontre a regra que você deseja reabrir e clique em **Reabrir** .
3. Atualize o formulário e envie-o novamente para aprovação.

Atualize uma regra de exceção aprovada

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de modificar datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis (vis) sejam movidos para o estado Aberto.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
As regras de grupo são reaplicadas a esses VIS. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação mais uma vez.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na caixa de diálogo Cancelar regra, clique em **Regra de cancelamento** .
   A regra retorna para o estado Rascunho e o VUL associado é excluído. Os VIS relacionados são reabertos e as regras de grupo são aplicadas aos VIS individuais.

Exclua uma regra de exceção

Exclua uma regra de exceção que não é mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável (VI) durante a ingestão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os VIS relacionados são reabertos e as regras de grupo são aplicadas aos VIS individuais.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir** .
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os VIS relacionados são reabertos e as regras de grupo são aplicadas aos VIS individuais.

Marcar e aprovar um falso positivo

Itens vulneráveis (VIS) e tarefas de correção (VULs) podem ser marcados como falsos positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

- Marcar como falso positivo
- Edição em massa para falso-positivo
- Aprovar ou rejeitar falso positivo

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma tarefa de VI ou correção é marcada como falso positivo, o solicitante recebe um e-mail de confirmação. Ao mesmo tempo, o aprovador recebe um e-mail informando que uma tarefa de VI ou correção foi marcada como falso positivo.

A partir de v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Marcar como falso positivo

Marque um item vulnerável (VI) ou tarefa de correção (VUL) como falso positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se um item de configuração tiver sido desativado, mas o scanner ainda estiver levantando um problema relacionado a ele, marque-o como falso positivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: Responsável pela correção

Você pode solicitar falsos positivos do Resposta a vulnerabilidades Espaços de trabalho. Consulte Solicite um falso positivo para um item vulnerável ou corrija a tarefa.

Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis (ou tarefas de correção)** > **Tudo**.
2. Abra o vi ou VUL que você deseja marcar como falso positivo e clique em **Marcar como falso positivo** .
   O vi ou VUL deve estar em um **Aberto** estado.
3. No formulário Falso positivo, insira os detalhes em **Informações adicionais** e clique em **Aprovação da solicitação** .
   A solicitação é enviada para aprovação e o Estado do VI ou VUL muda para **Em Revisão** .

Edição em massa para falso-positivo

Use a edição em massa para marcar vários itens vulneráveis (Vits) como falso-positivos. Se vários Vits forem selecionados, uma tarefa de correção será formada com esses itens.

Importante: Como administrador ou analista, você pode usar o recurso de edição em massa no Espaço do Gerenciador de vulnerabilidades para marcar vários Vits como falso-positivos. Para obter mais informações, consulte Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária: Responsável pela correção

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Tudo** e selecione os itens que você deseja marcar como falso positivo.
   Os itens selecionados devem estar no estado Aberto, Em investigação ou Aguardando implementação.
2. Clique em **Edição em massa** .
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Estado	Estado dos itens vulneráveis. Selecione Encerrado para marcar como falso positivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Motivo	Subestado do Estado selecionado. Se você selecionou Encerrado como o Estado, selecione Falso positivo aqui para marcar como falso positivo.
Cancelar atribuição	Envie uma solicitação para limpar os campos Atribuído a e Grupo de atribuição.
Solução preferencial	Solução direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Selecione Manualmente ou Usar recomendações de atribuição, se estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma nova tarefa de correção é criada contendo o VIS selecionado e esta tarefa é enviada para aprovação.

Aprovar ou rejeitar falso positivo

Como um aprovador falso positivo, você pode aprovar ou rejeitar solicitações falso positivo de outros usuários.

Importante:

Como um aprovador de falso positivo, você pode aprovar ou rejeitar as solicitações de falso positivo no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.false_positive_approver para itens vulneráveis
- sn_vul.app_false_positive_approver para itens vulneráveis à aplicação

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Nota: Um falso positivo pode ter um limite de tempo. Somente o aprovador pode definir a data de término.

Soluções de análise e emissão de relatórios para Resposta a vulnerabilidades

O monitoramento da correção de vulnerabilidades envolve a exibição de tendências, o gerenciamento de riscos e o monitoramento de grupos de atribuição. Você pode revisar problemas de alto risco, cargas de trabalho de grupo de atribuição, adiamentos e vulnerabilidades recorrentes. Resposta a vulnerabilidades oferece ferramentas, relatórios e procedimentos para tornar esse processo mais produtivo e eficiente.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Os analistas de vulnerabilidades também podem usar o padrão Resposta a vulnerabilidades painéis em **Tudo** > **Resposta a vulnerabilidades** > **Visão geral**.

Importante:

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel também pode ser exibido na IU da Nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e. Painéis no Espaço de correção de TI .

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Resposta a vulnerabilidades processo de correção

A maior parte da correção de vulnerabilidades é feita a partir do registro da tarefa de correção de no Resposta a vulnerabilidades Espaços de trabalho. Em Tarefas de correção (RTS) no estado Em investigação, você pode executar várias tarefas.

- Criar solicitações de mudança.
- Adicione anotações de trabalho e descrições de vulnerabilidades na tarefa de correção.
- Adie a tarefa de correção e os itens vulneráveis nela para uma data posterior.
- Feche a tarefa de correção.
- Rastreie novas obrigações de conformidade regulatória, que geralmente são urgentes.

- Faça login na sua instância Resposta a vulnerabilidades.
- Revise os painéis e relatórios da Gestão de vulnerabilidades e de terceiros para localizar áreas com problema. Por exemplo, exiba painéis que mostram o envelhecimento da tarefa de correção (RT) por estados ou itens vulneráveis de alto risco (VIS) após a data de destino de correção.
- Revise o estado das tarefas de correção, em ordem de risco.
- Revise a priorização das tarefas ajustando as calculadoras de pontuação de risco se a pontuação de risco não estiver sendo calculada corretamente ou adiando VIS ou RTS, conforme necessário. Consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade ou Adie uma tarefa de correção para obter mais informações sobre essas opções.
- Revise os itens vulneráveis adiados prestes a reabrir e tome medidas adicionais conforme necessário. Se você quiser iniciar e rastrear atividades de mudança em seus ativos, tarefas de correção e itens vulneráveis correspondentes, para obter mais informações, consulte Gestão de mudanças para Resposta a vulnerabilidades para outras ações.
- Revise o feedback das Operações DE TI.

  Depois de ser notificado de que uma solicitação de mudança foi resolvida, aguarde a próxima verificação. As verificações são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o estado for Corrigido, os itens vulneráveis serão encerrados automaticamente durante a importação. O grupo fecha quando todos os itens vulneráveis do grupo são corrigidos.
- Se o estado não for Corrigido, o VI será movido automaticamente de volta para Em investigação.

- Itens vulneráveis definidos como "Resolvido" em sua instância, mas não transferidos para "Encerrado/Corrigido" pelas execuções de integração de terceiros serão reabertos se forem detectados durante novas verificações.

  Para Qualys Detecções, se o scanner continuar a encontrar os VIS que foram definidos como "Resolvido", mas não foram transferidos para "Encerrado/Corrigido" por verificações subsequentes, esses VIS serão movidos de volta para "Aberto" quando a data da última descoberta for posterior à data de resolução.

  Para Rapid7 detecções, uma opção agora está disponível no Rapid7 Página de configuração em sua instância para reabrir os VIS resolvidos por idade. Se habilitado, os VIS definidos como "Resolvido", mas não transitam para "Encerrado/Corrigido" pelas verificações subsequentes, retornam para "Aberto" após o número de dias que você insere.

Solução de gestão de vulnerabilidade Andamento da implantação

Métricas de implantação abrangentes para tarefas de correção e entradas de vulnerabilidade estão incluídas em Solução de gestão de vulnerabilidade em **Status de correção** em vulnerabilidades, itens vulneráveis. Identifique facilmente qual tarefa de correção ou vulnerabilidade está atrasando o andamento da resolução. Detalhar como a vulnerabilidade é identificada ou quais aspectos dos ativos afetados podem estar causando o problema de correção. Atualize o status de suas métricas usando **Atualizar status** link relacionado nos formulários de vulnerabilidade, soluções e tarefa de correção.

Usando o padrão Resposta a vulnerabilidades painéis

. Resposta a vulnerabilidades O painel Visão geral (Gestão de vulnerabilidades) fornece uma visão executiva das vulnerabilidades e itens vulneráveis, ajudando o administrador de vulnerabilidades a identificar áreas de preocupação rapidamente. . Resposta a vulnerabilidades O painel de correção (Correção de vulnerabilidade) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços de trabalho, Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Os analistas de vulnerabilidades também podem usar o padrão Resposta a vulnerabilidades painéis.

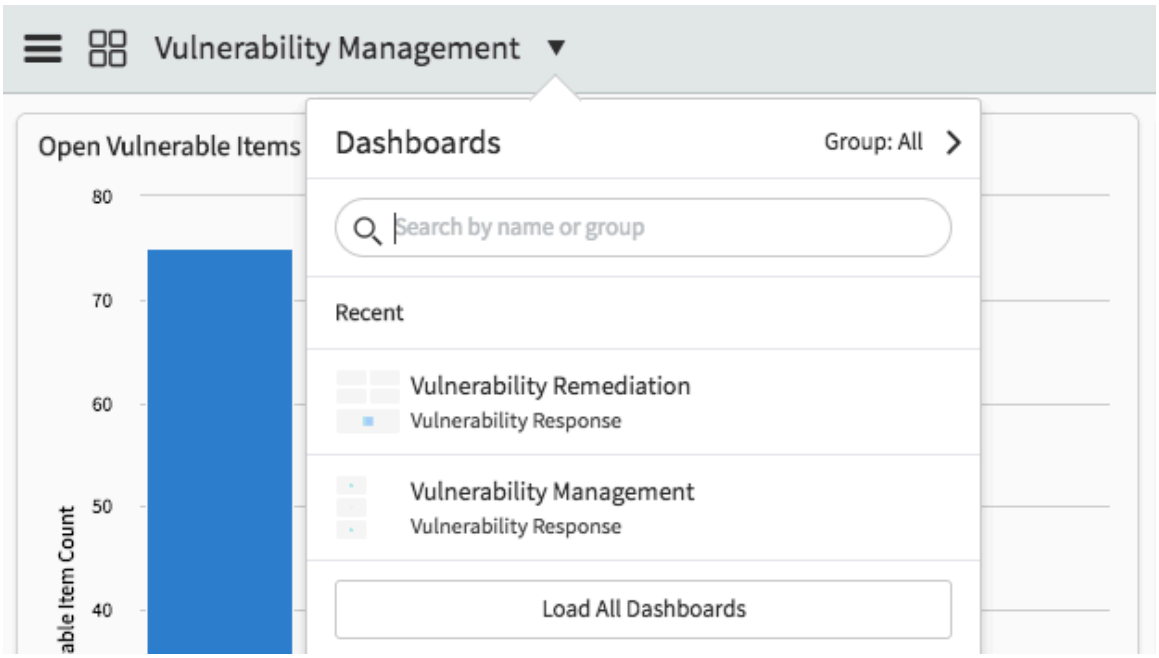
Funções necessárias: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O padrão Resposta a vulnerabilidades painéis no ambiente legado

Esses relatórios estão incluídos como parte do Performance Analytics para Resposta a vulnerabilidades e não exigem uma assinatura separada. Para abrir um, selecione a lista de seleção para expandi-la e escolha um painel. Como alternativa, insira o nome de um painel no campo de pesquisa.



Nota:

. Performance Analytics Pacote de conteúdo para Resposta a vulnerabilidades A aplicação é instalada e ativada, o painel Gestão de vulnerabilidades (PA) é exibido automaticamente no módulo Visão geral. Este painel contém relatórios que cobrem todas as fases do ciclo de vida da gestão de vulnerabilidades.

Para obter informações sobre os relatórios incluídos no Pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades, consulte Painel de Gestão de vulnerabilidades [PA] .

Para obter informações sobre o painel do CISO e os relatórios de cobertura de varredura, consulte Painel do CISO da Gestão de vulnerabilidades .

Painel da Gestão de vulnerabilidades

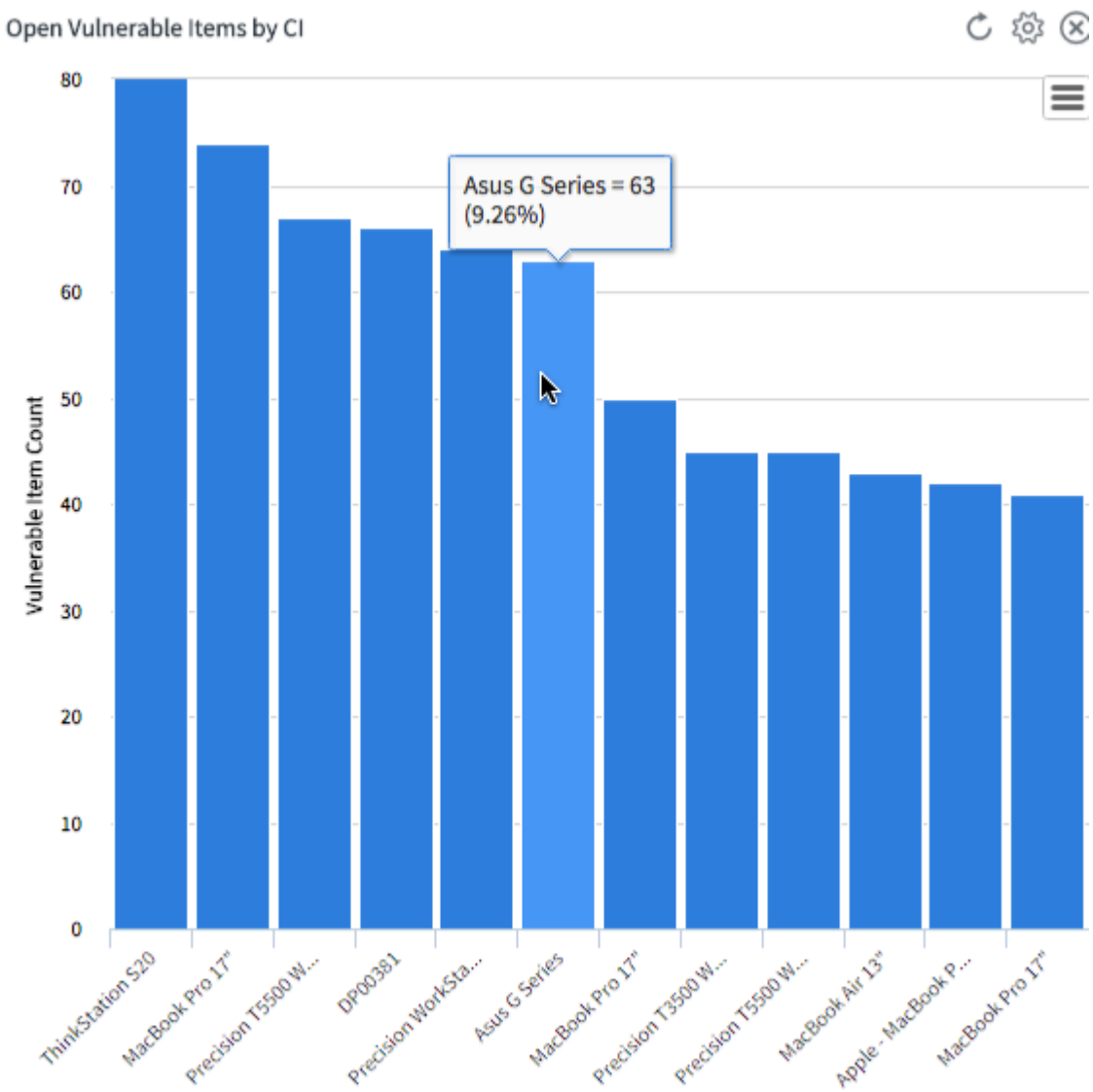
Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota:

Se painéis personalizados forem necessários, consulte Criar e usar painéis para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios de Visão geral da vulnerabilidade

Nome	Visual	Descrição
Itens vulneráveis abertos por IC	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada item de configuração (IC), do mais para o menos.
Itens vulneráveis por status da meta de correção	Barra	Exibe o número de itens vulneráveis que estão se aproximando do destino, em trânsito e no destino passado. **Nota:** Itens no estado Adiado, Resolvido ou Encerrado não são incluídos.
Itens vulneráveis adiados que expiram esta semana	Gráfico	Exibe o número de itens vulneráveis adiados programados para serem reativados em sete dias.
Itens vulneráveis abertos por vulnerabilidade	Barra	Exibe o número de itens vulneráveis em aberto para cada vulnerabilidade, da maior para a menor.
Vulnerabilidades por modelo	Barra	Exibe o número de itens vulneráveis registrados para cada modelo (classe de IC), do mais para o menos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de Visão geral da vulnerabilidade

Nome	Visual	Descrição
Vulnerabilidades por semana	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Modelos mais vulneráveis	Donut	Exibe modelos (classes de IC) com os itens mais vulneráveis.
Vulnerabilidades por fornecedor	Barra	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.
Vulnerabilidades por impacto	Barra	Exibe o número de entradas de vulnerabilidade para os tipos de rede afetados.
Fornecedores mais vulneráveis	Donut	Exibe fornecedores com os itens mais vulneráveis.
ICs mais vulneráveis	Donut	Exibe ICs com os itens mais vulneráveis.
Vulnerabilidades por pontuação	Barra	Exibe o número de entradas de vulnerabilidade por pontuações de vulnerabilidade.
Itens vulneráveis reabertos	Lista	Lista os itens vulneráveis reabertos e sua idade.
ICs mais vulneráveis por classe	Donut	Exibe ICs com os itens mais vulneráveis.
Idade do Item Vulnerável	Lista	Lista o número de dias desde que os itens vulneráveis foram abertos pela última vez.
ICs com vulnerabilidade por data	Lista	Lista os itens de configuração que foram verificados nos últimos 30 dias.
ICs não verificados	Lista	Lista itens de configuração que nunca foram verificados quanto a vulnerabilidades.

Painel de correção de vulnerabilidade

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

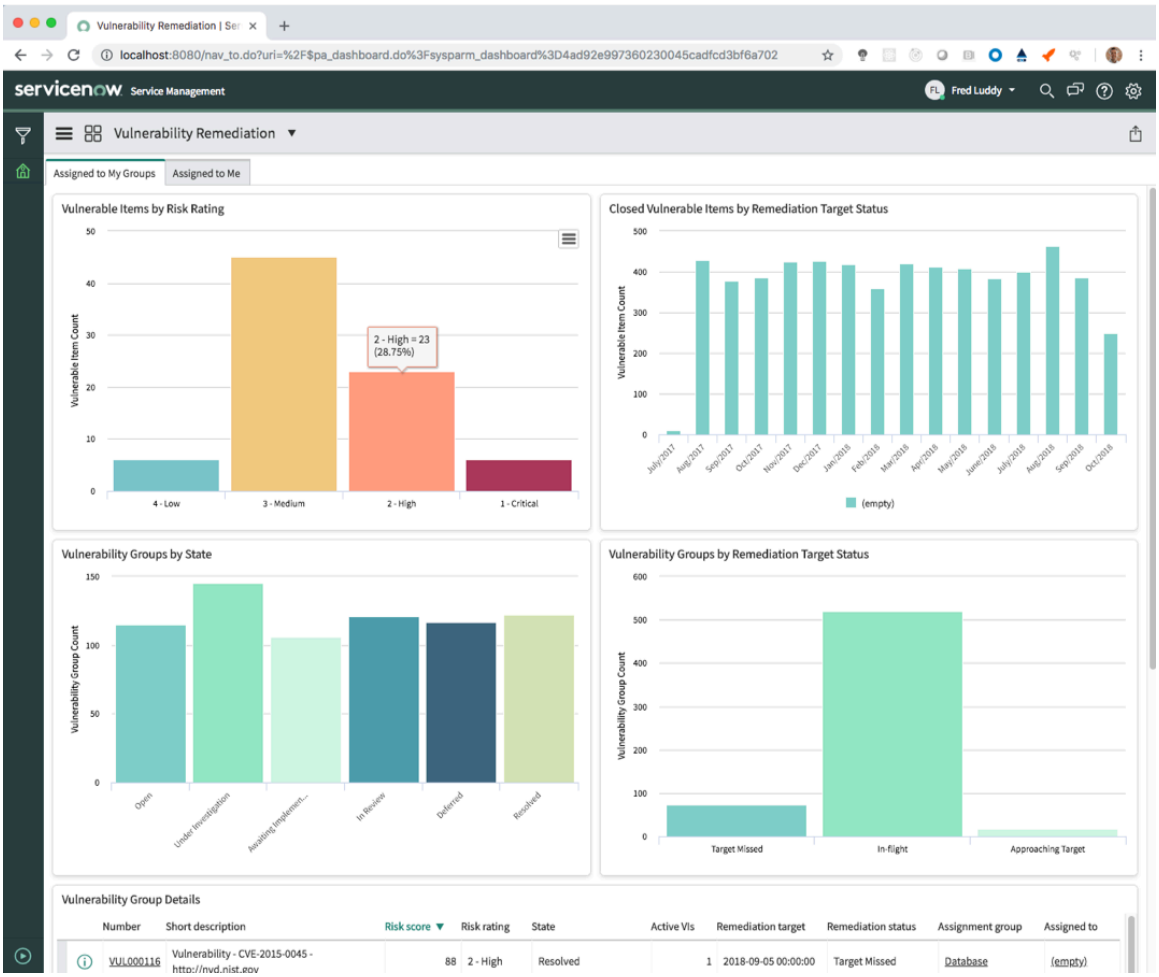
O painel Correção de vulnerabilidades contém as seguintes guias: **Atribuído a Meus grupos** , **Atribuído a mim** e **Solicitado por mim** . As guias Atribuído aos Meus grupos e Atribuído a mim mostram os mesmos relatórios. A guia anterior relata os grupos de atribuição aos quais você pertence e a última por itens vulneráveis ou tarefas de correção atribuídas a você. A guia Solicitado por mim relata os falsos positivos e as exceções solicitadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Painel de correção de vulnerabilidade



Tradução automática

Relatórios

Atribuído a Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Itens vulneráveis por classificação de risco	Barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.
Itens vulneráveis encerrados por status da meta de correção	Barra	Número de itens vulneráveis encerrados, agrupados por status da meta de correção no período selecionado.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuído a Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Tarefas de correção por estado	Barra 	Número de tarefas de correção ativas (RTS) agrupadas por estado.
Tarefas de correção por status do meta de correção	Barra 	Número de RTS ativos agrupados por status de destino de correção. Este relatório exclui itens vulneráveis adiados.
Detalhes da tarefa de correção	Lista 	Detalhes do registro da tarefa de correção em uma lista.

Solicitado por mim

Nome	Visual	Descrição
Status solicitações de falso-positivo e de exceção	Barra 	Número de solicitações ativas enviadas por você.
Tarefas de correção de falso-positivo e adiadas expirando	Barra 	Número de tarefas de correção adiadas e falso-positivas (RTS), agrupadas por até a data.

Painel Aprovações de vulnerabilidades

O painel Aprovações de vulnerabilidade contém os seguintes relatórios para aprovadores de exceção e falso-positivos.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Nome	Visual	Descrição
Solicitações de falso-positivo e exceção por idade com minha aprovação pendente	Barra 	Número de aprovações pendentes para você, agrupadas por data de criação.
Minha aprovação, exceção rejeitada e solicitações falso-positivo	Barra	Número de solicitações de aprovação aprovadas ou rejeitadas, agrupadas por estado de aprovação.
Todas as Tarefas de correção por classificação de risco com aprovação pendente	Barra 	Número de tarefas de correção com aprovação pendente, agrupadas por classificação de risco.
Todas as solicitações de aprovação de falso positivo e pendentes agrupadas por motivo	Barra 	Número de solicitações de aprovação pendentes agrupadas por motivo.

Soluções para Análise da plataforma e relatórios Para Gestão de vulnerabilidades

Soluções para Análise da plataforma e relatórios contém pré-empacotado Performance Analytics e. Emissão de relatórios conteúdo para uso com outros ServiceNow AI Platform produtos. Esta Solução de análise e emissão de relatórios permite rastrear o volume, o desempenho e o andamento das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

. Performance Analytics para Resposta a vulnerabilidades o pacote de conteúdo não é instalado automaticamente com Resposta a vulnerabilidades aplicação. Está disponível no ServiceNow Store como uma assinatura separada.

Performance Analytics para Resposta a vulnerabilidades contém dois painéis:

- Painel de Gestão de vulnerabilidades (PA)
- Painel do diretor de segurança da informação (CISO) da Gestão de vulnerabilidades

Instalação e exibição dos painéis necessários

As seguintes funções e tarefas estão associadas a esta Solução:

- ServiceNow AI Platform Administrador (administrador): Instale e ative esta Solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Para instalar esta aplicação, consulte Instale e configure a aplicação Performance Analytics for Vulnerability Response [PA] .

Nota: Configure e teste Soluções de análise e emissão de relatórios em uma instância de não produção antes de habilitá-las na produção.

As Soluções de análise e relatório fornecem todos os registros de configuração necessários para analisar as aplicações padrão. Personalize esses registros para uso em seu ambiente de produção.

Para exibir o painel de Gestão de vulnerabilidades (PA), navegue até **Resposta a vulnerabilidades** > **Visão geral** > **.**

Para exibir o painel de CISO da Gestão de vulnerabilidades, navegue até **Resposta a vulnerabilidades** > **Painel do CISO** > **.**

Termos principais

Análise de desempenho (PA)

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde às principais perguntas de negócios para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável (VI)

Uma vulnerabilidade de segurança relatada por um verificador de vulnerabilidades de terceiros que está presente em um item de configuração (IC).

Tarefa de correção

As tarefas de correção são criadas e atribuídas automaticamente às equipes DE TI com base no grupo associado aos itens vulneráveis em um esforço de correção. As equipes DE TI e os responsáveis pela correção exibem as tarefas de correção no Espaço de correção de TI. Consulte Resposta a vulnerabilidades Espaços de trabalho para obter mais informações

.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador de PA

Define uma medição de desempenho realizada em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, Itens vulneráveis críticos atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, VI Ativo.

Exiba visualizações de dados em tempo real

Para ver o que está acontecendo hoje com os itens mais críticos em seu Resposta a vulnerabilidades, Você pode exibir determinados relatórios no painel Gestão de vulnerabilidades (PA) em tempo real. Exibir esses relatórios em tempo real ajuda a gerenciar seus itens vulneráveis (VIS) mais importantes e corrigi-los rapidamente. Você pode exibir os seguintes relatórios em tempo real:

- Guia Visão geral - Itens vulneráveis por grupo de atribuição
- Guia ICs vulneráveis
  - ICs (Itens de configuração) vulneráveis sem responsáveis
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções
  - Itens vulneráveis adiados por motivo
  - Solicitações de adiamento prestes a expirar
  - Itens vulneráveis adiados pelo gerente de CIO
- Guia Correção - Itens vulneráveis não atribuídos

Para obter mais informações, consulte Exiba relatórios do Performance Analytics para Resposta a vulnerabilidades [PA] em tempo real .

Gestão de vulnerabilidade CISO painel

Com Gestão de vulnerabilidade CISO Exiba dados como principais métricas de desempenho (KPIs) para correção de vulnerabilidades, veja os riscos mais altos, verifique a cobertura da verificação e saiba como reduzir os riscos.

Funções necessárias de ServiceNow AI Platform

- sn_vul.vulnerability_ciso para exibir o painel.
- sn_vul.ciso_write para editar o painel.

Ativando o painel do CISO

Para ativar o painel do CISO, você deve instalar o Performance Analytics para Resposta a vulnerabilidades E ativam o trabalho correspondente do Performance Analytics. Para obter mais informações, consulte Soluções de análise e emissão de relatórios para resposta a vulnerabilidades .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos de uso

Usuário	Uso do painel
CISOs (Chief Information Security Officers, diretores de segurança da informação)	CISOs (Chief Information Security Officers, diretores de segurança da informação) podem usar o painel do CISO para obter informações sobre o programa de gestão de vulnerabilidades de suas organizações. O painel fornece dados para ajudá-los a identificar rapidamente os dados como eles podem usar para reduzir as vulnerabilidades em seus ambientes.

Usando o painel do CISO

Os usuários executivos, como os diretores de segurança da informação (CISOs) em sua organização, podem exibir o painel do CISO para Resposta a vulnerabilidades para entender a eficácia do programa de gestão de vulnerabilidades. Você pode exibir o painel do CISO navegando até **Resposta a vulnerabilidades** > **Painel do CISO**. Use os filtros de nível superior para filtrar relatórios por classificação de risco, faixa etária ou voltados para a Internet. Alguns relatórios exibem dados de tendências durante um período de tempo. Você pode exibir a tendência das métricas importantes regularmente, analisar o risco geral à segurança dos negócios e identificar as áreas que precisam de melhoria.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel também pode ser exibido na IU da Nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e. Painéis no Espaço de correção de TI .

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Executando os trabalhos agendados

Execute os trabalhos agendados nesta ordem para atualizar os dados nos relatórios:

1. Atualizar tabelas do painel
2. [PA VR] PAINEL DO CISO

Trabalhos agendados para o painel do CISO

Nome do trabalho agendado	Descrição
Atualizar tabelas do painel	Trabalho agendado diariamente que você deve executar antes do trabalho Painel do CISO [PA VR] para que você possa coletar os dados do CISO. Ao executar este trabalho agendado, você atualiza os relatórios de cobertura de varredura. As informações atualizadas incluem os itens de configuração operacional (ICs) que são verificados nos últimos 90

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos agendados para o painel do CISO

Nome do trabalho agendado	Descrição
	dias, suas classes e o número total de ICs operacionais que correspondem a essas classes. Executar este trabalho agendado atualiza os relatórios no **Ações recomendadas** também. **Nota:** ICs operacionais se referem aos ICs que têm um status operacional como Operacional .
[PA VR] PAINEL DO CISO	Depois que o trabalho agendado Atualizar tabelas do painel estiver concluído, execute este trabalho agendado para preencher todos os relatórios no **Visão geral do CISO** guia.

Guias do painel do CISO

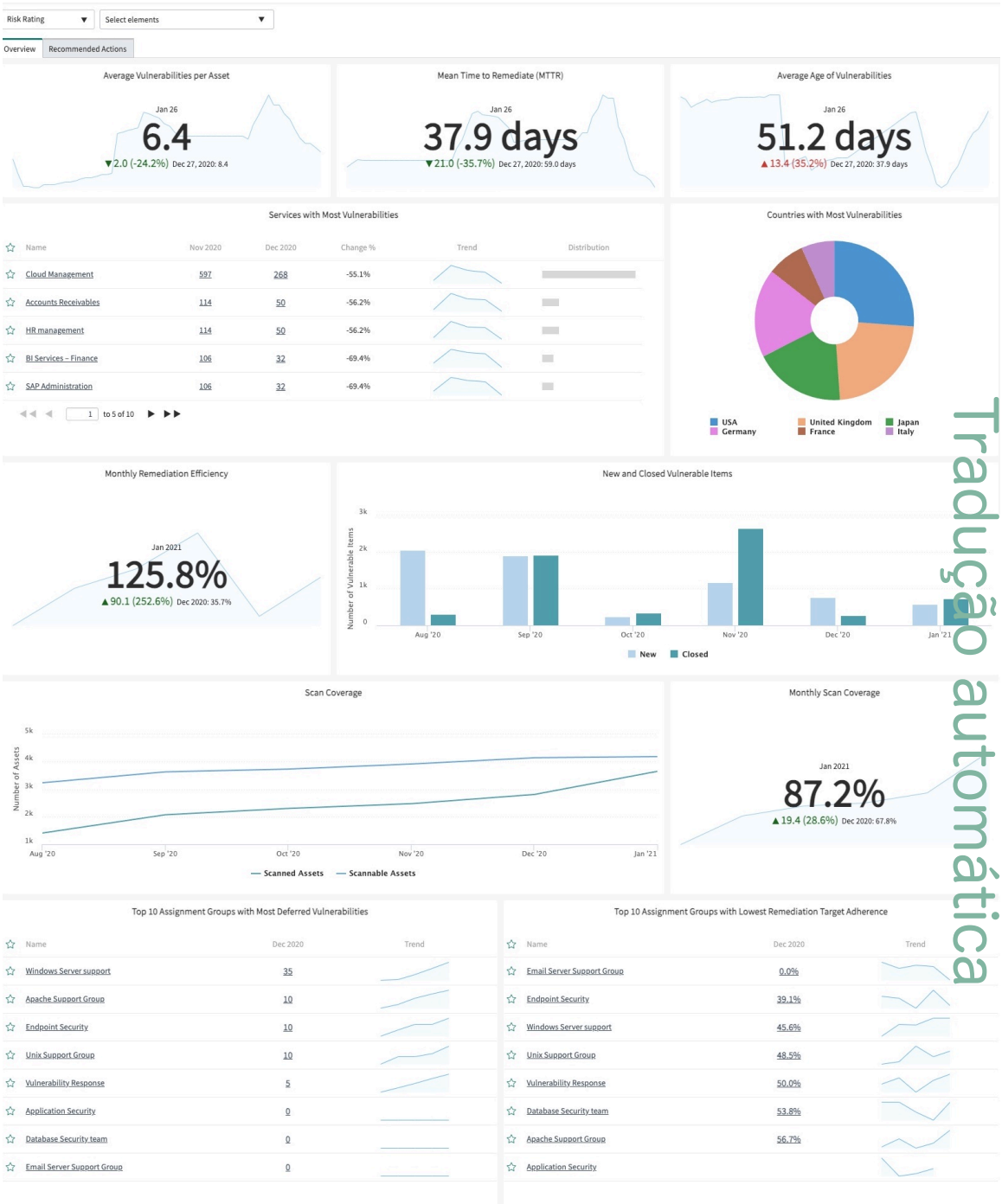
Este painel fornece informações sobre os riscos presentes na Gestão de vulnerabilidades. Você pode exibir vulnerabilidades e seus dados relacionados por região, idade, serviços e outros detalhamentos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia "Visão geral"

A guia Visão geral contém relatórios que fornecem rapidamente a postura de segurança da sua organização.



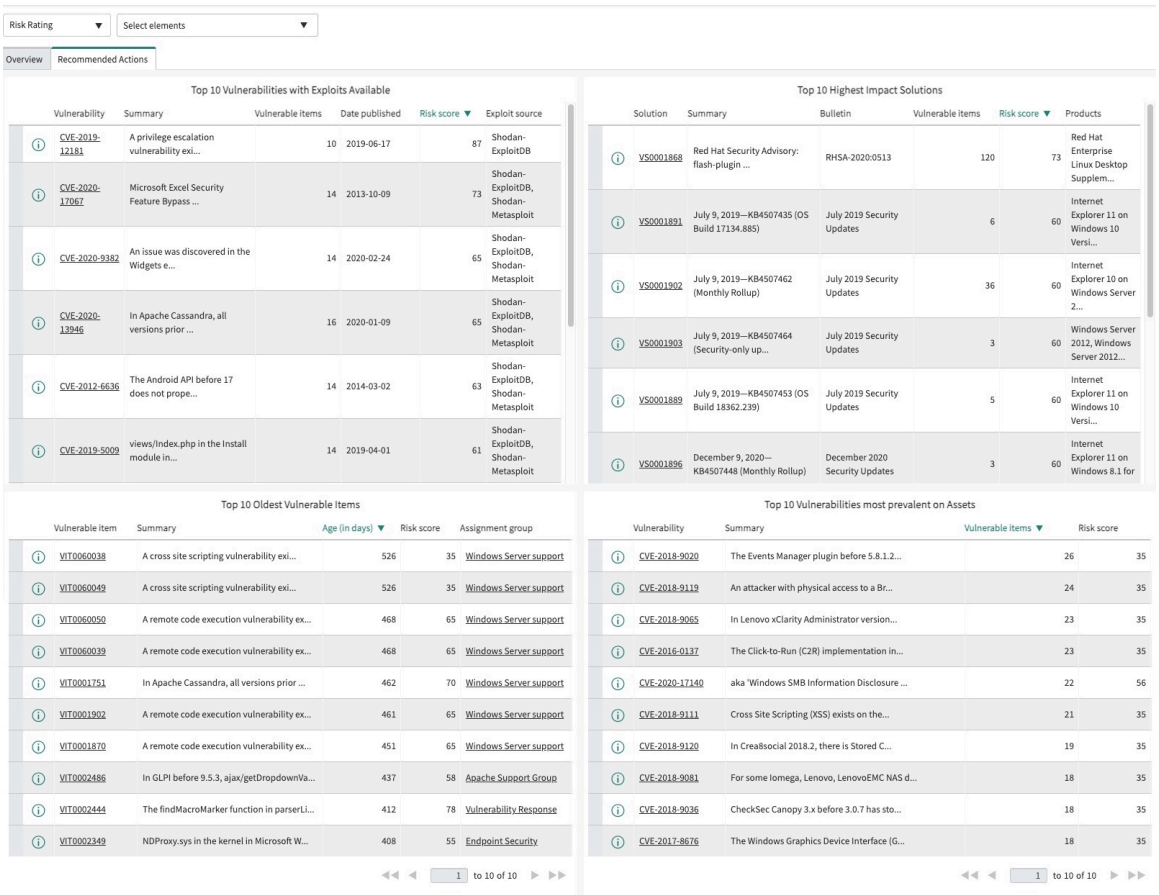
Nota: O filtro de nível superior só pode ser usado para alguns relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Ações recomendadas

A guia Ações recomendadas contém relatórios que fornecem informações sobre vulnerabilidades exploráveis, antigas e prevalentes. Ele também contém soluções que recomendam ações para reduzir os riscos. Execute o. **Atualizar tabelas do painel do CISO** trabalho agendado para atualizar os relatórios nesta guia.



Indicadores

Para exibir os indicadores, navegue até **Performance Analytics** > **Indicadores**.

1. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
2. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros marcando a caixa de seleção Coletar registros.

Duração total de itens vulneráveis encerrados

A duração total do VIS encerrado é medida diariamente como Dias. O objetivo desse indicador é minimizar a pontuação.

Ativos verificáveis

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo desse indicador é maximizar a pontuação.

Serviços com mais vulnerabilidades

Serviços com mais vulnerabilidades são medidos diariamente em unidades numéricas. O objetivo desse indicador é minimizar a pontuação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades médias por ativo

[[Itens vulneráveis ativos]] / [[Itens de configuração vulneráveis ativos]

Itens vulneráveis encerrados

Itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo desse indicador é maximizar a pontuação.

Tempo médio de correção dos itens vulneráveis

[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]

Cobertura de verificação atual

Calcula a cobertura de varredura atual em porcentagem.

Ativos verificados

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo desse indicador é maximizar a pontuação.

Itens vulneráveis encerrados (meta atingida)

Itens vulneráveis encerrados (meta atingida) são medidos diariamente em unidades numéricas. O objetivo desse indicador é maximizar a pontuação.

Percentual de itens vulneráveis encerrados que cumpriram a meta

[[Itens vulneráveis encerrados (Meta atingida) / SOMA por mês]] / [[Itens vulneráveis encerrados / SOMA por mês]] *100

Itens vulneráveis ativos

Itens vulneráveis ativos são medidos diariamente em unidades numéricas. O objetivo desse indicador é minimizar a pontuação.

Idade média dos itens vulneráveis

A Idade Média do VIS Ativo é medida diariamente em unidades Dias. O objetivo desse indicador é minimizar a pontuação.

Nota: Personalizar o cálculo de Idade e Idade de encerramento para Itens vulneráveis (VIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade fechada para VIS, consulte KB1703270 artigo da base de conhecimento.

Itens de configuração vulneráveis ativos

ICs vulneráveis ativos são medidos diariamente em unidades numéricas. O objetivo desse indicador é minimizar a pontuação.

Eficiência de correção mensal

[Número de itens vulneráveis encerrados durante um mês] / [Número de itens vulneráveis novos ou reabertos no mesmo mês]

Novos itens vulneráveis

Novos itens vulneráveis são medidos diariamente em unidades numéricas. O objetivo desse indicador é minimizar a pontuação.

Itens vulneráveis adiados

O VIS adiado é medido diariamente em unidades numéricas. O objetivo desse indicador é minimizar a pontuação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhamentos

- Grupo de atribuição: Aplica-se a alguns relatórios de VI.
- Classificação de risco: Aplica-se a relatórios de VI.
- Faixa etária: Aplica-se a relatórios de VI.
- Encerrado: Aplica-se a relatórios para VIS encerrados.
- Voltado para a Internet: Indica se o IC pertence à classe de hardware e é voltado para a Internet.
- Região: O parâmetro de IC do CMDB usado é Local. Este local indica o país de origem do item de configuração.

Nota: Personalizar o cálculo de Idade e Idade de encerramento para Itens vulneráveis (VIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade fechada para VIS, consulte KB1703270 artigo da base de conhecimento.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades médias por ativo	Pontuação única	Número médio de itens vulneráveis ativos para cada item de configuração.
Tempo médio para correção (MTTR)	Pontuação única	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução. **Nota:** O valor de Idade Encerrada é calculado quando os dados são coletados. O valor é a diferença entre a data da última abertura e a data e hora do trabalho de coleta.
Idade média das vulnerabilidades	Pontuação única	Idade média dos itens vulneráveis ativos em dias.
Serviços com mais vulnerabilidades	Lista e Linha	Média mensal de itens vulneráveis ativos para serviços na empresa. **Nota:** Para obter informações sobre como definir as classificações de serviço que você deseja exibir nos relatórios de Resposta a vulnerabilidades e nas listas relacionadas, consulte a guia Serviços em Painel de Gestão de vulnerabilidades [PA] .
Países com mais vulnerabilidades	Donut	Principais 10 países com o maior número de itens vulneráveis.
Eficiência de correção mensal	Pontuação única	Percentual de itens vulneráveis encerrados dividido por novos itens vulneráveis no mês atual.
Itens vulneráveis novos e encerrados	Barra	Número de novos itens vulneráveis importados e número de itens vulneráveis encerrados em um mês.
Cobertura de verificação	Linha	Número de ativos verificados em comparação com o número total de ativos verificáveis, mostrados ao longo do tempo. As classes de IC incluídas no widget são especificadas no módulo Configuração de cobertura de verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		Para obter informações sobre como configurar o módulo Cobertura de varredura, consulte Configure os relatórios de cobertura de varredura .
Cobertura de verificação mensal	Pontuação única	Percentual de ativos verificados dividido pelo número total de ativos verificáveis para o mês atual. Para obter informações sobre como configurar o módulo Cobertura de varredura, consulte Configure os relatórios de cobertura de varredura
10 principais grupos de atribuição com vulnerabilidades mais adiadas	Lista e Linha	Os 10 principais grupos de atribuição com o maior número de itens vulneráveis adiados, adiados com base na média mensal.
10 principais grupos de atribuição com menor adesão à meta de correção	Lista e Linha	Os 10 principais grupos de atribuição cujos itens vulneráveis têm a menor adesão aos destinos de correção.

Ações recomendadas

Nome	Tipo	Tabela de origem	Descrição
10 principais vulnerabilidades com explorações disponíveis	Lista	Item principal da vulnerabilidade [sn_vul_analytics_top_item]	Vulnerabilidades ativas com explorações disponíveis para todos os fornecedores de inteligência contra ameaças que usam a estrutura de exploração de VR.
Principais 10 soluções de maior impacto	Lista	Item principal da vulnerabilidade [sn_vul_analytics_top_item]	Patches ou soluções preferenciais com as pontuações de risco mais altas para itens vulneráveis ativos. Este relatório usa os recursos do Vulnerability Solution Management (VSM), que correlaciona patches da Microsoft e da Red Hat a vulnerabilidades no ambiente. O VSM ajuda a identificar a solução preferencial para vulnerabilidades.
Principais 10 itens vulneráveis mais antigos	Lista	Item principal da vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos com a idade mais alta. Resolva esses itens para reduzir a idade média da vulnerabilidade na guia Visão geral.
Principais 10 vulnerabilidades mais prevalentes em ativos	Lista	Item principal da vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos disponíveis para o maior número de ativos.

Configure os relatórios de cobertura de varredura

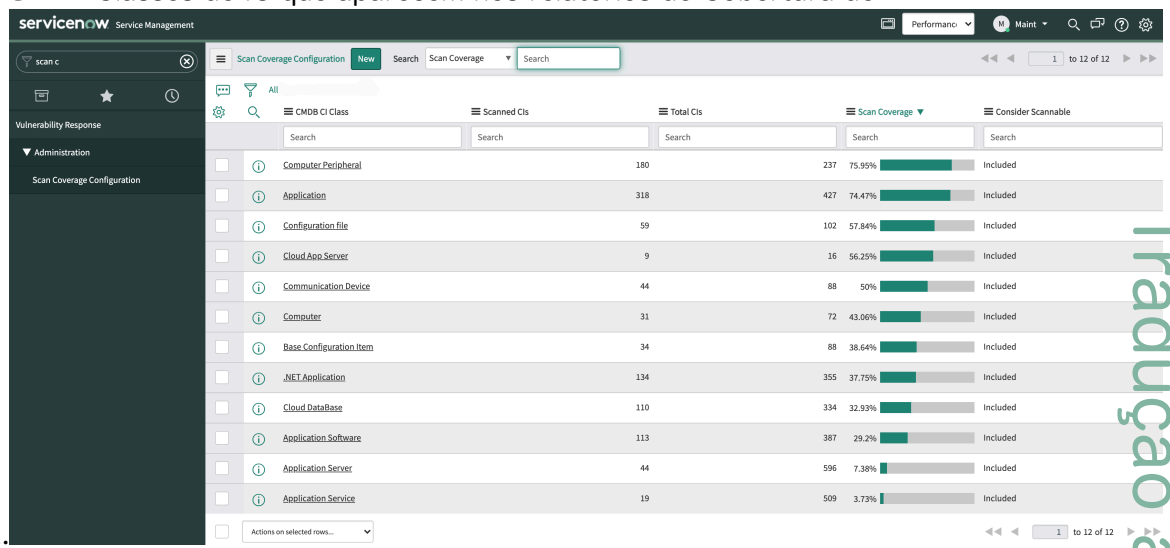
Permita que os usuários executem relatórios de cobertura de varredura no painel do CISO. Com esses relatórios, seus usuários podem ver qual é a cobertura de verificação da organização durante um período de tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Por Que e Quando Desempenhar Esta Tarefa
A cobertura de verificação mostra o número de ativos que estão sendo verificados pelos verificadores de vulnerabilidades para as várias classes nos últimos 90 dias. Esses ativos são comparados com o número de ativos verificáveis no Configuration Management Database (CMDB). Por padrão, o módulo Configuração de cobertura de varredura inclui CMDB Classes de IC, às quais pelo menos um ativo verificado foi correspondido. Você pode adicionar uma classe de IC do CMDB Para o relatório Cobertura de varredura que é exibido no painel do CISO. Você pode incluir ou excluir CMDB Classes de IC que aparecem nos relatórios de Cobertura de varredura.



Procedimento
1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configuração de cobertura de verificação**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de cobertura de varredura

Campo	Descrição
Classe de IC do CMDB	Classe de IC que deve ser adicionada ao Relatório de cobertura de varredura no painel do CISO. **Nota:** Se uma classe de IC já existir no módulo Configuração de cobertura de varredura, ela não será incluída nesta lista.
Considerar verificável	Opção para definir se a classe de IC deve ser incluída ou não. Inclua uma classe de IC se quiser que os dados sejam adicionados aos relatórios de cobertura de varredura. Se excluídos, os dados dessa classe de IC não serão adicionados.

4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure os indicadores de PA para o Painel do CISO

Monitore os indicadores de CISO automatizados e formulados para que você possa gerenciar os dados de vulnerabilidade em sua instância.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades tem indicadores automatizados e formulados.

Termos principais

Indicador

Define uma medição de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional. Um exemplo é um Item vulnerável ativo.

Fonte do indicador

Conjuntos de dados que consistem em registros filtrados de uma tabela ou exibição de banco de dados para aumentar a eficiência. Um exemplo é VI.Ativo (voltado para a Internet).

Detalhamentos

Filtro de detalhamentos e agrupar pontuações de indicador usando atributos qualitativos, como Prioridade, Categoria e Grupo de atribuição.

Trabalhos agendados

Os trabalhos agendados são executados para preencher os dados de origem do indicador. O trabalho programado diário do Painel de CISO do [PA VR] está desabilitado por padrão. Você deve ativá-lo para coletar pontuações de indicador para o painel do CISO.

Procedimento

1. Navegar até **Tudo** > **Performance Analytics** > **Indicadores** e escolha uma das seguintes opções:
   - Indicadores Automatizados
   - Indicadores de Fórmula

   Para obter mais informações sobre indicadores, consulte Indicadores do Performance Analytics .
2. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
3. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

   Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros selecionando **Coletar registros** caixa de seleção.

   Nota: Ativar Coletar registros em um indicador pode causar problemas de desempenho, como levar muito mais tempo e memória necessária para executar o trabalho de coleta de dados.

   O número máximo de linhas que você pode buscar para uma origem de indicador é 1,000,000.

Painel Integridade de resposta a vulnerabilidades SecOps

O painel Integridade de resposta a vulnerabilidades é uma ferramenta projetada para capacitar as organizações com informações abrangentes sobre a implementação e o uso de suas aplicações de resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A avaliação de integridade geral é determinada pela agregação de vários fatores críticos em configuração, implementação, integração, desempenho, dados, e processo. Exiba o painel agregado para cada categoria das seguintes aplicações:

- Resposta a vulnerabilidades
- Resposta a vulnerabilidades de aplicações
- Resposta a vulnerabilidades do contêiner
- Conformidade da configuração

Instalando o Painel de integridade de resposta a vulnerabilidades SecOps

Para instalar e configurar o Painel de integridade de resposta a vulnerabilidades SecOps para Resposta a vulnerabilidadesaplicações em seu ServiceNow AI Platform, navegue até ServiceNow® Store E ative o plug-in SecOps Health Analytics (sn_sec_analytics).

Funções necessárias de ServiceNow AI Platform

Funções necessárias: sn_sec_analytics.admin, sn_sec_analytics.read

Trabalho programado

Para exibir o trabalho agendado, navegue até **Tudo** > **Scheduler do Sistema** > **Trabalhos agendados** > **Colete métricas do painel de integridade**. O trabalho programado "Coletar métricas do painel de integridade" é executado diariamente às 00:00 horas. Ele gera os dados para o painel Integridade de resposta a vulnerabilidades SecOps. Você também pode optar por executar o trabalho agendado manualmente.

Casos de uso

Para obter exemplos de como as pessoas em sua organização usariam este painel, consulte estes casos de uso.

Usuário	Uso do painel
Administrador de vulnerabilidades	Ajuda a entender a pontuação de integridade do Resposta a vulnerabilidades aplicações. Também é útil destacar as áreas que precisam de melhorias. O Painel de integridade de resposta a vulnerabilidades lida somente com a integridade da implementação e do uso. Ele não ajuda no gerenciamento de vulnerabilidades ou ativos.
Administrador do suporte	Ajuda a identificar os problemas de desempenho, personalização e configuração usando KPIs. Com base na integridade da aplicação, você pode executar uma análise extra ou fornecer uma recomendação aos usuários.
Parceiro de implementação	Ajuda você a avaliar Resposta a vulnerabilidades integridade da implementação para configurações, complementos, personalizações e integrações e fornece recomendações de melhoria para os usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

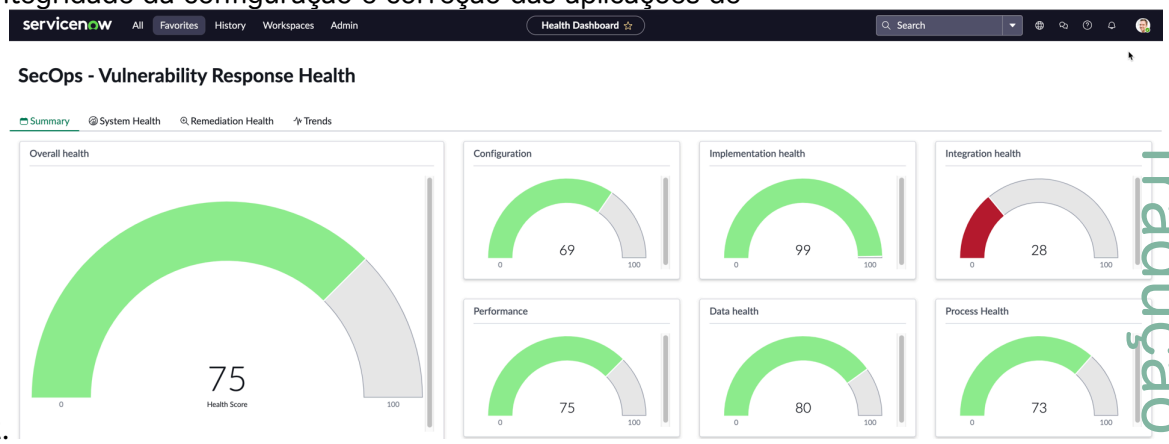
As guias do Painel de integridade de resposta a vulnerabilidades SecOps

Para exibir o painel Integridade de resposta a vulnerabilidades do SecOps, navegue até **Integridade do Security Operations** > **Integridade da Resposta a vulnerabilidades**. Cada cor no painel representa o seguinte:

- Verde: Seguro
- Amarelo: Aviso
- Vermelho: Crítico

Guia Resumo

Este painel comunica a pontuação de integridade geral para a integridade da configuração e correção das aplicações de VR.

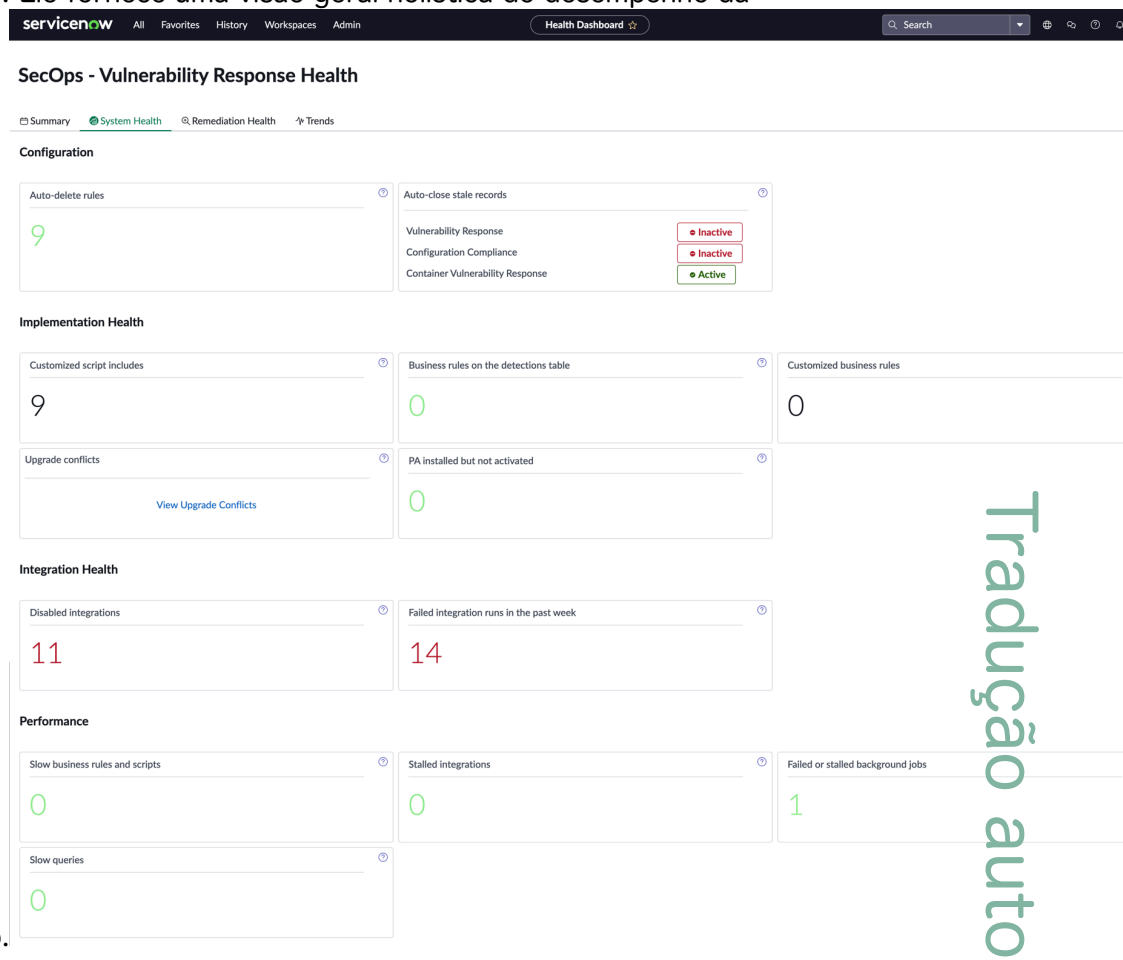


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Integridade do sistema

Este painel exibe a configuração e a integridade da integração da sua implementação. Ele fornece uma visão geral holística do desempenho da implementação.

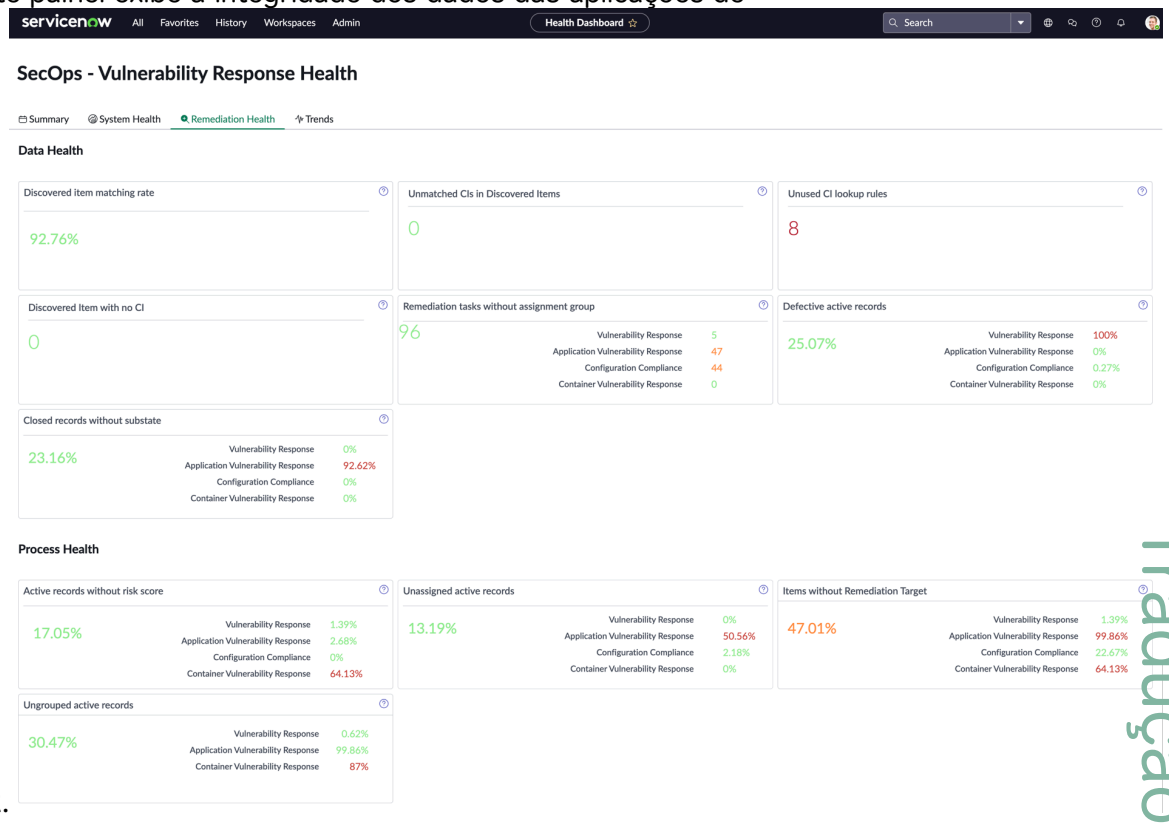


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

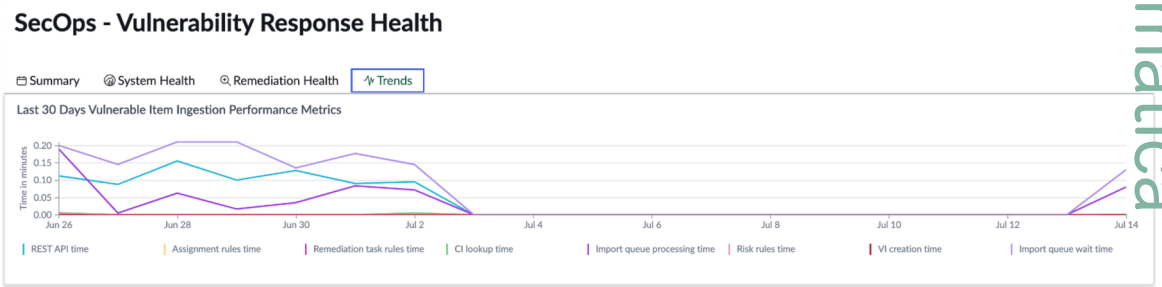
Guia Integridade da correção

Este painel exibe a integridade dos dados das aplicações de VR.



Guia Tendências

Este painel exibe as tendências das métricas de desempenho de ingestão de item vulnerável nos últimos 30 dias para as aplicações de VR.



Relatórios

Nota: Os valores de limite fazem parte do sistema de base. Você pode configurar os valores com base em seus requisitos.

Resumo

Título	Descrição
Integridade geral	Pontuação geral de integridade das aplicações de VR. Para obter mais informações, consulte os relatórios das métricas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo

Título	Descrição
Configuração	Integridade geral da configuração das aplicações de VR.
Integridade da implementação	Integridade geral da implementação das aplicações de VR.
Integridade da integração	Integridade geral da integração das aplicações de VR.
Desempenho	Pontuação geral de integridade do desempenho das aplicações de VR.
Integridade dos dados	Integridade geral dos dados das aplicações de VR.
Integridade do processo	Pontuação geral de integridade do processo das aplicações de VR.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Configuração				
Regras de exclusão automática	Exibe o número de regras de exclusão automática habilitadas.	Revise e resolva as regras de exclusão automática inativas.	3	1
Fechar automaticamente registros obsoletos	Fecha detecções obsoletas automaticamente. Para obter mais informações, consulte o tópico "Fechar detecções obsoletas automaticamente no Vulnerability Response" em servicenow.com/docs.	Reduza o volume de detecções obsoletas. Habilite esta opção para fechar as detecções obsoletas que não são encerradas pelos scanners.	3	1
Integridade da implementação				
Inclusões de script personalizadas	Número de "inclusões de script" personalizadas.	Minimize "inclusões de script" personalizadas para upgrades mais fáceis.	10	12
Regras de negócio na tabela de detecções	Número de regras de negócios personalizadas na tabela de detecção.	Minimize as regras de negócios para upgrades mais fáceis.	4	8

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Regras de negócios personalizadas	Número de regras de negócios personalizadas antes da criação de registros no CMDB.	Use as regras de negócio padrão em registros.	5	8
Conflitos de upgrade	Conflitos como regras de negócio e scripts identificados em um upgrade.	Revise e resolva os conflitos de upgrade.	10	15
PA instalado, mas não ativado	Indica se o painel do Performance Analytics não está habilitado.	Ative o painel do PA.	10	15
Integridade da integração				
Integrações desabilitadas	Número de integrações que foram desabilitadas.	Revise e habilite as integrações necessárias.	6	9
Falhas na execução de integração na semana passada	Número de execuções de integração que não foram bem-sucedidas na semana passada.	Revise e resolva a causa das execuções de integração com falha.	9	12
Desempenho				
Scripts e regras de negócios lentos	Scripts e regras de negócio cujo tempo médio de execução superior a 10 ms e contagem de execução superior a 10 000.	Revise e resolva as regras de negócios de execução lenta.	10	15
Integrações atrasadas	Número de integrações que atingiram o tempo limite antes da conclusão.	Revise e resolva a causa das integrações paradas.	10	15
Trabalhos em segundo plano com falha ou travados	Trabalhos em segundo plano com falha ou tempo esgotado na semana passada.	Revise e resolva a causa dos trabalhos com falha.	5	10
Consultas lentas	Consultas cujo tempo médio de execução é maior que 10 ms	Revise e resolva as regras de negócios de execução lenta.	10	15

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
	e a contagem de execução é maior que 10 000.			

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Integridade de dados				
Taxa de correspondência do item descoberto	Número de itens descobertos correspondentes aos ICs existentes.	Revise a integridade do seu CMDB e a lógica de regras de pesquisa de IC.	50	20
ICs incompatíveis em itens descobertos	Itens descobertos em estado incompatível.	Revise a integridade do seu CMDB e a lógica de regras de pesquisa de IC.	9	12
Regras de pesquisa de IC não utilizadas	Regras de pesquisa de IC que não estão associadas a nenhum item descoberto.	Altere o status das regras de pesquisa de IC não utilizadas para Inativo.	4	6
Item descoberto sem IC	Item descoberto sem item de configuração.	Revise e reaplique as regras de pesquisa de IC.	9	12
Registros ativos com defeito	Registros sem um item de configuração ou vulnerabilidade.	Descontinuar os ICs usando a opção Gestão de ciclo de vida do IC do CMDB. **Nota:** Excluir ICs diretamente pode resultar em Vits órfãos.	40	60
Tarefas de correção sem grupo de atribuição	Tarefas de correção ativas cujo grupo de atribuição ainda não foi atribuído.	Atribua tarefas de correção a um grupo de atribuição e revise as regras de atribuição existentes.	40	60

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Registros encerrados sem subestado	Registros que são encerrados sem um subestado.	Forneça informações no campo Motivo ao fechar os registros.	40	50
Integridade do processo				
Registros ativos sem pontuação de risco	Registros ativos com pontuação de risco de 0 ou sem pontuação de risco atribuída.	Revise e resolva as regras de risco.	40	60
Registros ativos não atribuídos	Registros sem um grupo de atribuição.	Atribua um grupo aos registros e revise as regras de atribuição existentes.	30	50
Itens sem destino de correção	Itens sem data de destino de correção.	Revise e resolva as regras de destino de correção. Essas regras devem incluir todos os registros.	30	50
Registros ativos desagrupados	Registros que não estão incluídos em uma regra de tarefa de correção.	Revise as regras da tarefa de correção.	40	60

Tendências

Título	Descrição
Métricas de desempenho de ingestão de item vulnerável nos últimos 30 dias	Tempo médio necessário para ingerir itens vulneráveis e processar várias regras nos últimos 30 dias.

Modificando os valores de limite

Você pode modificar os valores de limite dos dados do painel Integridade do SecOps VR com base em suas preferências.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integridade do Security Operations** > **Configuração** > **Métricas**.
2. Na página Dados do painel de integridade, abra o registro que você deseja modificar.
3. Atualize o registro e salve.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de vulnerabilidade(PA) painel

Rastreie o volume, o desempenho e o andamento das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado, por exemplo. Obtenha rapidamente informações sobre sua exposição a vulnerabilidades e quais serviços de negócios são afetados.

Funções necessárias de ServiceNow AI Platform

Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Gerentes de TI, analistas de TI, responsáveis pela correção de vulnerabilidades	Ajude sua organização a lidar com o aumento de incidentes de segurança devido a vulnerabilidades exploradas, determinando com eficiência quais itens vulneráveis apresentam mais risco. Esses painéis fornecem uma exibição gráfica da atividade de item vulnerável e ajudam a projetar planos de correção e andamento do status. Você pode se concentrar nos KPIs associados a ativos críticos afetados e vulnerabilidades de alta visibilidade.

Para exibir o painel de Gestão de vulnerabilidades (PA), navegue até **Resposta a vulnerabilidades** > **Visão geral**.

Veja relatórios que mostram dados de tendências ao longo do tempo. Os relatórios com dados em tempo real estão listados abaixo. Exiba tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

Para obter mais informações sobre como exibir seus relatórios de PA com pontuações em tempo real, consulte Exiba relatórios do Performance Analytics para Resposta a vulnerabilidades [PA] em tempo real .

Tradução automática

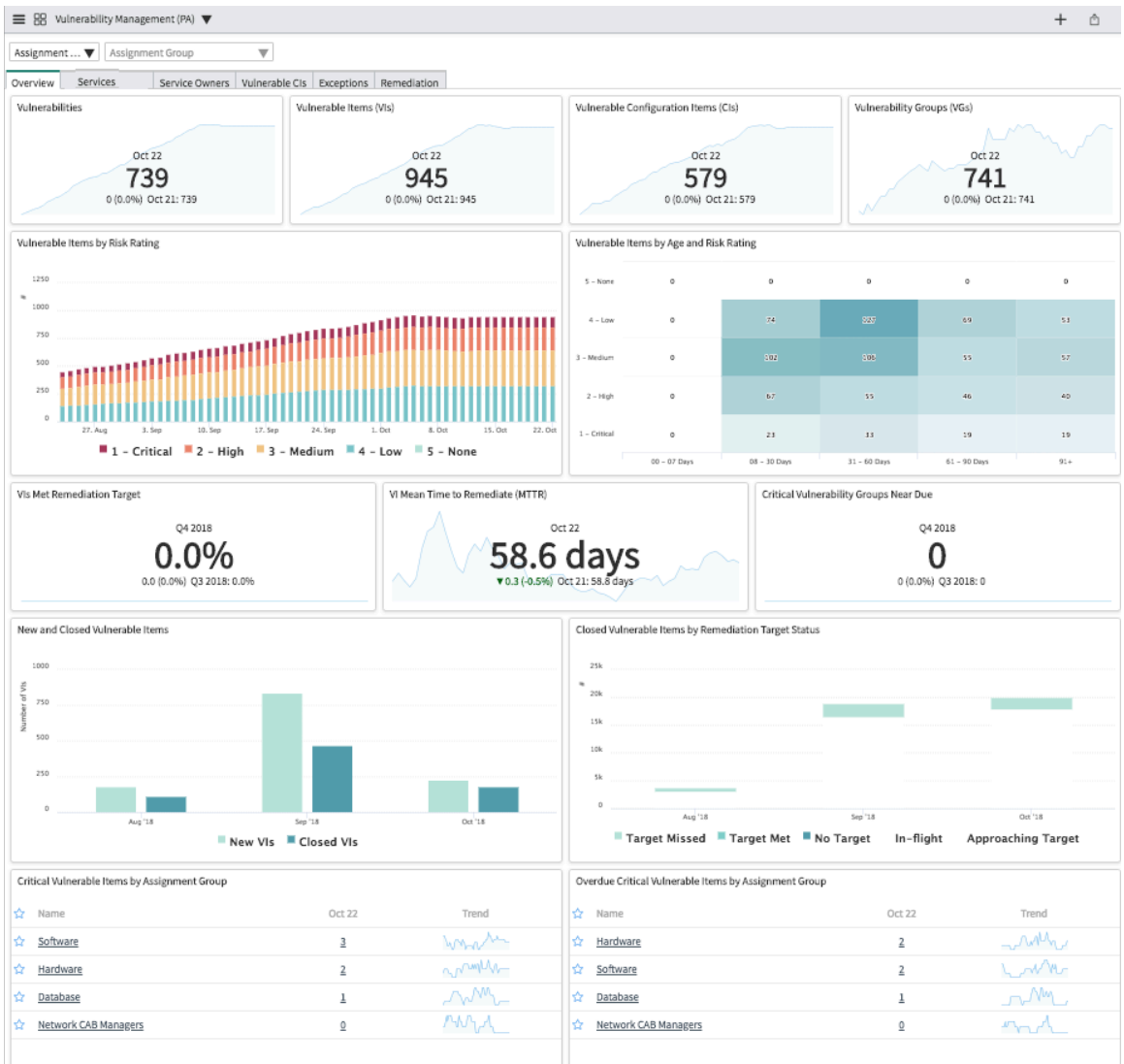
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As guias do painel Gestão de vulnerabilidades [PA]

Guia "Visão geral"

Este painel comunica KPIs para risco e prevalência de vulnerabilidade, ativos afetados, adesão à meta de correção e andamento da correção.

Na guia Visão geral, você pode exibir o relatório Itens vulneráveis críticos por grupo de atribuição que é executado com base no trabalho agendado.



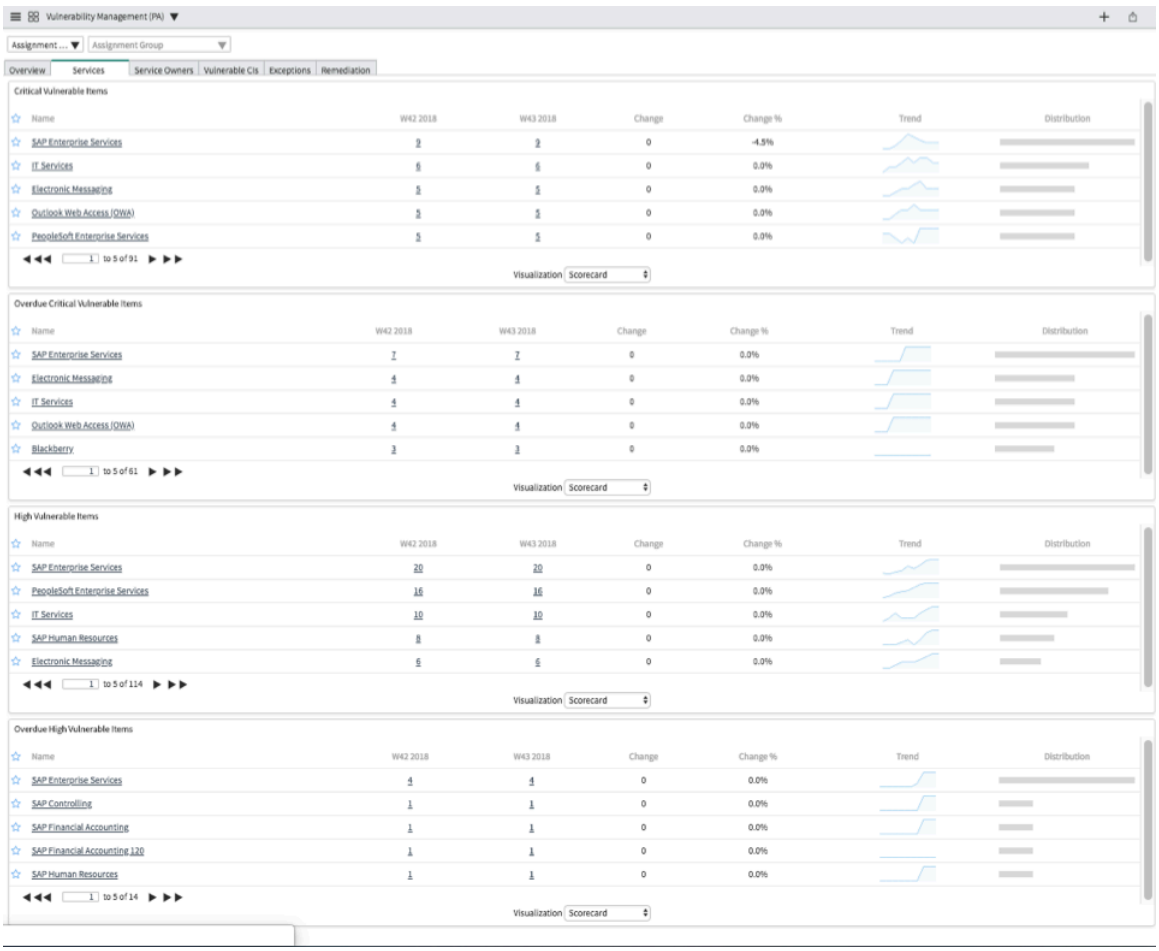
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Serviços de negócio

Este painel expõe o risco de vulnerabilidade no nível de serviço de negócios. Compartilhar essas informações com a organização pode ajudar os gerentes de serviço a corrigir vulnerabilidades de forma imediata e proativa e direcionar a empresa para um modelo de responsabilidade compartilhada de segurança da informação.

Você pode mudar a classe de serviço para serviços técnicos ou de aplicações usando a propriedade do sistema `sn_vul.service_classifications` .

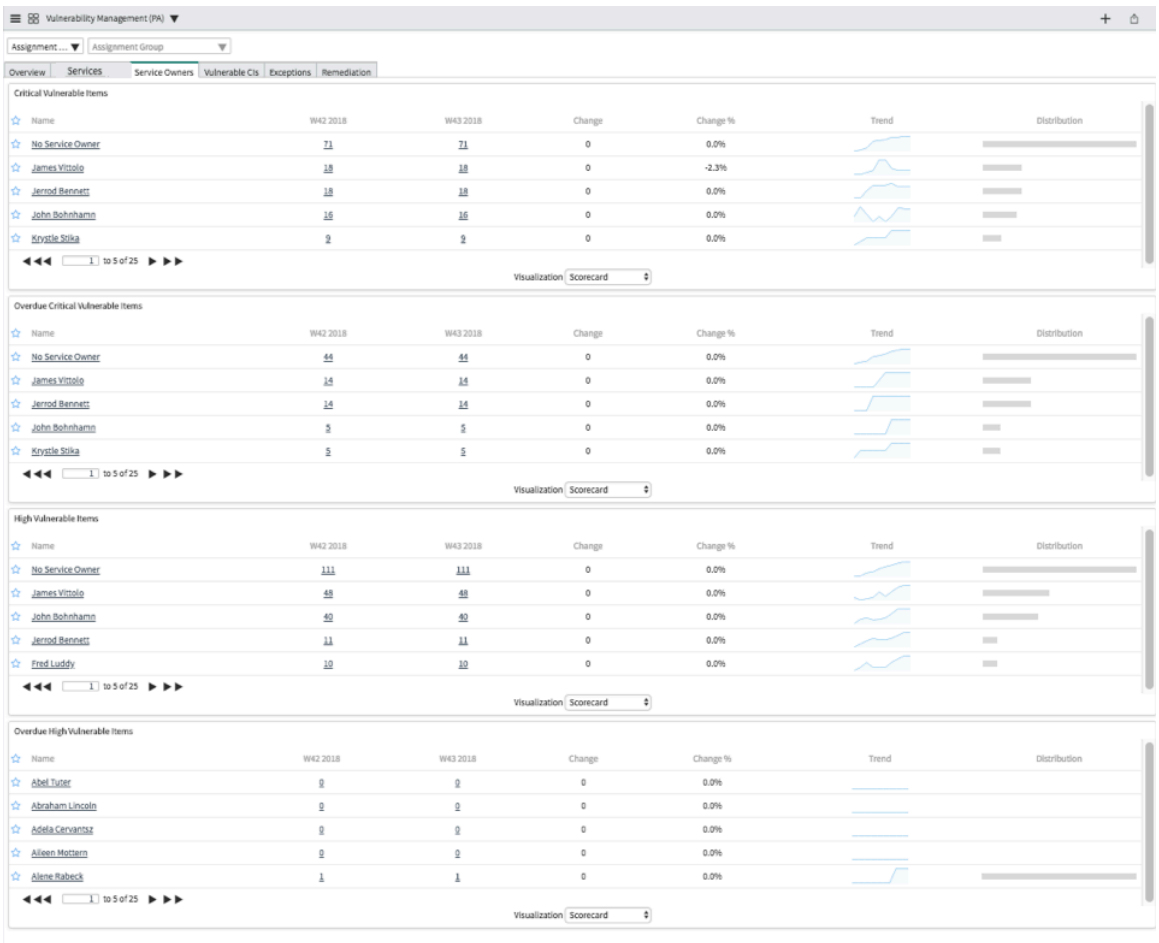


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Responsáveis pelo serviço

Este painel agrega o risco de vulnerabilidade do nível de serviço de negócio para os responsáveis pelo serviço, os executivos responsáveis por esses serviços de negócio. Ele mostra quais executivos estão assumindo o maior risco de vulnerabilidade e quais podem exigir mais ajuda para incentivar atividades de correção imediata.



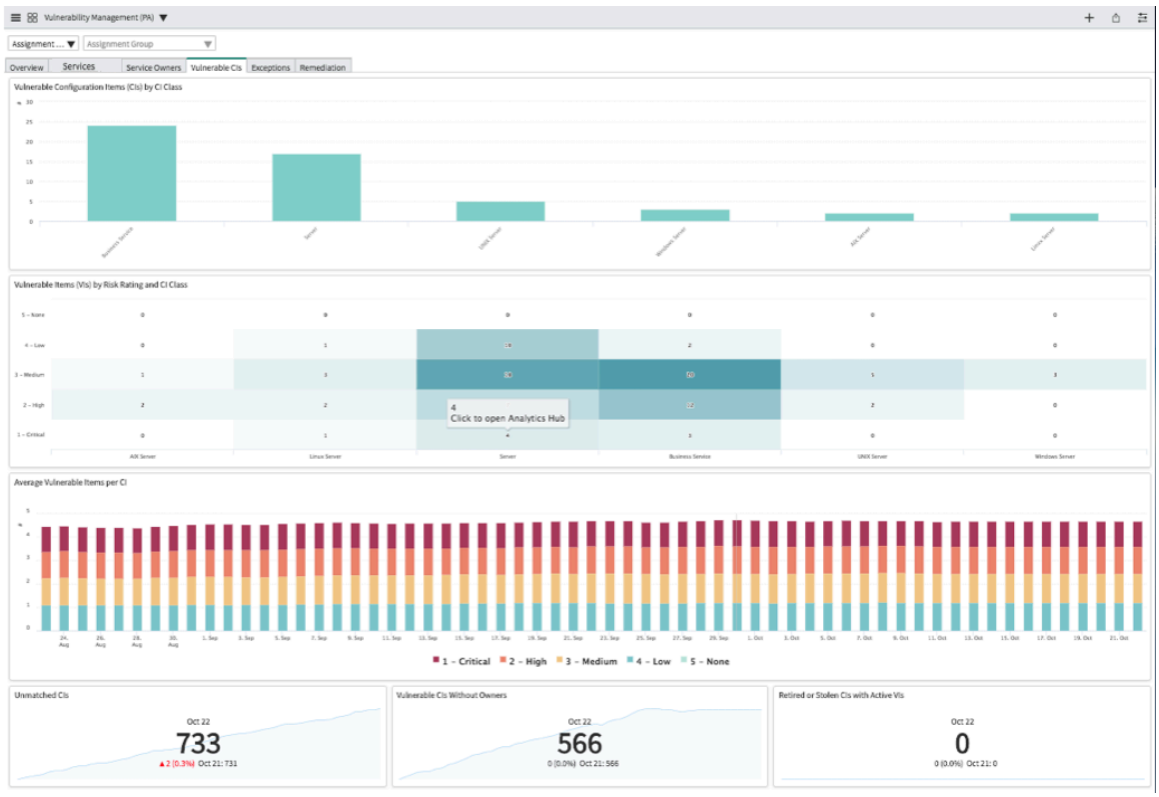
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia ICs vulneráveis

Este painel mostra o escopo e a composição de ICs com vulnerabilidades ativas e quais categorias de ICs precisam de mais atenção. Identifique ativos desativados com itens vulneráveis ativos e confirme se os ativos foram desativados. Exiba o número de ICs vulneráveis que não têm informações de propriedade, para que você possa identificar proativamente os proprietários desses ativos antes que uma vulnerabilidade crítica afete esses sistemas.

Na guia ICs vulneráveis, você pode exibir os ICs vulneráveis sem proprietários e ICs descontinuados ou roubados com relatórios de VIS ativos em tempo real.



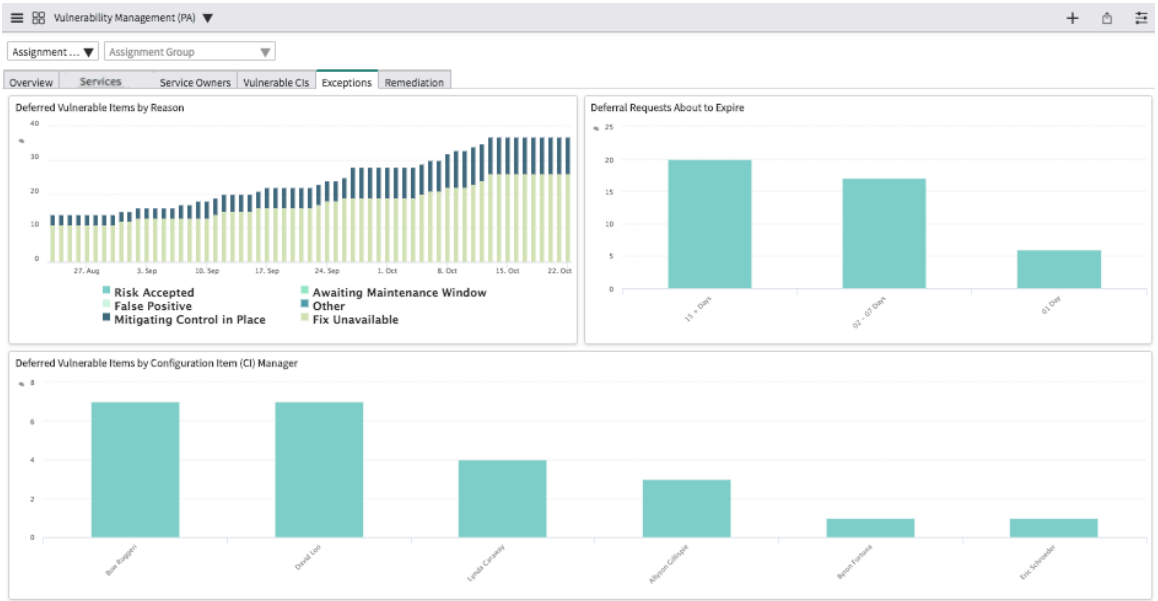
Guia Exceções

Este painel ajuda você a entender onde sua organização está assumindo riscos devido a adiamentos potencialmente excessivos e a reconsiderar as opções de correção.

Você pode exibir itens vulneráveis adiados por motivo, Solicitações de adiamento expirando, Exceções para itens vulneráveis críticos por grupo de atribuição e Solicitações de exceção por solicitante.

Tradução automática

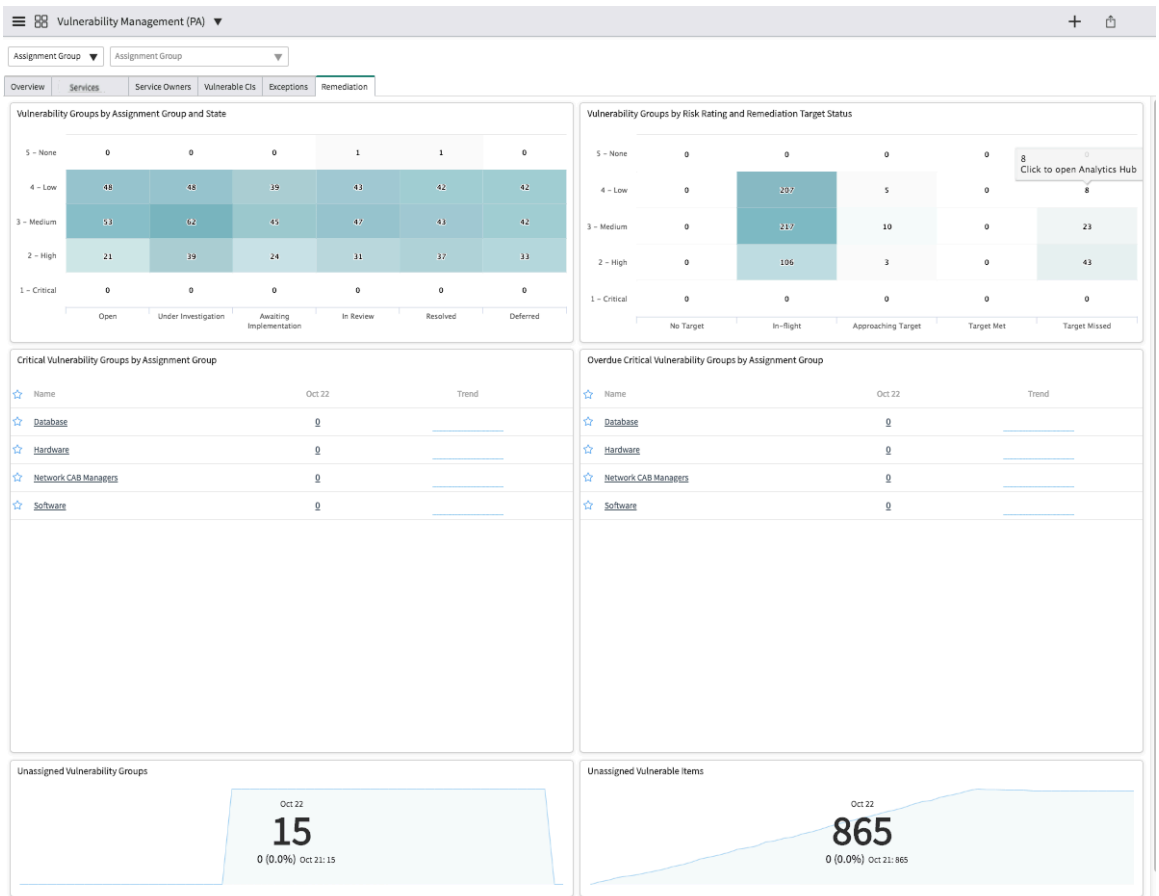
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Guia Correção

Este painel ajuda você a entender o andamento de suas ações de correção e quais equipes de suporte precisam de mais assistência com a conclusão.

Na guia Correção, você pode exibir o relatório de Itens vulneráveis não atribuídos em tempo real.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Indicadores de resposta a vulnerabilidades

Há vários indicadores usados para medir e rastrear o andamento da correção de vulnerabilidades no Resposta a vulnerabilidades aplicação.

A opção Coletar registros dos indicadores está desabilitada por padrão para Resposta a vulnerabilidades aplicação. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar Coletar registros manualmente e exibir os registros que compõem as pontuações.

Vulnerabilidades distintas

Vulnerabilidades distintas com count_active_vi > 0. O objetivo é minimizar.

Itens vulneráveis críticos que estão atrasados mas não adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Percentual de meta de correção atingida de itens vulneráveis

([[Itens vulneráveis encerrados > Destino de correção: Meta atingida]] / [[Itens vulneráveis encerrados]]) * 100 . O objetivo é maximizar.

Itens vulneráveis não atribuídos

Todos os Itens vulneráveis ativos nos quais o Grupo de atribuição e os campos Atribuição a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos (serviços)

É a contagem na fonte de dados VIS ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de alta vulnerabilidade atrasados (serviços)

É a contagem na fonte de dados VIS ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Tarefas de correção não atribuídas

Todas as tarefas de correção ativas em que os campos Grupo de atribuição e Atribuído a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Novos itens vulneráveis

É a contagem na fonte de dados VI.New, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de configuração vulneráveis

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Soma da duração de itens vulneráveis encerrados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É a soma da fonte de dados VI.Encerrado, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção não adiadas

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Tempo médio de correção do item vulnerável

[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]

Itens vulneráveis críticos atrasados (serviços)

É a contagem na fonte de dados VIS ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração desativados

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de adiamento

É a contagem na fonte de dados Solicitações de adiamento ativas, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Itens vulneráveis por itens de configuração

É a contagem nos ICs da fonte de dados com VIS ativo, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Itens vulneráveis encerrados

Itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo é maximizar.

Itens de configuração incompatíveis

Lista os hosts descobertos por scanners de vulnerabilidade de terceiros que não correspondem a nenhum IC existente no CMDB.

Tarefas de correção crítica que estão atrasadas mas não adiadas

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens de configuração vulneráveis sem grupo de suporte

É a contagem na fonte de dados VI.Open, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção crítica sem postergação

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de alta vulnerabilidade (serviços)

É a contagem na fonte de dados VIS ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração distintos com itens vulneráveis ativos

É a contagem distinta nos ICs da fonte de dados com VIS ativo, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Número médio de itens vulneráveis por item de configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[[Itens vulneráveis ativos]] / [[ICs vulneráveis]] . O objetivo é minimizar.

Tarefas de correção

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de adiamento (criadas)

É a contagem na fonte de dados Closed.Requests, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Detalhamentos

Os seguintes nomes de detalhamento se aplicam aos indicadores no painel:

- Idade
- Momento do fechamento
- Grupo de Atribuição
- Classe do IC
- Gerenciador de IA
- Idade do Adiamento
- Motivo do Adiamento
- Solicitantes da exceção
- Explorar Vetor de Ataque
- Explorar Itens Existentes
- Explorar Nível de Habilidade
- Regra de meta de correção
- Status da meta de correção
- Status da meta de correção (Encerrado)
- Pontuação de risco
- Serviço
- Importância do Serviço
- Responsável pelo serviço
- Gravidade
- Estado

Nota: Personalizar o cálculo de Idade e Idade de encerramento para Itens vulneráveis (VIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade fechada para VIS, consulte KB1703270 artigo da base de conhecimento.

Fonte de detalhamento

- Grupo de atribuição: Aplica-se a relatórios VI ou RT
- Existe exploração: Aplica-se a relatórios de VI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Explorar vetor de ataque: Aplica-se a relatórios de VI.
- Nível de habilidade de exploração: Aplica-se a relatórios de VI.
- Status de destino de correção: Aplica-se a relatórios de VI e RT.
- Classificação de risco: Aplica-se a relatórios VI e RT.
- Estado: Aplica-se a relatórios VI e RT.

Visualizações de dados

Título	Tipo	Descrição
Vulnerabilidades	Pontuação única	Número de vulnerabilidades associadas a um ou mais itens vulneráveis ativos.
Itens vulneráveis (IVs)	Pontuação única	Número de itens vulneráveis ativos (não encerrados).
Itens de configuração (ICs) vulneráveis	Pontuação única	Número de itens de configuração (ICs) associados a um ou mais itens vulneráveis ativos.
Tarefas de correção	Pontuação única	Número de tarefas de correção ativas (não encerradas).
Itens vulneráveis por classificação de risco	Barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.
Itens vulneráveis por idade e classificação de risco	Mapa térmico	Número de itens vulneráveis ativos agrupados por classificação de risco e idade (em dias).
Meta de correção atendida de IVs	Pontuação única	Percentual de itens vulneráveis encerrados que atenderam às datas de meta de correção nos trimestres atual e anterior. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medido como incrementos de 24 horas).
Tempo médio de correção do VIS (MTTR)	Pontuação única	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
		Nota: O valor de Idade Encerrada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e a hora do trabalho de coleta.
Tarefas de correção críticas próximas ao vencimento	Pontuação única	Número de tarefas de correção ativas que se aproximam da data de destino de correção. A data de destino de correção de uma tarefa de correção é definida como a data de vencimento mais próxima que pertence a um item vulnerável ativo no grupo. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medido como incrementos de 24 horas). Este relatório exclui tarefas de correção adiadas.
Itens vulneráveis novos e encerrados	Barra	Número de itens vulneráveis novos e encerrados no período selecionado. **Nota:** O valor de Idade Encerrada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e a hora do trabalho de coleta.
Itens vulneráveis encerrados por status da meta de correção	Barra	Número de itens vulneráveis encerrados, agrupados por status da meta de correção no período selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
		Nota: O valor de Idade Encerrada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e a hora do trabalho de coleta.
Itens vulneráveis críticos por grupo de atribuição	Lista e Linha	Número de itens vulneráveis ativos, com uma classificação de risco crítica, agrupados por grupo de atribuição.
Itens vulneráveis críticos e atrasados por grupo de atribuição	Lista e Linha	Número de itens vulneráveis ativos com uma classificação de risco crítico e após as datas de destino de correção, agrupados por grupo de atribuição. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medido como incrementos de 24 horas). Este relatório exclui itens vulneráveis adiados.

Serviços de negócio

Nome	Tipo	Descrição
Itens vulneráveis críticos	Barra de Lista, Linha e Distribuição	Número de itens vulneráveis ativos com uma classificação de risco crítico, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos que estão atrasados	Barra de Lista, Linha e Distribuição	Número de itens vulneráveis ativos com uma classificação de risco crítico e após as datas de destino de correção, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Serviços de negócio

Nome	Tipo	Descrição
		A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de alto risco e após as datas de destino de correção, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
Itens vulneráveis críticos	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de risco crítico, agrupados por responsável pelo serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos que estão atrasados	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de risco crítico e após as datas de destino de correção, agrupados por responsável pelo serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
		A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por responsável pelo serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Barra de Lista, Linha e Distribuição  	Número de itens vulneráveis ativos com uma classificação de alto risco e após as datas de destino de correção, agrupados por responsável pelo serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e percentual) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

ICs Vulneráveis

Nome	Tipo	Descrição
Itens de configuração (ICs) vulneráveis por classe de IC	Barra 	Números de itens de configuração com vulnerabilidades ativas, agrupados por classe de IC no CMDB.
Itens vulneráveis (VIs) pela Classe de IC	Mapa de árvore 	Número de VIS ativos divididos por classe de IC.
Média de Itens vulneráveis por IC	Barra 	Número médio de itens vulneráveis que pertencem a um item de configuração, agrupados conforme a classificação de risco.
ICs incompatíveis	Pontuação única 	Número de itens de configuração importados que não correspondem a nenhum IC existente no CMDB.
ICS vulneráveis sem grupo de suporte	Pontuação única 	Número de itens de configuração vulneráveis que não têm um grupo de suporte atribuído.
ICs desativados ou roubados com IVs ativos	Pontuação única 	Número de itens de configuração marcados **Descontinuado** ou **Roubado** No CMDB que têm itens vulneráveis ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exceções

Nome	Tipo	Descrição
Itens vulneráveis adiados por motivo	Barra	Número de itens vulneráveis adiados, agrupados por motivo de adiamento.
Solicitações de adiamento prestes a expirar	Barra	Número de solicitações de adiamento associadas a tarefas de correção ou itens vulneráveis que estão prestes a ser reabertos para revisão. Eles são agrupados pelo número de dias restantes até reabrirem. Se as notificações por e-mail estiverem definidas, um e-mail será enviado.
Itens vulneráveis adiados por gerente de item de configuração (IC)	Barra	Número de itens vulneráveis adiados agrupados pelo gerente para o item de configuração associado.

Correção

Nome	Tipo	Descrição
Tarefas de correção por classificação de risco e estado	Mapa térmico	Número de tarefas de correção ativas agrupadas por classificação de risco e estado.
Tarefas de correção por classificação de risco e status da meta de correção	Mapa térmico	Número de tarefas ativas agrupadas por classificação de risco e status de destino de correção. Este relatório exclui itens vulneráveis adiados.
Tarefas de correção críticas por grupo de atribuição	Lista e Linha	Número de tarefas de correção ativas com uma classificação de risco crítico agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção críticas em atraso por grupo de atribuição	Lista e Linha	Número de tarefas de correção ativas com uma classificação de risco crítico e após as datas de destino de correção, agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção não atribuídas	Pontuação única	Número de tarefas de correção ativas sem um atribuído ou grupo de atribuição.
Itens vulneráveis não atribuídos	Pontuação única	Número de itens vulneráveis ativos sem um atribuído ou grupo de atribuição.

Exibir Performance Analytics para Resposta a vulnerabilidades Relatórios em tempo real

Para gerenciar seus itens vulneráveis (VIS) mais importantes e ajudá-lo a corrigi-los rapidamente, exiba relatórios sob demanda, em tempo real no painel Gestão de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades (PA). . Performance Analytics para Resposta a vulnerabilidades o aplicativo está disponível com uma assinatura separada do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Para obter mais informações sobre os relatórios de Performance Analytics para Resposta a vulnerabilidades, consulte Painel de Gestão de vulnerabilidades [PA] .

Para obter mais informações sobre a configuração e instalação do Performance Analytics para Resposta a vulnerabilidades aplicação, consulte Instale e configure o. Performance Analytics para Resposta a vulnerabilidades Aplicação [PA].

Se não for exibido, para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão geral**. Na parte superior do painel, as guias de relatório são exibidas.

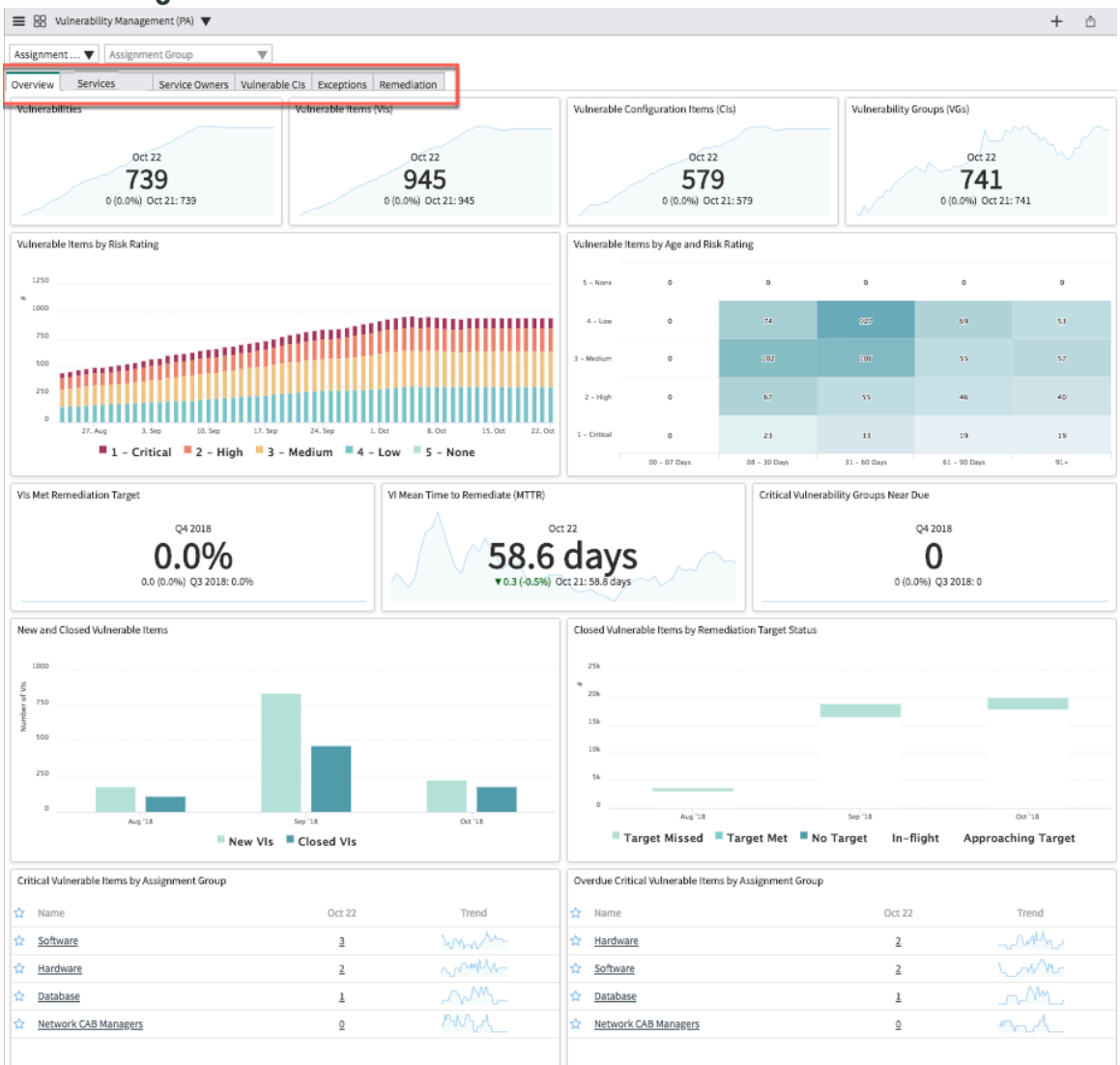
A partir da versão 19,0 de Resposta a vulnerabilidades Este painel também pode ser exibido na IU da Nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e. Painéis no Espaço de correção de TI .

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia "Visão geral"



Exiba os relatórios a seguir nas guias do painel Gestão de vulnerabilidades (PA) em tempo real.

- Guia "Visão geral"
  - Itens vulneráveis críticos por grupo de atribuição
- Guia ICs vulneráveis:
  - ICs vulneráveis sem responsáveis
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções:
  - Itens vulneráveis adiados por motivo
  - Solicitações de adiamento prestes a expirar
  - Itens vulneráveis adiados pelo gerente de CIO
- Guia Correção:
  - Itens vulneráveis não atribuídos

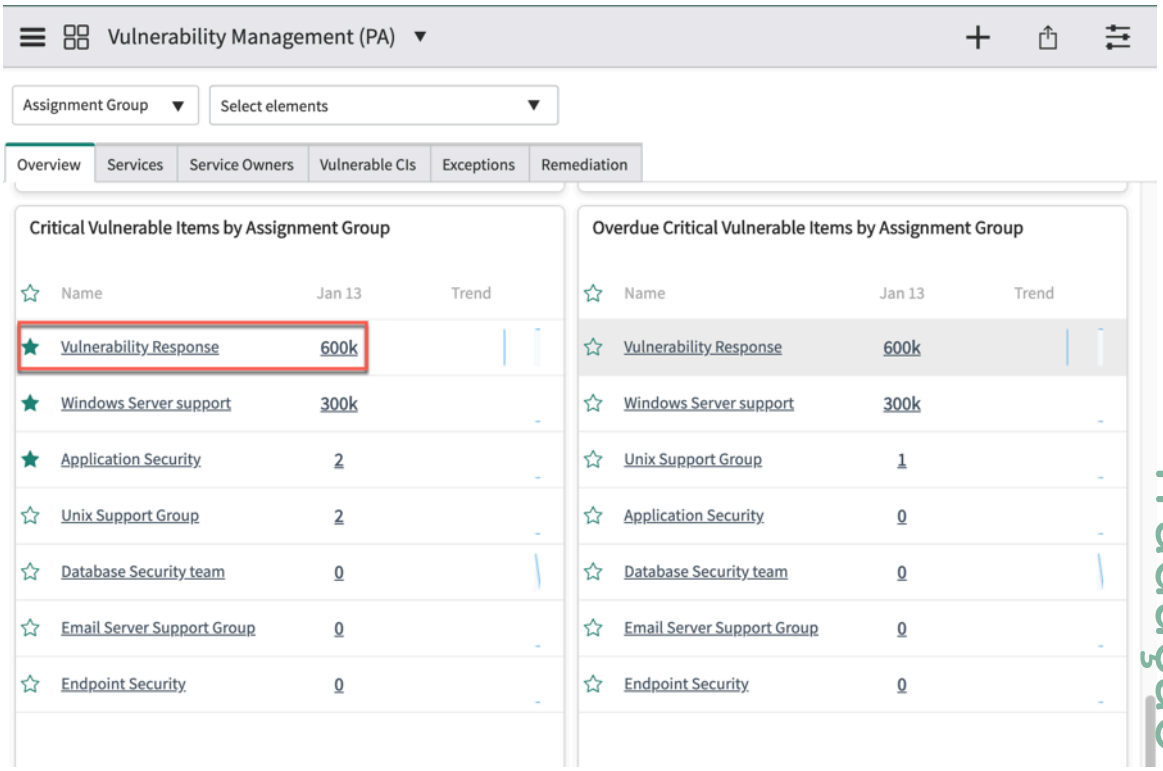
Para exibir pontuações em tempo real, com uma das guias selecionadas que contém relatórios em tempo real, siga estas etapas:

Tradução automática

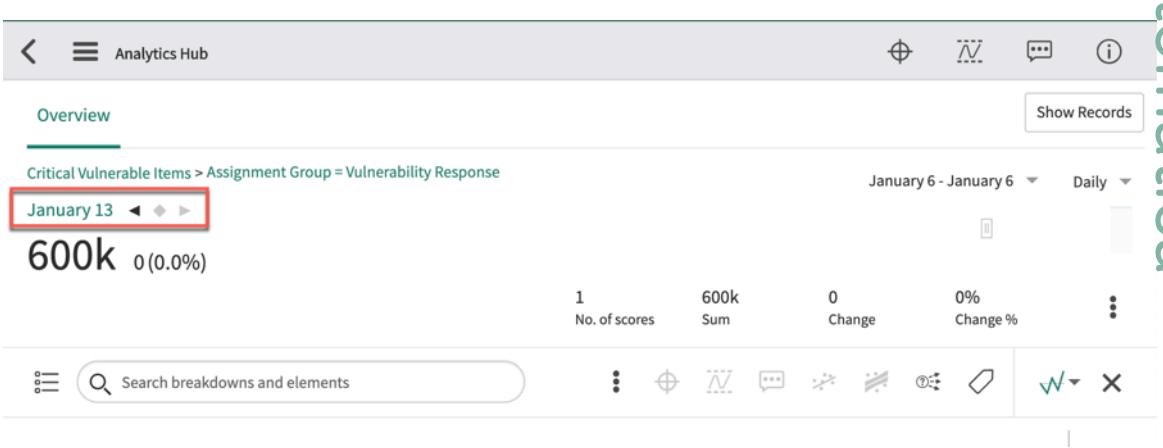
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No relatório, por exemplo, Itens vulneráveis críticos por grupo de atribuição, clique em um dos links exibidos.



2. No registro exibido, clique na data.

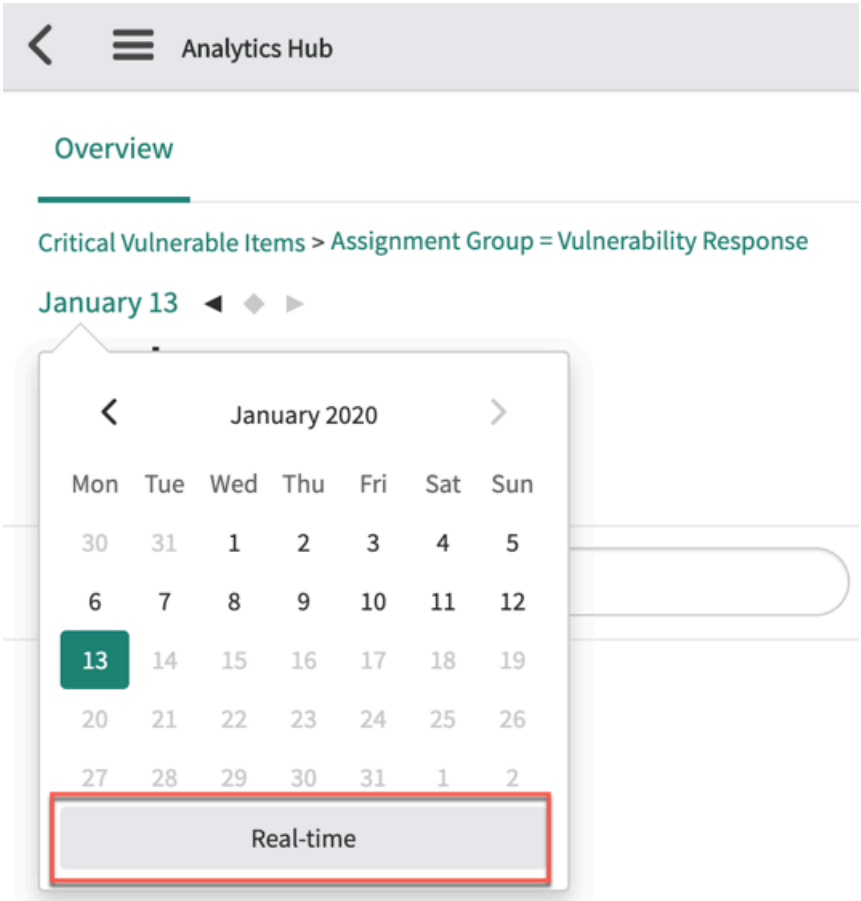


3. No calendário exibido, clique em Tempo real.

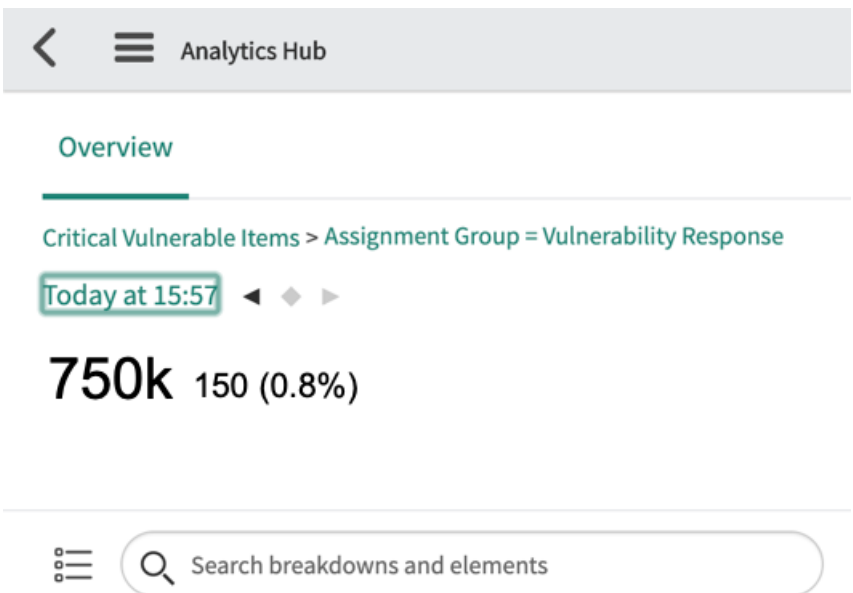
   Se um relatório não oferecer suporte a uma pontuação em tempo real, o botão Tempo real não será exibido no calendário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Pode levar alguns minutos para que o valor seja atualizado. A data atual, os registros, o número de novos registros desde o último relatório e a mudança percentual do último relatório também são exibidos.



4. **Opcional:** Para exibir os registros que compõem o relatório, com o relatório em tempo real exibido, no canto superior direito, clique em **Mostrar registros** .
   Uma lista de registros que compõem a pontuação é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exiba Performance Analytics indicadores para Resposta a vulnerabilidades[PA]

Exibição automatizada e formulada Performance Analytics indicadores que representam os dados de vulnerabilidade em sua instância.

Antes de Iniciar

A opção Coletar registros dos indicadores está inativa por padrão para a aplicação Performance Analytics - Content Pack Vulnerability Response. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar Coletar registros manualmente e exibir os registros que compõem as pontuações.

Nota: Ativar Coletar registros em um indicador pode afetar seu desempenho e prolongar consideravelmente o tempo e a memória necessários para executar o trabalho de coleta de dados.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou pa.viewer

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades tem indicadores automatizados e formulados.

Termos principais

Indicador do PA

Define uma medição de desempenho realizada em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, Itens vulneráveis críticos atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, VI Ativo.

Coletar registros

Quando habilitado, armazena registros na memória e fornece acesso ao Hub de análise.

Detalhamentos

Detalhamentos filtro e agrupar registros coletados. Os detalhamentos podem aumentar o uso da memória, especialmente à medida que o número e a diversidade aumentam.

Exclusões de detalhamento

Determinadas exclusões removem determinados detalhamentos, o que pode reduzir o consumo de memória.

Procedimento

1. Para indicadores automatizados, navegue até **Performance Analytics** > **Indicadores** > **Indicadores Automatizados**.
2. Para indicadores formuladas, navegue até **Performance Analytics** > **Indicadores de Fórmula**.

   Para obter informações detalhadas sobre indicadores, consulte Indicadores do Performance Analytics .
3. Em ambos os casos, pesquise em **Aplicação** > **Performance Analytics**.

Tradução automática

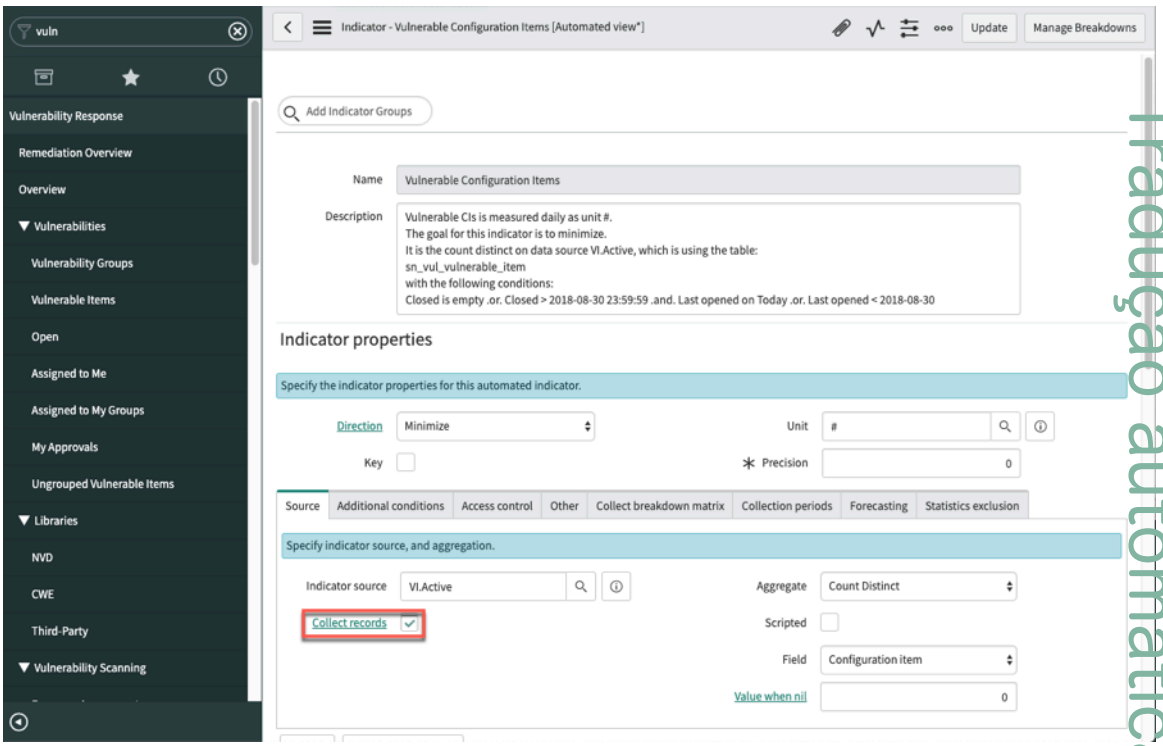
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se ele não estiver em sua exibição padrão, adicione **Aplicação** coluna usando o ícone de engrenagem ( ) no canto superior esquerdo da página. A coluna Aplicação é exibida no menu suspenso Pesquisar.

4. **Opcional:** Para habilitar Coletar registros em uma Performance Analytics para Resposta a vulnerabilidades, siga estas etapas:

   a. Com a lista de indicadores automatizados exibida, na coluna Nome, clique no indicador para o qual você deseja habilitar a coleta de registros.
   O registro do indicador é exibido.

   b. Na seção Propriedades do indicador com a guia Origem selecionada, marque a caixa de seleção Coletar registros.



Tradução automática

   c. Escolha um para continuar.

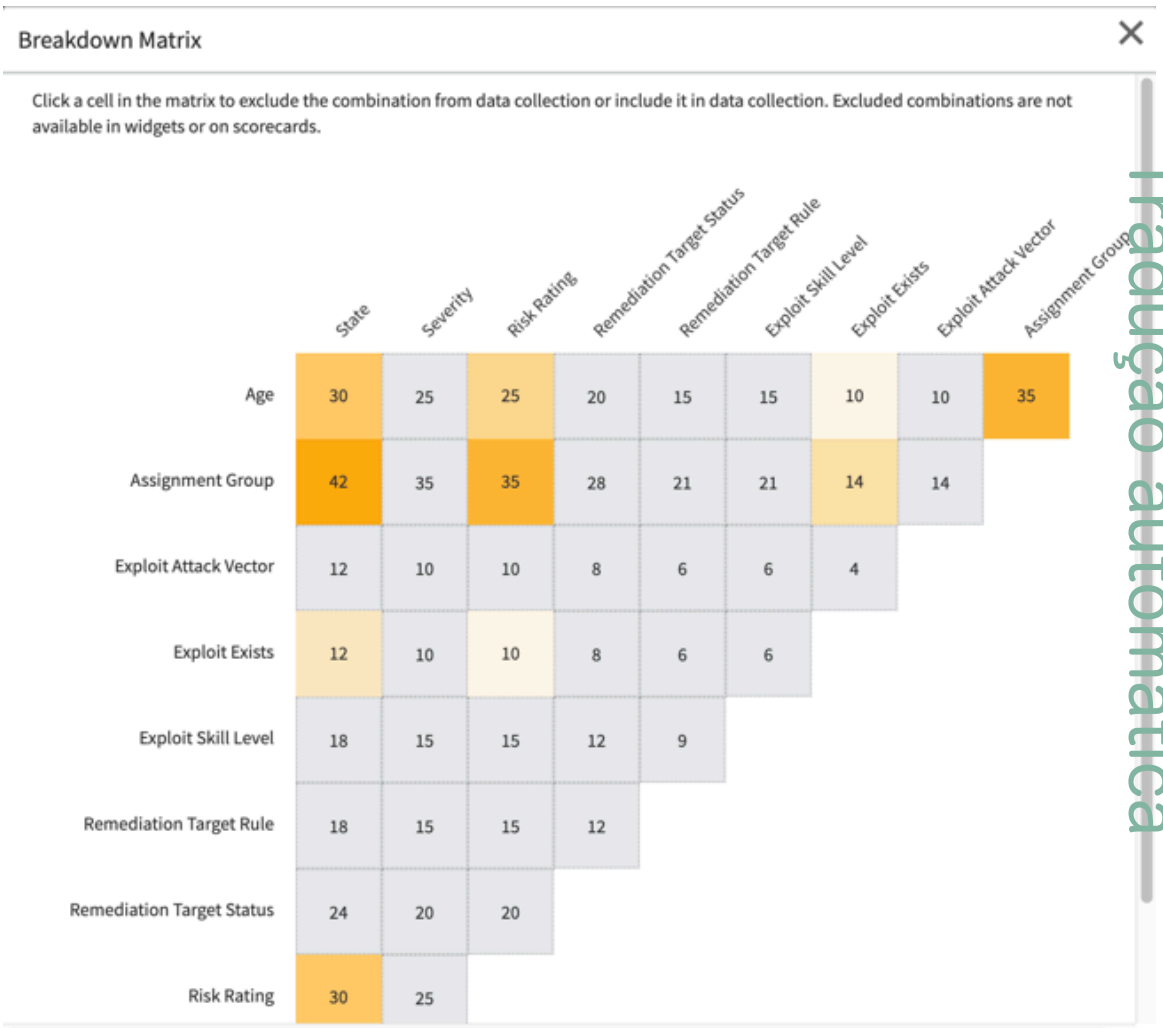
Opção	Descrição
Atualizar	Salve suas edições e retorne à lista de indicadores.
Gerenciar Detalhamentos **Nota:** Se você optar por reativar detalhamentos de segundo nível, poderá aumentar significativamente o consumo de memória e tornar o trabalho de coleta de dados mais lento. Por padrão, exclusões de detalhamento de segundo nível foram aplicadas aos seguintes indicadores:	Reative detalhamentos de segundo nível para os indicadores listados ou edite detalhamentos de outros indicadores. (Optional) Para obter mais informações sobre detalhamentos do Performance Analytics, consulte Detalhamentos do Performance Analytics .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
▪ Itens de configuração vulneráveis ▪ ICs descontinuados ▪ IVs adiados	

d. Clique em **Gerenciar detalhamentos** .

e. No formulário exibido, clique em **Configurar Matriz de detalhamento** .
O formulário Matriz de detalhamento é exibido. As combinações excluídas são selecionadas e exibidas com cores, conforme mostrado na figura a seguir.



f. Para remover a exclusão e reativar uma combinação excluída, clique em uma célula selecionada.

g. No canto superior direito do formulário, clique em **Fechar** Para retornar o formulário Gerenciar detalhamento.

h. Clique na seta Voltar para retornar ao registro do indicador.

i. Clique em **Atualização** Para salvar suas edições e retornar à lista de indicadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estrutura de relatórios agregados

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas dinâmicas complexas e de longa execução para melhorar o desempenho.

A estrutura de relatórios agregados melhora o desempenho ao:

- usando menos recursos e renderizando relatórios mais rapidamente,
- Agregação de dados e reutilização de agregações e detalhamentos (Agrupar por) e.
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis, use a estrutura de relatórios agregados fornecida em Resposta a vulnerabilidades Comum junto com os relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- ServiceNow AI Platform Administrador (admin): Instale e ative isso Solução para Performance Analytics e relatórios e fazer as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Sn_vul_cmn.admin): Criar agregações.
- VR write(sn_vul_cmn.write): Edite os dados nas agregações e nos resultados agregados.
- VR read (sn_vul_cmn.read): Revise os dados nas agregações e nos resultados agregados.
- Analista de vulnerabilidades (sn_vul.vulnerability_analyst): Revise os resultados agregados.

Tópicos relacionados

Configure uma agregação para dados de origem

Execute várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Crie um relatório usando uma agregação

Configure uma agregação para dados de origem

Para analisar o desempenho de um aspecto específico em um processo de negócios registrado em um ServiceNow, crie uma agregação específica para o aspecto e crie um relatório para esta agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Relatórios de agregados** > **Definições de agregação** > **Tudo** e clique em **Novo** .
2. Em **Nome** dê à agregação um nome descritivo.
3. Em **Descrição** forneça uma breve descrição sobre a agregação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Em **Origem** preencha os campos.

Campos da guia Origem

Campo	Descrição
Tabela	Tabela da qual você deseja buscar os dados do relatório. Este menu suspenso contém somente tabelas app sec common, app-vul, app-vulc, app-vul-contêiner e vulnerabilidade da aplicação.
Agregar função	Função a ser aplicada à coluna selecionada em **Campo** . ○ **Contagem** Número de registros. ○ **Soma** Soma total dos valores na coluna selecionada em **Campo** . ○ **Média** Média de todos os valores em uma coluna selecionada em **Campo** . ○ **Máximo** Valor máximo na coluna selecionada em **Campo** . ○ **Mínimo** Valor mínimo da coluna selecionada em **Campo** . ○ **Contagem distinta** Valores exclusivos na coluna selecionada em **Campo** .
Campo	Coluna na qual você deseja aplicar a função. **Nota:** Este campo não aparece quando você seleciona **Contagem** em **Função agregada** campo.

5. Em **Condições adicionais** forneça a condição em **Condições** campo para selecionar um conjunto específico de registros para os quais você deseja obter os resultados agregados.
6. Em **Agrupar por** , selecione as colunas da tabela pelas quais você deseja agrupar ou empilhar os dados. Você pode selecionar até dois detalhamentos.

   Se você selecionar **data** em qualquer campo de grupo por, **Tendência por** o campo é exibido. Você pode obter os resultados de agregação categorizados por semana, dia, minutos etc. selecionando as opções em **Tendência por** campo.

7. Em **Programação** selecione ou crie uma programação de agregação, que define a frequência na qual você pode executar a agregação para buscar os dados.
   Para criar uma programação de agregação, consulte Execute várias agregações simultaneamente.

   Nota: Você não pode programar a execução de agregação para uma definição de agregação inativa.

8. Clique em **Enviar** para criar a agregação.
   A agregação aparece na lista Agregação. Na frequência predefinida, a agregação é executada e um registro é criado junto com uma data e hora de execução na lista relacionada Execuções agendadas para cada execução.
9. Navegar até **Tudo** > **Resultados agregados** E abra sua agregação para ver os resultados agregados e as execuções programadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os resultados agregados são listados em **Resultados agregados** lista relacionada. Se a execução de agregação falhar, consulte **Anotações** coluna em **Execuções programadas** lista relacionada para obter mais informações.

10. **Opcional:** Selecione **Executar agora** para coletar os resultados de agregação, independentemente da programação de agregação.
    Se você encerrar a execução programada quando ela estiver em andamento, nenhuma mudança será feita nos resultados agregados. Você também pode excluir ou desativar uma agregação.

O que Fazer Depois

Crie um relatório usando sua agregação. Para obter mais informações sobre como criar um relatório usando uma agregação, consulte Crie um relatório usando uma agregação.

Tópicos relacionados

- Estrutura de relatórios agregados
- Execute várias agregações simultaneamente
- Configure o número de agregações que podem ser executadas simultaneamente
- Crie um relatório usando uma agregação

Execute várias agregações simultaneamente

Você pode programar a execução de várias agregações usando uma única programação de agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa

Suponha que você queira executar seis agregações ao mesmo tempo. Crie uma programação de agregação e adicione todas as agregações a ela. Essas agregações são executadas na frequência e hora definidas.

Procedimento

1. Navegar até **Tudo** > **Relatórios de agregados** > **Agendamento**.
2. Selecione **Novo**.
3. No formulário Programação de agregação, preencha os campos.

Campo	Descrição
Nome da programação	Nome da programação de agregação.
Programar trabalho	Execução de script programada que define a frequência na qual as agregações devem ser executadas. Você pode criar um trabalho programado selecionando **Novo** botão.

4. Selecione **Enviar**.
   A programação de agregação aparece na lista de programação de agregações.
5. Abra sua programação de agregação.
6. Selecione **Editar** , adicione as agregações ao **Lista de Agregação** e selecione **Salvar** .
   As agregações selecionadas aparecem na lista relacionada Agregações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você adicionar uma agregação inativa a uma programação, a execução programada não será iniciada.

7. Selecione **Atualizar**.
   Essas agregações são executadas na frequência definida na programação de agregação.

Tópicos relacionados

- Estrutura de relatórios agregados
- Configure uma agregação para dados de origem
- Configure o número de agregações que podem ser executadas simultaneamente
- Crie um relatório usando uma agregação

Configure o número de agregações que podem ser executadas simultaneamente

Um novo processador ou um trabalho em segundo plano, o Processador da Estrutura de relatórios agregados é enviado com o sistema de base, que executa os trabalhos agendados relacionados à tabela Estrutura de relatórios agregados. Isso permite que todo o subsistema seja executado em segundo plano e permite uma melhor utilização dos recursos do sistema quando eles estão disponíveis.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Configuração de trabalho em segundo plano - Calculadora de resultado de agregação comum de resposta a vulnerabilidades**.
2. Defina o número de agregações que você deseja executar simultaneamente no **Threads simultâneos máximos** arquivado e selecione **Salvar** .
   Por padrão, quatro agregações são executadas simultaneamente.
3. Navegue até a lista Grupos de processadores de trabalho em segundo plano, **sn_sec_cmn_background_job_processor_pool.list**e selecione **Novo** Para criar um processador de trabalho em segundo plano para a Estrutura de relatórios agregados.
   Para obter mais informações sobre como criar um grupo de processadores de trabalhos em segundo plano, consulte Processamento paralelo avançado para trabalhos em segundo plano na Resposta a vulnerabilidades .

Nota: O número de processadores de trabalho em segundo plano deve ser igual ao número máximo de threads simultâneos fornecido no **Configuração de trabalho em segundo plano - Calculadora de resultado de agregação comum de resposta a vulnerabilidades** formulário. Consulte Etapa 2 .

Tópicos relacionados

- Estrutura de relatórios agregados
- Configure uma agregação para dados de origem
- Execute várias agregações simultaneamente
- Crie um relatório usando uma agregação

Crie um relatório usando uma agregação

Para visualizar e analisar os dados específicos de uma agregação que você criou, gere um relatório fornecendo uma condição para a agregação no construtor de condições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: pa_admin

Procedimento

1. Navegar até **Tudo** > **Relatórios** > **Criar novo(a)**.
2. Em **Dados** preencha os campos.

Campos da guia Dados

Campo	Descrição
Nome do relatório	Nome do relatório.
Tipo de origem	Tipo da origem da qual os dados são obtidos. Selecione **Tabela** .
Tabela	Nome da tabela para a qual a agregação é criada. Selecione a tabela Resultados agregados **Resultado agregado [sn_vul_cmn_aggregate_result]** .

3. No Construtor de condições, defina a condição da agregação para a qual você deseja gerar um relatório.

Condição no construtor de condições

Parte	Descrição
Campo	Selecione **Agregação** .
Operador	Selecione . .
Valor	Nome da agregação.

4. Em **Dados** , selecione **Próximo** .
5. Em **Tipos** , selecione como você deseja visualizar os dados e selecione **Próximo** .
   Para obter mais informações sobre os tipos de relatório, consulte Criando Relatórios .

   As visualizações compatíveis são gráfico de barras, gráfico de pizza e mapa térmico. Você pode modificar os gráficos de linha e outras visualizações de tendências para usar as visualizações compatíveis com resultado agregado para representar os mesmos dados. A exibição de lista não é compatível.
6. Em **Configurar** preencha os campos.

Campo	Descrição
Agrupar por	Agrupa os dados pelo campo selecionado. Selecione o campo que você escolheu em **Agrupado por 1** . #unique_505_Connect_42_group-by agregação.
Empilhar por	Organiza os dados em camadas com base no campo selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Selecione o campo que você escolheu em **Agrupado por 2** . #unique_505_Connect_42_group-by agregação. **Nota:** Relatórios de barras e barras horizontais usam dados empilhados. Outros tipos de relatório permitem somente o agrupamento.
Agregação	Aplicar **Mínimo** ou **Máximo** função em **Valor** .

7. Em **Estilo** preencha os campos conforme apropriado e selecione **Executar** .
   Para obter mais informações sobre os campos em **Configurar** e. **Estilo** guias, consulte Criando um relatório vídeo.
8. No Construtor de condições, defina a condição da agregação para a qual você deseja gerar um relatório e selecione **Executar** .

   O relatório é exibido.
9. Para classificar os valores no eixo X, selecione **Adicionar classificação** .

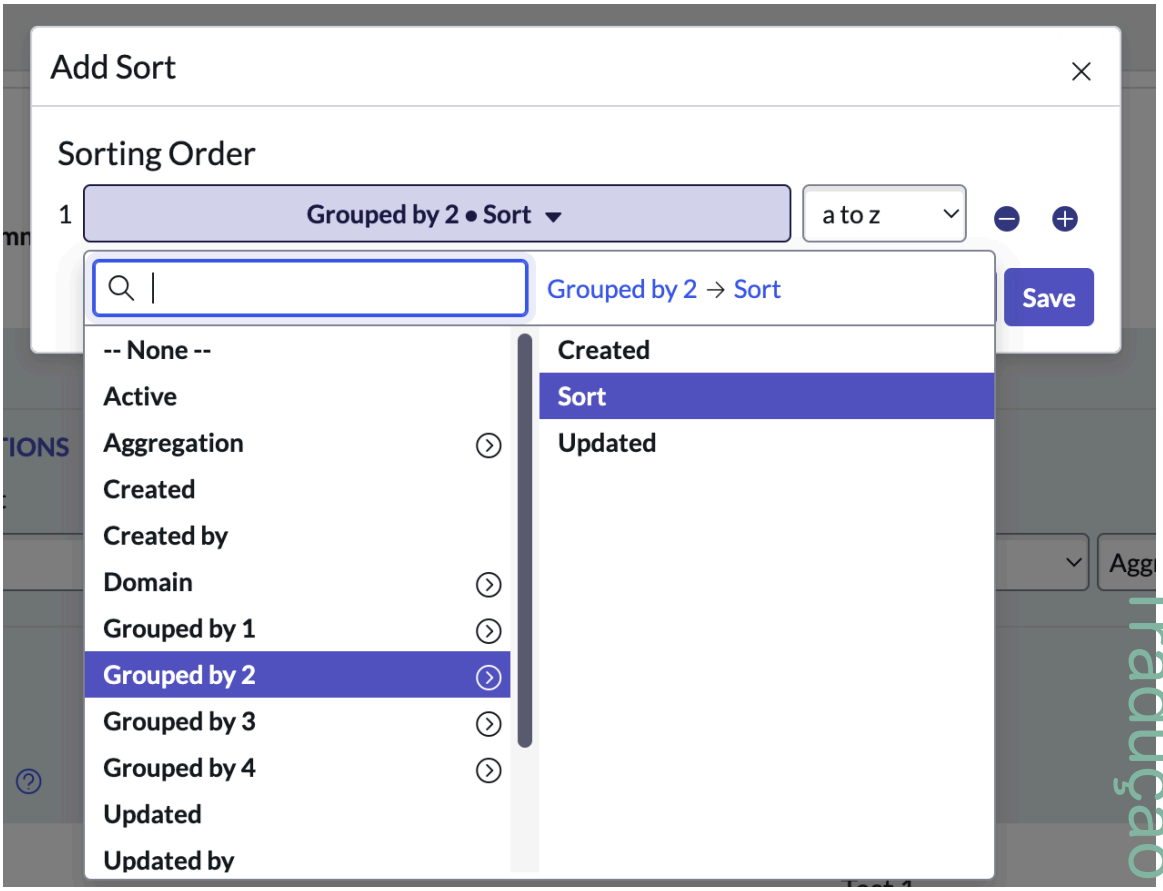
   a. Para cadeias de caracteres, forneça a condição como **Agrupado por > a-z ou z-a.** para classificar as cadeias de caracteres em ordem alfabética.

   b. Para valores de tipo de dados inteiros e de data, forneça a condição como **Agrupado por.classificar > a-z ou z-a.** para classificar os valores em ordem crescente e decrescente, respectivamente.

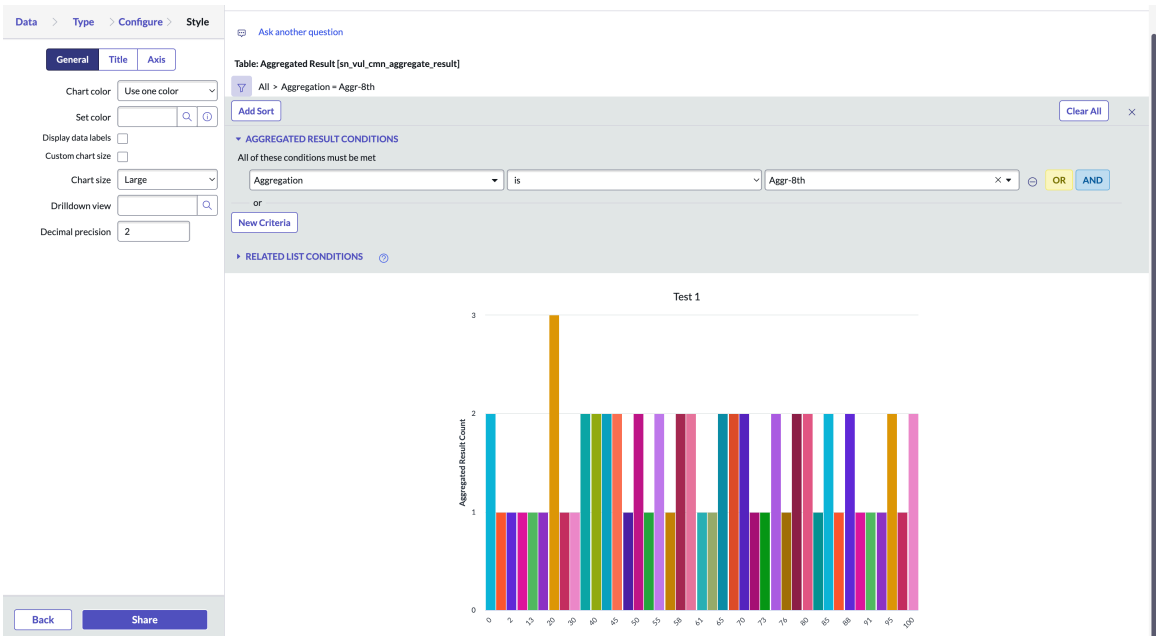
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classificando números inteiros no eixo X.



c. Selecione **Executar**.
Os valores inteiros e de data são classificados no eixo X.



10. Selecione **Salvar** para salvar seu relatório.
O relatório gerado para uma agregação é exibido em **Resultados** respectivo **Agregação** formulário.

11. Opcional: Adicione seu relatório a um painel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como adicionar um relatório a um painel, consulte Adicione um relatório a um painel dinâmico .

. **Gestão de vulnerabilidades[agregado]** o painel que consiste em relatórios criados usando a estrutura de relatórios em cache é enviado com o sistema de base. Para exibir este painel, navegue até **Tudo** > **Performance Analytics** > **Painéis** > **Tudo** > **Gestão de vulnerabilidades [Agregado]**. As agregações ativas correspondentes aos relatórios neste painel são enviadas com o sistema de base.

12. Compartilhe seu relatório com outros usuários.
Para obter mais informações sobre como compartilhar relatórios, consulte Distribuir relatórios .

Tópicos relacionados

Configure uma agregação para dados de origem

Estrutura de relatórios agregados

Execute várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Resposta a vulnerabilidades informações de referência

Os tópicos a seguir fornecem links, informações de referência, solução de problemas e artigos de conhecimento, além de dados de campo nos formulários e registros encontrados em Resposta a vulnerabilidades.

Abaixo estão listados alguns links para outros recursos que você pode achar úteis, começando com um link para o artigo Links da base de conhecimento para suporte e solução de problemas de VR/CC na Base de conhecimento HI.

- Links da base de conhecimento para suporte e solução de problemas de VR/CC
- Para obter mais informações sobre aplicações e compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .
- Vídeos de Operações de segurança
- Desenvolver treinamento
- Desenvolver documentação
- Trabalhe com um especialista em implementação para alcançar os resultados de negócios desejados com o. Central de sucesso do cliente .
- Faça um curso do Vulnerability Response para adquirir conhecimento e obter ROI mais rapidamente. Para se inscrever, consulte Treinamento e certificação da ServiceNow .
- Encontre componentes instalados com uma aplicação
- Orquestração de resposta a vulnerabilidades
- Dicas para escrever integrações
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de implementação do Resposta a vulnerabilidades aplicação

Esta check-list lista as etapas necessárias para uma implementação básica do Resposta a vulnerabilidades aplicação em seu ServiceNow AI Platform® instância. Quando você concluir essas tarefas, o sistema de base estará pronto para operação e verificação.

Antes de Iniciar

Funções necessárias: administrador para baixar e ativar aplicações e atribuir funções, sn_vul.vulnerability_admin para configurar Resposta a vulnerabilidades.

Procedimento

1. Considere criar e imprimir um PDF desta check-list para que você possa marcar as tarefas ao concluí-las.
2. Para gerar um PDF, clique em **Salvar como PDF** ícone (Na parte superior do tópico e clique em Tópico selecionado.

Resposta a vulnerabilidades tarefas de check-list de implementação básica para administrador

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você obteve todos os direitos e baixou (**Instalar** as seguintes aplicações do ServiceNow® Store em seu ServiceNow AI Platform instância: ○ Resposta a vulnerabilidades ○ Resposta a vulnerabilidades Integração com o NIST National Vulnerability Database ○ Qualys Integração para Operações de segurança **a.** Para verificar se as aplicações estão disponíveis em sua instância, navegue até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e pesquise por [sn_vul], [sn_vul_nvd] e [sn_vul_qualys]. **b.** Se você não conseguir localizar as aplicações, consulte Operações de segurança e o ServiceNow Store para obter mais informações sobre como obter direito e baixar as aplicações.
☐	Como um usuário com a função de administrador, navegue **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ativar (**Instalar** . Resposta a vulnerabilidades junto com suas dependências em seu ServiceNow AI Platform instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Nota: Durante a instalação do Resposta a vulnerabilidades, você tem a opção de instalar dados de demonstração. Os dados de demonstração serão necessários se você quiser executar testes automatizados para confirmar se sua instância funciona após a instalação. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção para evitar corrupção de dados e indisponibilidade. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em não produção ou produção. Assistente de configuração para Resposta a vulnerabilidadesé instalado automaticamente junto com a aplicação . O Assistente de configuração é necessário para configurar o. Resposta a vulnerabilidades aplicação. Além disso, ele é usado para instalar e configurar o. Qualys Aplicação Integration for Security Operations usada neste exemplo, bem como outras aplicações que oferecem suporte e são compatíveis com Resposta a vulnerabilidades. Para obter mais informações sobre como instalar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades.
☐	Como um usuário com a função de administrador, no Assistente de configuração, navegue até **Tudo** > **Usuários e grupos de resposta a vulnerabilidades** e atribua usuários com o necessário Resposta a vulnerabilidades funções de persona. **a.** No Assistente de configuração, exiba os usuários existentes e todas as funções que já estão atribuídas clicando em **Módulo Administração de usuários** link. **b.** Na lista, clique em um nome de usuário para abrir o registro e clique em **Funções** lista relacionada. Todas as funções atribuídas a este usuário são exibidas. **c.** Navegue de volta para **Usuários e grupos de resposta a vulnerabilidades** No Assistente de configuração e siga as instruções para atribuir a função sn_vul.vulnerability_admin. **Nota:** A função sn_vul.vulnerability_admin é necessária para continuar com a configuração. Como alternativa, você pode continuar com a configuração como um usuário com a função de administrador. (Opcional) Você também pode atribuir as funções Gerente de item de configuração (IC) [sn_vul.ci_manager] e Aprovador de exceção [sn_vul.exception_approver], mas essas personas não são necessárias para as tarefas de configuração restantes. Para obter mais informações sobre como atribuir as funções de persona usando o Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre usuários e como atribuir funções a usuários e grupos, consulte Administração de usuários .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
☐	**a.** Navegar até **Tudo** > **Administração** > **Integrações** e verifique **Integração abrangente do CWE 2000** está ativado e executa o trabalho agendado para importar dados. **b.** Como um usuário com a função de administrador, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** e ativar (**Instalar** Integração de resposta a vulnerabilidades com a aplicação NVD. Execute as integrações de NVD e CWE como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros e. Configure e execute o trabalho agendado para atualizar registros CWE Para obter mais informações sobre como instalar, configurar e exibir as bibliotecas NVD e CWE.
☐	Como um usuário com a função de administrador, navegue **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ative Qualys Aplicação de integração para Operações de segurança. Antes de instalar e executar um produto de scanner de terceiros, como Qualys Que tem uma biblioteca, você deve primeiro instalar e executar as Integrações NVD e CWE para ingerir dados de vulnerabilidade. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.
☐	(Opcional) Como um usuário com a função de administrador, se você instalou dados de demonstração com Resposta a vulnerabilidades, você pode executar o. Resposta a vulnerabilidades Pacote de testes ATF para verificar se as aplicações foram instaladas com sucesso. **Nota:** Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção para evitar corrupção de dados e indisponibilidade. Para obter mais informações, consulte Execute o pacote de testes ATF (Automated Test Framework) para Resposta a vulnerabilidades. Para obter mais informações sobre testes automatizados, consulte Automated Test Framework (ATF) .

3. Continue com a configuração das aplicações que começam na seção Configurações de resposta a vulnerabilidades.

Revisar essas configurações ajuda você a entender como Resposta a vulnerabilidades funciona conforme você continua a configurar seu ambiente. Para a integração do scanner usada neste exemplo, é necessário editar as configurações.

Os conceitos usados neste exemplo de configuração para Qualys o produto se aplica a outras aplicações de scanner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Qualys credenciais são necessárias para configurar a aplicação. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por Qualys para que você tenha acesso a eles.

Funções necessárias: sn_vul.vulnerability_admin ou, como alternativa, admin.

Resposta a vulnerabilidades tarefas de check-list de implementação básica para administrador de vulnerabilidades

Tarefa	Descrição
☐	Revise as Regras de atribuição de vulnerabilidades. As regras de atribuição atribuem automaticamente itens vulneráveis (VIS) ao grupo de atribuição apropriado. Para obter mais informações, consulte, Resposta a vulnerabilidades visão geral das regras de atribuição. Para obter mais informações sobre como configurar Resposta a vulnerabilidades Usando o Assistente de configuração, consulte Configurando Resposta a vulnerabilidades Usando o Assistente de configuração.
☐	Revise as regras da tarefa de correção. As regras de tarefa de correção agrupam automaticamente itens vulneráveis (VIS) conforme são importados com base em determinadas condições. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção.
☐	Revise as Calculadoras de risco. As calculadoras de risco pontuam itens vulneráveis para priorização. Você pode configurar calculadoras para incorporar características do item de configuração (IC), disponibilidade de exploração e gravidade da vulnerabilidade relatada pelo fornecedor de avaliação de vulnerabilidade (scanner). Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
☐	Revise as Regras de destino de correção. As regras de destino de correção definem linhas de tempo de correção para tarefas de VIS e correção. Para obter mais informações, consulte Resposta a vulnerabilidades regras de destino de correção.
☐	Na seção Configuração de integração, revise Qualys as configurações da aplicação e definem e programam suas importações de dados. **a.** Clique em **Integrações do scanner** . **b.** Na página Aplicações instaladas, clique em **Editar** . **c.** Insira suas credenciais e clique em **Próximo** . **d.** Leia as descrições da KnowledgeBase Configuration.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	e. Revise a página Configuração de detecção de host para Configurações de importação, Regras de pesquisa de IC e Cronogramas de importação. **f.** Quando estiver satisfeito com as configurações desta página, clique em **Executar agora** para importar dados. Clique em **Exibir detalhes** link exibido para exibir o status de execução da integração de vulnerabilidade. **g.** (Opcional) Continuar a editar as definições de configuração. **h.** Clique em **Concluir** Para concluir a instalação e a configuração no Assistente de configuração. Para obter mais informações sobre como configurar o. Qualys aplicação, consulte Configure o. Qualys Vulnerability Integration Usando o Assistente de configuração.

O que Fazer Depois

Parabéns! Você instalou com sucesso o. Resposta a vulnerabilidades E configurou-o e um aplicativo de scanner usando o Assistente de configuração. O sistema de base agora está pronto para operação.

Para baixar, instalar e configurar outros aplicativos para Resposta a vulnerabilidades, siga as mesmas etapas e conceitos que você concluiu para a check-list anterior. Consulte os tópicos específicos fornecidos para cada aplicação para obter mais informações.

Para obter mais informações sobre os aplicativos compatíveis disponíveis que estão disponíveis para você no ServiceNow Store para Resposta a vulnerabilidades, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

Para obter mais informações sobre como usar Resposta a vulnerabilidades, consulte Explorar o. Resposta a vulnerabilidades aplicação.

Resposta a vulnerabilidades estados da tarefa de correção

As integrações de terceiros importam dados de detecção de item vulnerável que criam novos itens de vulnerabilidade (Vits) ou atualizam os Vits existentes. os estados de detecção atualizam os estados de VIT na medida em que estão abertos ou encerrados.

Para obter mais informações sobre como o estado de uma detecção afeta o estado de uma VIT, consulte Detecções, tarefas de correção e estados de itens vulneráveis.

Com Gestão de mudanças para Resposta a vulnerabilidades, Há um relacionamento sincronizado entre os campos de estado das tarefas de correção e os campos de estado das Solicitações de mudança (CHG) no produto Resposta a vulnerabilidades. À medida que uma solicitação de mudança avança pelo ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente. Depois que uma solicitação de mudança é implementada, a tarefa de correção é resolvida automaticamente. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v23.0 de Resposta a vulnerabilidades:

- . **Aprovação do estado da tarefa de correção** O fluxo de trabalho foi descontinuado e substituído pela Aprovação do estado da tarefa de correção de fluxo no designer de fluxo.
- . **Fechar** o botão foi removido para uma tarefa de correção e o fechamento de uma tarefa de correção é orientado pelo scanner.

A tabela a seguir lista os estados da tarefa de correção e as ações que você pode executar em uma tarefa de correção no respectivo estado:

estados da tarefa de correção

Estado	Descrição
Aberto	Estado após a criação. A partir deste estado, você pode: **Mostrar IVs duplicados** Identificar Vits duplicados relatados por vários scanners no sistema. Você pode marcar o VIT duplicado como Resolvido ou Encerrado. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando Vulnerabilidades e exposições comuns (CVE) . Para obter mais informações, consulte Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável. **Iniciar Investigação** Atribua esta tarefa de correção a uma pessoa ou grupo para começar a investigar. **Marcar como falso positivo** Marque um item ou grupo como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas, na realidade, não houver vulnerabilidade. **Solicitar exceção** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item ou grupo até a data em que uma exceção é solicitada. **Resolver** Marque como Resolvido para mover o item ou grupo para um estado Resolvido. **Criar mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção e Associe uma tarefa de correção a uma solicitação de mudança existente. **Tarefa de correção dividida** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Divida uma tarefa de correção no Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados da tarefa de correção

Estado	Descrição
	Adiar Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Excluir** Confirmar a exclusão. Remove o grupo.
Sob Investigação	Acionado por **Iniciar investigação** botão. Neste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Criar mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção e Associe uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Divida uma tarefa de correção. **Crie uma solicitação de mudança** Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção. **Aguardando Implementação** Muda o estado para Aguardando implementação. Este estado indica que as tarefas de correção foram referenciadas fora de um Resposta a vulnerabilidades. **Adiar** Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.
Adiado	Acionado por **Exceção de solicitação** botão. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser encerrado até ser aprovado. Neste estado, você pode: **Criar mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados da tarefa de correção

Estado	Descrição
	de correção e Associe uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para um novo VG. Consulte Divida uma tarefa de correção. **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. As informações de adiamento aparecem em **Encerrar/Adiar** guia. Na data de adiamento, o grupo é reaberto para correção.
Aguardando Implementação	Acionado por **Aguardando implementação** botão. Neste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Criar mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção e Associe uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Divida uma tarefa de correção. **Crie uma solicitação de mudança** Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção. **Adiar** Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Resolver** Adicionar anotações. O estado se torna Resolvido. As anotações aparecem em **Resolução** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados da tarefa de correção

Estado	Descrição
	Excluir Confirmar a exclusão. Remove a tarefa de correção.
Resolvido	Acionado a partir de **Resolver** botão. A partir deste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Criar mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção e Associe uma tarefa de correção a uma solicitação de mudança existente. **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. As anotações aparecem em **Anotações** guia. As informações de resolução aparecem em **Resolução** guia.
Encerrado	Acionado pelo scanner. Neste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. As informações de fechamento aparecem em **Encerrar/Adiar** guia.

- O responsável pela correção só pode marcar um item vulnerável ou tarefa de correção como resolvido. Com base na confirmação do scanner, este item resolvido ou tarefa de correção pode ser marcado como encerrado ou reaberto.
- . **Excluir** o botão está disponível para o administrador quando há vários itens vulneráveis criados manualmente e eles precisam ser encerrados ou excluídos.
- Se você determinar que os itens são de baixo risco, aguardando uma janela de mudança ou um patch, poderá mudar a tarefa de correção para o Adiamento vermelho estado por um período definido .Você pode solicitar uma exceção usando **Exceção de solicitação** opção.

Nota: Quando as tarefas de correção são adiadas ou encerradas, você pode especificar resoluções para definir melhor os motivos para isso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando uma VIT é reaberta, manual ou automaticamente, acontece o seguinte:
  - O estado de VIT muda para Aberto. O estado da tarefa de correção original não é atualizado.
  - O VIT é reavaliado e colocado em uma tarefa de correção nova ou existente que é baseada nas regras de tarefa de correção ativas.

  Isso preserva seu histórico e permite correções adicionais.

- Quando uma tarefa de correção é criada (automática ou manualmente), ou dividida, é **Estado** , **Motivo** e **Até** os campos são avaliados. No caso da ação de divisão, esses campos são avaliados para as tarefas de correção antigas e novas. Quando um VIT é atualizado, o **Estado** , **Motivo** e **Até** os campos de todas as tarefas de correção associadas são avaliados.
  - Se todos os Vits em uma tarefa de correção forem adiados e tiverem o mesmo motivo, o estado da tarefa de correção mudará para **Adiado** E o motivo dos Vits é atribuído à tarefa de correção. Se o motivo dos Vits for diferente, o motivo da tarefa de correção mudará para **Nenhum** .
  - O mais próximo **Até** A data de todos os Vits é atualizada em **Até** campo da tarefa de correção.
  - Se você reabrir qualquer VIT, o estado da tarefa de correção mudará para **Aberto** .

  Esta avaliação é feita pelo *`Rollup vulnerability item values to vulnerability and group`*trabalho agendado, que é executado a cada 15 minutos.

Detecções, tarefas de correção e estados de itens vulneráveis

Integrações de terceiros recuperam os dados de detecção de item vulnerável. Detecções são ocorrências distintas de vulnerabilidades conforme relatadas pelos scanners.

Os dados de detecção são emparelhados com itens vulneráveis (VIS, Vits) e o estado de VI é atualizado com base no estado das detecções. Se uma VI não for encontrada, uma nova será criada. As detecções são abertas ou fechadas somente pelos dados encontrados diretamente por um scanner.

Se todas as detecções forem encerradas para um item vulnerável, esse item vulnerável será encerrado. No registro VI, o estado é Encerrado/Fixo. Quando todos os VIS são encerrados para uma tarefa de correção, a tarefa de correção é encerrada. Caso contrário, o fluxo de estado permanece o mesmo.

Os VIS encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e o VIS puder ser correspondido à nova vulnerabilidade.

A partir da versão 20,0 de Resposta a vulnerabilidades Se uma detecção estiver obsoleta e o VI associado estiver no estado Encerrado, o estado do VI não fará a transição para Encerrado - obsoleto. Evitar que o VI seja reaberto quando uma nova detecção for identificada, para que você possa evitar passar por todo o processo de solicitação e aprovação de falso-positivo. Para reverter esse comportamento, desmarque **Ignorar detecções obsoletas para VIS encerrados** Caixa de seleção no formulário Configuração de fechamento automático. Para obter mais informações, consulte Fechar automaticamente detecções obsoletas em Resposta a vulnerabilidades.

De acordo com a inclusão de script, *`DetectionBase`*método *`_shouldReOpenVI()`*Se o VI tiver sido encerrado anteriormente com um subestado de Fixo, obsoleto ou IC desativado, ele será reaberto e a detecção será mapeada para o VIT existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, digamos que a data de encerramento de uma VI seja posterior à data mais recente de uma detecção. Esses registros de VI permanecerão encerrados. No entanto, se você vir que uma VI fechada anteriormente foi reaberta, isso significa que a VI foi fechada por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando uma nova detecção é encontrada que corresponde à VIT fechada que tem a mesma vulnerabilidade no item de configuração da VI, a VI é reaberta.

Tarefas de correção e estados de item vulnerável

Tarefas de correção e estados de itens vulneráveis podem afetar uns aos outros. Na maioria das vezes, um estado de tarefa de correção atualiza o estado do item vulnerável, com o estado de tarefa de precedência mais alta usado para atualizar os itens vulneráveis no grupo.

A precedência de estado é a seguinte.

Encerrado > **Adiado** > **Resolvido** > **Em revisão** > **Aguardando Implementação** > **Sob Investigação** > **Aberto**

- Quando um grupo de itens vulneráveis está em uma tarefa de correção e não é alterado em um nível individual, eles têm o mesmo estado da tarefa de correção.
- Quando a tarefa de correção passa do estado Aberto para Aguardando implementação, todos os VIS na tarefa de correção são movidos para o estado Aguardando implementação.
- Quando a tarefa de correção é adiada, a VI também é adiada. A partir da versão 16,5, você pode rastrear o número de vezes que um item vulnerável, item vulnerável à aplicação, item vulnerável ao contêiner ou uma tarefa de correção é adiada. O trabalho agendado, `set deferral counts` É executado diariamente para contabilizar contagens para os registros que são adiados mais de uma vez na coluna Contagem de adiamentos nos módulos de vários adiamentos para VR, AVR e CVR. Todas as contagens de VIS associadas a uma tarefa de correção serão coletadas e publicadas se uma tarefa de correção for adiada mais de uma vez.

Itens vulneráveis atualizados somente por tarefas de correção

Os itens correspondem ao estado da tarefa de correção, se não tiverem sido atualizados individualmente, com estas exceções:

- Se o estado da tarefa de correção mudar para Encerrado e sua resolução para Cancelado ou Corrigido com exceção, o item não será afetado e assumirá o estado de qualquer outra tarefa de correção que o contenha. Se o item vulnerável não estiver em outra tarefa de correção, ele será revertido para o estado Aberto.
- Se o estado do item vulnerável for Encerrado/Corrigido (atualizado por uma verificação ou importação), quando a tarefa de correção mudar seu estado, o item vulnerável permanecerá no estado Encerrado/Corrigido. Esta condição é verdadeira, independentemente do estado em que a tarefa de correção esteja.

Itens vulneráveis em estados definidos individualmente

Itens vulneráveis, em um estado atualizado no item, como os itens encerrados ou adiados individualmente, não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele compara seu estado com todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Nota:** O estado Encerrado/Fixo é um caso especial. Para os itens vulneráveis definidos com o estado Encerrado/Fixo, se todos os itens vulneráveis em uma tarefa de correção estiverem definidos como Encerrado/Corrigido, como quando um scanner descobrir que todas as vulnerabilidades foram corrigidas, a tarefa de correção será marcada automaticamente como Encerrado/Corrigido.

As tarefas de correção contêm campos de atribuição vazios

Se o estado do VIS em uma tarefa de correção mudar de Resolvido para Aberto, o estado da tarefa de correção também será atualizado de Resolvido para Em investigação.

No entanto, se ambos forem **Atribuído a.** e. **Grupo de atribuição** Os campos na tarefa de correção estão vazios, a tarefa de correção permanece no estado Resolvido e não é movida para Em investigação.

O grupo de atribuição para itens vulneráveis nem sempre é atualizado quando sua tarefa de correção é atualizada

Se o grupo de atribuição de uma VI no estado Aberto for atualizado manualmente, ele não será atualizado novamente quando o grupo de atribuição da tarefa de correção for atualizado. Essas informações não são substituídas porque o grupo de atribuição do VI foi atualizado intencionalmente e pode fazer parte de outra tarefa de correção.

Cenários de roll-up e roll-down de estado

Os cenários de roll-up e roll-down de estado sincronizam automaticamente o status das tarefas de correção (RTS) e dos itens vulneráveis (Vits), garantindo atualizações em tempo real em ambos. Essa interação dinâmica reduz o acompanhamento manual, aumenta a precisão e fornece aos usuários uma exibição atualizada do andamento, tornando a gestão de vulnerabilidades mais eficiente e ajudando os usuários a tomar decisões informadas rapidamente.

Comportamento de acúmulo

Quando os estados de item vulnerável (VIT) mudam, essas mudanças podem se propagar até o nível da tarefa de correção (RT). A tabela a seguir resume os principais cenários de acúmulo em que as mudanças no estado de item vulnerável (VIT) podem influenciar o estado da tarefa de correção (RT) associada, com base nas condições de fechamento, reatribuições e adiamentos.

Cenários de acúmulo

Estado de VIT	Estado de RT
Aberto > Em investigação	Permanece aberto
Aberto > Encerrado-Falso-Positivo	Permanece aberto
Abrir > Em Revisão	Permanece aberto
Aberto > Adiado (qualquer subestado)	Aberto > Adiado
Aberto > Resolvido	Permanece aberto
Aberto > Encerrado-Cancelado	Permanece aberto
Aberto > Encerrado-fixo	Aberto > Encerrado-fixo
Aberto > Encerrado-Corrigido com exceções	Aberto > Encerrado
Encerrado-fixo > Abrir	Fechado - fixo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cenários de acúmulo

Estado de VIT	Estado de RT
Aberto > Encerrado-fixo; (após a próxima verificação) > Resolvido	Permanece aberto
Aberto > Encerrado-Inválido	Permanece aberto
Aberto > Encerrado-obsoleto	Aberto > Encerrado-Cancelado
Encerrado-obsoleto > Abrir	Encerrado-Cancelado
Aberto > Encerrado-Resultado inválido	Permanece aberto
Aberto > Encerrado-Inválido	Permanece aberto
Encerrado > Encerrado-IC desativado	Aberto > Encerrado-Cancelado
Aguardando implementação - Patch agendado	Permanece aberto
Aguardando implementação - Patch não programado	Permanece aberto
Aguardando implementação - Patch programado (data de destino ausente)	Permanece aberto
Em investigação > IC encerrado desativado	RT1: Em investigação > Encerrado-Cancelado RT2: Em investigação > Encerrado-Cancelado
RT: Resolvido; reabre VIT	Se atribuído, RT: Resolvido > Em investigação; Caso: Aberto
VIT1: Encerrado-fixo VIT2: Em investigação Se VIT2 reabrir e VIT1 permanecer resolvido.	RT1: Em investigação RT2: Encerrado-fixo
VIT1: Encerrado-obsoleto VIT2: IC encerrado desativado	Aberto > Encerrado-Cancelado
VIT1: Resolvido VIT2: IC encerrado desativado	Permanece aberto
VIT1: Encerrado-fixo VIT2: IC encerrado desativado	Aberto > Encerrado-Cancelado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cenários de acúmulo

Estado de VIT	Estado de RT
VIT1: Encerrado-fixo VIT2: Encerrado-obsoleto	Aberto > Encerrado-fixo
VIT1: Closed-<any sub-state> VIT2: Adiado	Aberto > Adiado Até a data carregada fwd como VIT2

Comportamento de rolagem

Quando o estado de uma tarefa de correção muda, o estado geralmente é propagado para os Vits associados, a menos que seja substituído por atualizações manuais ou exceções específicas. A tabela a seguir resume os principais cenários de rolagem em que as mudanças no estado da tarefa de correção (RT) podem afetar o estado do item vulnerável (VIT) associado, com base em regras de precedência e condições especiais.

Cenários de rolagem

Estado de RT	Estado de VIT
Aberto > Em investigação	Aberto > Em investigação
Aberto > Encerrado-Falso-Positivo	Aberto > Encerrado-Falso-Positivo
Abrir > Em Revisão	Abrir > Em Revisão
Aberto > Adiado (subestado: Motivo fornecido)	Aberto > Adiado (subestado: Motivo fornecido)
Aberto > Resolvido	Aberto > Resolvido
Aberto > Encerrado-Cancelado	Permanece aberto
Aberto > Encerrado-Corrigido com exceções	Permanece aberto
RT1: Aberto > Em investigação RT2: Aberto	Aberto > Em investigação
RT1: Aberto > Em investigação > Aguardando implementação RT2: Sob investigação	Aberto > Em investigação > Aguardando implementação
RT1: Aguardando implementação > Adiado RT2: Aguardando implementação	Aguardando implementação > Adiado
RT1: Aguardando implementação > Encerrado-Cancelado RT2: Sob investigação	Aguardando implementação> Em investigação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cenários de rolagem

Estado de RT	Estado de VIT
Aberto > Encerrado-Corrigido com exceções Observações Finais: VIT2 permanece em aberto	VIT1: Aberto > Encerrado-fixo VIT2: Aberto
Aberto > Resolvido Observações finais: VIT2: Aberto>Resolvido	VIT1: Aberto > Encerrado-fixo VIT2: Aberto
Aberto > Resolvido VIT2 reabre; VIT1 permanece resolvido; RT: Resolvido > Aberto	VIT1: Aberto > Encerrado-fixo VIT2: Aberto

Estado da tarefa de correção para itens vulneráveis (Vits) em vários grupos

Quando um VIT está em várias tarefas de correção (RT nas tabelas a seguir) e seu próprio estado não foi definido, o estado do grupo de precedência mais alto determina o estado desse VIT, conforme mostrado na tabela a seguir.

Exemplos de estados de item vulnerável

Estado de tarefas de correção	Estado do item vulnerável
RT 1: **Aberto** > **Sob Investigação** RT 2: **Aberto**	**Sob Investigação** Quando o RT 1 está sob investigação e o RT 2 está aberto, o VI muda para Em investigação. Após a pesquisa, entre RT 1 e RT 2, RT 1 tem o estado com a precedência mais alta.
RT 1: **Em investigação** RT 2: **Aberto** > **Sob Investigação**	**Em investigação** Quando o RT 2 está sob investigação e o RT 1 está sob investigação, o VI permanece como sob investigação. Após a pesquisa, entre RT 1 e RT 2, eles têm o estado com a mesma precedência.
RT 1: **Em investigação** RT 2: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o RT 2 está aguardando implementação e o RT 1 está sob investigação, o VI muda para Aguardando implementação. Após a pesquisa, entre RT 1 e RT 2, RT 2 tem o estado com a precedência mais alta.
RT 1: **Sob Investigação** > **Adiado** RT 2: **Aguardando Implementação**	**Adiado** Quando o RT 1 é adiado e o RT 2 está aguardando implementação, o VI muda para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de estados de item vulnerável

Estado de tarefas de correção	Estado do item vulnerável
	Adiado. Após a pesquisa, entre RT 1 e RT 2, RT 1 tem o estado com a precedência mais alta.

Itens vulneráveis em casos especiais de vários grupos

Estado da tarefa de correção	Estado do item vulnerável
RT 1: **Sob Investigação** RT 2: **Aguardando Implementação** > **Encerrado (fixo ou cancelado)**	**Sob Investigação** Quando o RT 2 é encerrado/fixo ou encerrado/cancelado e o RT 1 está sob investigação, o VI muda de Aguardando implementação (anteriormente a precedência mais alta) para Em investigação (atualmente a precedência mais alta).
RT 1: Qualquer estado RT 2: Qualquer estado	Se o status da origem do item vulnerável for Corrigido (atualizado por uma verificação ou importação), quando o grupo mudar seu estado, o item vulnerável mudará seu estado para Encerrado/Corrigido. Esta condição é verdadeira, independentemente dos estados em que os outros grupos associados estão. A pesquisa de item vulnerável para o estado do grupo não ocorre.

Quando um estado de VI é definido individualmente, seu estado é considerado ao avaliar a precedência, como em qualquer outra tarefa de correção. Quando uma VI pertence a mais de uma tarefa de correção, a tabela a seguir lista as atualizações feitas.

Casos especiais definidos individualmente pelo estado do item vulnerável

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado de RT 1: **Sob Investigação** Estado de RT 2: **Sob Investigação** > **Aguardando Implementação** Estado do VI original: **Sob Investigação** > **(Definido no VI)**	**Aguardando Implementação** Quando o RT 2 passou para Aguardando implementação e o RT 1 permaneceu sob investigação, o VI muda para Aguardando implementação (a precedência mais alta).
RT 1: **Sob Investigação** RT 2: **Sob Investigação** > **Aguardando Implementação** Estado do VI original: **Adiado** > **(Definido no VI)**	**Adiado** Quando o RT 2 passou para Aguardando implementação e o RT 1 permaneceu sob investigação, o VI permanece no estado Adiado (a precedência mais alta).

A tabela a seguir mostra que, quando duas tarefas de correção com itens vulneráveis comuns são adiadas, o estado é adiado até que a data mais recente seja atingida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos especiais de estado adiado do item vulnerável

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado de RT 1: **Em análise (até abril de 10)** Estado de RT 2: **Sob Investigação** > **Em análise (até abril de 30)** Estado do VI original: **Em análise (até abril de 10)** > **(Definido no VI)**	**Adiado (até abril de 30)** Quando o RT 2 passou para Adiado (até abril de 30) e o RT 1 permanece adiado (até abril de 10), o VI muda de Adiado (até abril de 05) para o estado Adiado (até abril de 30).
RT 1: **Em análise (até julho de 15)** RT 2: **Sob Investigação** > **Em análise (até julho de 10** Estado do VI original: **Adiado** > **(Até julho de 15)**	**Adiado (até julho de 15)** Quando o RT 2 passou para Adiado (até Jul-10) e o RT 1 permanece Adiado (Jul-15), o VI permanece em Adiado (até Jul-15).

Configurações adicionais para Domain Separation

Para execução e resultados precisos, as seguintes precauções e configurações são necessárias para a separação de domínio em Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações.

Não modifique as lógicas de negócios e os processos no domínio global para evitar problemas para que todas as mudanças mais recentes sejam atualizadas a cada upgrade. Duplique todas as lógicas e processos de negócios em cada domínio separadamente e certifique-se de que eles estejam inativos no domínio global. Caso contrário, as lógicas de negócios e os processos no domínio global terão precedência sobre o domínio secundário. Suponha que você tenha criado uma regra de risco em um domínio secundário e o domínio global também tenha uma regra de risco semelhante, então a regra do domínio global tenha precedência sobre a regra do domínio secundário.

Reavaliação de calculadoras e regras

Antes da v20.0, quando você reaplica calculadoras ou regras, o. `executar novamente` o sinalizador é definido como verdadeiro e uma regra de negócio é acionada para executar um trabalho de programação que reaplica as calculadoras e as regras. A partir da v20.0, você não precisa depender de `executar novamente` sinalizador. Ao clicar em **Reaplicar Calculadora** um trabalho em segundo plano é acionado que reaplica as calculadoras e as regras. Isso permite que você crie calculadoras e regras para todos os domínios.

Configurações para calculadoras de acúmulo

Em um domínio, somente uma calculadora de acúmulo deve estar ativa para uma tabela. Por exemplo, considere a tabela Tarefa de correção, *sn_vul_vulnerability*com a calculadora de acúmulo, **Acúmulo de tarefa de correção** no domínio global. Se você duplicar esta calculadora de acúmulo alterando os pesos da mesma tabela no mesmo domínio, haverá discrepâncias nos cálculos de acúmulo. Portanto, certifique-se de ativar apenas uma calculadora de acúmulo se houver duas ou mais calculadoras de acúmulo para uma tabela no mesmo domínio.

Campos do formulário Itens descobertos

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) no Configuration Management Database (CMDB) Quando são importados usando as Regras de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pesquisa de IC. Registros de ICs incompatíveis são criados automaticamente durante as importações de integração de vulnerabilidades de terceiros e incluídos nos itens descobertos. No entanto, para ativos de nuvem que não estão presentes em CMDB CL, o registro é criado na classe de recursos de nuvem.

Campos de Itens descobertos

As informações nesses registros são ingeridas a partir de registros de terceiros e classificadas durante a importação.

Esses campos são encontrados nos registros listados na tabela Itens descobertos [sn_sec_cmn_src_ci].

Para exibir dados importados nos campos listados nas tabelas a seguir, você deve ter, no mínimo, a função sn_vul.read_all.

Campo	Descrição
Número	Identificador atribuído ao registro.
Item de configuração	Item de configuração importado da integração de origem de terceiros. A partir da v12.0, o Item de configuração é o IC mais recente da lista de ICs após a filtragem dos desativados.
Classe	Classe atribuída ao IC durante a importação por Resposta a vulnerabilidades.
Origem	Origem importada da integração de origem de terceiros.
Regra de correspondência de IC	A regra de correspondência de IC que foi usada para criar o item.
V18.0: Tipo de correspondência para o DI	Tipo de correspondência usado para criar o item descoberto. As opções são: • Criado por VR • Criado por IRE • Correspondido por pesquisa de IC • Correspondido por IRE • Correspondido manualmente (começando com v24.0.6 de Resposta a vulnerabilidades, você pode exibir esta opção adicional. Esta opção será definida automaticamente se você atualizar manualmente um IC no formulário Item descoberto.) Essas informações só estão disponíveis para dados preenchidos para Resposta a vulnerabilidades v18.0 e posterior. Em dados existentes, esta coluna não contém nenhum valor. **Nota:** Se você reaplicar as regras de pesquisa de IC, alguns ICs em DIS poderão ser atualizados, resultando no preenchimento desta coluna.
Outros ICs correspondentes	Lista de outros itens de configuração correspondentes à regra de pesquisa de IC.
Estado	Estado do IC que é determinado durante a importação. As opções são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• **Correspondido** : Um item de configuração correspondente foi encontrado no CMDB. • **Incompatível** Nenhuma correspondência encontrada no CMDB. Um registro de espaço reservado é criado.
Criação em	Data em que o registro do Item descoberto foi criado.
Atualização em	Data em que o registro do Item descoberto foi atualizado.
Atualização de	Usuário que atualizou os dados.
Marcador de host	Marcadores de host atribuídos a este item descoberto durante a importação. Você pode ter até 31 marcadores de host por item descoberto.
Nome de domínio totalmente qualificado	Dados associados a este IC encontrados no CMDB.
Endereço MAC	Dados associados a este IC encontrados no CMDB.
Sistema operacional	Sistema operacional associado a este IC.
NetBIOS	NetBIOS importado da integração de origem de terceiros.
Endereço IP	Dados associados a este IC encontrados no CMDB.
Dados de origem	Dados mais recentes associados a este IC da origem.
V16: Dados de origem inicial	Dados iniciais associados a este IC da origem.
V16: Reavaliar IC	Recebe dados do scanner. Se houver dados atualizados, o valor será definido como verdadeiro. **Nota:** Os valores de dados de origem são recalculados de acordo com os dados de origem mais recentes. Quando os dados atualizados são recuperados do scanner, os dados de origem são atualizados. O valor de dados de origem existente é movido para o campo Dados de origem inicial. Para reavaliar os itens descobertos, ative Reaplique as regras de pesquisa de IC nos itens descobertos alterados trabalho agendado.
Agente existe	Indica verdadeiro se o agente estiver instalado no ativo. . HostUID e. UUID Os valores na coluna Dados de origem estão vazios, este valor é preenchido como verdadeiro . **Nota:** Este campo aparece a partir de v19.0 de Resposta a vulnerabilidades.

A partir da v23.0 de Resposta a vulnerabilidades. **% De conformidade do resultado do teste (IC)** A coluna mostra a porcentagem de resultados de teste que estão em conformidade com o IC correspondente. Para obter esse valor, você deve definir CalcTRConformidade para CI . verdadeiro em **Atualizar métricas de correção** trabalho agendado.

Nota: . **% De conformidade do resultado do teste (IC)** O valor é preenchido somente para os itens descobertos que têm um valor não vazio em **Data da última verificação de conformidade da configuração** ou **Data da última verificação de conformidade fora de infraestrutura** colunas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 18,0 de Resposta a vulnerabilidades, Qualys, Tenable para Resposta a vulnerabilidades e. Rapid7 os scanners podem receber os seguintes metadados adicionais para ativos de nuvem.

Campo	Descrição
Provedor de serviços em nuvem	Nome do provedor de serviço de nuvem que oferece serviços de computação em nuvem. Por exemplo, Amazon Web Services(AWS), Microsoft Azure e. Google Cloud Platform (GCP).
Região da nuvem	Local onde o recurso foi hospedado.
Conta de nuvem	Conta fornecida por provedores de serviço em nuvem, como AWS, GCP e assim por diante para acessar serviços de computação em nuvem.
Tipo de recurso de nuvem	Tipos de ativos presentes na nuvem, como máquina Amazon Elastic Compute Cloud (EC2), AWS Buckets do S3 e assim por diante.
ID do recurso	Identificador exclusivo atribuído a um recurso em um ambiente de computação em nuvem. Este ID é usado para identificar e gerenciar o recurso.
Nome do recurso	Nome definido pelo usuário usado para identificar e gerenciar um recurso em um ambiente de computação em nuvem.
Imagem	Uma imagem de máquina virtual ou uma imagem de servidor é uma máquina virtual pré-configurada que contém um sistema operacional, aplicativos e outros softwares. Por exemplo, Imagem de máquina da Amazon.

Uma nova regra de pesquisa de IC, "ID de recurso de nuvem", foi introduzida para corresponder aos ICs de nuvem com base nos metadados de nuvem.

Resposta a vulnerabilidades campos do formulário vulnerabilidade

As vulnerabilidades são criadas automaticamente quando os registros são baixados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou integrações de terceiros e armazenados em **Bibliotecas** em Resposta a vulnerabilidades.

Campos de entrada de NVD

Para exibir dados importados nos campos listados nas tabelas a seguir, você deve ter, no mínimo, a função sn_vul.read_all.

Esses campos são encontrados nos registros listados na tabela Entradas do banco de dados nacional de vulnerabilidades [sn_vul_ntd_entry].

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Classificação de risco	(Oculto quando nenhum Vits está associado à vulnerabilidade) Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta base **Classificação de risco** Não é igual ao registro Solução **Classificação de risco.**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pontuação de risco	(Oculto quando nenhum Vits está associado à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Esta base **Pontuação de risco** Não é igual ao registro Solução **Pontuação de risco.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de gravidade, consulte Crie um Resposta a vulnerabilidades mapa de severidade.
Exploração presente	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Nível de habilidade da exploração	O nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque da exploração	Vetor de ataque mais vulnerável das explorações desta vulnerabilidade. Disponível quando SAM NVD está habilitado.
IVs ativos	(Oculto quando nenhum Vits está associado à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado. Se não houver nenhum VIS ativo para esta vulnerabilidade, **Classificação de risco** e. **Pontuação de risco** não são exibidos.
Entrada de CWE	Referência ao elemento de enumeração de pontos fracos comuns ao qual esta vulnerabilidade se encaixa melhor.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Ameaças (começando com Resposta a vulnerabilidades versão 20,0)	Inteligência contra ameaças fornecida por Qualys. Com esses dados, você pode entender os motivos, os objetivos e os comportamentos de ataque de um agente de ameaça.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando nenhum Vits está associado à vulnerabilidade) Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Exploração CISA (Esta guia está disponível somente quando a aplicação CISA está instalada.)	
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.
Data de inclusão	Data em que a vulnerabilidade foi adicionada ao catálogo da CISA.
Produto	Produto no qual a vulnerabilidade foi identificada.
Fornecedor/projeto	Fornecedor associado à vulnerabilidade identificada.
Ransomware conhecido A partir de v21.0 de Resposta a vulnerabilidades.	Selecionado quando o campo **Conhecido por ser usado em campanhas de ransomware** É ingerido do catálogo Vulnerabilidades exploradas conhecidas (KEVs) da CISA. O sinalizador é definido no nível CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) e acumulado para a entrada de terceiros (TPE).
Status da Correção (Oculto quando nenhum VIS está associado à vulnerabilidade)	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Atualizar status	Exibe data e hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação de risco e classificação • Métricas como Vits ativos, Total de Vits da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando nenhum Vits está associado à vulnerabilidade)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.
Soluções	(Oculto quando nenhum Vits está associado à vulnerabilidade) Todos Solução de gestão de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Pontos fracos	Importado **Fraqueza** Dados associados a CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns).
Software Vulnerável	(Oculto quando o software está associado ao CVE) Dados de enumeração de plataforma comum (CPE) importados associados à vulnerabilidade.
Kits de Malware de Vulnerabilidade	Malware importado de várias origens de scanner para uma vulnerabilidade.

Campos de entrada de vulnerabilidade do CWE

Esses campos são encontrados nos registros listados na tabela CWEs [sn_vul_cwe].

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para Categorias e Pontos fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.
Probabilidade de exploração	Qual a probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Desconhecido • Baixo(a) • Média • Alto(a)
10 principais posições da OWASP	Posição numérica desta vulnerabilidade na lista dos 10 principais OWASP.
Posição SANS para 25	Posição numérica desta vulnerabilidade na lista dos 25 principais SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Estável • Preterido • Obsoleto • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualização em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivo** . Preenchido somente para 24/862 pontos fracos.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório** . Preenchido somente para 51/863 pontos fracos.
URL	artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.
Execução de integração	A execução de integração na qual este CWE foi importado.
Seções	
Detalhes adicionais	Descrições de conceito de software que explicam melhor o ponto fraco. Inclui: • Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que o ponto fraco é introduzido, por exemplo, **Implementação** , **Arquitetura e Design** e assim por diante.
Exemplos demonstrativos	Exemplos de código do ponto fraco com descrições de acompanhamento.
Mitigações potenciais	Detalhes sobre como evitar a fraqueza, incluindo em qual fase do ciclo de vida da aplicação ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/antecede, requiredby/requer (para pontos fracos compostos), CanAlsoBe, PeerOf, MemberOf.
Exemplos observados	Alguns CVEs que são representativos desta fraqueza.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: Confidencialidade Impacto: Ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Campos de entrada de vulnerabilidade de terceiros

Esses campos são encontrados nos registros listados na tabela Entradas de vulnerabilidade de terceiros [sn_vul_third_party_entry].

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Versão 16,0: CVEs	Várias vulnerabilidades e exposições comuns (CVEs) associadas a esta vulnerabilidade de terceiros.
Origem	Origem da vulnerabilidade - seja um scanner ou teste físico.
Classificação de risco	Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte, Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta base **Classificação de risco** Não é igual ao registro Solução **Classificação de risco**
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para seu ambiente, com base na pontuação de risco. **Nota:** Esta base **Pontuação de risco** Não é igual ao registro Solução **Pontuação de risco.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de gravidade, consulte Crie um Resposta a vulnerabilidades mapa de severidade.
Exploração presente	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nível de habilidade da exploração	O nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque da exploração	Vetor de ataque mais vulnerável das explorações desta vulnerabilidade.
IVs ativos	Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado.
Categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Tipo de correção	Tipos de ações de correção. • Patch • Mudança de configuração • Mudança de Configuração e Patch • Contramedida
Entrada de CWE	Referência ao elemento de enumeração de pontos fracos comuns ao qual esta vulnerabilidade se encaixa melhor.
PCI	Quando a caixa de seleção é marcada, a vulnerabilidade é sinalizada por risco significativo de exposição de informações de pagamento.
Gravidade de PCI	Nível de risco de exposição das informações de pagamento. [Somente Qualys.]
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados CVSS v3 importados, não disponíveis antes de 2015.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Solução preferencial	Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Anotações de correção	Descrição da solução de correção extraída do fornecedor.
Status da Correção	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Atualizar status	Exibe data e hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação de risco e classificação • Métricas como VIS ativo, total de VIS da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
CVEs	Registro CVE (Common Vulnerability Enumeration, enumeração de vulnerabilidades comuns) associado a esta vulnerabilidade.
Categorias	Categorias associadas a esta vulnerabilidade.
Explorações	Explorações associadas a esta vulnerabilidade.
Kits de Malware de Vulnerabilidade	Kits de malware associados a esta vulnerabilidade.
Soluções (Rapid7)	Informações da solução das integrações da solução Rapid7. Exibido quando disponível.
Estruturas de Exploração	Estruturas de exploração associadas a esta vulnerabilidade.
Soluções	Solução de gestão de vulnerabilidade soluções associadas a esta vulnerabilidade.
Exploração CISA	
CISA existe	A exploração da CISA existe para a tabela de entrada Vulnerabilidades de terceiros.
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.

Campos do formulário de tarefa de correção

Usando tarefas de correção, o analista pode monitorar o andamento e conduzir o processo de mediação com mais eficiência.

Esses campos são encontrados nos registros listados na tabela Tarefa de correção [sn_vul_vulnerability].

Para exibir dados importados nos campos listados nas tabelas a seguir, você deve ter, no mínimo, a função sn_vul.read_all.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de tarefa de correção

Campo	Descrição
Número	O número do item vulnerável (VI) gerado automaticamente para este registro.
Classificação de risco	Acúmulo de pontuações de risco de item vulnerável separadas em intervalos: Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte, Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta base **Classificação de risco** Não é igual ao registro Solução **Classificação de risco.**
Pontuação de risco	Acúmulo das pontuações de risco de todos os itens vulneráveis associados a esta tarefa de correção. Quantidade de risco que os itens vulneráveis, coletivamente, representam para o seu ambiente. **Nota:** Esta base **Pontuação de risco** Não é igual ao registro Solução **Pontuação de risco.**
Meta da correção	Data em que os itens vulneráveis devem ser corrigidos, desde que identificados pela primeira vez. Para obter mais informações sobre metas de correção, consulte Resposta a vulnerabilidades regras de destino de correção.
Status da correção	Status da correção da tarefa. É determinado pelo item vulnerável com a data de vencimento mais próxima. Para grupos em aberto, os estados incluem: • Em andamento • Perto da meta • Meta não atingida Para grupos encerrados, os estados incluem: • Nenhuma Meta • Meta atingida • Meta não atingida Para datas de destino de correção calculadas, se a tarefa for encerrada, o status geral de correção de todos os itens vulneráveis encerrados será mostrado na tarefa. Esses determinam se a tarefa atendeu à data ou não. O status de correção de uma tarefa encerrada é **Nenhum destino** se nenhum dos itens encerrados tiver uma data de destino de correção. É **Meta perdida** se algum de seus itens encerrados perdeu a data de destino. É **Meta atingida** Se pelo menos um VI fechado atingiu sua meta e nenhum dos outros falhou.
Estado	Status do andamento da tarefa. Os estados incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

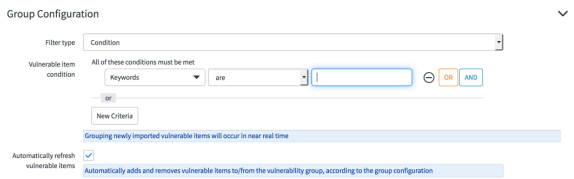
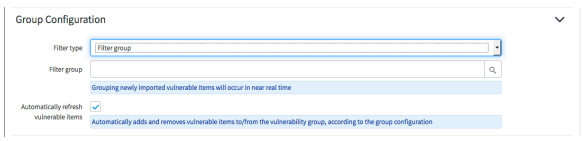
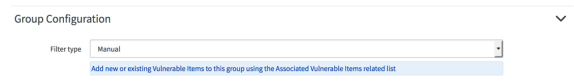
Campos de tarefa de correção

Campo	Descrição
	• Aberto • Sob Investigação • Aguardando Implementação • Adiado • Em revisão • Resolvido • Encerrado Para obter mais informações sobre os estados, consulte Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável.
Até a data para redução de risco	Data em que os controles compensatórios aplicados à tarefa de correção expiram. **Nota:** Este campo aparece somente quando o valor está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criação em	Data em que esta tarefa de correção foi criada.
Atualização em	Data em que esta tarefa de correção foi atualizada pela última vez.
Vulnerabilidade	Vulnerabilidade aplicável à tarefa. (Visível quando o grupo é formado com base em uma única vulnerabilidade.)
Descrição resumida	Breve descrição desta tarefa de correção.
Em Revisão (Visível quando o RT está no estado Em revisão)	
Solicitação de	Indivíduo que solicitou o adiamento.
Motivo desejado	Motivo do adiamento.
Estado desejado	O estado solicitado do aprovador.
Subestado desejado	O motivo solicitado ao aprovador.
Adiamento (Visível quando a tarefa está no estado Adiado)	
Adiado por	Indivíduo que adiou a tarefa.
Adiar expiração	Data em que o adiamento expira.
Motivo para adiar	Motivo do adiamento.
Resolução (Visível quando o RT está no estado Resolvido)	
Resolvido por	Indivíduo que resolveu a tarefa de correção.
Data de resolução	Data em que a tarefa de correção foi resolvida.
Anotações de resolução	Informações adicionais.
Fechar (Visível quando o RT está no estado Encerrado)	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de tarefa de correção

Campo	Descrição
Encerrado por	Indivíduo que resolveu a tarefa de correção.
Encerrado	Data em que a tarefa de correção foi encerrada.
Anotações de encerramento	Informações adicionais.
Configuração do grupo (visível em todos os estados)	
Tipo de filtro	Tipo de filtragem usado para selecionar vulnerabilidades para o grupo: **Condição**  **Nota:** Atualiza uma vez por hora. **Grupo de filtros**  **Nota:** Atualiza uma vez por hora. **Manual** 
Status da Correção	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
%Vis corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa.
Total de IVs	Número total de itens vulneráveis nesta tarefa.
%Vis corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa.
Anotações (visível em todos os estados)	
Descrição	Descrição do grupo ou das ações de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de tarefa de correção

Campo	Descrição
Comentários adicionais	Informações adicionais.
Atividades	Anotações do sistema.
Links relacionados	
Examinar Itens Vulneráveis Novamente	Aciona uma nova verificação dos itens vulneráveis para determinar se eles foram corrigidos.
Status da atualização	Exibe data e hora da última atualização. Acumula o seguinte do VIS na tarefa: • Estado de tarefas de correção • Pontuações de risco e classificações de risco • Data e status de destino de correção (se aplicável) • Métricas como VIS ativo, total de VIS da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis nesta tarefa.
ANS de tarefas	SLAs da plataforma associados a esta tarefa.
Soluções Preferenciais	Soluções preferenciais dos itens vulneráveis nesta tarefa.
Solicitações de mudança	Solicitações de mudança associadas a esta tarefa.
Aprovações Solicitadas	(Visível quando a tarefa está no estado Em revisão.) Lista de aprovadores. Depois que o adiamento é aprovado, a tarefa de correção passa para o estado Adiado.

Campos do formulário Configuração do questionário

Você pode definir um questionário distinto para uma coleção distinta de vulnerabilidades ou tarefas de correção filtrando as vulnerabilidades ou tarefas de correção respectivamente na seção Configuração do questionário de VR do formulário Configurações para Gestão de exceções de VR.

O formulário Configuração do questionário aparece quando você seleciona **Novo** Botão na seção Configuração do questionário de VR do formulário Configurações para Gestão de exceções de VR.

Campos do formulário Configuração do questionário

Campo	Descrição
Nome	Nome do questionário.
Regra de aprovação	Regra de aprovação para a qual o questionário é aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do formulário Configuração do questionário

Campo	Descrição
	• **Solicitação de exceção para grupos de vulnerabilidades** • **Solicitação de exceção para itens vulneráveis** • **Falso positivo para grupos de vulnerabilidades** • **Falso positivo para itens vulneráveis** • **Questionário para compensar controles de grupos vulneráveis** para solicitações de redução de risco da tarefa de correção. • **Questionário para compensar controles de itens vulneráveis** para solicitações de redução de risco do item vulnerável.
Descrição	Descrição resumida da configuração do questionário.
Ordem	O questionário com ordem mais baixa aparece durante as solicitações.
Ativo	Habilitado por padrão, o que significa que o questionário está em uso.
Tabela	Tabela para a qual a regra de aprovação é aplicável. • Item vulnerável [sn_vul_vulnerable_item para as regras de aprovação relacionadas a itens vulneráveis. • Tarefa de correção [sn_vul_vulnerability] para as regras de aprovação relacionadas a tarefas de correção.
Condição	Condição dos registros para os quais o questionário deve aparecer. Você pode aplicar a condição em todos os campos de um item vulnerável e tarefa de correção, exceto **Motivo** .
Questionário	Questionário que aparece quando um responsável pela correção solicita uma exceção, falso-positivo ou redução de risco.

Tópicos relacionados

Configure a Gestão de exceções para Resposta a vulnerabilidades

Configurar questionário para redução de risco

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades campos de formulário de item vulnerável

Itens vulneráveis são criados automaticamente durante as importações de integração de vulnerabilidades de terceiros.

Campos de item vulnerável

Para exibir dados importados nos campos listados nas tabelas a seguir, você deve ter, no mínimo, a função sn_vul.read_all.

Esses campos são encontrados nos registros listados na tabela Itens vulneráveis [sn_vul_vulnerable_item].

Se você habilitou a verificação de vulnerabilidades SAM NVD, os registros são comparados com o software em seu Configuration Management Database (CMDB) E correspondências são encontradas com software vulnerável ou itens de configuração (ICs).

Campo	Descrição
Selecione marcador de segurança	Marcador de segurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo aparece somente depois que o item vulnerável é salvo.
Número	Número de item vulnerável gerado automaticamente para este registro.
Origem	Scanner que encontrou este item vulnerável.
Classificação de risco	Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta base **Classificação de risco** Não é igual ao registro Solução **Classificação de risco.**
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Esta base **Pontuação de risco** Não é igual ao registro Solução **Pontuação de risco.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável.
Item de configuração	Ativo afetado.
Estado	O padrão deste campo é **Aberto** , mas você pode mudá-lo para **Em investigação** se a vulnerabilidade estiver pronta para correção imediata.
Até a data de redução de risco	Data em que os controles compensatórios aplicados ao item vulnerável expiram. **Nota:** Este campo aparece somente quando o valor da pontuação de risco original está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criação em	Data em que este item vulnerável foi criado em sua instância.
Aberto pela última vez	Data em que o item vulnerável foi aberto mais recentemente em sua instância. Inicialmente, é igual à data de criação do item vulnerável. No entanto, se ele foi encerrado, reaberto, a data da última abertura conterá a data e a hora da reabertura.
Atualização em	Data da última verificação.
Idade	Duração da qual o VI está ativo desde a data em que foi aberto pela última vez. Se o VI estiver fechado, o valor do campo Idade será definido como zero. Para obter mais informações sobre o campo Idade, consulte Cálculo e exibição de idade do item vulnerável. Para obter mais informações sobre como personalizar o cálculo da duração da idade, consulte KB1703270 artigo.
Vulnerabilidade	
Resumo	Descrição da vulnerabilidade.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de gravidade, consulte Crie um Resposta a vulnerabilidades mapa de severidade.
Pontuação de vulnerabilidade (v3)	Pontuação CVSS v3.
Pontuação de vulnerabilidade (v2)	Pontuação do CVSS v2.
Exploração presente	Sim, se pelo menos uma exploração estiver associada às vulnerabilidades associadas a este item vulnerável.
Vetor de ataque da exploração	Vetor de ataque mais vulnerável das explorações das vulnerabilidades associadas a este item vulnerável.
Nível de habilidade da exploração	Nível de habilidade mais baixo necessário para explorar as vulnerabilidades associadas a este item vulnerável.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Ameaça	Informações relevantes sobre a ameaça. Extraído do registro de entrada vulnerável. **Nota:** Todas as mudanças feitas aqui atualizam o registro de entrada vulnerável.
Anotações de correção	Solução relevante para a ameaça, extraída do registro de entrada vulnerável.
Correção Disponível somente com Solução de gestão de vulnerabilidade.	
Solução preferencial	Solução preferencial importada do registro de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: As mudanças manuais feitas aqui não mudam o registro de vulnerabilidade e permanecem inalteradas no VI após importações subsequentes.
Resumo	Resumo importado do registro da solução.
Tipo de solução	Solução potencial ou preferencial.
Detecção inicial	
Nome DNS	Nome do nome do serviço de nomes de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Detecções	
Status	Estado da detecção.
Primeiro encontrado	Data em que a origem de terceiros encontrou a detecção neste ativo pela primeira vez.
Último encontrado	Data em que a origem de terceiros encontrou a última detecção neste ativo.
Nome DNS	Nome do nome do serviço de nomes de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Horas encontradas	Número de vezes que esta vulnerabilidade foi detectada neste ativo pela origem de terceiros.
Execução de integração	Execução de integração que importou a detecção.
Fechar Disponível depois que o item vulnerável for corrigido e encerrado. Os itens nesta seção são somente leitura.	
Encerrado por	Quem fechou o item vulnerável.
Encerrado	Data em que o item vulnerável foi encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Anotações de encerramento	Informações incluídas no fechamento.
Idade do encerramento	Período de tempo após o qual o VI foi encerrado. Se o VI for reaberto, o valor do campo Idade encerrada será definido como zero. Para obter mais informações sobre como o campo Idade encerrada, consulte Cálculo e exibição de idade do item vulnerável. Para obter mais informações sobre como personalizar o cálculo da duração do encerramento por idade, consulte KB1703270 artigo.
Anotações	
Anotações de trabalho/comentários adicionais	Qualquer informação relevante. Marque a caixa de seleção para adicionar comentários adicionais. Começando com Resposta a vulnerabilidades V20.0, você pode adicionar anotações de trabalho na seção Anotações para um item vulnerável adiado.
Atividade	Aparece somente quando uma anotação de trabalho é criada.
Links relacionados	
Calcular Pontuação de Risco	Quando **Gravidade da vulnerabilidade** ou **Pontuação de risco** calculadoras está habilitado, o. **Pontuação de risco** o campo foi atualizado.

A seguir estão as listas relacionadas de itens vulneráveis.

Lista relacionada	Descrição
Tarefas de correção	Tarefas associadas a este item vulnerável.
Tarefas que afetam	Tarefas associadas a este item vulnerável.
Endereços IP associados	Disponível se Qualys Vulnerability Integration A aplicação Integração de vulnerabilidades está instalada. Endereços IP encontrados durante a desduplicação.
Serviços afetados	Serviços de negócio afetados por este item vulnerável. Mostrado quando essas informações estão disponíveis em cmdb registro. Essas informações podem ser inseridas manualmente ou usando ServiceNow® Mapeamento de serviços aplicação. Consulte Mapeamento de serviços para obter mais informações. Se um IC afetado associado ao item vulnerável for adicionado ou atualizado, as informações nesta lista relacionada serão atualizadas automaticamente quando o registro for salvo.
Aprovações de mudança de estado	Status das solicitações de mudança e outras informações de aprovação associadas ao VIT.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Tíquetes de Qualys	Qualys informações de integração de tíquete associadas a este item vulnerável.

Campos de formulário de solução

As soluções são criadas automaticamente quando os registros são baixados de integrações de soluções de terceiros e armazenados em **Soluções** em Resposta a vulnerabilidades.

Campos de entrada de integração da solução

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
Número	Identificador atribuído à solução.
Origem	Origem da solução.
ID da origem	Identificador de origem desta solução.
Classificação de risco	Separa o registro de Solução **Pontuação de risco** Em intervalos de Crítico a Nenhum. Para obter mais informações sobre a solução **Classificação de risco** , consulte Solução de gestão de vulnerabilidade. **Nota:** Solução **Classificação de risco** não é igual a **Item vulnerável** , **Entrada de vulnerabilidade de terceiros** e **Tarefa de correção** registros **Classificação de risco** .
Pontuação de risco	Cálculo ponderado com base em **Pontuação de risco** e a contagem de itens vulneráveis com esta solução como **Solução preferencial** . Para obter mais informações sobre a pontuação de risco da solução, consulte Solução de gestão de vulnerabilidade. **Nota:** Registro de solução **Pontuação de risco** não é igual a **Item vulnerável** , **Entrada de vulnerabilidade de terceiros** e **Tarefas de correção** registros **Pontuação de risco** . Disponível quando SAM NVD está habilitado, mas se não houver itens vulneráveis (VI) ativos associados a uma vulnerabilidade, a solução **Pontuação de risco** definido como zero.
Maior substituição	Indica que nenhuma solução o substitui.
Tipo de solução	Que tipo de solução é. As opções são: • Solução alternativa • Mitigação • Correção do Fornecedor • Patch • Acúmulo • Direito

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Não Corrigirá • Nenhum disponível
Requer reinicialização	Reinicialização necessária. As opções são: • Sim • Não • Talvez
Data de publicação	Data em que a vulnerabilidade foi publicada pela origem.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez pela origem.
Resumo	Resumo da correção da solução.
Informativo	Boletim de segurança associado à solução.
Categorias dos Produtos	Categorias de produtos às quais a solução se aplica.
Produtos	Produtos aos quais a solução se aplica.
Detalhes da solução	
Descrição	Se nenhum conteúdo estiver disponível na origem da solução, você será direcionado para outra seção ou solução relevante para obter mais informações.
Links	Recursos da internet importados associados à solução.
Detalhes da Vulnerabilidade	
Anotações sobre vulnerabilidade	Resumo das vulnerabilidades corrigidas pela solução.
Status da Correção	
Destinos de solução preferenciais Status de correção para itens vulneráveis e seus itens de configuração (ICs) exclusivos, para os quais esta é a solução preferencial. **Nota:** Um IC exclusivo é aquele que é contado apenas uma vez, independentemente de quantos VIS ele está associado.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se ao VIS para o qual esta solução é preferencial. Esta contagem exclui VIS adiados.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.
Percentual de ICs corrigidos	Percentual de conclusão de ICs exclusivos corrigidos (o que significa que todos os VIS desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Destinos de solução preferenciais (inclui adiados) Status de correção para itens vulneráveis e seus ICs exclusivos, incluindo adiados, para os quais esta é a solução preferencial.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se ao VIS para o qual esta solução é preferencial.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é preferencial para correção.
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é preferencial para correção.
Percentual de ICs corrigidos	Percentual de conclusão de ICs exclusivos corrigidos (o que significa que todos os VIS desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Possíveis destinos da solução Status de correção para itens vulneráveis e seus ICs exclusivos, com uma vulnerabilidade relacionada a esta solução.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
Possíveis destinos da solução (inclui adiados) Status de correção para itens vulneráveis e seus ICs exclusivos, incluindo adiados, com uma vulnerabilidade que pode ser corrigida por esta solução, incluindo contagens de soluções preferenciais.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção.
Anotações	
Anotações internas	Campo editável fornecido para o especialista em correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Links relacionados	
Atualizar status	Data e hora em que o status de correção foi atualizado pela última vez. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação de risco e classificação • Métricas da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta solução como a solução preferencial para correção.
Vulnerabilidades de Terceiros	Vulnerabilidades de terceiros associadas a esta solução.
CVEs	Vulnerabilidades comuns de Vulnerabilidade e exposição (CVE) associadas a esta solução.
Tarefas de correção	Tarefas de correção que contêm itens vulneráveis relacionados a esta solução preferenciais para correção.
Soluções Anteriores	Soluções anteriores que resolvem uma ou mais vulnerabilidades desta solução.
Soluções Substitutas	Soluções posteriores que resolvem todas as vulnerabilidades desta solução. Esta lista fica vazia quando **maior substituição** está marcada.

Configurações do fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição

Você pode projetar o fluxo de trabalho de aprovação para a remoção de atribuições de itens vulneráveis (VIS, Vits), tarefas de correção, itens vulneráveis à aplicação (AVITs) e itens vulneráveis do contêiner (CVITs) para você e seu grupo.

VIT, tarefa de correção, AVIT e CVIT têm uma regra de aprovação padrão. Cada regra de aprovação tem uma configuração de aprovação padrão. Cada configuração de aprovação tem um nível de aprovador padrão. As regras de aprovação para Vits, tarefa de correção, AVIT e CVIT são habilitadas por padrão. Como administrador, você pode executar as seguintes ações navegando até **Tudo** > **Resposta a vulnerabilidades** > **Minhas aprovações** > **Regras de aprovação** e selecionando a regra de aprovação apropriada.

- habilite ou desabilite uma regra de aprovação.
- criar e atualizar uma configuração de aprovação.
- defina condições para itens vulneráveis e tarefas de correção às quais as regras de aprovação se aplicam.
- criar e atualizar vários níveis de aprovador.

A tabela a seguir mostra as regras de aprovação padrão, as configurações de aprovação e os níveis de aprovador para um VIT, tarefa de correção, AVIT e CVIT que são enviados com o sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de aprovação padrão, configurações de aprovação e níveis de aprovador

Tipo	Regra de aprovação	Configuração de aprovação	Níveis de aprovação
VIT ou VI	Solicitação de mudança do campo de item vulnerável	Solicitação de mudança do campo de item vulnerável	Solicitação de cancelamento de atribuição de nível 1 para VI
Tarefa de correção	Solicitação de mudança do campo Grupo de vulnerabilidades	Solicitação de mudança de campo de vulnerabilidade	Nível 1: não atribuir solicitação para VG
AVIT	Solicitação de mudança do campo de item vulnerável da aplicação	Solicitação de mudança de campo de vulnerabilidade da aplicação	Cancelar atribuição de item de vulnerabilidade do app
CVIT	Aprovação para gestão de contêiner	Configuração padrão Cancelar atribuição de CVIT	Nível de aprovação de desatribuição de CVIT – 1

Para obter mais informações sobre como aprovar solicitações de cancelamento de atribuição, consulte Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades.

Resposta a vulnerabilidades exemplos de regra de tarefa de correção

Exemplos de regras de tarefa de correção usando vulnerabilidade e risco, impacto ou item de configuração (IC).

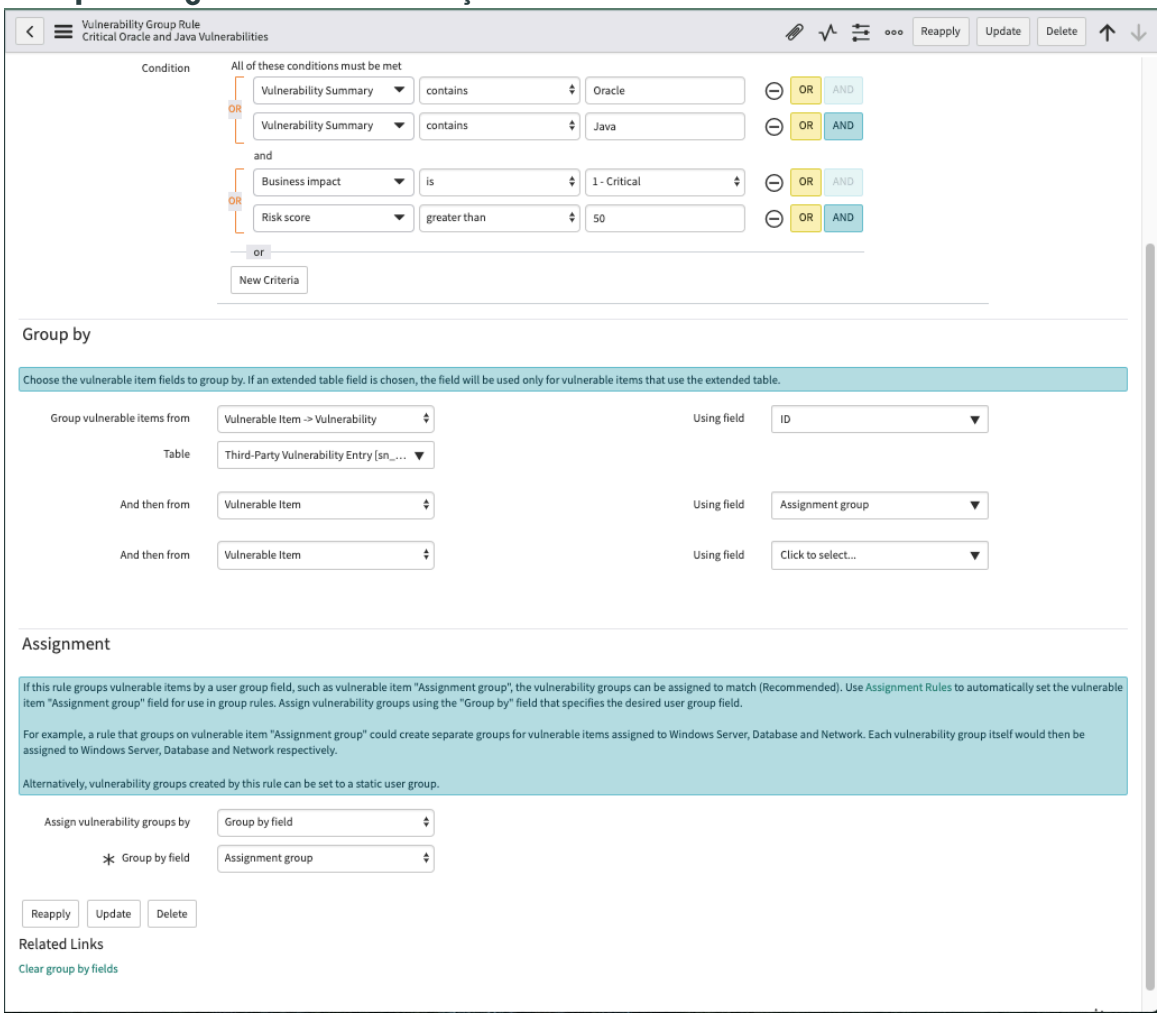
Regra de tarefa de correção para agrupar itens vulneráveis Java e Oracle de alto risco

Este exemplo mostra um passo a passo da regra que agrupa itens vulneráveis Java e Oracle por vulnerabilidade e os atribui aos respectivos grupos de suporte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de regra de tarefa de correção



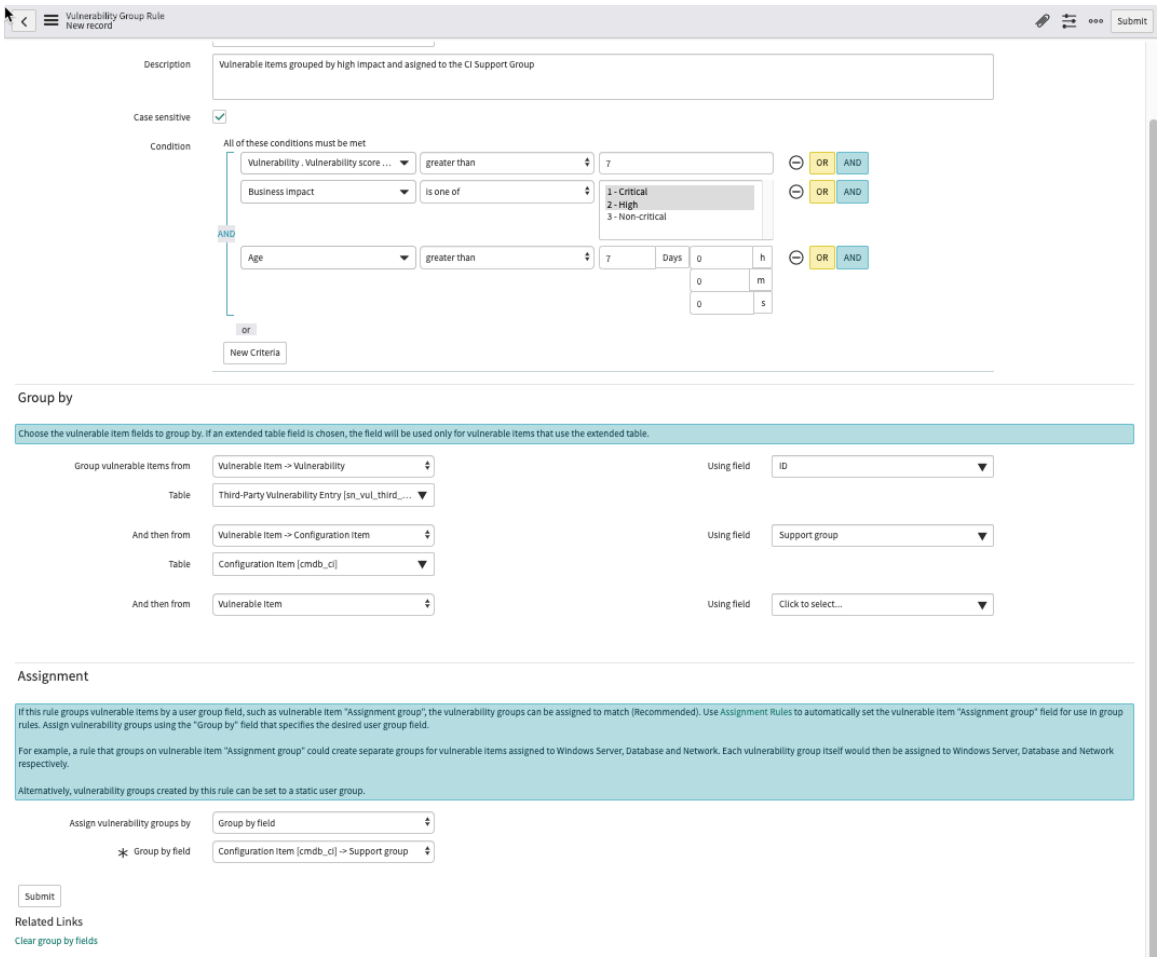
Clique com o botão direito do mouse no cabeçalho para **Salvar** .

Regra de tarefa de correção para agrupar todos os itens vulneráveis de alto impacto por vulnerabilidade e grupo de suporte de IC

Este exemplo mostra as configurações de campo de formulário para uma regra de grupo para itens vulneráveis de alto impacto que os atribui ao grupo de suporte de IC.

Tradução automática

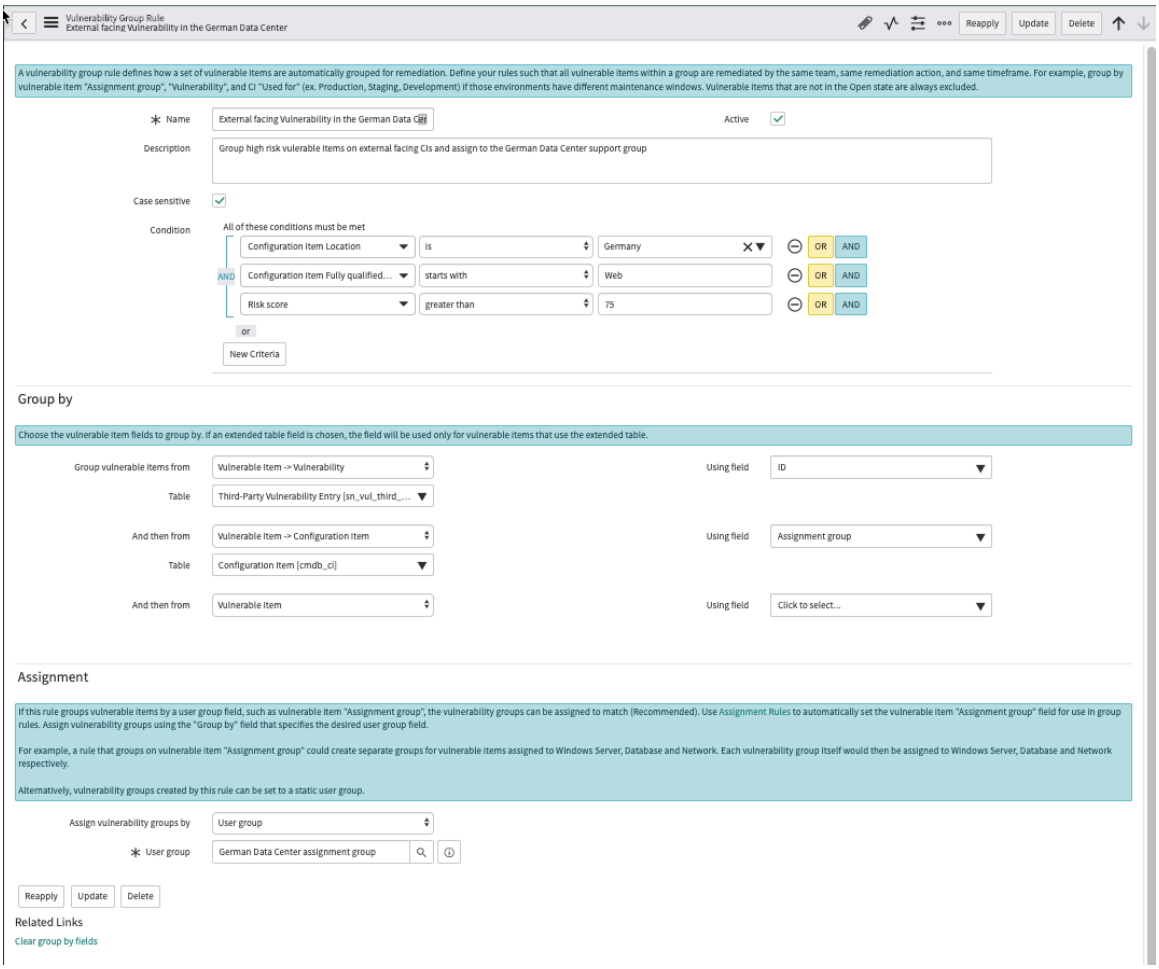
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Regra de tarefa de correção para agrupar todas as vulnerabilidades de alto risco em um IC externo em um datacenter alemão

Este exemplo mostra as configurações de campo de formulário para uma regra de grupo para vulnerabilidades de alto risco em ICs externos em um datacenter alemão. Eles são atribuídos ao grupo de atribuição de datacenter alemão.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de cálculo de pontuação de risco para Resposta a vulnerabilidades

Você pode determinar as calculadoras de pontuação de risco para gerar pontuações de risco que usam a vulnerabilidade e os dados de ativos exclusivos da sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas.

Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela:

Campo	Ponderação	Detalhamento de peso
Severidade.Vulnerabilidade	50	Padrão: 20 1 - Crítico: 100 2 - Alto: 80 3 - Médio: 60 4 - Baixo: 40 5 - Nenhum: 20

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
Vulnerability.Exploit existe	50	Padrão: 50 Sim: 100 Não: 0

Suponha também que os itens vulneráveis mostrados nesta tabela estejam presentes no sistema:

ID	Gravidade da vulnerabilidade	Existe exploração de vulnerabilidade
VIT00001	1 - Crítico(a)	1 - Sim
VIT00002	2 - Alta	1 - Sim
VIT00003	3 – Médio	2 – Não
VIT00004	4 - Baixa	2 – Não
VIT00005	5 - Nenhum	2 – Não

O cálculo da pontuação de risco para os itens vulneráveis é calculado com base na fórmula:

`Pontuação de risco: (W (gravidade) * FV (gravidade). W(exploit exists) * FV(exploit exists)) / 100`

onde **.** é o peso e. **FV** é a porcentagem ponderada do valor do campo.

A pontuação de risco resultante para esses itens vulneráveis é descrita nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 – Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	2 – Alto (50% x 80)	1 – Sim (50% x 100)	90
VIT00003	3 – Médio (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Nota: Para VIT00005, como o valor da severidade está vazio, a ponderação padrão é aplicada.

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Campo	Ponderação	Detalhamento de peso
Severidade.Vulnerabilidade	50	• Padrão: 20 • 1 - Crítico: 100 • **2 - Alto: 70** valor revisado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
		• 3 - Médio: 60 • 4 - Baixo: 40
Vulnerability.Exploit existe	50	• Padrão: 50 • Sim: 100 • Não: 0

A pontuação de risco dos itens vulneráveis após reaplicar a calculadora é mostrada nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 – Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	**2 – Alto (50% x 70)** valor revisado	1 – Sim (50% x 100)	**85** valor revisado
VIT00003	3 – Médio (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Tratamento de erros para detecções

Erros são registrados ao criar detecções ou criar e atualizar itens vulneráveis durante o processamento dos anexos. Se um processo de integração de vulnerabilidade falhar, os erros serão registrados na guia "Log de integrações de vulnerabilidades".

Esses erros são registrados em log, com uma das seguintes categorias.

Campo	Descrição
Criação de VI	Erro ao criar ou atualizar a detecção.
Detecção	Erro ao criar uma detecção.

Experiência de dispositivos móveis Resposta a vulnerabilidades

Como responsável pela correção, você pode acessar Resposta a vulnerabilidades(VR) no seu ServiceNow AI Platform® instância com seu Android ou iOS dispositivo móvel.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades

Para se familiarizar com os conceitos de resposta a vulnerabilidades e como este produto pode ajudar sua organização, consulte Noções básicas sobre a resposta a vulnerabilidades.

Nota: Antes de instalar o. App Resposta a vulnerabilidades para celular mobile familiarize-se com Mobile Agent .

Visão geral

Como um usuário com a função de responsável pela correção (sn_vul.remediation_owner), o. App Resposta a vulnerabilidades para celular permite exibir e pesquisar as vulnerabilidades, tarefas de correção e atribuições no ServiceNow AI Platform instância diretamente do seu Android ou iOS dispositivo móvel.

Você será notificado quando tarefas de correção (RTS) ou VIS forem atribuídas a você ou ao seu grupo de atribuição. Este aplicativo oferece ao responsável pela correção a flexibilidade de reatribuir, editar campos e iniciar a correção sem estar vinculado à área de trabalho.

Você tem acesso a vulnerabilidades, itens de vulnerabilidade, módulos e todas as soluções. Você pode executar as seguintes tarefas no seu dispositivo móvel:

- Exibir e atualizar tarefas de correção.
- Exibir solicitações de mudança.
- Reatribua uma tarefa de correção ou item de vulnerabilidade a outro membro de um grupo de atribuição.
- Exiba notificações quando uma tarefa de correção crítica for atribuída a você ou a um de seus grupos de atribuição.
- Edite um subconjunto de campos em registros de tarefa de correção.
- PESQUISE tarefas de correção que correspondam a critérios de pesquisa específicos.

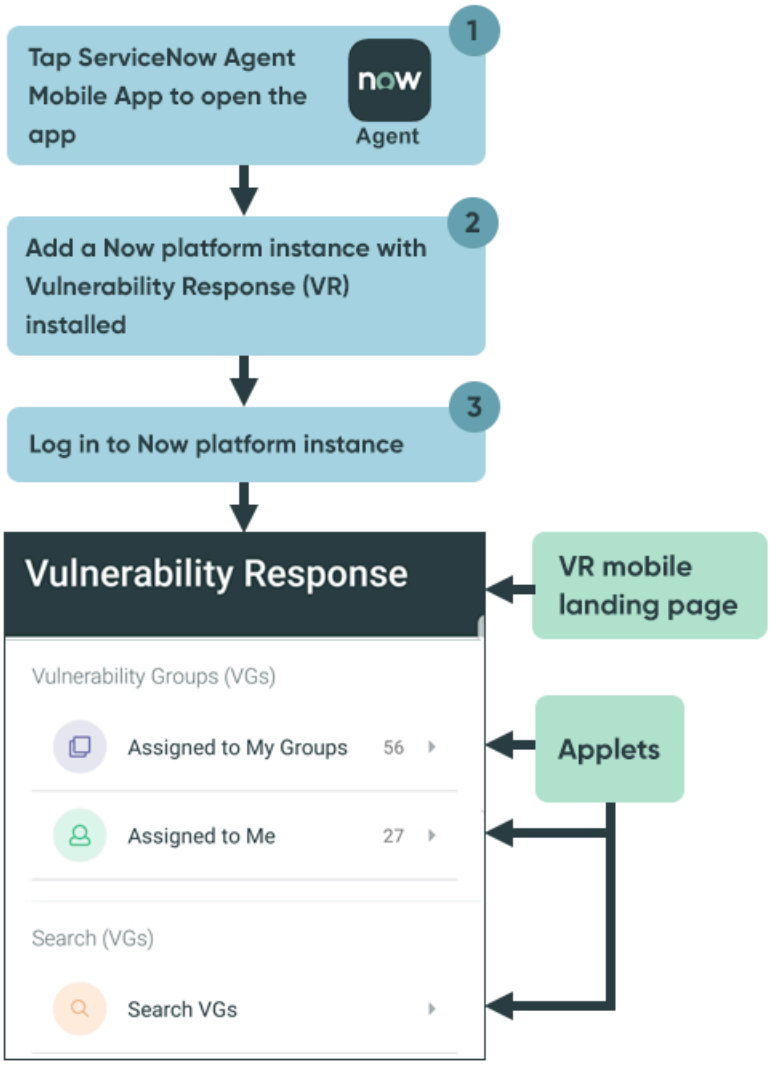
A figura a seguir ilustra como você faz login no seu ServiceNow AI Platform do seu dispositivo móvel e da tela principal do App Resposta a vulnerabilidades para celular exibido depois que você faz login.

Para obter instruções passo a passo sobre como configurar seu ServiceNow AI Platform e instale o. App Resposta a vulnerabilidades para celular, consulte Configurar check-list para App Resposta a vulnerabilidades para celular. Para obter instruções sobre como fazer login, consulte Faça login no App Resposta a vulnerabilidades para celular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

App Resposta a vulnerabilidades para celular



Aplicações

As aplicações são ServiceNow componentes de software, como Resposta a incidentes de segurança(SIR), Resposta a vulnerabilidades(VR), Governança, risco e conformidade(GRC) e outro ServiceNow produtos que fornecem recursos e funcionalidades específicos em seu ServiceNow AI Platform instância. Depois de instalar os aplicativos principais que têm aplicativos para celular em seu ServiceNow AI Platform esses aplicativos são exibidos como ícones na parte inferior do seu dispositivo móvel.

Ícone de Resposta a vulnerabilidades no dispositivo móvel

Pastas

Cada um ServiceNow® Mobile a aplicação contém pastas que separam os miniplets por categorias. Na imagem anterior, Tarefas de correção e Pesquisa (VGS) são as pastas do App Resposta a vulnerabilidades para celular.

Applets

Miniaplicativos são as diferentes opções na aplicação. Na imagem anterior, os ícones em Tarefas de correção e Pesquisa (VGS) são os miniaplicativos disponíveis para App Resposta a vulnerabilidades para celular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte os tópicos a seguir para obter mais informações sobre os miniaplicativos do App Resposta a vulnerabilidades para celular.

Configurar check-list para App Resposta a vulnerabilidades para celular

A check-list a seguir inclui as tarefas de configuração que você deve concluir em ServiceNow AI Platform® e no seu dispositivo móvel antes de usar o. App Resposta a vulnerabilidades para celular.

Antes de Iniciar

Mais informações seguem cada etapa na coluna à direita. Tempo estimado para concluir esta tarefa: 15-20 minutos.

Funções necessárias: administrador, sn_vul.remediation_owner

Seu dispositivo móvel foi configurado com sucesso para App Resposta a vulnerabilidades para celular. A próxima etapa é fazer login no App Resposta a vulnerabilidades para celular e adicione um ServiceNow AI Platform para seu dispositivo móvel.

Procedimento

1. Como opção, imprima esta check-list e use-a para orientá-lo nas tarefas necessárias para instalar o. App Resposta a vulnerabilidades para celular.
2. Verifique se cada item na lista está concluído para que você possa fazer login no App Resposta a vulnerabilidades para celular e adicione um ServiceNow AI Platform instância.

Check-list para dispositivos móveis

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você tem Resposta a vulnerabilidades aplicação principal instalada em um ServiceNow AI Platform instância. . ServiceNow AI Platform instância que você exibe em seu dispositivo móvel. **Nota:** . Resposta a vulnerabilidades aplicação principal e ServiceNow AI Platform a instância deve ser da mesma versão da família. **a.** Para verificar se a aplicação principal está instalada em sua instância, navegue até **Plug-ins** e pesquise Resposta a vulnerabilidades. **b.** . Resposta a vulnerabilidades a aplicação principal ainda não está instalada, clique em **Instalar** para instalá-lo. Para obter mais informações sobre como instalar o. Resposta a vulnerabilidades aplicação principal, consulte Instalar Resposta a vulnerabilidades. Para obter mais informações sobre como obter o. Resposta a vulnerabilidades aplicação principal no ServiceNow Store obter direito, instalar aplicações principais e ativar dependências, consulte Operações de segurança e o ServiceNow Store.
☐	Como um usuário com a função de administrador, verifique se você tem App Resposta a vulnerabilidades para celular instalado no ServiceNow AI Platform instância que você deseja exibir em seu dispositivo móvel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Nota: . App Resposta a vulnerabilidades para celular e o. ServiceNow AI Platform a instância deve ser da mesma versão da família. . App Resposta a vulnerabilidades para celular e o. Resposta a vulnerabilidades a aplicação deve ser compatível. Para obter mais informações sobre a compatibilidade da aplicação Resposta a vulnerabilidades, consulte Matriz de compatibilidade de conformidade de configuração e resposta a vulnerabilidades . Baixe e instale o. App Resposta a vulnerabilidades para celular em ServiceNow Store em seu ServiceNow AI Platform instância. Ao instalar o. App Resposta a vulnerabilidades para celular suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também estão instaladas. Para verificar se essas dependências estão instaladas: **a.** Navegar até **Tudo** > **Plug-ins**. **b.** PESQUISE os IDs do plug-in (com.glide.sg e com.glide.sg.agent_native_client). **c.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para App Resposta a vulnerabilidades para celular. Para obter mais informações sobre como obter o. App Resposta a vulnerabilidades para celular aplicação no ServiceNow Store obter direito, instalar aplicações e ativar dependências, consulte Operações de segurança e o ServiceNow Store.
☐	Como um usuário com a função de administrador, em seu ServiceNow AI Platform, verifique se você atribuiu aos usuários móveis o necessário ServiceNow AI Platform funções. **a.** Para exibir as funções atribuídas a um usuário, navegue até **Tudo** > **Administração** > **Usuários**. **b.** Selecione o nome de usuário seguido pela lista relacionada Funções. Todas as funções atribuídas a este usuário são exibidas. **c.** Verifique se um usuário foi atribuído ou atribua a um usuário a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar solicitações de mudança e tarefas de correção. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **d.** Verifique se um usuário foi atribuído ou atribua a um usuário a função de responsável pela correção (sn_vul.remediation_owner). Usuários com a função sn_vul.remediation_owner podem ler registros de vulnerabilidade e solução. Esta função é adicionada automaticamente quando você atribui a função itil. **e.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos. **Nota:** Se você tiver um grande número de usuários para o aplicativo para celular, como alternativa, poderá atribuir a função sn_vul.remediation_owner a um grupo. Cada usuário adicionado ao grupo herda esta função.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações sobre regras de atribuição e grupos, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Para obter mais informações sobre usuários e como atribuir funções a usuários e grupos, consulte Administração de usuários .
☐	Como um usuário com a função de responsável pela correção (sn_vul.remediation_owner), baixe o mais recente ServiceNow® Aplicativo Agent em seu dispositivo móvel.  O aplicativo Agent mais atual está disponível na Apple iOS App Store e Google Play Store.
☐	Como um usuário com a função sn_vul.remediation_owner, verifique se as notificações estão habilitadas em seu dispositivo móvel e em seu ServiceNow AI Platform instância. As notificações informam quando tarefas críticas de correção são atribuídas a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no App Resposta a vulnerabilidades para celular e navegue diretamente até o registro. Para habilitar notificações no seu ServiceNow AI Platform para que eles sejam exibidos em seu dispositivo móvel, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	a. Verifique se você baixou e instalou o. App Resposta a vulnerabilidades para celular em seu ServiceNow AI Platform instância. **b.** Em Configurações do sistema em seu ServiceNow AI Platform Em Notificações, verifique se você habilitou **Aplicação para celular da ServiceNow** . Para obter mais informações sobre como configurar notificações, consulte Como definir preferências de notificação em IU principal . ServiceNow AI Platform as notificações também são exibidas na tela mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Faça login no App Resposta a vulnerabilidades para celular

Abra o aplicativo Vulnerability Response Mobile e adicione um ServiceNow AI Platform Instância com Resposta a vulnerabilidades para seu dispositivo móvel.

Antes de Iniciar

Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para App Resposta a vulnerabilidades para celular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

App Resposta a vulnerabilidades para celular



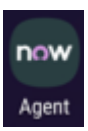
Função necessária: Responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5-7 minutos.

Procedimento

1. Em seu dispositivo móvel, toque em **Agente da ServiceNow** aplicação.



Se você ainda não estiver conectado a um ServiceNow AI Platform, a tela Instâncias é exibida.

2. . ServiceNow AI Platform instância com Resposta a vulnerabilidades a aplicação principal ainda não foi adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na tela Instâncias exibida, toque no ícone de adição ( ).
É exibida uma tela solicitando que você insira e salve um endereço de um ServiceNow AI Platform instância.

b. Preencha os campos.

Nome do campo	Descrição
Insira o endereço da instância ou leia um código QR.	Escolha um para continuar: ▪ . .service-now.com insira o nome do seu ServiceNow AI Platform instância, por exemplo, vrmobilenewyorkagent . ▪ Insira um endereço. Este endereço é o URL do seu ServiceNow AI Platform instância que você deseja exibir em seu dispositivo móvel. ▪ Digitalize um código QR.
(Opcional) Insira o apelido	Insira um apelido para esta instância. Se você tiver várias instâncias adicionadas ao dispositivo, os apelidos poderão ajudá-lo a localizar rapidamente um ServiceNow AI Platform instância.

c. Toque em **Salve e faça login**

3. Em ServiceNow Tela de login exibida, insira o Nome de usuário e a Senha do ServiceNow AI Platform instância que você deseja adicionar e tocar **Login** .
A tela principal de Resposta a vulnerabilidades é exibida. Você fez login com sucesso no App Resposta a vulnerabilidades para celular!

4. Depois de fazer login, verifique se as notificações estão habilitadas no App Resposta a vulnerabilidades para celular.

a. Na tela principal na parte inferior, toque em **Notificação** .

b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
Notificações do ServiceNow AI Platform São exibidos na tela Notificações em App Resposta a vulnerabilidades para celular.

5. Depois de fazer login em uma instância no seu dispositivo móvel, ele será o padrão ServiceNow AI Platform instância no dispositivo.
Se você quiser exibir outro ServiceNow AI Platform no dispositivo, você deve fazer logout da instância padrão. Para fazer logout:

a. Toque em **Configurações** ícone.

b. Toque em **Logout** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tela Instâncias é exibida com qualquer ServiceNow AI Platform instâncias que você adicionou ao dispositivo móvel.

c. **Opcional:** Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Resultado

Se a tela Instâncias do App Resposta a vulnerabilidades para celular não é exibido depois que você toca em **Agente da ServiceNow** em seu dispositivo, verifique se **Agente da ServiceNow** é permitido como um app confiável no seu dispositivo. Para permitir o acesso como um app confiável, navegue até as configurações e gestão geral de dispositivos em seu dispositivo e toque na opção (Aplicativo de confiança etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois que você inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha do ServiceNow AI Platform a instância está correta.

Se você tiver problemas para exibir a tela principal, verifique sua conexão de rede.

Se você não puder exibir a tela Instâncias depois de tocar em **Agente da ServiceNow** , tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app da Apple iOS App Store ou Google Play Store e tente reinstalá-lo.

Exiba, atribua e edite tarefas de correção com App Resposta a vulnerabilidades para celular

Exiba, atribua ou edite os campos nos registros de tarefa de correção (RT) atribuídos ao seu grupo. Navegue por vulnerabilidades, itens de vulnerabilidade e registros de soluções e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Antes de Iniciar

Função necessária: Responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

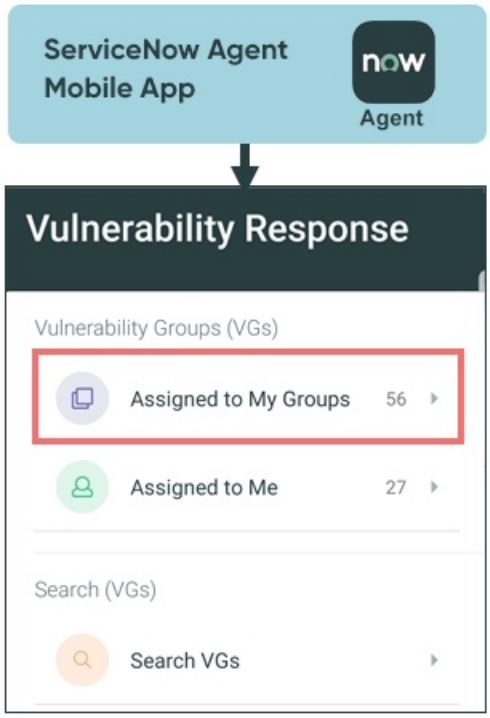
Atribua registros RT (VUL) a você mesmo ou reatribua-os a outro membro do seu grupo. Como alternativa, exiba os detalhes dos registros de tarefa de correção ativos, itens vulneráveis (VI), vulnerabilidades de NVD e soluções antes de editar, atribuir ou corrigir. Tempo para concluir esta tarefa: 5-10 minutos.

Procedimento

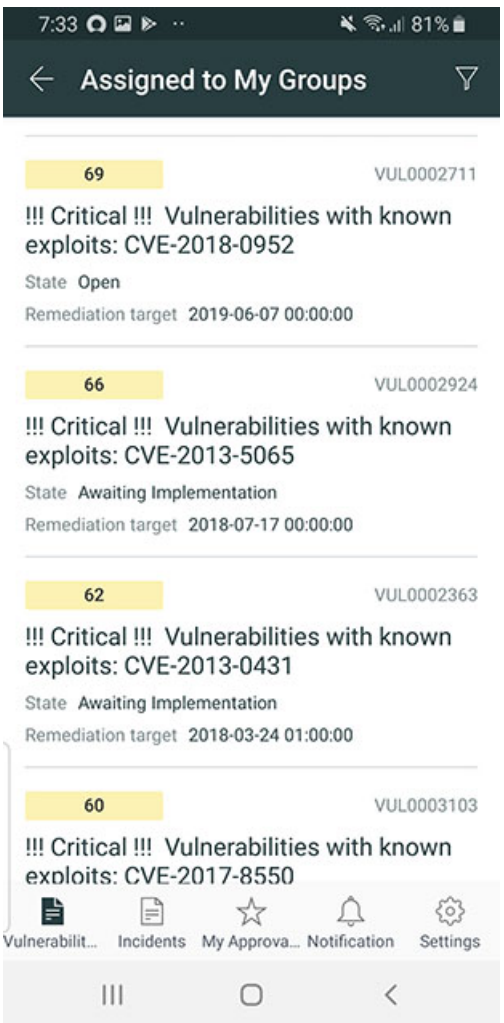
1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no App Resposta a vulnerabilidades para celular.
2. Com a tela principal Resposta a vulnerabilidades exibida, toque em **Atribuído a Meus grupos** .
   Se você sair do App Resposta a vulnerabilidades para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A lista de registros abertos atribuídos ao seu grupo é exibida.



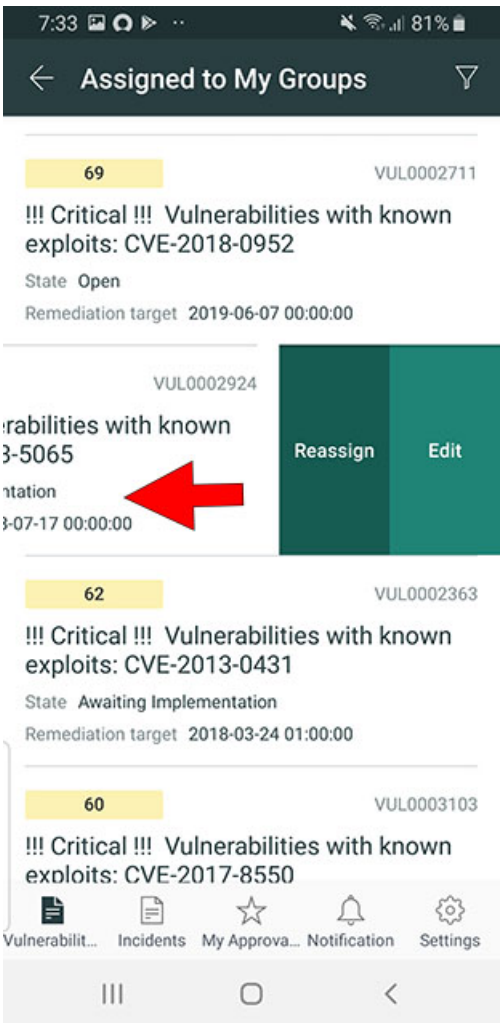
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. **Opcional:** Consulte PESQUISE tarefas de correção com App Resposta a vulnerabilidades para celular para pesquisar registros que correspondam a critérios específicos.

4. Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista.
   Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

5. Para reatribuir ou editar um registro diretamente da lista, com a lista de registros abertos exibida, deslize para a esquerda em um registro para abrir o menu.



6. Escolha um no menu exibido para continuar.

Opção	Descrição
Atribuir a mim	Se o registro RT já estiver atribuído a você, essa opção não será exibida. Toque em **Atribuir a mim** Para atribuir o RT a si mesmo. Seu nome é exibido no campo Atribuído a no registro. É exibida uma mensagem confirmando a atribuição.

Tradução automática

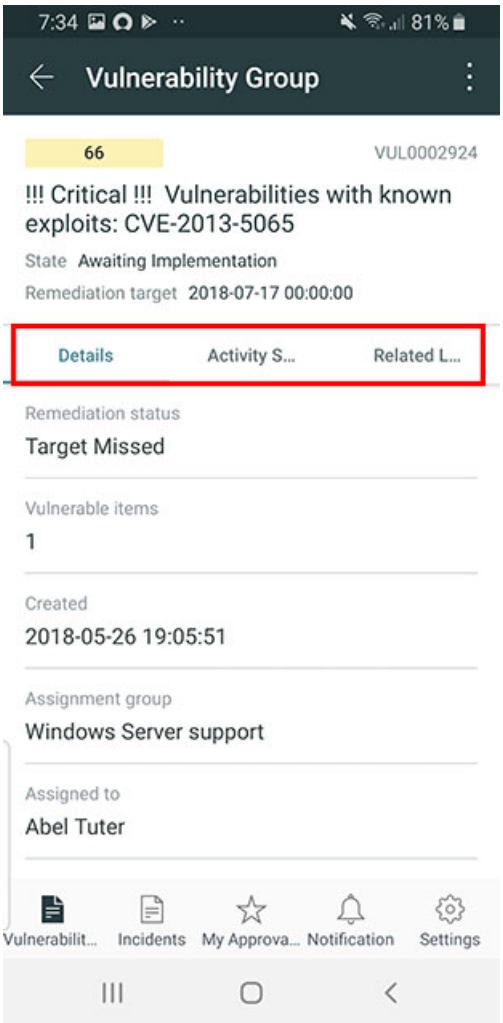
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Reatribuir	Para reatribuir o RT a um grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Na lista, toque em um grupo ou insira texto no campo de pesquisa. Para atribuir ou reatribuir o RT a um membro de um grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira texto no campo de pesquisa. Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.
Editar	**a.** Toque em **Editar** . **b.** Expanda os campos e selecione uma opção na lista exibida ou insira texto no campo Pesquisar. Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

7. Como alternativa, para exibir os detalhes de um registro de vulnerabilidade em aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído aos Meus grupos exibida, toque em um registro na lista.
8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir anotações de trabalho ou listas relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos do registro de RT. Toque no ícone de menu (⋮) no canto superior direito da tela para exibir as opções disponíveis. As opções exibidas neste menu expandido variam. As ações de correção que você pode executar em seus itens vulneráveis variam e dependem do valor exibido no campo Estado do registro. Para obter mais informações sobre o campo Estado e suas opções de correção, consulte Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ○ Exiba a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

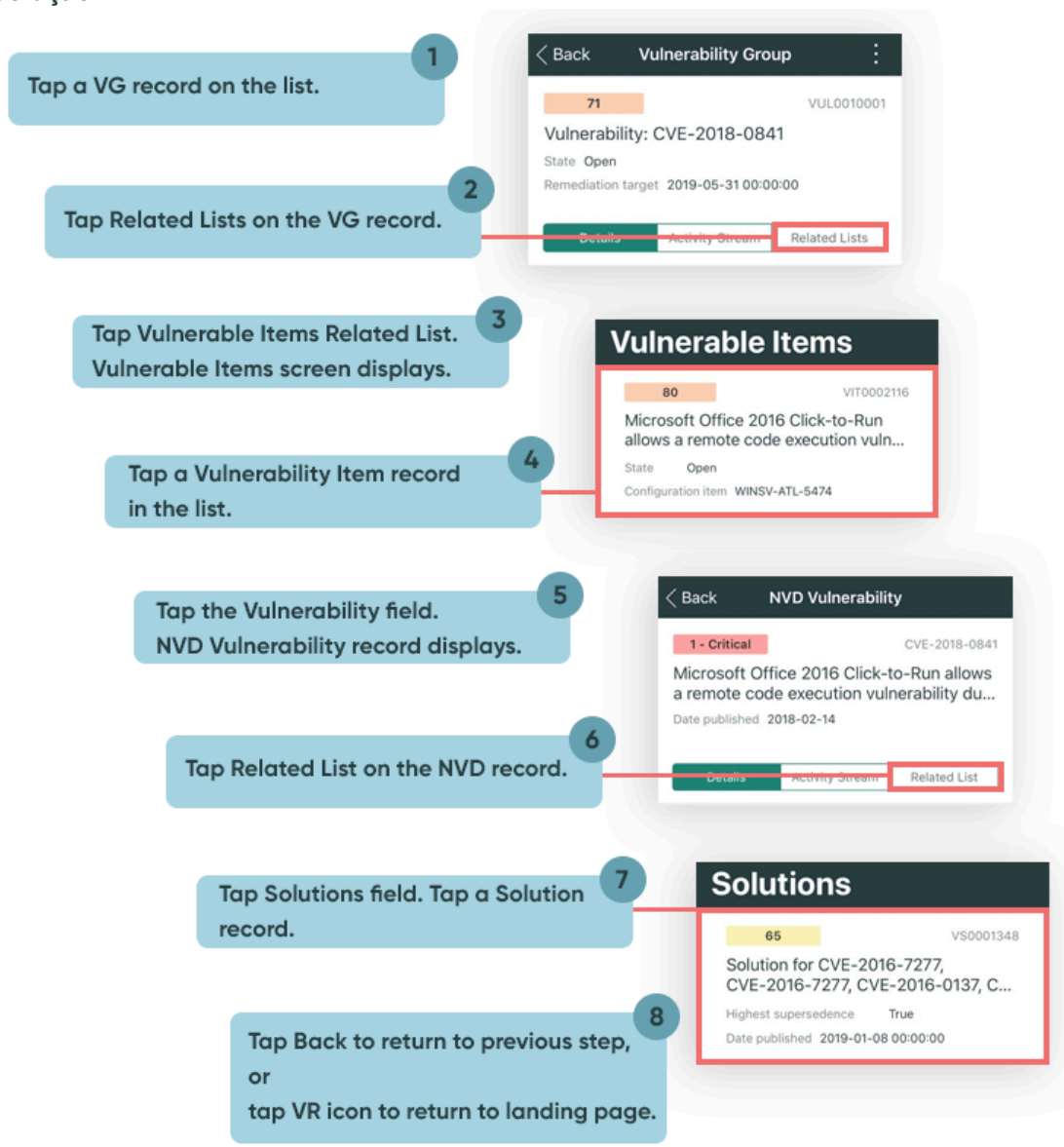
Opção	Descrição
	adição ( para adicionar uma anotação de trabalho ou anexar um arquivo. ○ Toque no ícone de menu ( no canto superior direito da tela para exibir as opções de correção disponíveis.
Listas relacionadas	Com a guia Listas relacionadas selecionada, exiba qualquer uma das listas relacionadas do registro de RT que estão preenchidas. ○ Toque em **Itens vulneráveis** . Toque em um registro de item vulnerável (VI) e navegue até o registro de solução preferencial. Consulte a figura que segue a tabela para obter um mapa de navegação e mais detalhes. ○ Toque em **Solicitações de mudança** . Exiba uma lista das solicitações de mudança associadas a este registro. ○ Quando exibido, toque no ícone de menu ( no canto superior direito de uma tela para exibir as opções de correção disponíveis.

A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção para o registro de solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem abordados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação da tarefa de correção por meio de um registro de Solução



Tradução automática

9. Depois de revisar, editar ou corrigir, escolha um para continuar.

Opção	Descrição
Toque em um ícone na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Resposta a vulnerabilida– des para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notifi– cações do ServiceNow AI Platform e o. App Resposta a vulnerabilidades para celular. ○ Toque em **Configurações** e escolha um para continuar.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Reatribuir e editar tarefas de correção atribuídas a você com App Resposta a vulnerabilidades para celular

Exiba, atribua ou edite os campos nos registros de tarefas de correção atribuídos a você. Navegue por registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem abordados.

Antes de Iniciar

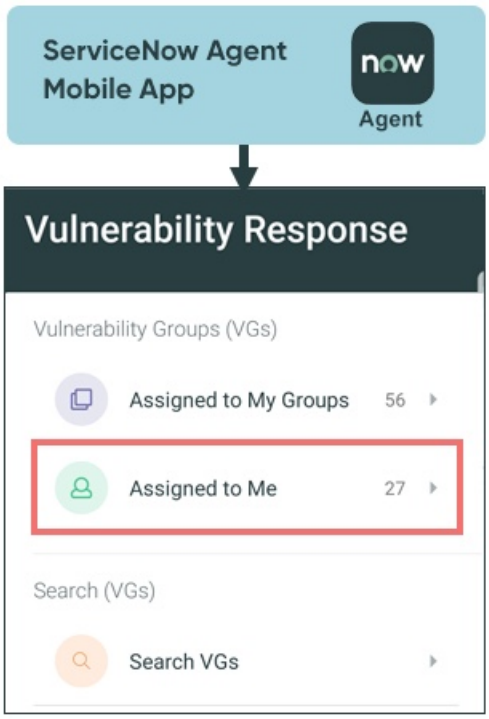
Função necessária: Responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Reatribua ou edite registros atribuídos a você. Exiba os detalhes dos registros de tarefas de correção ativas, registros de itens vulneráveis (VI), vulnerabilidades e soluções antes de editar, atribuir ou corrigir. Tempo para concluir esta tarefa: 5-10 minutos.

Procedimento

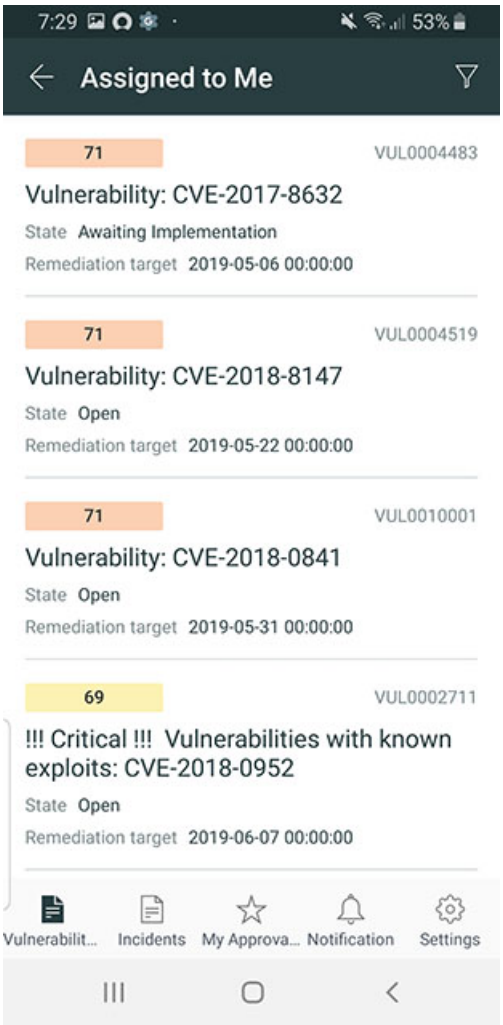
1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no App Resposta a vulnerabilidades para celular.
2. Com **Resposta a vulnerabilidades** tela principal exibida, toque em **Atribuído a mim** .
   Se você sair do App Resposta a vulnerabilidades para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A lista de registros de tarefa de correção atribuídos a você é exibida.

Tradução automática

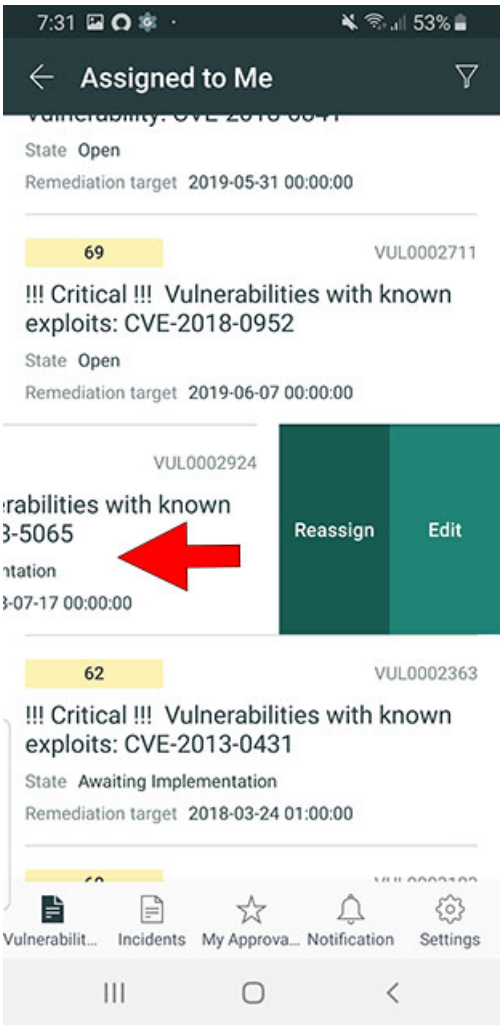
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte PESQUISE tarefas de correção com App Resposta a vulnerabilidades para celular para pesquisar registros que correspondam a critérios específicos.
4. Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista.
   Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.
5. Para reatribuir ou editar o registro diretamente da lista, com a tela Atribuído a mim exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Escolha um para continuar.

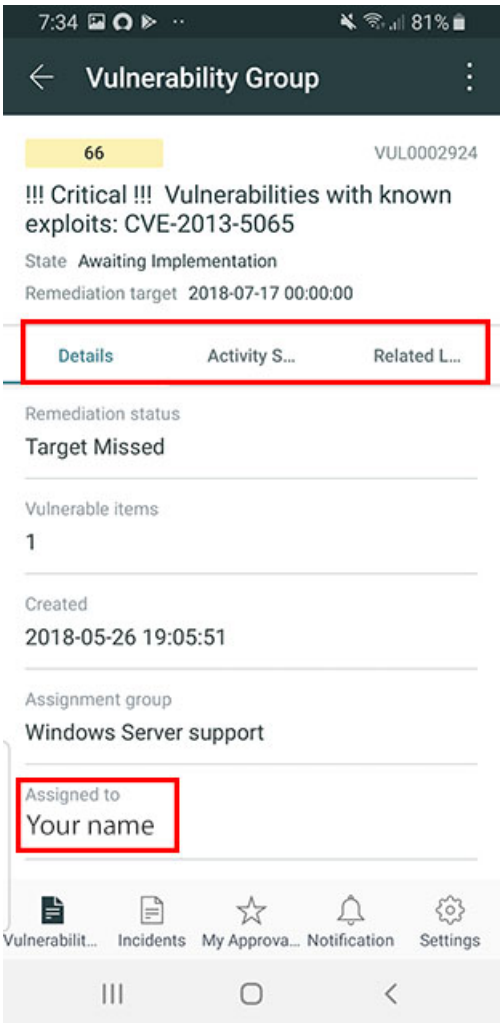
Opção	Descrição
Reatribuir	Para reatribuir a tarefa a outro grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo da lista exibida ou insira texto no campo de pesquisa. Para atribuir ou reatribuir o RT a um membro de um grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira texto no campo de pesquisa. Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Editar	**a.** Toque em **Editar** . **b.** Expanda os campos e selecione uma opção na lista exibida ou insira texto. **c.** Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

7. Como alternativa, para exibir os detalhes de um registro aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído a mim exibida, toque em um registro na lista.
8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir anotações de trabalho ou listas relacionadas.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos do registro da tarefa de correção. Toque no ícone de menu (no canto superior direito da tela para exibir as opções disponíveis. As opções exibidas neste menu expandido variam. As ações de correção que vo–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cê pode executar em seus itens vulnerá–veis variam e dependem do valor exibido no campo Estado do registro. Para obter mais informações sobre o campo Estado e su–as opções de correção, consulte Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ○ Exiba a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição (para adicionar uma anotação de trabalho ou anexar um arquivo. ○ Toque no ícone de menu (no canto superior direito da tela para exibir as op–ções de correção disponíveis.
Guia Listas relacionadas	Com a guia Lista relacionada selecionada, exiba as listas relacionadas do registro que estão preenchidas. ○ Toque em **Solicitações de mudança** . Exi–ba uma lista das solicitações de mudança associadas a este registro. ○ Toque em **Itens vulneráveis** . Toque em um registro de item vulnerável (VI) e na–vegue até o registro de solução prefe–rencial. Consulte a figura que segue a tabela para obter um mapa de navegação e mais detalhes. ○ Quando exibido, toque no ícone de menu (no canto superior direito da tela pa–ra exibir as opções de correção disponí–veis.

A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção para o registro de solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem abordados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação do RT por meio de um registro de Solução



Tradução automática

9. Escolha um para continuar.

Opção	Descrição
Toque em um ícone na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Resposta a vulnerabilida– des para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notifi– cações do ServiceNow AI Platform e o. App Resposta a vulnerabilidades para celular. ○ Toque em **Configurações** e escolha um para continuar.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância. Para fazer log-in, toque em **Logout** .

PESQUISE tarefas de correção com App Resposta a vulnerabilidades para celular

PESQUISE tarefas de correção que correspondam aos critérios de pesquisa específicos selecionados.

Antes de Iniciar

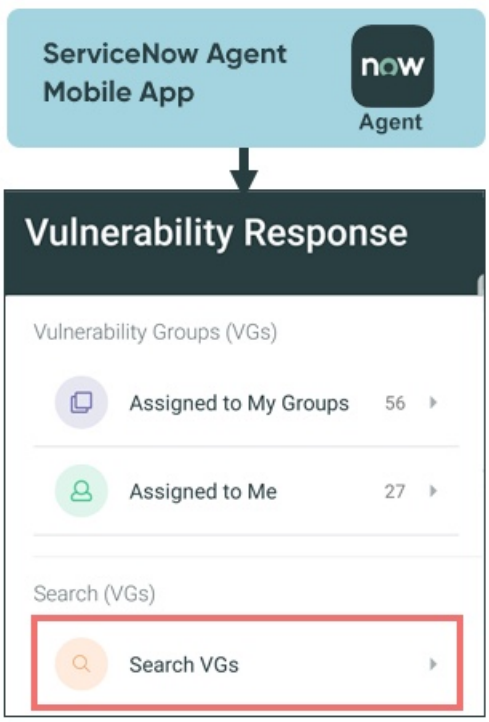
Função necessária: Responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5-7 minutos.

Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no App Resposta a vulnerabilidades para celular.
2. Com **Resposta a vulnerabilidades** tela principal exibida, toque em **RTS de pesquisa** .
   Se você sair do App Resposta a vulnerabilidades para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



3. Na tela Pesquisar exibida, toque nos campos e preencha o formulário com os critérios de pesquisa desejados.

   Siga as instruções após a tabela para editar critérios de pesquisa, limpar critérios de pesquisa ou enviar uma pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Toque neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
Número	Toque na tela e insira um número de RT, por exemplo, (VUL0002372) Este número é exibido no canto superior direito do registro de RT. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS. Toque no ícone Fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTS.	Insira um número RT, por exemplo, (VUL0002372). Este número é exibido no canto superior direito do registro de RT. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.
Classificação de risco	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS. Toque no ícone Fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTS.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.
Status da correção	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS. Toque no ícone Fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTS.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.
Estado	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS. Toque no ícone Fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTS.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.
Motivo	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS. Toque no ícone Fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTS.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Toque neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .
Atribuição a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .
Descrição resumida	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS.	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.
Descrição	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTS.	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** Para retornar à tela Pesquisar RTS. No campo expandido, toque em **Cancelar** Para limpar a entrada e retornar à tela Pesquisar RTS.

Para Android Dispositivos, com a tela Pesquisar RTS exibida e todos os seus critérios inseridos, escolha um para continuar.

Opção	Descrição
Limpe ou modifique os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios inseridos, com a tela Pesquisar RTS exibida, toque na seta para voltar para limpar todos os campos e retornar à tela principal Resposta a vulnerabilidades. A pesquisa não é enviada e os critérios de pesquisa são limpos. Como alternativa, para editar um campo,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Com a tela Pesquisar RTS exibida, toque em um campo com critérios de pesquisa para expandi-lo. ○ Toque em um item para desmarcá-lo. Toque em Todos para selecionar todos os itens. Toque em **Todos** novamente para limpar todos os itens. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** . ○ Toque no ícone de marca de seleção para salvar as mudanças e retornar à tela Pesquisar RTS.
Envie uma pesquisa	Com a tela Pesquisar RTS exibida com os critérios de pesquisa inseridos, toque no ícone enviar ( ). Os registros da tarefa de correção que correspondem aos critérios de pesquisa são exibidos. Após a conclusão da pesquisa, os critérios de pesquisa não são salvos.

4. Para iOS Dispositivos, com a tela Pesquisar RTS exibida, escolha um para continuar.

Opção	Descrição
Limpe ou modifique os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios e retornar à tela principal, toque no ícone Fechar (X). Os critérios de pesquisa inseridos não são salvos. Como alternativa, para editar um campo: **a.** Com a tela Pesquisar RTS exibida, toque em um campo com critérios de pesquisa para expandi-lo. **b.** Toque em um item na lista para desmarcá-lo ou toque em **Limpar tudo** . Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** . **c.** Toque em **Concluído** Para salvar as mudanças e retornar à tela Pesquisar RTS.
Envie uma pesquisa	Com a tela Pesquisar RTS exibida com os critérios de pesquisa inseridos, toque em **Pesquisa** . Os registros de RT que correspondem aos seus critérios de pesquisa são exibidos. Após a conclusão da pesquisa, os critérios de pesquisa não são salvos.

5. Opcional: Se sua pesquisa retornar vários registros, você poderá Filtrar registros com App Resposta a vulnerabilidades para celular para refinar os resultados da pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtrar registros com App Resposta a vulnerabilidades para celular

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na ServiceNow AI Platform.

Antes de Iniciar
Função necessária: Responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa
Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro ().
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
   Um campo comum para inserir critérios de pesquisa para registros de tarefa de correção é o campo Estado.
3. Nas opções exibidas, toque na caixa de seleção ou toque em um item para o filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.
4. Toque no ícone Voltar ( ou **CONCLUÍDO** para salvar suas mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover todos os filtros e restaurar a configuração padrão.
5. **Opcional:** Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone de interseção () Para criar E condições.
7. Como alternativa, toque no ícone de interseção () Para criar condições OR.
8. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **CONCLUÍDO** .
   Na tela, somente os registros que correspondem aos critérios de filtro são exibidos.

Tópicos relacionados

PESQUISE tarefas de correção com App Resposta a vulnerabilidades para celular

Orquestração de resposta a vulnerabilidades

Com Orquestração de Resposta de vulnerabilidade Fluxos de trabalho e atividades com os quais você pode interagir e recuperar dados de sistemas e ambientes baseados em Windows ou UNIX usando a orquestração de fluxo de trabalho. Ao enriquecer os dados, você pode encurtar o ciclo de vida da correção.

Para obter mais informações sobre como editar fluxos de trabalho ou criar fluxos de trabalho personalizados, consulte Explorando fluxos .

Verificar fluxo de trabalho de vulnerabilidade

O **Resposta a vulnerabilidades** > **Vulnerabilidade de verificação** o fluxo de trabalho verifica novamente uma tarefa de correção.

Antes de Iniciar
Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado por **Verificar novamente o grupo vulnerável** durante um **Fechar/Ignorar** ação.

Tradução automática

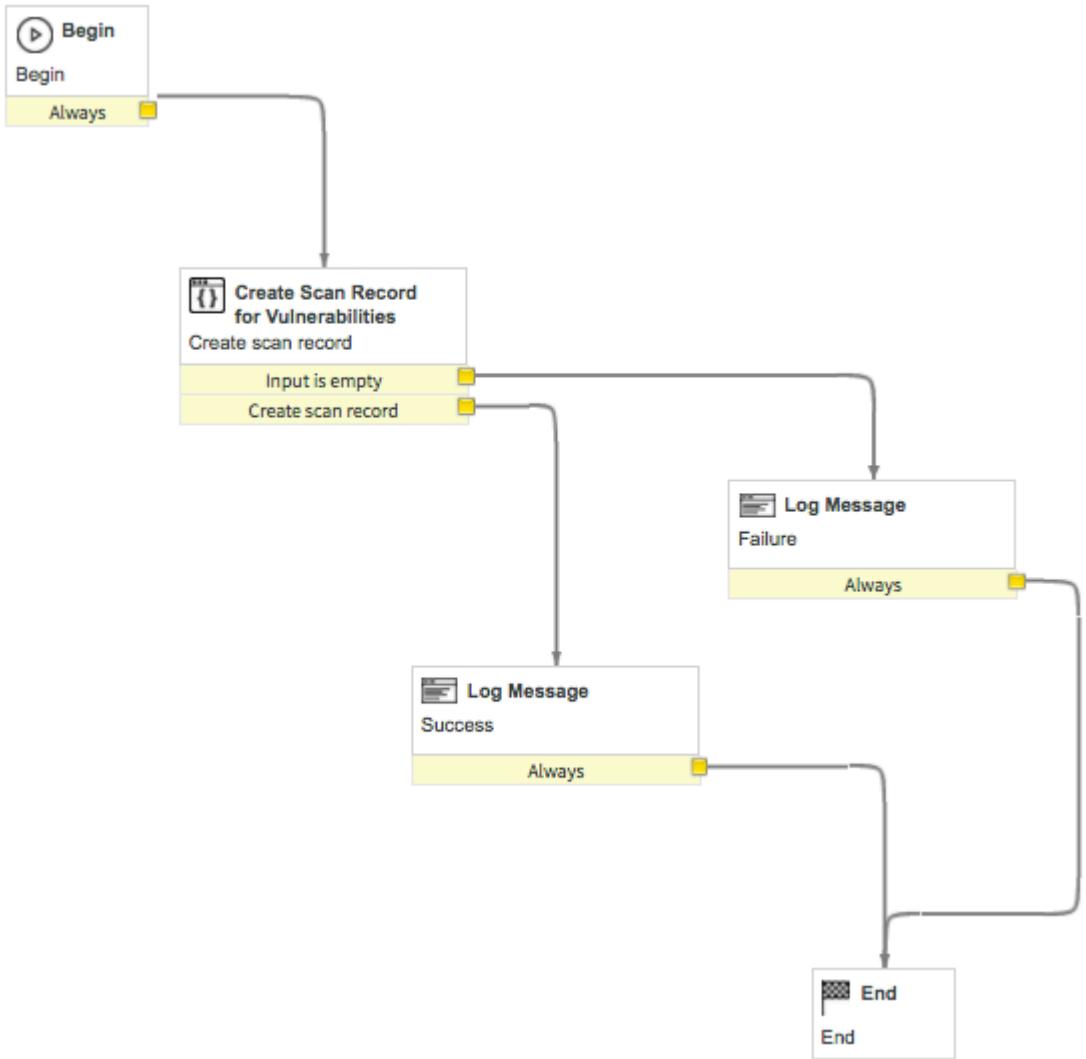
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades do processo de fluxo de trabalho incluem:

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de Log

Fluxo de trabalho de Vulnerabilidade de verificação



Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra um registro de tarefa (VUL).
3. Clique em **Fechar**.
4. Escolha **Encerrado** para **Estado desejado** .
5. Escolha **Corrigido** para **Subestado** .
6. Escolha **Aguarde a confirmação da próxima verificação** para **Fechar agora?**
   Para a tarefa de correção e os itens vulneráveis, o. **Estado** muda para **Confirmação pendente** . **Subestado** muda para **Corrigido** e uma nova verificação é executada.

Verificar fluxo de trabalho do item de vulnerabilidade

O**Resposta vulnerável** > **Verificar item de vulnerabilidade** o fluxo de trabalho verifica novamente um item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: nenhuma

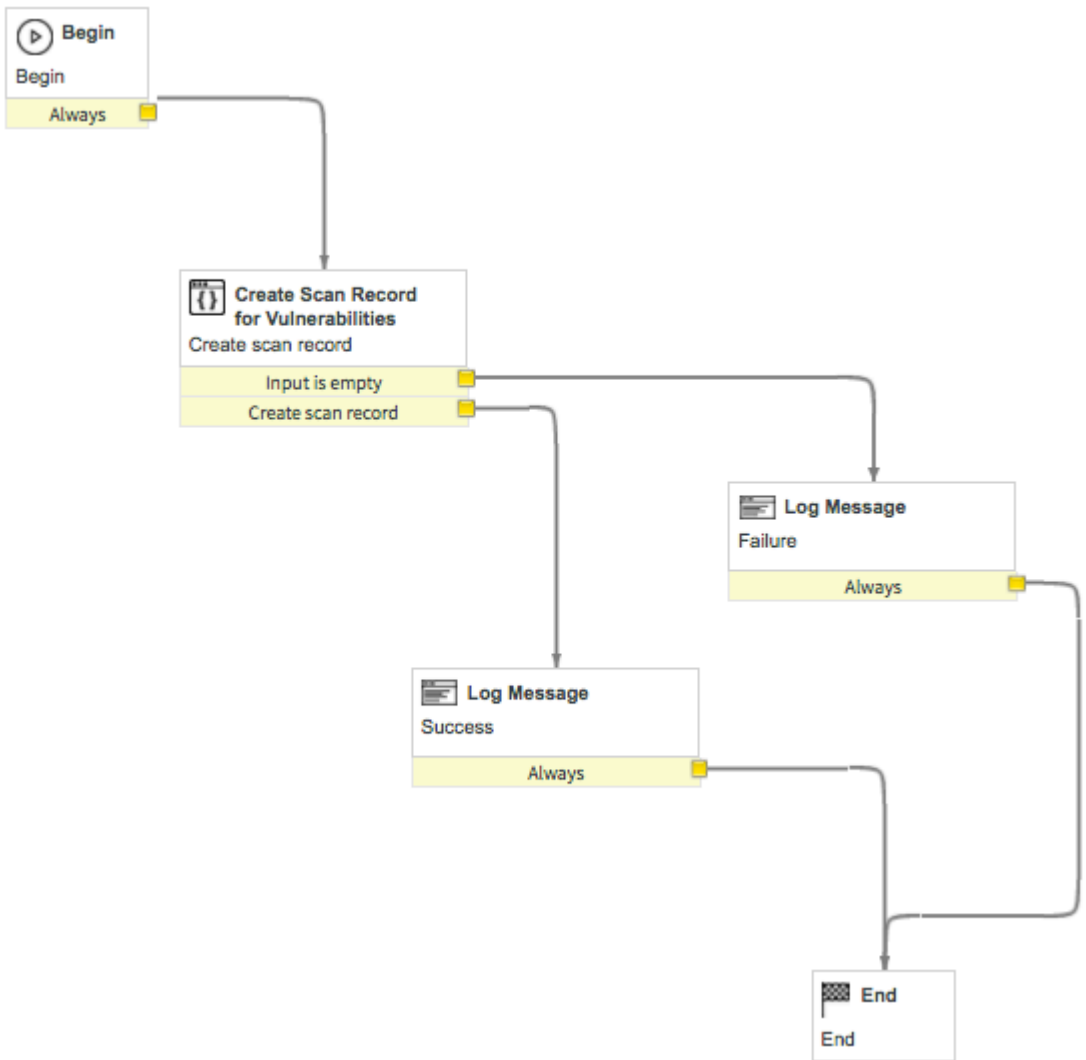
Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado por **Nova verificação da vulnerabilidade** durante um **Fechar/Ignorar** ação.

As atividades do processo de fluxo de trabalho incluem:

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de Log

Fluxo de trabalho de Vulnerabilidade de verificação



Tradução automática

Procedimento

1. Navegar até **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item de vulnerabilidade.
3. Clique em **Fechar/Ignorar** .
4. Escolha **Encerrado** para **Estado desejado** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Escolha **Corrigido** para **Subestado** .
   . **Estado** do grupo muda para **Confirmação pendente** . **Subestado** muda para **Corrigido** e uma nova verificação é executada.

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Verificações de vulnerabilidade para um ou vários itens vulneráveis podem ser executadas usando **Criar registro de verificação para vulnerabilidades** atividade de fluxo de trabalho incluída no sistema de base. Quando a entrada é passada para a atividade, ela cria um registro de verificação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
taskids [string]	Uma cadeia de caracteres de sysIds separados por vírgulas que definem as entradas esperadas. Esse campo é obrigatório.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ScanResult [booliano]	Retorna verdadeiro se a entrada não estiver vazia. Um registro de verificação é criado para os taskIds.

Resposta a vulnerabilidades de aplicações

. Resposta a vulnerabilidades de aplicações Recurso (AVR) do ServiceNow® Resposta a vulnerabilidades A aplicação importa itens vulneráveis à aplicação (AVITs) e, de acordo com as regras, permite corrigir vulnerabilidades da aplicação. Resposta a vulnerabilidades está disponível por assinatura separada.

A partir do AVR v19.0, algumas tabelas de chaves e nomes de colunas foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação. Para obter a lista completa de termos atualizados, consulte Exibição de produto do Resposta a vulnerabilidades de aplicações.

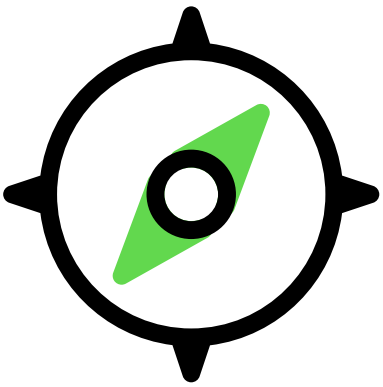
A partir da v19.0 de Resposta a vulnerabilidades, Você pode ingerir dados de vulnerabilidade de Análise de composição de software (SCA) e Lista de materiais de software (SBOM) para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Explorando Resposta a vulnerabilidades de aplicações e Integração de Resposta a vulnerabilidades com Veracode.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

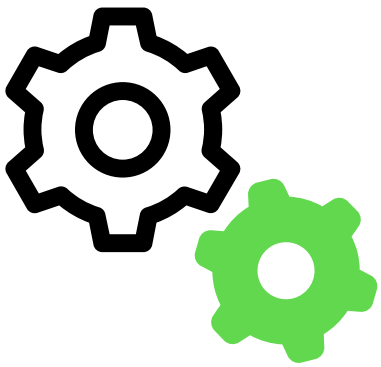
Resposta a vulnerabilidades de aplicações

Explorar



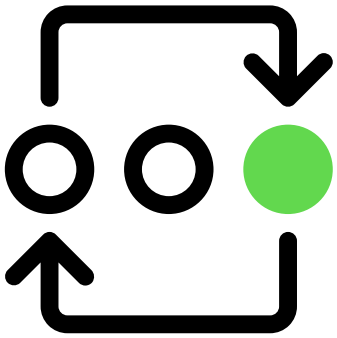
Saiba mais sobre os conceitos e recursos de Resposta a vulnerabilidades da aplicação.

Configurar



Configurar Resposta a vulnerabilidades da aplicação.

Integrar



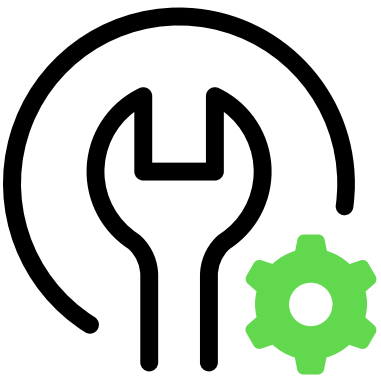
Estenda a Resposta a vulnerabilidades da aplicação integrando com outras aplicações.

Use os Espaços de resposta a vulnerabilidades



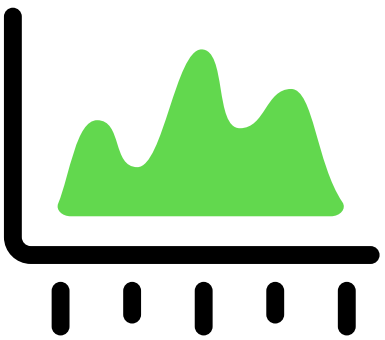
Saiba como monitorar, gerenciar e corrigir AVITs nos espaços de trabalho Gerenciador de vulnerabilidades, Correção de TI e Avaliação de vulnerabilidades.

Corrigir



Saiba como corrigir vulnerabilidades da aplicação.

Análise e emissão de relatórios



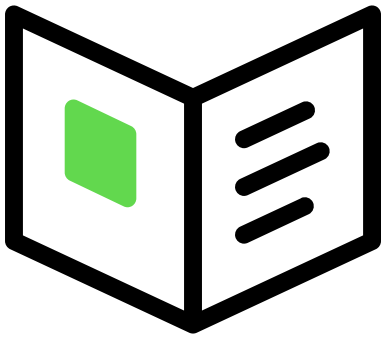
Exibir análise de resposta a vulnerabilidades da aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações

Referência



Obtenha detalhes sobre os componentes de Resposta a vulnerabilidades da aplicação, como campos, tabelas e propriedades.

Solucionar problemas e obter ajuda

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

Explorando Resposta a vulnerabilidades de aplicações

Vulnerabilidades de aplicações são vulnerabilidades em seus aplicativos de software personalizados que são verificados durante todo o ciclo de vida de desenvolvimento da aplicação.

Visão geral de Resposta a vulnerabilidades de aplicações e versões disponíveis

Resposta a vulnerabilidades de aplicações(AVR) é a parte do Resposta a vulnerabilidades aplicação que processa vulnerabilidades da aplicação.

Versões disponíveis

Versão de lançamento	Notas da versão
Resposta a vulnerabilidades v23.0 Resposta a vulnerabilidades v2.0 Resposta a vulnerabilidades v21.0	Resposta a vulnerabilidades de aplicaçõesnotas da versão Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis

Versão de lançamento	Notas da versão
Resposta a vulnerabilidades v20.0 Resposta a vulnerabilidades v19.0 Resposta a vulnerabilidades v18.2	do Vulnerability Response e Mudanças no esquema de versão

Como funciona

Os dados de vulnerabilidade são importados de fontes internas e externas, como a enumeração de pontos fracos comuns (CWE) ou integrações de terceiros. Depois que os dados são importados, eles são comparados com os dados da aplicação em seu Configuration Management Database (CMDB) e processados em Resposta a vulnerabilidades de aplicações aplicação. Se houver uma correspondência entre os dados de vulnerabilidade da aplicação importados e os dados no seu CMDB, um item vulnerável à aplicação (AVIT) será criado.

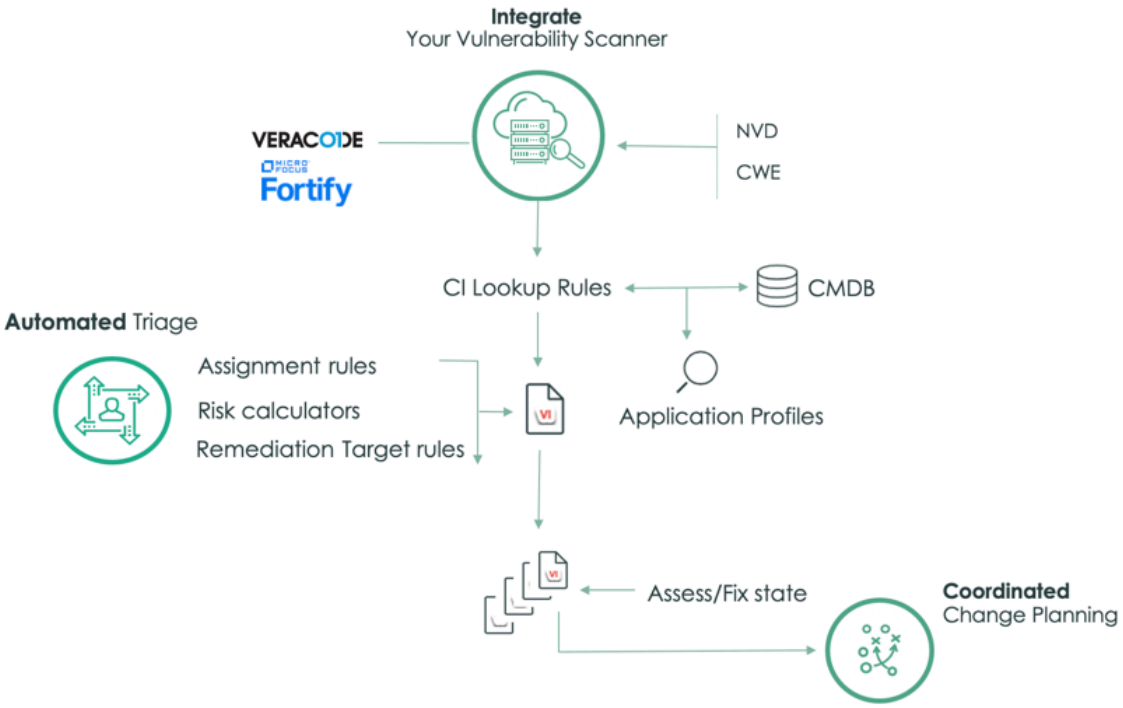
. Resposta a vulnerabilidades de aplicações inclui os seguintes recursos principais:

- Integre com scanners de terceiros compatíveis para importar dados de vulnerabilidade.
- Compare os dados relacionados a vulnerabilidades da aplicação e determine se vulnerabilidades da aplicação são encontradas em uma aplicação.
- Priorizar, corrigir e gerenciar itens vulneráveis à aplicação (AVIT) Cada vulnerabilidade da aplicação representa uma entrada de vulnerabilidade nas bibliotecas CWE ou de terceiros.
- A partir da versão 18,0 de Resposta a vulnerabilidades, Você pode monitorar e corrigir AVITs no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI respectivamente. Para obter mais informações, consulte Espaço do gerente de vulnerabilidade e Espaço de correção de problemas de TI.
- Correlacionar Resposta a vulnerabilidades de aplicações usando calculadoras e bibliotecas para ajudá-lo a executar as tarefas a seguir.
  - Crie itens vulneráveis à aplicação automaticamente usando **Regras de pesquisa de IC** . Durante a importação, vulnerabilidades de terceiros são associadas a um CWE para criar um AVIT.
  - Crie regras de atribuição para automatizar as atribuições de itens vulneráveis da aplicação.
  - Use grupos de calculadoras para determinar o impacto nos negócios, especificar condições variadas usando filtros, aplicar cálculos simples ou usar um script.
  - Crie regras de destino de correção que definam o intervalo de tempo esperado para corrigir itens vulneráveis à aplicação para que você possa monitorar as próximas atividades de correção.
- Relacione uma única vulnerabilidade de terceiros a várias entradas de CWE e encontre o CWE primário de uma vulnerabilidade para ajudá-lo a determinar o risco. Para obter mais informações sobre **CWE primário** , consulte Campos Vulnerabilidade da aplicação.
- Use registros do CWE baixados do banco de dados do CWE ou importados de integrações de terceiros como referência para ajudar você a decidir se deve escalar uma vulnerabilidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar Resposta a vulnerabilidades de aplicações para acompanhar o fluxo de informações, da integração à investigação e, em seguida, à resolução.



Tipos de dados de vulnerabilidade importados

Resposta a vulnerabilidades de aplicações o oferece suporte aos seguintes tipos de dados importados de vulnerabilidade da aplicação.

Nota: Antes da v19.0, os dados de SAST, SCA, IAST e de testes de invasão não eram ingeridos e podem levar em conta as diferenças entre o que é mostrado em Veracode, Fortify e Invicti e o que aparece em Resposta a vulnerabilidades de aplicações.

DAST (Dynamic Application Security Testing, teste dinâmico de segurança da aplicação)

As verificações DAST encontram vulnerabilidades da aplicação enviando entradas para suas aplicações e monitorando suas respostas enquanto elas estão em execução. Esta abordagem pode imitar um ataque externo. Durante a verificação dinâmica, um serviço em execução (URL) é verificado quanto a vulnerabilidades. Os resultados da vulnerabilidade incluem um local de URL de uma vulnerabilidade descoberta.

Teste estático de segurança da aplicação (SAST)

As verificações do SAST revisam o código-fonte das aplicações em repouso e ajudam você a encontrar vulnerabilidades na maneira como você escreveu seu código. A verificação do SAST ocorre em código-fonte não compilado e, portanto, existe independentemente de qualquer serviço de aplicações. Os resultados retornados incluem um local de número de arquivo e linha de uma vulnerabilidade descoberta.

Teste interativo de segurança de aplicações (IAST)

As verificações do IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.

Análise de composição de software (SCA)

A partir da v19.0 de Resposta a vulnerabilidades, Você pode ingerir vulnerabilidades de Análise de composição de software (SCA). Os dados de vulnerabilidade do SCA ajudam a identificar pontos fracos no software de código aberto que está sendo usado em seus aplicativos de software.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Teste de invasão

Você configura solicitações de avaliação de teste de invasão em Resposta a vulnerabilidades de aplicações ajudá-lo a entender onde estão os pontos fracos da sua aplicação e o que você pode fazer para corrigi-los.

Lista de materiais de software

Upload Lista de materiais de software(SBOM) para identificar vulnerabilidades em seus componentes de código-fonte aberto. Para obter mais informações, consulte Explorando Lista de materiais de software.

Casos de uso

Alguns dos seguintes casos de uso DO DAST são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Relacione os resultados da verificação DAST a uma aplicação existente quando houver um registro no CMDB de Descoberta ou uma integração de terceiros.
- Relacione o resultado da verificação DAST a uma aplicação verificada recém-inserida quando uma nova aplicação não tiver sido identificada e/ou armazenada anteriormente no CMDB.
- Armazene os resultados da verificação DAST para um CMDB ao gerenciar suas aplicações em um produto diferente de ServiceNow®.
- Armazene os resultados da verificação DAST para um CMDB se você tiver personalizado anteriormente para alguma outra finalidade.
- Crie uma aplicação para o repositório de código-fonte manualmente.

Alguns dos casos de uso do SAST compatíveis são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Crie um IC para o repositório de código de origem manualmente.
- Armazene os resultados da verificação SAST que estão sem um serviço de aplicações relacionado.

Integrações de terceiros

As integrações de terceiros compatíveis com Resposta a vulnerabilidades de aplicações estão disponíveis como aplicações separadas no ServiceNow Store. Para obter mais informações, consulte Integração do Resposta a vulnerabilidades de aplicações a outras aplicações.

Principais recursos

- Uma API compartilhada importa DAST, SAST, IAST E dados do SCA e resultados de testes manuais da caneta. Consulte Teste de invasão.
- Uma API separada é usada para importar dados do SBOM. Para obter mais informações, consulte Explorando Lista de materiais de software e Integração de Resposta a vulnerabilidades com Veracode.

Regras de pesquisa de IC

Pesquisa automaticamente correspondências nos dados da aplicação no Configuration Management Database (CMDB).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de atribuição

Atribua automaticamente vulnerabilidades da aplicação com base em grupos de usuários, campos de grupo de usuários e scripts.

Calculadoras de risco

Priorize e classifique automaticamente o impacto de AVITs usando calculadoras, com base em qualquer critério, usando filtros de condição.

Mapeamento de severidade

Calcular automaticamente os valores iniciais para campos em itens vulneráveis à aplicação. As entradas de vulnerabilidade têm severidade de origem e severidade normalizada (com base no mapeamento de gravidade). A gravidade está vinculada à enumeração de pontos fracos comuns (CWE).

Regras de meta da correção

Defina o intervalo de tempo esperado para corrigir um item vulnerável à aplicação.

Emissão de relatórios

Obtenha rapidamente informações sobre sua postura de segurança, tendências de correção e 10 principais aplicações ou unidades de negócios com os AVITs mais críticos.

Ambos os tipos de verificações são comuns na versão da aplicação. Uma versão da aplicação, que define um **Nome** cadeia de caracteres, é o ponto de vinculação para agrupar resultados de vulnerabilidade verificados no lado do scanner. Desta forma, o AVR sabe a qual versão da aplicação os resultados pertencem ao importar resultados de verificação por meio da integração.

Uma tabela secundária Item de configuração [cmdb_ci], Aplicações verificadas [sn_vul_app_scan_application], foi criada em Resposta a vulnerabilidades aplicação e escopo. Esta tabela armazena a abstração da versão da aplicação e fornece gráficos de serviço por meio de seus relacionamentos do CMDB. Eles podem ser visualizados no **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Aplicações** módulo. A exibição de lista para aplicações verificadas contém **Departamento** e. **Grupo de suporte** adicionado durante a configuração.

Itens vulneráveis à aplicação (AVITs)

Para vulnerabilidades da aplicação, o AVR relaciona uma vulnerabilidade a uma aplicação para criar o registro de item vulnerável à aplicação (AVIT). Devido às várias definições do que constitui uma aplicação no CMDB, Resposta a vulnerabilidades de aplicações limita aplicações a aplicações verificadas. Aplicações verificadas são as aplicações verificadas em seu ambiente identificadas pelo AVR como **Nome** e. **ID** . AVITs são baseados no resumo da verificação mais recente até a confirmação **Corrigido** pelo scanner. Se um AVIT não for mais encontrado, ele permanecerá vinculado ao resumo da verificação em que foi visto pela última vez.

Itens vulneráveis à aplicação podem ser exibidos no **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Vulnerabilidades** > **Itens vulneráveis** módulo.

Se uma aplicação for removida do CMDB, todos os AVITs associados serão encerrados.

Para obter informações sobre campos de formulário AVIT, consulte Campos de Item vulnerável da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupos de usuários e funções em Resposta a vulnerabilidades de aplicações

Muitas vezes, uma equipe trabalha em conjunto para criar, gerenciar e supervisionar o gerenciamento de vulnerabilidades da aplicação. Existem funções estratégicas, bem como funções operacionais, entre os membros da equipe. Na maioria das organizações, você pode participar de mais de uma função e geralmente compartilhar funções com outras pessoas. Resposta a vulnerabilidades de aplicações Usa três grupos de usuários que contêm funções granulares: Gerenciador da App-Sec, Campeão de segurança da aplicação e Desenvolvedor. Consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções para obter mais informações sobre esses grupos e funções.

Resposta a vulnerabilidades de aplicações estados

Resposta a vulnerabilidades de aplicações Oferece um modelo de estado para o status de seus itens vulneráveis à aplicação (AVITs) e ajuda você a determinar quando e como corrigir seus AVITs.

Um item vulnerável à aplicação tem vários estados possíveis, consulte estados de item vulnerável à aplicação (AVI) para obter mais informações.

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações. Para obter mais informações, consulte Resposta a vulnerabilidades aplicações e. CSDM tabelas.

Configuração da Resposta a vulnerabilidades de aplicações

Antes de executar Resposta a vulnerabilidades de aplicações em seu ServiceNow AI Platform instância, você deve configurá-la.

Como configurar o Resposta a vulnerabilidades de aplicações

Execute as etapas de configuração a seguir antes da configuração para garantir que sua configuração esteja concluída.

Antes de Iniciar

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar Resposta a vulnerabilidades.
Verifique se o Performance Analytics para Resposta a vulnerabilidades está instalado e ativado para ver Resposta a vulnerabilidades de aplicações relatórios.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instale e configure o. Performance Analytics para Resposta a vulnerabilidades Aplicação [PA].
Verifique se o Integração de Resposta a vulnerabilidades com Veracode está instalado, ativado e configurado. (Não execute as integrações neste momento.)	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Veracode.
Verifique se a integração do CWE 2000 está sendo executada em Resposta a vulnerabilidades.	Para verificar a integração, consulte Verifique se o trabalho agendado para atualizar registros NVD está em execução.
[Opcional] Verifique se a integração NVD está sendo executada em Resposta a vulnerabilidades.	Para verificar, consulte Verifique se o trabalho agendado para atualizar registros CWE está em execução.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o usuário com a função de administrador instalará a aplicação e atribuirá usuários aos seguintes grupos de usuários: Gerente da App-Sec, Campeão de segurança e Desenvolvedor. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados. **Nota:** Resposta a vulnerabilidades de aplicações A configuração não está disponível no recurso Assistente de configuração em Resposta a vulnerabilidades.

Função necessária: Grupo de usuários do gerenciador de apps-sec

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Operações de segurança** > **CMDB** > **Regras de pesquisa**.
   Consulte Crie uma regra de pesquisa de IC Para criar ou modificar Regras de pesquisa de IC para seu ambiente.
2. Navegar até **Resposta a vulnerabilidades de aplicações** > **Administração**.
3. Selecione **Regras de atribuição** .
   Consulte Criar ou editar Resposta a vulnerabilidades de aplicações regras de atribuição para criar ou modificar regras de atribuição de aplicações para seu ambiente.
4. Selecione **Calculadoras de vulnerabilidades** .
   Consulte Calcule o risco em Resposta a vulnerabilidades de aplicações automaticamente para criar ou modificar calculadoras de vulnerabilidade da aplicação para seu ambiente.
5. Selecione **Regras de destino de correção** .
   Consulte Criar ou editar regras de destino de correção da aplicação para criar ou modificar destinos de correção de aplicações para seu ambiente.
6. Selecione **Mapas de gravidade normalizados** .
   Consulte Mapeie a gravidade de um item vulnerável à aplicação automaticamente para criar ou modificar mapas de gravidade para seu ambiente.
7. Navegue até qualquer um deles **Integração de vulnerabilidade da Veracode** > **Integrações** ou **Integrações de vulnerabilidade do Fortify** > **Integrações**.
8. Abra a Integração da lista de aplicações Veracode ou a Integração da lista de aplicações FORTIFY sob demanda.
9. Se ele ainda não tiver sido executado, selecione **Executar agora** .

   Nota: O outro Veracode ou Fortify as integrações estão inativas por padrão.

   Para obter os status de execução de integração, consulte Exiba Veracode Status da execução de importação da Integração de vulnerabilidades da aplicação ou Exiba Integrações de vulnerabilidade do Fortify status da execução da importação.
10. Depois que a integração da lista de aplicações Veracode ou FORTIFY on Demand concluir sua execução, navegue até **Resposta a vulnerabilidades de aplicações** > **Administração** > **Aplicações**.
11. Para cada aplicação, insira um valor para **Grupo de suporte** (usado por regras de atribuição) e para **Departamento** (usado na emissão de relatórios).
    Para atualizar várias entradas, consulte Edite vários registros em uma lista usando o editor de lista para concluir a tarefa em massa.

    Nota: Para ver a atualização automática **Unidade de negócios** atualize a página. Para obter informações sobre campos de formulário de aplicação verificados, consulte Campos da aplicação verificados.
12. Retorne à lista Integrações e ative a outra Veracode ou Fortify integrações.
    Consulte Ativar Resposta a vulnerabilidades de aplicações Integrações para definir suas importações de integração de dados delta.

    . Veracode e. Fortify as integrações são encadeadas e serão executadas consecutivamente quando ativadas.
13. **Opcional:** Navegar até **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de atribuição**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. **Opcional:** Se você escolheu **Item de configuração: Grupo de suporte** para **Campo Grupo de usuários** Ao criar ou editar suas regras de atribuição anteriormente, os valores adicionados à exibição de lista de aplicações verificadas estão disponíveis para uso agora.
Suas regras de atribuição são editadas.

b. Selecione **Atualizar**.

c. Na exibição de lista Regras de atribuição de vulnerabilidade, selecione **Aplicar mudanças** Para reaplicar as regras de atribuição aos seus AVIS.

Resultado

. Resposta a vulnerabilidades de aplicações a configuração está concluída.

O que Fazer Depois

Navegar até **Resposta a vulnerabilidades de aplicações** > **Visão geral** e consulte Painel do Application Vulnerability Management [PA] para obter informações sobre sua postura geral de segurança.

Verifique se o trabalho agendado para atualizar registros CWE está em execução

Use registros de enumeração de pontos fracos comuns (CWE) baixados do banco de dados do CWE para referência ao decidir se uma vulnerabilidade deve ser escalonada. Atualize registros de pontos fracos comuns do banco de dados de enumeração de pontos fracos comuns em uma base programada regularmente. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione **Integração abrangente do CWE 2000** trabalho agendado.
3. Verifique se o **Ativo** a caixa de seleção está marcada.

   Nota: As configurações neste formulário são compartilhadas por Resposta a vulnerabilidades e. Resposta a vulnerabilidades de aplicações. Modificar as configurações de integração requer coordenação com e experiência em Resposta a vulnerabilidades e. ServiceNow.

4. Se a caixa estiver marcada, você estará pronto.

   Nota: Se a caixa não estiver marcada, esta integração pode precisar ser configurada em Resposta a vulnerabilidades. Consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

   Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

   . **CWE primário** O campo contém a entrada CWE. Se houver mais de um CWE associado a uma vulnerabilidade, consulte Campos Vulnerabilidade da aplicação Para obter informações sobre como o CWE primário é determinado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verifique se o trabalho agendado para atualizar registros NVD está em execução

Identifique os repositórios que você deseja atualizar regularmente. Você pode executar um trabalho agendado para atualizar registros do National Vulnerability Database (NVD) noite ou semanalmente. Se ele ainda não estiver em execução, você poderá habilitar o trabalho

Antes de Iniciar

Funções necessárias: Grupo do gerenciador de apps-sec

A integração NVD é executada como um trabalho agendado diariamente às segundas-feiras às 00:00:00, por padrão.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione **NIST National Vulnerability Database** trabalho agendado.
3. Verifique se o **Ativo** a caixa de seleção está marcada.

   Nota: As configurações neste formulário são compartilhadas por Resposta a vulnerabilidades e. Resposta a vulnerabilidades de aplicações. Modificar as configurações de integração requer coordenação com e experiência em Resposta a vulnerabilidades e. ServiceNow.

4. Se a caixa estiver marcada, você estará pronto.

   Nota: Se a caixa não estiver marcada, esta integração pode precisar ser configurada em Resposta a vulnerabilidades. Consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

   Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

Ativar Resposta a vulnerabilidades de aplicações Integrações

Habilitar Resposta a vulnerabilidades de aplicações integrações para executar atualizações regulares.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Integrações**.
2. Selecione uma integração.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. Repita conforme necessário para cada integração.
   Após a execução inicial, as integrações são encadeadas para fazer importações delta para execuções subsequentes.

Definir Resposta a vulnerabilidades de aplicações notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações falso-positivas. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas para criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultado
A partir de v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para os usuários com a função sn_vul.app_sec_manager .
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul.app_security_champion, ou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Crie ou edite notificações de destino de correção em Resposta a vulnerabilidades de aplicações

Os administradores de vulnerabilidades podem editar a notificação de destino de correção ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo** .
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultado
A partir de v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para usuários com a função, sn_vul.app_sec_manager .
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul.app_security_champion, ou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de exceções em Resposta a vulnerabilidades de aplicações

Quando sua organização não pode cumprir um gerenciamento de vulnerabilidades publicado ou política de segurança, padrão ou diretriz, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável à aplicação (AVIT) que não pode ser corrigido de acordo com a política.

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

Nota:

A partir de v21.0 de Resposta a vulnerabilidades de aplicações, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável à aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Ciclo de vida de uma exceção

Definição de uma exceção

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

Solicitando uma exceção

Como desenvolvedor, você pode solicitar uma isenção para um AVI usando o processo de gestão de exceções. Depois que o analista de segurança da aplicação aprova esta solicitação, o AVI é movido para **Adiado** estado.

Importante: Você pode solicitar exceções para AVTIs e RTS no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI, respectivamente. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade e Solicite uma exceção no Espaço de correção de problemas de TI.

Regras de exceção

A partir da v20, você pode criar regras de exceção para adiar automaticamente itens vulneráveis à aplicação (AVI) existentes e novos por um período específico se eles corresponderem às condições da regra. Usar regras de exceção para adiar automaticamente o AVIS minimiza o risco de perder acordos de nível de serviço. As regras podem ajudá-lo a gerenciar vários itens, porque você está eliminando a intervenção manual. Consulte Criar uma regra de exceção.

Solicitando uma extensão para uma regra de exceção

A partir da v20, você pode enviar uma solicitação de extensão para **Adiado até** data de uma regra de exceção. Você pode solicitar uma extensão para uma regra se descobrir que um grande número de registros criados pela regra não está sendo resolvido por ela **Adiado até** Data, a data em que a tarefa de correção para de aceitar novos AVIS. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento em sua regra existente. Você pode inserir datas de até um ano a partir da data atual e deve incluir um motivo para a extensão. Uma solicitação de extensão requer aprovação de dois níveis de grupos de aprovação separados.

Aprovando uma solicitação de exceção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

AVITs que não podem ser corrigidos imediatamente são revisados por analistas de segurança de aplicações, avaliados quanto a risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicione um aprovador de exceção para Resposta a vulnerabilidades de aplicações.

Importante: Você pode aprovar ou rejeitar solicitações de exceção no Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade.

Nota:

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

- Reabrir
- Obtenha mais detalhes

Acompanhamento de uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando **Aprovações de mudança de estado** Do AVIT.

Expiração de uma solicitação de exceção e solicitação de uma extensão para uma regra de exceção

Quando uma solicitação de exceção para um AVI específico expira, o AVI afetado é revertido para seu **Aberto** estado.

No entanto, a partir da v20, você pode enviar uma solicitação para estender o. **Adiado até** data na regra de exceção.

Configure a Gestão de exceções para Resposta a vulnerabilidades de aplicações

Limitar a duração de uma exceção solicitada e adicionar um questionário à solicitação de exceção ou falso positivo usando o módulo . Por padrão, uma exceção é solicitada usando ServiceNow® Resposta a vulnerabilidades de aplicações módulo. Você também pode solicitar uma exceção usando GRC: Gestão de políticas e conformidade integração.

Antes de Iniciar

Função necessária: sn_vul.app_manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Resposta a vulnerabilidades habilitado, você pode limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o GRC: Gestão de políticas e conformidade o módulo está instalado, você pode selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite que você solicite uma exceção que especifica o objetivo de Política e controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que levantou a exceção ou a solicitação de falso positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador da exceção entenda o motivo da solicitação da exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.

   Nota: Começando com Resposta a vulnerabilidades versão 17,1, você pode selecionar uma Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade. Você deve ativar o. GRC plug-in a ser usado GRC: Gestão de políticas e conformidade para solicitar uma exceção. Mudar a configuração não afeta os dados existentes.

3. Preencha os campos no formulário com base na opção selecionada.
   - Se você selecionou Resposta a vulnerabilidades e preencha os campos no formulário.

     Formulário de Configurações do Gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação falso-positivo é exibido por padrão.

   - Se você selecionou GRC: Gestão de políticas e conformidade e preencha os campos no formulário.

     Formulário de Configurações do Gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação falso-positivo é exibido por padrão.

4. Selecione **Save** (Salvar).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure regras de aprovação para Gestão de exceções

Começando com Resposta a vulnerabilidades de aplicações v15.0, use o designer de fluxo para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades de aplicações(AVR) Pela primeira vez, o Flow Designer é habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Se você for um usuário de VR existente, a opção padrão será Fluxo de trabalho.
Se você implantou Resposta a vulnerabilidades de aplicações v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation*definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Resposta a vulnerabilidades de aplicações antes da v15.0, o valor desta propriedade do sistema era definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota: Você não pode reverter para usar o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis da aplicação
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso-positivo para itens vulneráveis da aplicação

Nota: Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação . (dias) A partir de v21.0 de Resposta a vulnerabilidades de aplicações	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir de v21.0 de Resposta a vulnerabilidades de aplicações	Data após a qual o aprovador é notificado para executar uma ação.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Adiando correção em Resposta a vulnerabilidades de aplicações

A partir da v20.0, você pode adiar a correção com **Aguardando implementação** informe que está disponível para itens vulneráveis à aplicação (AVI) e tarefas de correção conforme eles se movem por seus ciclos de vida. Você só pode fazer a transição de registros para este estado manualmente selecionando **Aguardando implementação** De AVI e registros de tarefa de correção no **Em investigação** estado.

Caso de uso

Como especialista em correção, você pode mover um registro para **Aguardando implementação** para que sua equipe saiba que sua pesquisa e trabalho em uma tarefa estão concluídos. Você pode escolher esta atualização se achar que uma correção está pronta para implementação, mas não está disponível. Um exemplo de uma correção indisponível é um patch de software. Se a janela de manutenção de um patch não estiver disponível quando você terminar sua pesquisa, você poderá mover a tarefa para **Aguardando implementação** até que o patch possa ser implantado.

Campos necessários

Há dois campos obrigatórios editáveis nos registros AVI e de tarefa de correção que estão no estado Aguardando implementação:

Data do compromisso de correção

A data de correção planejada.

Plano de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A descrição do plano de correção para correção. Este texto é exibido nas Anotações no registro.

Campos e propriedades do sistema

Duas propriedades do sistema definidas como verdadeiro por padrão para o modal que aparece quando você faz a transição de um registro para **Aguardando implementação** . Se deixado nas configurações padrão:

sn_vul.remediation_fields

Conjuntos **Data do compromisso de correção** e. **Plano de correção** como campos obrigatórios. Se definido como falso estes campos são opcionais.

sn_vul.waiting_implementation

Exibe o modal com **Data do compromisso de correção** , **Plano de correção** campos depois de selecionar **Aguardando implementação** em um registro. Se definido como falso , Você pode mudar o estado de um AVI para Aguardando implementação sem um prompt para inserir uma data de compromisso ou um plano.

Módulo de data de compromisso de correção perdida

Exiba todos os Avis que perderam as datas de compromisso de correção no **Data de compromisso de correção perdida** módulo. Navegar **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis** > **Data do compromisso de correção perdido** para exibir a lista.

Rolagem de estado das tarefas de correção para os AVIS

O botão de ação de IU para fazer a transição de um registro **Aguardando implementação** só está visível em itens vulneráveis à aplicação e registros de tarefa de correção em **Em investigação** estado. Para rolagem de estado para baixo, no modal que aparece quando você seleciona **Aguardando implementação** em uma tarefa de correção, há uma opção para **Substituir Avis existentes** .

Opção	Descrição
Selecione **Substituir Avis existentes** .	Selecione esta opção para substituir as datas de compromisso de correção e os planos de correção de quaisquer AVIS existentes na tarefa já em **Aguardando implementação** estado. Se selecionado, este recurso reverterá os dados de data e plano na tarefa de correção para o Avis.
Sair **Substituir Avis existentes** desativado.	Deixe a opção desativada para manter os valores de data e plano intactos para qualquer Avis existente na tarefa já em **Aguardando implementação** estado. Se desativado, o Avis já está em **Aguardando implementação** preservam a data e os dados do plano existentes e não são afetados pela rolagem de estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de rolagem

Digamos que você deseja fazer a transição de uma tarefa de correção de **Aberto** . **Aguardando implementação** para que você possa atualizar a data de compromisso da tarefa e as informações de plano para uma janela de manutenção de patch de software. Suponha que haja um AVI nesta tarefa no **Aguardando implementação** e você deseja atualizar a data de compromisso e as informações do plano para corresponder à tarefa de correção.

Para substituir a data do Avis e os dados do plano para que correspondam à tarefa de correção, marque a caixa de seleção para **Substituir Avis existentes** quando solicitado. Os valores de data e plano do AVI se tornam os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação** .

Se você não selecionar a opção de substituição neste caso, e houver um AVI em **Aguardando implementação** , A data original e os dados do plano no AVI permanecem intactos. Os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação** Não são usados em nenhum Avis que já esteja em **Aguardando implementação** estado na tarefa.

Se um AVI em uma tarefa estiver em **Resolvido** ou **Encerrado-Corrigido** e você faz a transição da tarefa para **Aguardando implementação** selecionando **Substituir Avis existentes** Não muda o Avis de **Encerrado-Corrigido** e. **Resolvido** . **Aguardando implementação** devido a uma precedência de estado mais alta.

Se a substituição não estiver selecionada ao mover a tarefa para **Aguardando implementação** E já há um AVI **Aguardando implementação** e você move a tarefa de volta para **Aberto** ou **Em investigação** , O AVI permanece em **Aguardando implementação** .

Adicione um aprovador de exceção para Resposta a vulnerabilidades de aplicações

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Uma solicitação de exceção para um item vulnerável à aplicação é aprovada usando o fluxo de aprovação de dois níveis padrão. A solicitação pode ser aprovada por dois níveis de aprovadores. Adicionar usuários ao grupo de primeiro nível é obrigatório. Se não houver usuários no segundo nível, a solicitação será aprovada após a aprovação de primeiro nível.

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.
2. Na coluna Nome, pesquise **Exceção** e clique em **Aprovador de exceção da aplicação - Nível 1** .

   Nota: A partir de Resposta a vulnerabilidades de aplicações V12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio de fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção ou falso positivo é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Tudo** > **Propriedades do sistema** e selecione *sn_vul.app_exception_approver_L1*, *sn_vul.app_exception_approver_L2*ou *sn_vul.app_false_positive_approver_group*para mudar o valor da propriedade.

3. No formulário Aprovador de exceção da aplicação de grupo - Nível 1, clique na lista relacionada Membros do grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário de usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário da instância e encerrar todas as sessões ativas do usuário. O sistema impede que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ○ Listas de usuários ○ Lista de seleção em campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário do local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
7. **Opcional:** Repita as etapas 1 a 5 para criar um Aprovador de exceção de aplicação - Nível 2. O aprovador deve navegar até **Resposta a vulnerabilidades da aplicação** > **Minhas aprovações** e aprovar solicitações.

Solicitando e aprovando uma exceção em Resposta a vulnerabilidades de aplicações

Você pode solicitar o adiamento da correção de um item vulnerável à aplicação e de uma tarefa de correção por um período especificado.

Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Você também pode criar regras de exceção e solicitar uma extensão de exceção para uma regra de exceção. Por padrão, dois níveis de aprovação são necessários para adiamentos, regras de exceção e solicitações de extensão de exceção.

Para solicitar ou aprovar uma exceção, consulte:

- Solicite uma exceção para um item vulnerável à aplicação
- Solicite uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade
- Aprovar regras de exceção e solicitações de extensão de regra de exceção em Resposta a vulnerabilidades de aplicações
- Solicite uma extensão para uma regra de exceção em Resposta a vulnerabilidades de aplicações

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir de v21.0 de Resposta a vulnerabilidades de aplicações, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável à aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Solicite uma exceção para um item vulnerável à aplicação

Solicite uma exceção para um item vulnerável à aplicação que não pode ser corrigido imediatamente. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Importante: Você pode solicitar exceções para um item vulnerável à aplicação e uma tarefa de correção no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade e Solicite uma exceção no Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária: Grupo de desenvolvedores

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** > **Tudo** e selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Em investigação.

   Nota:

   A partir de v21.0 de Resposta a vulnerabilidades de aplicações, o estado anterior de um item vulnerável à aplicação é armazenado em **backup_state** campo.

2. No formulário Item vulnerável da aplicação, clique em **Exceção de solicitação** .

   Nota: Dependendo de Resposta a vulnerabilidades selecionado ou GRC: Gestão de políticas e conformidade em **Resposta a vulnerabilidades de aplicações** > **Gestão de exceção** , o formulário Solicitar exceção muda. Se GRC: Gestão de políticas e conformidade, consulte Solicite uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade

3. Se Resposta a vulnerabilidades Estiver selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo reverte para seu **Aberto** estado. **Nota:** A partir da versão 18,0 de Resposta a vulnerabilidades de aplicações(AVR), um item vulnerável da aplicação adiada pode ser fechado e reaberto por um scanner. Se o item for reaberto antes que a janela de exceção expire, o estado do AVIT será revertido para o estado Adiado respeitando a janela de exceção ativa. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_avit_in_active_exception_window como verdadeiro. Além disso, a data Adiado até persiste mesmo depois que o AVIT é encerrado ou a exceção expira. A função necessária é sn_vul.app_manage_exception_configuration para leitura e gravação.
Motivo	Selecione **Motivo** . As opções são: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Redução do controle no local ○ Outro Para ver como adicionar novas opções de motivo, consulte Defina o mapeamento do motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser atualizado pelo responsável pela correção.

4. Clique em **Aprovação da solicitação** para enviar a solicitação de exceção.
   O estado do item de vulnerabilidade da aplicação muda para Em revisão. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicite uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade

Solicitar exceções de política usando GRC capacidade de gestão de exceções de política no Gestão de políticas e conformidade aplicação a partir de Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Antes de usar a Integração de exceção de política para solicitar exceções de política, você deve baixar o. GRC: Gestão de políticas e conformidade aplicação do ServiceNow Store.

Função necessária: sn_vul.remediation_ responsável

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** (ou **Tarefas de correção**)> **Todos** e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Exceção de solicitação** .
3. Se GRC: Gestão de políticas e conformidade Estiver selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começará. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e o estado do item vulnerável ou grupo muda de Adiado para Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** Que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

a. Clique em **Aprovação da solicitação** para enviar a solicitação de exceção.
O estado dos itens vulneráveis muda para Em revisão e uma exceção de política é criada. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

b. Clique na lista relacionada Exceções de política para exibir a exceção de política.

c. Clique no número da exceção de política.

d. Em **Aprovador** , selecione o nome do aprovador.

e. Clique na guia Origem e selecione um objetivo de controle no **Objetivo de controle** campo.

f. Clique na guia Avaliação de risco e selecione a classificação de risco em **Classificação de risco** campo.

g. Salve o formulário.

h. Clique na guia Controles afetados e clique em Adicionar para adicionar os controles.

i. Salve o formulário.

Nota: Você pode criar uma revisão de conformidade clicando em **Solicitar revisão de conformidade** .

j. O formulário de aprovação é enviado ao aprovador.

k. Como aprovador, você pode aprovar a solicitação clicando em **Aprovar** ou solicite aprovação adicional clicando em **Solicitar aprovação adicional** .
O estado do registro muda para Adiado. O motivo informado é aquele que você selecionou ao gerar a solicitação de exceção. A guia Adiamento fornece anotações adicionais sobre o registro.

Nota: Se a solicitação for rejeitada, o registro será movido para o estado anterior.

4. Clique em **Enviar**.
Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma exceção para uma tarefa de correção de aplicação

Solicite uma exceção para adiar uma tarefa de correção de aplicação por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções do Resposta a vulnerabilidades Espaços de trabalho. Consulte Solicite uma exceção no Espaço de correção de problemas de TI.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Funções necessárias: sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de aplicações no ambiente clássico.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção** > **Tudo**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Em investigação ou Aguardando implementação.
3. No registro da tarefa de correção da aplicação, selecione **Exceção de solicitação** .
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Aprovar regras de exceção e solicitações de extensão de regra de exceção em Resposta a vulnerabilidades de aplicações

Aprove solicitações de exceção para itens vulneráveis à aplicação que não podem ser corrigidos imediatamente. Você deve avaliar essas solicitações de risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Defina o mapeamento do motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar

Você deve ter a aplicação GRC: Policy and Compliance Management instalada. Esta aplicação está disponível no ServiceNow® Store com uma assinatura separada.

Para obter detalhes sobre os requisitos do sistema e a compatibilidade da família, consulte a lista de aplicativos no site ServiceNow Store .

Função necessária: sn_vul.compliance.manager e sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Tudo** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

   Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

2. Clique no registro de integração da sua aplicação, por exemplo, **Resposta a vulnerabilidades da aplicação** , **Resposta a vulnerabilidades** e assim por diante.
3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista Opções de motivo, clique em **Novo** .
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Opções de motivo, execute as seguintes etapas:
   a. Na lista Opções de motivo, clique em **Novo** .
   b. Clique no ícone de lupa.
   c. Clique em **Nova**.
   d. No formulário, preencha os campos.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos do motivo da exceção de política para as respectivas aplicações. Para navegar até esta tabela, insira sn_vul_policy_reason_mapping.LIST no navegador de filtros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Pedido para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham **Padrão** o campo selecionado estará disponível.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Solicite uma extensão para uma regra de exceção em Resposta a vulnerabilidades de aplicações

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Funções necessárias: Gerente da App-Sec sn_vul.app_sec_manager, Campeão de segurança sn_vul.app_security_champion.

Por Que e Quando Desempenhar Esta Tarefa

Em um registro de regra de extensão, você pode solicitar uma extensão para **Adiado até** data somente se a regra estiver em **Aprovado** estado. Você pode solicitar esta extensão para uma regra se descobrir que um grande número de registros criados pela regra não está sendo resolvido por ela **Adiado até** Data, a data em que a tarefa de correção para de aceitar novos AVIS. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento em sua regra existente.

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até a qual a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Correção indisponível ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas e nos itens vulneráveis à aplicação. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end

Solicite uma extensão para uma tarefa de correção adiada em Resposta a vulnerabilidades de aplicações

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Na aprovação da solicitação, as mudanças na tarefa de correção também são transferidas para os itens vulneráveis da aplicação, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis à aplicação devem estar no estado Adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicite uma extensão para um item vulnerável da aplicação adiada em Resposta a vulnerabilidades de aplicações

Solicite uma extensão para um item vulnerável da aplicação adiada antes que ele atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis**.
2. Abra um item vulnerável da aplicação adiada.
3. Selecione **Extensão da solicitação** .

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável da aplicação é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até a qual o item vulnerável da aplicação adiada deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Um e-mail é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Crie, exclua e cancele uma regra de exceção para Resposta a vulnerabilidades de aplicações

Crie uma regra para solicitar uma exceção automaticamente para itens vulneráveis à aplicação (AVI) que atendam a condições específicas.

Antes de Iniciar

Por exemplo, você pode criar uma regra com uma condição baseada em uma vulnerabilidade específica conhecida ou crítica que você sabe que não pode corrigir imediatamente. Com esta regra, você pode adiar os novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

- A regra de exceção é aplicada a partir do **Válido de** até **Válido até** data que você insere no registro de regra.
- A tarefa de correção (AVUL) é criada depois que a regra é aprovada para correspondência de Avis no **Adiado** estado.
- O método de agrupamento para este AVUL é conhecido como Regras de exceção.
- Não é possível fechar, reabrir ou excluir este AVUL. Avis novos e reabertos são adiados e adicionados a este AVUL a partir de **Válido de** data até que o grupo expire em **Válido até** data.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Funções necessárias: App SEC Manager sn_vul.app_sec_manager e Security Champion sn_vul.app_security_champion.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de exceção**.
2. Na página Novo registro de Regra de exceção, selecione **Novo** .
3. Preencha os campos.

Campo	Descrição
Nome	Nome da regra de exceção.
Estado	Somente leitura: Rascunho
Válida de	Data a partir da qual esta regra está ativa para adiar AVIS.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor mais baixo precede um maior.
Válida até	Data em que a tarefa de correção para de aceitar novos AVIS.
Adiado até	Data até que as tarefas de correção e os AVIS sejam adiados. Nesta data, os AVULs são encerrados e todos os Avis saem das tarefas e são reabertos. As regras de grupo são reaplicadas a esses AVIS.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção está atribuída para rastrear os AVIS adiados.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condições de filtro para especificar quais Avis correspondem a esta regra.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	pelo trabalho agendado *Associate existing AVIs with Auto Exception Rule*começando com novos dados. Se você habilitar a opção Executar nos dados existentes, um trabalho agendado será executado uma vez nos dados existentes no **Válido de** data.

4. Adicione o grupo de atribuição ao criar a regra.
5. Escolha um.

Opção	Descrição
Salve a regra	Salve suas mudanças e a regra será exibida na lista de regras de exceção [sn_vul_auto_exception_rule]. Até que você envie a regra de exceção para aprovação, ela permanecerá em **Rascunho** estado.
Envie a regra	Se você enviar a regra, o status da solicitação mudará para **Em revisão** . Uma aprovação de regra de exceção requer dois níveis de aprovação, um do Aprovador de exceção da aplicação - Nível 1 e outro do Aprovador de exceção da aplicação - Nível 2.

Depois que a regra é aprovada, ela passa para **Aprovado** estado. Sua regra avalia Avis com *Associate existing AVIs with Auto Exception Rule scheduled*trabalho. Se você selecionou **Executar nos dados existentes** Ele avalia os Avis existentes. Uma tarefa de correção é criada automaticamente para a regra e todos os AVIS correspondentes que atendem às condições são associados à tarefa.

O trabalho agendado executa a regra de exceção uma vez nos dados existentes. A regra não é executada novamente nos dados existentes, mesmo se nenhum Avis for encontrado. Ele só avalia novos dados porque os AVIS existentes que corresponderam à regra já foram adiados.

6. Para excluir uma regra, selecione **Excluir** no registro de regra de exceção.
   A seguinte mensagem é exibida: Se você excluir a regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras da tarefa de correção serão aplicadas aos Avis individuais e a regra de exceção será excluída.
7. Selecione **Manter regra** para parar ou **Excluir regra** para continuar.
8. Para desativar uma regra, mas mantê-la na lista Regras de exceção, selecione **Cancelar** .
   A seguinte mensagem é exibida: Se você cancelar esta regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras da tarefa de correção serão aplicadas aos itens vulneráveis individuais e a regra de exceção será movida para o estado de rascunho.
9. Selecione **Manter regra** para parar ou **Cancelar** para mover a regra para **Rascunho** e desative-o.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Configure tarefas de correção (AVULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis à aplicação (AVI) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que os AVIS sejam atribuídos automaticamente a tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Acompanhamento de contagens de adiamentos para itens vulneráveis à aplicação e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável à aplicação, item vulnerável ao contêiner ou tarefa de correção é adiado. . `set deferral counts`O trabalho agendado é executado diariamente para contabilizar contagens para os registros que são adiados mais de uma vez na coluna Contagem de adiamentos. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Noções básicas sobre as regras de tarefa de correção

As regras de tarefa de correção permitem que você defina como os itens vulneráveis à aplicação são agrupados e atribuídos automaticamente. Uma regra padrão **Vulnerabilidade** Está incluído no sistema de base que coleta AVIS com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis no AVI. Esses valores podem incluir item de configuração (IC), entrada de vulnerabilidade e similares.

Há regras de tarefa para Resposta de vulnerabilidade da aplicação que estão incluídas com Resposta a vulnerabilidades aplicação que está disponível quando você o ativa.

Você pode criar várias condições com o construtor de condições. Na seção Agrupar por, depois de definir um par de campos, outra linha será exibida. Você pode ter até seis **Agrupar por** seleções. Você também pode automatizar a atribuição de grupo. Para obter mais informações, consulte Atribua itens vulneráveis à aplicação em Resposta a vulnerabilidades de aplicações automaticamente e Filtrando em Resposta a vulnerabilidades.

Por exemplo, você pode agrupar os itens vulneráveis da aplicação pelo item de configuração ou pelo modelo do produto. Você pode ter uma regra de tarefa para vulnerabilidades de baixa gravidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades que expõem a empresa a mais riscos. Consulte Criar, editar e excluir Resposta a vulnerabilidades de aplicações regras de tarefa de correção para obter mais informações sobre as opções que você tem disponíveis.

Um conjunto diferente de regras pode ser usado para itens vulneráveis à aplicação que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado à regra da tarefa de correção **Agrupar por** valores para fazer a descrição resumida do novo registro.

Quando um novo item vulnerável à aplicação é criado, importado ou reaberto após ser encerrado, as regras são avaliadas em relação a ele. Um AVI só é avaliado uma vez, automaticamente, a menos que seja reaberto após ser encerrado ou que as regras sejam reaplicadas manualmente.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

  Nota: O campo Descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidades mais longos estão truncados.

  A regra verifica se há uma correspondência **Aberto** Tarefa de correção atribuída ao mesmo grupo de atribuição que o AVI.

  - Se a tarefa for encontrada, o AVI será adicionado à tarefa existente no **Aberto** estado.
  - Se não houver tarefa no **Aberto** encontrado, a regra cria um **Alto risco: QID-32342** A atribui ao mesmo grupo de atribuição que o AVI e coloca o AVI na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições da regra da tarefa de correção antes de colocá-la em uma tarefa de correção, muitas regras podem afetar o desempenho. Configure suas regras de tarefa para que as condições ajudem a evitar a criação de tarefas de correção duplicadas.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelo **Regras de atribuição** No AVI ao agrupar os itens e atribuir a tarefa de correção para corresponder aos AVIS.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras em **Regras de atribuição** módulo. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Quando uma regra de tarefa é excluída da exibição de formulário ou de lista, você tem a opção de excluir tudo **Aberto** tarefas criadas por essa regra. Tarefas que não estão no **Aberto** os estados são excluídos.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use **Reaplicar** botão na página de regra da tarefa de correção para executar novamente a regra alterada em todos os ativos **Aberto** tarefas de correção criadas por essa regra. Exclui e recria tarefas de correção com base na regra alterada automaticamente.

Reaplicar verifica somente as tarefas de correção existentes.

Depois de selecionar **Reaplicar** a seguinte mensagem é exibida: Reaplicar esta regra de tarefa de correção excluirá e recriará as tarefas de correção para esta regra. As tarefas de correção que não estão no estado Aberto não são excluídas .

Criar tarefas de correção e adicionar AVIS manualmente

Você cria uma tarefa de correção de aplicação (AVUL) a partir de outro registro de tarefa de correção de aplicação e adiciona itens vulneráveis à aplicação (AVITs) manualmente. Para obter mais informações, consulte Crie uma tarefa de correção de aplicação manualmente em Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação e atualização de regras de tarefa de correção e AVI

Se um IC ou modelo de produto de uma verificação estiver associado a uma vulnerabilidade conhecida, um AVI será criado. Depois de criado, o AVI é avaliado em relação às condições das regras de tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma tarefa será criada para o AVI.

Se qualquer propriedade capturada nas condições de filtragem da tarefa de correção for atualizada ou alterada em um AVI, o AVI atualizado também será avaliado em relação às regras da tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma tarefa será criada para o AVI.

Rollup de estado e rolldown

Se você atualizar uma tarefa de correção para Aberto ou de Aberto para Em investigação, o novo estado será revertido para Todos os AVIS associados. A rolagem de estado ocorre imediatamente depois que você muda o estado.

O acúmulo de estado do Avis para a tarefa de correção ocorrerá somente se todos os Avis na tarefa estiverem em **Adiado** ou **Encerrado- Corrigido** estados. O acúmulo é feito com *`Rollup application vulnerable item values to vulnerability and group`*trabalho agendado, que é executado a cada 15 minutos. O estado não é acumulado até que o trabalho seja executado. Para que um estado ocorra do AVIS para a tarefa de correção, todos os AVIS devem estar no mesmo estado.

Criar, editar e excluir Resposta a vulnerabilidades de aplicações regras de tarefa de correção

Você pode criar regras para agrupar automaticamente itens vulneráveis à aplicação (AVI) em tarefas de correção (AVUL) com base nas condições de filtro. Essas regras agrupam automaticamente os Avis conforme são importados ou criados manualmente.

Antes de Iniciar

Se você criar uma nova regra, ela não se aplicará aos dados existentes. Depois de enviá-lo, ele será executado em relação às novas importações.

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou selecione **Novo** .
3. Preencha os campos no formulário ou edite-os.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra da tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre	Determina se uma condição diferencia maiúsculas de minúsculas ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
maiúsculas e minúsculas	**Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. Por padrão, (**Distinção entre maiúsculas e minúsculas** caixa de seleção não marcada), o texto de pesquisa inserido no construtor de condições nos registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefa. Um exemplo de condição é **Vulnerabilidade** > **é** > **VULNENT123451** (uma vulnerabilidade importada conhecida). Qualquer Avis que tenha esta vulnerabilidade corresponde a esta condição.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis da aplicação de	A tabela que a regra usa para agrupar Avis. Selecione os elementos na árvore: ○ Item vulnerável da aplicação [sn_vuln_vulnerable_item] ○ Item de configuração de item vulnerável da aplicação [cmdb_ci] ○ Vulnerabilidade da aplicação de item vulnerável da aplicação [sn_vul_third_party_entry] ○ Modelo de produto de item vulnerável da aplicação **Nota:** Se você escolher uma tabela estendida, o **Usando o campo** é aplicado somente a itens vulneráveis à aplicação que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar AVIS. Selecione Condições na árvore. **Nota:** Você pode criar condições de grupo por para que nem todos os AVIS que compartilham dados sejam atribuídos à mesma tarefa de correção. Por exemplo, se você selecionar Grupo de atribuição e Endereço IP como os campos Usando, e vários Avis corresponderem à condição de filtragem inicial **Vulnerabilidade** Esses AVIS podem ser atribuídos a grupos de atribuição distintos para correção usando as muitas opções disponíveis na seção Agrupar por. As condições Agrupar por oferecem flexibilidade para criar tarefas de correção distintas que podem ser atribuídas a grupos diferentes, mesmo que compartilhem alguns dados.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir tarefas de correção automaticamente, a opção Atribuição é usada além de **Agrupar por** opções para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para que cada AVI seja colocado em uma tarefa com um conjunto de grupos de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Agrupar por campo: Se você selecionou qualquer campo de grupo de usuários no **Usando o campo** valores em **Agrupar por** , eles aparecem no menu suspenso. ◦ Grupo de usuários: Use a lista de pesquisa para selecionar um grupo de usuários estático.

se você excluir uma regra da exibição de formulário ou de lista, terá a opção de excluir tudo **Aberto** tarefas de correção criadas por essa regra. Grupos que não estão em **Aberto** os estados são excluídos.

4. Selecione **Enviar** para novas regras.
   Depois de selecionar **Enviar** Sua regra é exibida na lista Regras da tarefa de correção [sn_vul_grouping_rule]. As situações a seguir iniciam sua regra.
   - Quando novos Avis são criados.
   - Ao selecionar **Reaplicar** . Você seleciona **Reaplicar** avaliar regras de tarefa somente em tarefas de correção existentes.
   - Quando os Avis são atualizados, por você ou pelo sistema.

     Se um AVI for atualizado, as regras de tarefa serão avaliadas quanto a correspondências com as tarefas de correção existentes. Algumas atualizações comuns que iniciam uma verificação de regras são:
     - Quando o Estado muda de Encerrado para Aberto ou de Encerrado para Em Investigação.
     - O item de configuração (IC) foi alterado.
     - A vulnerabilidade foi alterada.

   O sistema verifica se todas as regras de tarefa correspondem ao AVI atualizado. Se as condições de uma regra corresponderem às condições de uma tarefa de correção, os AVIs correspondentes serão atribuídos a ela.

   Se nenhuma correspondência for encontrada, uma nova tarefa de correção será criada.

   Para obter mais informações sobre acúmulo de estado do AVIS para tarefas de correção e acúmulo de estado das tarefas de correção para o AVIS, consulte Resposta a vulnerabilidades de aplicações tarefas de correção e visão geral de regras de tarefa.

   Para obter um exemplo de uma regra de tarefa de correção, consulte Resposta a vulnerabilidades de aplicações exemplos de regra de tarefa de correção.

5. Para excluir uma regra de tarefa, selecione a regra na lista Regras da tarefa de correção e selecione **Excluir** .
   A seguinte mensagem é exibida: A regra de tarefa de correção selecionada criou n tarefas de correção. Das tarefas de correção, n estão no estado Aberto. .

Opção	Descrição
Caixa de seleção desativada (padrão).	Exclua somente a regra. Tarefas que não estão no **Aberto** os estados são excluídos.
Caixa de seleção selecionada.	Inclua as tarefas de correção no **Aberto** estado quando você exclui a regra de tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Exclua a regra e todas as tarefas de correção no **Aberto** estado.

6. Escolha uma opção e selecione **Excluir** .

Crie uma tarefa de correção de aplicação manualmente em Resposta a vulnerabilidades de aplicações

Crie uma tarefa de correção de aplicação (AVUL) a partir de outro registro de tarefa de correção de aplicação e adicione itens vulneráveis à aplicação (AVITs) manualmente.

Antes de Iniciar

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção** > **Tudo**.
2. No canto superior direito da página, selecione **Novo** .
3. Na guia Configuração de grupo, para Método de agrupamento, selecione **Manual** .
4. Selecione **Enviar**.
5. Localize seu novo registro de tarefa (AVUL) na tabela Tarefas de correção da aplicação [sn_vul_app_vulnerability].
   O registro é criado no **Aberto** estado.
6. Abra o registro e adicione itens vulneráveis à aplicação novos ou existentes a este grupo usando a lista relacionada Itens vulneráveis à aplicação (**Editar** ou **Adicionar**).
7. Selecione **Atualização** Para salvar o registro ou outras ações de IU para fazer a transição do registro para outro estado.

Criar regras de fechamento automático

Use regras de fechamento automático para fechar AVITs mais antigos automaticamente com base nas condições de filtro definidas.

Antes de Iniciar

Função necessária: sn_vul.app_manage_auto_close_rules

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de fechamento automático**.
   O sistema de base fornece as seguintes regras de fechamento automático:

   Vulnerabilidades da aplicação verificadas pela última vez As vulnerabilidades não relatadas nos últimos 90 dias são transferidas para **Obsoleto** estado.

2. Selecione **Novo** para criar uma nova regra de fechamento automático.
3. No formulário, preencha os campos.

Campo	Valor
Nome	Nome da regra de fechamento automático.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
Ativo	Opção para ativar a regra. Se ativado, ele fecha automaticamente todas as detecções que correspondam aos critérios de filtro.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Tipos de integração	Integração de vulnerabilidade da aplicação
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.

. **Processador de regras de fechamento automático** o trabalho agendado é executado todas as noites. Ele identifica AVITs com base nas condições especificadas e faz a transição das correspondentes para **Obsoleto** estado. Nos casos em que há AVITs com status "Encerrado" e "obsoleto", o AVIT é encerrado com o subestado definido como **Corrigido** .

Configurar testes de invasão

Você pode configurar a duração do sprint e o esforço estimado para tipos de avaliação de teste de invasão. Isso fornece a funcionalidade de programação para os proprietários da aplicação, ajudando-os a determinar um intervalo de tempo provisório para suas solicitações de avaliação de teste de invasão.

Antes de Iniciar
Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa
Definir as configurações de avaliação de teste de invasão para a equipe de hacking ético também ajuda a determinar o grupo e o ponto de contato que recebe a solicitação de avaliação de teste de invasão.

A partir da v19.0 de Resposta a vulnerabilidades se você estiver usando Integração de Resposta a vulnerabilidades com Veracode, os testes de avaliação de invasão no Integração de Resposta a vulnerabilidades com Veracode são descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão que você configura em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Integração de Resposta a vulnerabilidades com Veracode.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. Use a primeira seção para configurar o grupo de atribuição.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração de teste de invasão

Campo	Descrição
Grupo de usuários da equipe de testes de invasão	Grupo ao qual a solicitação de avaliação de teste de invasão está atribuída.
Atribuído padrão das solicitações de avaliação de testes de invasão	Ponto de contato para a solicitação de avaliação de teste de invasão.

4. Selecione **Atualizar**.
5. Use a segunda seção para configurar sprints.
   Para obter detalhes, consulte Configurar sprints para teste de invasão.
6. Use a terceira seção para configurar os tipos de avaliação.
   Para obter detalhes, consulte Configure tipos de avaliação para testes de invasão.

Configurar sprints para teste de invasão

Configure a duração e a capacidade do sprint para a equipe de hacking ético para que eles possam gerenciar a capacidade de sprint para avaliações de teste de invasão.

Antes de Iniciar

Função necessária: Hacking ético

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. Selecione **Configurar** Opção para Configurar sprints.
3. No formulário, preencha os campos.

Formulário Configuração do Sprint

Campo	Descrição
Duração do sprint (dias)	Número de dias em um sprint.
Data de início	Data de início da duração do sprint.
Número de sprints	Número de sprints que podem ser gerados, com base nas datas de início e término do intervalo de sprint.
Data de término	Data de término da duração do sprint.
Capacidade de sprint	
Capacidade de sprint (h)	Capacidade de um sprint em horas.

4. Selecione **Gerar sprints** .
   Para exibir os sprints criados, selecione **Exibir sprints** .

Nota: Se os sprints forem gerados e estiverem em andamento, se você selecionar **Gerar sprints** para a mesma duração, o sprint atual é concluído como de costume. Os sprints restantes são recalculados com base na configuração de sprint atualizada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure tipos de avaliação para testes de invasão

Configure o esforço estimado para cada tipo de avaliação de teste de invasão. Isso permite que você gerencie a capacidade de cada sprint, estimando o esforço necessário para cada tipo de avaliação.

Antes de Iniciar

Função necessária: Hacking ético

Por Que e Quando Desempenhar Esta Tarefa

Cada sprint é atribuído a uma solicitação de teste de invasão. Com base no esforço estimado para o tipo de avaliação, as horas são ajustadas para refletir as horas de saldo do sprint.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. A partir da v19.0 de Resposta a vulnerabilidades, selecione **Configurar** Para exibir Tipos de avaliação, Tamanho da aplicação e esforço estimado.
3. **Opcional:** Selecione um registro de tipo de avaliação para atualizar os campos conforme necessário ou criar novos registros.

   (Optional) Os valores de tamanho da aplicação fornecem mais opções para ajudar a estimar o tempo e o esforço de teste com mais precisão. Você pode editar as horas desses registros ou selecionar **Novo** para criar suas próprias combinações.

   Você pode modificar o tipo de avaliação e o tamanho da aplicação em valores nos registros de solicitação de teste de invasão existentes para que possa programar testes para corresponder à capacidade de sprint. Por exemplo, se você preencher uma solicitação de teste, poderá não ver o número de sprints configurados, porque alguns sprints já foram usados para testes. As horas de esforço estimadas de um sprint corresponderem à combinação necessária para o tipo e o tamanho de um teste, elas não estarão disponíveis para novas solicitações.

   Você pode ver os sprints atribuídos a solicitações de teste em registros na lista de sprints de teste de invasão em **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão** > **Configurar sprints**. Consulte Configurar sprints para teste de invasão para obter mais informações sobre como configurar sprints.

   Os valores básicos para Tipo de avaliação, Tamanho da aplicação e esforço estimado são:

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Tamanho da aplicação	Esforço estimado (h)
Teste focado	Pequeno	20
Teste focado	Médio	30
Teste focado	Grande	40
Teste focado	Padrão	40
Teste novamente	Pequeno	10
Teste novamente	Médio	15
Teste novamente	Grande	20

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de avaliação	Tamanho da aplicação	Esforço estimado (h)
Teste novamente	Padrão	20
Teste de invasão completo	Pequeno	60
Teste de invasão completo	Médio	70
Teste de invasão completo	Grande	80
Teste de invasão completo	Padrão	80

4. Selecione Atualizar para salvar suas mudanças ou enviar para um novo registro.
5. Antes da v19.0, selecione **Configurar** Opção para Configurar tipos de avaliação.
6. Atualize os valores dos tipos de avaliação conforme necessário.
   Os valores base são:

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Esforço estimado (h)
Teste focado	40
Teste novamente	20
Teste de invasão completo	80

7. Salve as mudanças.

Integração do Resposta a vulnerabilidades de aplicações a outras aplicações

Resposta a vulnerabilidades suporte para integrações de terceiros.

Integrações de terceiros

As integrações de vulnerabilidades da aplicação ajudam a enriquecer os dados de vulnerabilidade da aplicação em sua instância recuperando dados de sistemas e fornecedores externos. Consulte os tópicos de visão geral a seguir para obter mais informações sobre integrações compatíveis:

- Integrações de vulnerabilidade do Fortify
- Integrações de vulnerabilidade de aplicação do GitHub
- Integração de vulnerabilidade do Invicti
- Integração de Resposta a vulnerabilidades com Veracode
- Integração de Resposta a vulnerabilidades com Black Duck
- Ingestão manual de vulnerabilidades para Resposta a vulnerabilidades da aplicação
- Integração do Atlassian Jira

Importante: No Espaço do gerenciador de vulnerabilidades, você pode criar um problema ágil manualmente usando ação de lista e. ação de formulário Rastrear a correção de AVITs e RTS.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Integrações de várias origens não são compatíveis com Resposta a vulnerabilidades de aplicações. Integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável à aplicação (AVI) nas integrações.

A tabela a seguir fornece uma lista de Resposta a vulnerabilidades de aplicações integrações criadas por ServiceNow® e parceiros para importar vulnerabilidades e criar itens vulneráveis.

Vulnerability Response - Integrações de infraestrutura

Fornecedor	Produto do fornecedor	Resumo da integração	Link da loja	Principais recursos	Criado por
Veracode	Análise dinâmica Veracode	Teste de importação, políticas e resultados Importar descobertas DO DAST Importar descobertas do SAST Importar descobertas do SCA			ServiceNow®
A Qualys FOI					ServiceNow®
					ServiceNow®
					Parceiro
					ServiceNow®
					ServiceNow®
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro
					Parceiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response - Integrações de infraestrutura

Fornecedor	Produto do fornecedor	Resumo da integração	Link da loja	Principais recursos	Criado por
					Parceiro
					Parceiro
					Parceiro

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações. Para obter mais informações, consulte Resposta a vulnerabilidades aplicações e. CSDM tabelas.

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Integrações de vulnerabilidades para Resposta a vulnerabilidades de aplicações são configurados para serem executados em uma base programada. No entanto, você pode executá-los manualmente quando necessário.

Função necessária: sn_vul.app_read_integrations

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Abra o registro da integração que você deseja executar.
3. Clique em **Executar Agora**.

Integração de Resposta a vulnerabilidades com Black Duck

. Resposta a vulnerabilidades integração com Integração de Resposta a vulnerabilidades com Black Duck Usa os dados importados da ferramenta Análise de composição de software (SCA) Black Duck para ajudar a determinar o impacto e a prioridade das falhas no seu código.

Visão geral da integração

Com Integração de Resposta a vulnerabilidades com Black Duck, Você pode coletar SCA e disponibilizar esses dados para ServiceNow AI Platform. A partir da v22.0.5 de Resposta a vulnerabilidades, Você pode importar os dados de vulnerabilidades do SCA para sua instância para identificar as vulnerabilidades em seus aplicativos de software. Para obter mais informações, consulte Explorando Lista de materiais de software.

Uma API compartilhada ingere os dados do SCA.

Nota: Cada registro de integração tem um usuário de execução configurado. O valor padrão para este usuário é Sistema de VR. Não mude este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que estão listados. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versões disponíveis da integração Black Duck

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Black Duck 1.0.5	Resposta a vulnerabilidades de aplicaçõesnotas da versão

Grupo de usuários e funções

. Integração de Resposta a vulnerabilidades com Black DuckÉ instalado por um usuário com a função de administrador e é configurado por um membro do grupo Gerenciador da App-Sec. Para obter mais informações, consulte o Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

Para obter os status de execução de integração, consulte Exiba Integração de Resposta a vulnerabilidades com Black Duck status da execução da importação

Para exibir dados nas vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparar tarefas de pré-integração para Integração de Resposta a vulnerabilidades com Black Duck

Planeje e execute as tarefas de pré-integração do Integração de Resposta a vulnerabilidades com Black Duck para que sua integração seja bem-sucedida. . Integração de Resposta a vulnerabilidades com Black Duck Presume que você esteja familiarizado com a aplicação Black Duck Software Composition Analysis (SCA) e as APIs.

Antes de Iniciar

Antes de instalar e configurar o. Integração de Resposta a vulnerabilidades com Black Duck, Você deve executar e instalar a integração Common Weakness Enumeration (CWE), que também é usada por Resposta a vulnerabilidades de aplicações. A integração do CWE é instalada com Resposta a vulnerabilidades por padrão.

Nota: Embora os dados do banco de dados de vulnerabilidades do NIST (NVD) não sejam necessários para instalar a Integração de vulnerabilidades da aplicação Black Duck, seria útil tê-los. Para obter informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Cada registro de integração tem um usuário de execução configurado. O valor padrão para este usuário é VR.System. Não mude este valor.

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância pelo número de itens vulneráveis à aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

. Integração de Resposta a vulnerabilidades com Black Duck Requer uma URL de API e um token de API.

Procedimento

Crie o token de API e as credenciais de chave.

a. Faça login na plataforma Black Duck.

b. Vá para o menu Conta de usuário e selecione **Credenciais de API** .

c. Selecione **Gerar credenciais de API** .

d. Registre suas credenciais para uso posterior.

Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Black Duck

Antes de executar a integração em sua instância, você deve concluir as etapas de instalação e configuração para que a ferramenta Análise de composição de software Black Duck (SCA) se integre corretamente ao Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Conclua a seguinte check-list de configuração antes da instalação. Você deve executar essas tarefas de configuração para que a ferramenta Análise de composição de software Black Duck (SCA) se integre corretamente com Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o usuário com a função de administrador instalará a aplicação e atribuirá usuários ao grupo Gerenciador da App-Sec. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Esta ferramenta SCA está disponível como uma assinatura separada.

Procedimento

1. Faça login na instância em que você deseja instalar Integração de Resposta a vulnerabilidades com Black Duck ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, Pesquise Integração de resposta a vulnerabilidades com a aplicação Black Duck.
4. Selecione o bloco Aplicação.
   Os detalhes sobre a aplicação que você está instalando são exibidos.

   Nota: Considere a leitura das seções Outros requisitos e dependências, conforme aplicável.

5. Selecione **App de solicitação** e insira seu Now Support credenciais de login.
6. Selecione **Obter** .
7. Insira o nome da instância e o motivo da instância e selecione **Validar instância** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione **Solicitar**.
   Você receberá um e-mail com as instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e selecione **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o. Integração de Resposta a vulnerabilidades com Black Duck para o seu ambiente. Veja Configure o Integração de Resposta a vulnerabilidades com Black Duck

Configure o Integração de Resposta a vulnerabilidades com Black Duck

Antes de executar o. Integração de Resposta a vulnerabilidades com Black Duck Em sua instância, você deve concluir as etapas de instalação e configuração para que a ferramenta Análise de composição de software (SCA) Black Duck se integre corretamente ao Resposta a vulnerabilidades de aplicações aplicação.

Antes de Iniciar

Função necessária: Grupo de usuários do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

. Integração de Resposta a vulnerabilidades com Black Duck está disponível como uma assinatura separada.

Procedimento

1. Navegar até **Tudo** > **Integração da vulnerabilidade de Blackduck** > **Configuração**.
2. Selecione o tipo de autenticação básica.
   A autenticação básica requer um MID Server para instâncias que estão no local. Você pode gerar o token de API necessário para autenticação básica da sua conta Black Duck.
3. No formulário, preencha os campos.
   Autenticação básica

Campo	Descrição
URL da API	URL da API Black Duck para instâncias corporativas ou no local. A instância no local é o URL do endpoint Black Duck.
Token de API	Token gerado a partir do console Black Duck.
MID Server	MID Server Necessário para instâncias que estão no local para autenticação básica.
Incluir SCA	Vulnerabilidades de verificações de Análise de composição de software (SCA) incluídas por padrão. As verificações do SCA identificam as vulnerabilidades em componentes de código-fonte aberto.
Selecione a opção para gerenciar falsos positivos na ServiceNow	ServiceNow Opção para Gerenciar falsos positivos. Deixe esta opção ativada se quiser fazer a triagem dos itens vulneráveis da aplicação (Avis) importados com **Origem** estados marcados como **Falso-positivo** ou **Possível falso-positivo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Avis com estes **Origem** estados que normalmente são mapeados para um **Encerrado** o estado em sua instância está mapeado para **Aberto** . Você pode solicitar um **Falso-positivo** Do registro AVI. ○ Desative uma ou ambas as opções se quiser preservar o. **Origem** estados que foram importados do scanner. ○ . **Exceção de solicitação** e. **Falso-positivo** As ações não estão visíveis no Avis.
Instância de Integração	Instância que você está usando para importar os dados.

4. Selecione **Credenciais Salvar e testar** .
5. Execute o. **Integração da lista de projetos Black Duck** antes de executar outras integrações.
   As outras integrações do Black Duck, como a integração da lista de aplicações Black Duck e a integração do item vulnerável da aplicação Black Duck, dependem dos dados atuais do projeto e da aplicação que você importou da integração da lista de projetos.

Exiba Integração de Resposta a vulnerabilidades com Black Duck status da execução da importação

Verifique o sucesso de suas execuções de integração, localize quaisquer problemas e confirme suas decisões de correção exibindo a lista relacionada Execuções de integração de vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Integração da vulnerabilidade de Blackduck** > **Integrações**.
2. Selecione uma integração.
3. Selecione a lista relacionada Execuções de integração de vulnerabilidades.
4. Verifique se todas as importações foram bem-sucedidas.
   Solução de problemas:

   As causas mais comuns para uma execução com falha incluem:
   - Interrupção de rede.
   - Um problema na transferência de dados que resulta em dados corrompidos durante uma transformação.

   Se você encontrar qualquer uma dessas condições, selecione **Executar agora** e execute novamente a integração.
5. Navegue até a lista de integrações e selecione o registro Integração Black Duck.
6. Selecione a lista relacionada Execuções de integração de vulnerabilidades e abra um registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transformação de dados para Integração de Resposta a vulnerabilidades com Black Duck

Depois de identificar os dados que você deseja importar, os dados serão recuperados do Integração de Resposta a vulnerabilidades com Black Duck processado por meio de um conjunto de fontes de dados e transformado em sua instância.

Integração de Resposta a vulnerabilidades com Black Duck

Os dados da API são carregados primeiro na tabela Importação de item AppVul Black Duck [sn_vul_blackduck_appvul_item_import], e a transformação de item AppVul Black Duck é usada para transformar as informações importadas.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de item AppVul do Pato Preto** . A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de item AppVul do Black Duck

Campo de origem	Campo de destino	Descrição
app_id	source_app_id	ID da aplicação.
issueid	source_avit_id	ID DO AVIT.
app_name	app_name	Nome da aplicação.
versão	app_version	Versão da aplicação.
build_id	source_scan_id	ID de compilação da aplicação.
account_id	account_id	ID da conta.
sandbox_id	sandbox_id	ID da área restrita.
last_update_time	last_scan_date	Hora da última atualização.
app_name e last_scan_date	scan_summary_name	Resumo da verificação.
life_cycle_stage	source_sdlc_status	Status do SDLC de origem.
nível	source_severity	Gravidade da origem.
category_name	categoria	Categoria.
source_severity	source_severity	Gravidade da origem.
Category_id, " cwe-" e cweId	source_entry_id	ID de entrada de origem.
source_vulnerability_summary	source_vulnerability_summary	Resumo da vulnerabilidade de origem.
source_recommendation	source_recommendation	Recomendação de origem.
descrição	descrição	Descrição da origem.
descrição	source_vulnerability_explanation	Explicação da vulnerabilidade de origem.
mitition_status_desc	source_mitition_status	Status de mitigação de origem.
remediation_status	source_remediation_status	Status de correção de origem.
linha	line_number	Linha na qual a falha foi encontrada.
módulo	application_module	Módulo da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de item AppVul do Black Duck

Campo de origem	Campo de destino	Descrição
sourcefile	source_notes	Anotações de origem.
affects_policy_compliance	accomes_with_policy	Os valores podem ser Sim ou Não com base nas informações de origem serem verdadeiras ou falsas.
Sourcefilepath e sourcefile	local	Mapeamento de localização de uma falha estática.
URL	local	Mapeamento de local para uma falha dinâmica.
Escopo, tipo, exploitLevel	source_additional_info	Campo Valor do nome preenchido com os valores da origem de falhas estáticas.

A tabela a seguir lista os scripts de transformação que são executados durante o processo de transformação.

Tempo e finalidade do script do mapa de transformação Black Duck

Script de mapa de transformação de Black Duck

Quando o script é executado	Finalidade
EmStart (quando um conjunto de importação cria transformação).	Script usado para processar o registro e atualiza o número de entidades criadas, atualizadas ou inalteradas e as que são importadas como parte desta integração. Este script é para uso interno e não deve ser modificado ou excluído.
Antes (antes que um conjunto de importação conclua a transformação)	Script usado para definir o comportamento de registros inválidos e que devem ser ignorados. Usado também para definir o objeto global para processamento de registro. Este script é para uso interno e não deve ser modificado ou excluído.

Mapeamento do estado de integração do Black Duck

A tabela a seguir mostra os estados de origem da Integração de vulnerabilidades do Black Duck e seus estados de destino em sua instância.

estados de origem do Pato Preto e seus correspondentes ServiceNow AI Platform estados

estados de origem Black Duck	Descrição dos estados de origem	Estado de destino no ServiceNow AI Platform
Novo(a)	A vulnerabilidade afeta esta versão do componente.	Aberto
Precisa de revisão	Não será possível determinar se uma vulnerabilidade afetar esta versão do componente.	Aberto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados de origem do Pato Preto e seus correspondentes ServiceNow AI Platform estados

estados de origem Black Duck	Descrição dos estados de origem	Estado de destino no ServiceNow AI Platform
Correção necessária	A correção é necessária para esta versão.	Aberto
Correção concluída	A correção desta vulnerabilidade está concluída.	Encerrado
Mitigado	A vulnerabilidade foi mitigada.	Encerrado
Corrigido	A vulnerabilidade foi corrigida.	Encerrado
Ignorado	A vulnerabilidade foi ignorada.	Encerrado

Importe as informações do projeto da instância de integração Black Duck

Importe as informações do projeto da instância de integração Black Duck para garantir que as integrações de vulnerabilidade sejam executadas sequencialmente. Uma integração bem-sucedida ajuda a identificar e ingerir os itens vulneráveis à aplicação (AVIS).

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Você pode importar todas as informações do projeto do Integração de Resposta a vulnerabilidades com Black Duck Na tabela Projetos Black Duck [sn_vul_blackduck_project]. Todos os atributos necessários, por exemplo, GUID do projeto, que são necessários para consultar diferentes versões do projeto, são capturados na tabela Projetos Black Duck [sn_vul_blackduck_project].

Procedimento

1. Navegar até **Tudo** > **Integração da vulnerabilidade de Blackduck** > **Integrações**.
2. Selecione uma integração.
   Por exemplo, você pode selecionar **Integração da lista de projetos Black Duck.**
3. Selecione **Executar agora**.

   Nota: Cada um Integração de Resposta a vulnerabilidades com Black Duck o destina-se a fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer ServiceNow E experiência em resposta a vulnerabilidades da aplicação.

   Após a conclusão da importação, você poderá ver os detalhes do projeto na tabela Projetos Black Duck [sn_vul_blackduck_project].
4. Para obter os status de execução de integração, consulte Exiba Integração de Resposta a vulnerabilidades com Black Duck status da execução da importação.
5. **Opcional:** Se você quiser modificar outros parâmetros de integração, navegue até a instância de integração.

Importação Integração de Resposta a vulnerabilidades com Black Duck Versões do projeto para a tabela Aplicações descobertas

Importe a integração do Vulnerability Response com as versões do projeto Black Duck para a tabela Aplicações descobertas [sn_vul_release] para que as integrações de vulnerabilidade do Black Duck sejam executadas sequencialmente. Uma integração bem-sucedida ajuda a identificar e ingerir os itens vulneráveis à aplicação (AVIS).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa
Você pode adicionar e exibir todas as diferentes versões dos projetos (consulte os detalhes na tabela Projetos do Black Duck) que foram importadas do Integração de Resposta a vulnerabilidades com Black Duck Na tabela Aplicações descobertas [sn_vul_release].

Procedimento

1. Navegar até **Tudo** > **Integração da vulnerabilidade de Blackduck** > **Integrações** .
2. Selecione uma integração.
   Por exemplo, você pode selecionar **Integração da lista de aplicações Black Duck** .
3. Selecione **Executar agora**.

   Nota: Cada versão de projeto das integrações tem o objetivo de fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer experiência da ServiceNow e em resposta a vulnerabilidades de aplicações.

   Após a conclusão da importação, você poderá ver as diferentes versões de um projeto na tabela Aplicações descobertas [sn_vul_release]. Se você estiver usando Regras de pesquisa de IC, essas aplicações descobertas serão vinculadas à tabela de item de configuração [cmdb_ci].
4. Veja o status das execuções de integração.
   Para obter mais informações, consulte Exiba Integração de Resposta a vulnerabilidades com Black Duck status da execução da importação.

Importe os itens vulneráveis da aplicação do Integração de Resposta a vulnerabilidades com Black Duck

Importe os itens vulneráveis à aplicação (Avis) da integração do Vulnerability Response com o Black Duck para que a integração seja executada sequencialmente. Uma integração bem-sucedida ajuda você a identificar e ingerir os Avis.

Antes de Iniciar
Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa
Você pode exibir os resultados da verificação no Integração de Resposta a vulnerabilidades com Black Duck Insira Avis em sua instância e aprimore seus dados de vulnerabilidade de terceiros. Por padrão, se o registro do scanner estiver no estado Encerrado, os Avis não serão criados. Você pode controlar os Avis existentes usando a propriedade sn_vul_create_closed.

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidades do Black Duck** > **Integrações**.
2. Selecione uma integração.
   Por exemplo, você pode selecionar **Integração de item vulnerável da aplicação Black Duck** .
3. Selecione **Executar agora**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . Integração de Resposta a vulnerabilidades com Black Duck o destina-se a fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer ServiceNow e. Resposta a vulnerabilidades de aplicações experiência.

Depois de importar todas as vulnerabilidades do SCA do Integração de Resposta a vulnerabilidades com Black Duck, Você pode exibir os Avis e os dados de vulnerabilidade de terceiros.

Defina os horários de importação para Integração de Resposta a vulnerabilidades com Black Duck

Defina a hora de início do Integração de Resposta a vulnerabilidades com Black Duck importações. Você pode definir as integrações com antecedência para obter melhor desempenho e execuções de importação mais rápidas.

Antes de Iniciar
Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa
Após a importação inicial, as integrações de vulnerabilidade do Black Duck fazem uma importação completa sempre que são executadas.

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidades do Black Duck** > **Integrações**.
2. Selecione uma integração.
3. Definir o novo **Hora de início** .
   A hora é calculada como horas no horário local. O tempo padrão para as importações de integração da lista de aplicações Black Duck é 00:00:00. As outras integrações são **Sob demanda** E são encadeados, o que significa que eles seguem uma sequência para serem executados após a integração da lista de aplicações Black Duck. Alterando o. **Hora de início** avançado ServiceNow e. Gestão de vulnerabilidades de aplicações experiência.
4. Selecione **Atualizar**.
   A nova hora é usada para a próxima importação programada.

Incluir itens vulneráveis à aplicação Black Duck fechada

Incluir itens vulneráveis à aplicação (Avis) encerrados durante as importações de integração de item vulnerável Black Duck porque, por padrão, eles não são criados durante as importações da integração. Se você quiser criá-los, altere a propriedade do sistema.

Antes de Iniciar
Certifique-se de que Integração de Resposta a vulnerabilidades com Black Duck está instalado e em execução.

Função necessária: administrador

Procedimento

1. No filtro de navegação, insira `sys_properties.list`.
2. Em **Nome** para a lista, insira `sn_vul.create_closed` .
3. Clique duas vezes em **Valor** e defina-o como **Verdadeiro**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione o ícone de marca de seleção verde .
   Os registros no estado Encerrado na próxima importação do Black Duck são criados como AVIS em Resposta a vulnerabilidades de aplicações.

Integrações de vulnerabilidade do Fortify

. Integrações de vulnerabilidade do Fortify usa dados importados do Fortify produto para ajudar você a determinar o impacto e a prioridade de falhas em seu código.

Integrações de vulnerabilidade do Fortify

. Fortify o produto coleta dados do scanner e disponibiliza esses dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao ServiceNow® Resposta a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente. Quando todas as integrações são ativadas, elas são encadeadas para serem executadas em sequência. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas da versão
Integração do Vulnerability Response com Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Resposta a vulnerabilidades de aplicaçõesnotas da versão Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações de vulnerabilidade do Fortify

Para exibir o. Integrações de vulnerabilidade do Fortify, navegue até **Integrações de vulnerabilidade do Fortify** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base. Essas integrações não estão todas ativas por padrão.

Todos os dias, os trabalhos agendados são encadeados para executar as integrações automaticamente em ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fortify Integrações de vulnerabilidades

Integração	Descrição
Fortify Integração da lista de aplicações sob demanda	Recupera Fortify dados do scanner de aplicações (vulnerabilidades, metadados) e enriquece seus dados de aplicações de terceiros. Esta integração está definida para ser executada diariamente às 00:00:00. Por padrão, ele está ativo.
Fortify Integração do resumo da verificação sob demanda	Recupera registros de verificação de Fortify. Esta integração está encadeada para ser executada após Fortify Integração da lista de aplicações sob demanda quando ativado. Por padrão, ele está inativo.
Fortify Integração de item vulnerável da aplicação sob demanda	Recupera os resultados da verificação de Fortify Insere AVITs e enriquece seus dados de vulnerabilidade de terceiros. Se o registro do scanner estiver em **Encerrado** AVITs não foram criados. AVITs existentes ainda estão atualizados. A partir da v2.3, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de Item vulnerável da aplicação. Esta integração está encadeada para ser executada após Fortify Integração do resumo da verificação sob demanda quando ativado. Por padrão, ele está inativo.

Para obter os status de execução de integração, consulte, Exiba Integrações de vulnerabilidade do Fortify status da execução da importação.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para Integrações de vulnerabilidade do Fortify

Bem-sucedida Integrações de vulnerabilidade do Fortify requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Integrações de vulnerabilidade do Fortify presume que você esteja familiarizado com Fortify Produto e API.

Antes de Iniciar

A integração Common Weakness Enumeration (CWE) também é usada por Resposta a vulnerabilidades de aplicações e devem estar em execução antes de instalar e configurar o. Integrações de vulnerabilidade do Fortify.

Nota: Os dados do NIST Vulnerability Database (NVD) não são necessários para instalar o. Integrações de vulnerabilidade do Fortify no entanto, eles fornecem enriquecimento e seria útil ter.

Para obter informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Função necessária: Gerenciador de apps-sec

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça qualquer mudança de configuração necessária com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis à aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

. Integrações de vulnerabilidade do Fortify Requer uma chave de API, segredo de API e URL de raiz da API, disponíveis no Fortify Conta sob demanda.

Procedimento

Para criar uma chave secreta de API:

a. Faça login no seu Fortify Portal sob demanda.

b. Navegar até **Tudo** > **Administração** > **Configuração** > **API**.

c. Adicione a ServiceNow como uma aplicação.

d. Clique em **Novo segredo** Para gerar um segredo de API.

e. Registre seu segredo de API para uso posterior.

Instale o. ServiceNow® Integração de Resposta a vulnerabilidades com Fortify

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Fortify o produto se integra corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo Gerenciador da App-Sec. Para obter informações sobre funções de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	grupo, consulte, Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: Gerenciador de apps-sec

Procedimento

1. Faça login na instância em que você deseja instalar Integrações de vulnerabilidade do Fortify ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, Pesquise Integração de resposta a vulnerabilidades com Fortify aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o. Integrações de vulnerabilidade do Fortify para o seu ambiente. Consulte Configure o Integrações de vulnerabilidade do Fortify.

Configure o Integrações de vulnerabilidade do Fortify

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Fortify o produto se integra corretamente ao Resposta a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Funções necessárias: Gerenciador de apps-sec

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se o Resposta a vulnerabilidades Integração com Fortify a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Fortify.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo Gerenciador de apps-sec. • O Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.
Para Integrações de vulnerabilidade do Fortify. tenha seu **ID da API** e. **Chave de API** pronto.	Contato Fortify para obter o. **ID da API** e. **Chave de API** .

Tradução automática

Procedimento

1. Faça login na instância em que você deseja instalar Fortify integrações de vulnerabilidade da aplicação em.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Resposta a vulnerabilidades integração com Fortify aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.
11. Quando a instalação for concluída, navegue até **Integrações de vulnerabilidade do Fortify** > **Configuração do FoD**.
12. No formulário, preencha os campos.

Formulário de configuração do FORTIFY sob demanda

Campo	Descrição
URL raiz da API	URL da instância do FORTIFY do usuário.
Chave de API	Identificador exclusivo enviado para Fortify API.
Segredo da API	Segredo do cliente fornecido por Fortify.
Incluir DAST	Opção para incluir vulnerabilidades de verificações DAST. As verificações DAST identificam vulnerabilidades no comportamento da aplicação geral.
Incluir SAST	Opção para incluir vulnerabilidades de verificações SAST. As verificações SAST identificam vulnerabilidades no código.
Triagem de exceções e falsos positivos na ServiceNow (a partir da v20.0 da Resposta a vulnerabilidades)	Selecione as opções para gerenciar a gestão de exceções e o Falso positivo para AVIS com ServiceNow fluxos de trabalho automaticamente após a importação. Essas opções são ativadas por padrão. Para obter um exemplo de caso de uso, consulte Gerenciar mapeamento de estado para adiamentos e falsos positivos em Resposta a vulnerabilidades de aplicações. **Gerencie exceções em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de Avis importados marcados para **Adiado** estado. Avis com **Origem** estados que normalmente são mapeados para um **Adiado** em vez disso, o estado em sua instância é mapeado para **Aberto** . Você **Solicite uma exceção** Do registro AVI. **Gerencie falsos positivos em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de Avis importados com **Origem** estados marcados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	como **Falso-positivo** ou **Possível falso-positivo** . Avis com estes **Origem** estados que normalmente são mapeados para um **Encerrado** o estado em sua instância está mapeado para **Aberto** . Você solicita um **Falso-positivo** Do registro AVI. ○ Desative uma ou ambas as caixas de seleção se quiser preservar o. **Origem** estados importados do scanner. ○ Esses AVIS são mapeados para os estados de destino e os estados Motivo de destino conforme são importados, mas não são triados pelos fluxos de trabalho de exceção e falso-positivo. . **Exceção de solicitação** e. **Falso-positivo** As ações não estão visíveis no Avis.
Triagem na ServiceNow (anterior à v20.0 do Vulnerability Response)	Gerencie a triagem de vulnerabilidades da aplicação em ServiceNow instância: ○ Marque a caixa de seleção para fazer a triagem dos Avis em ServiceNow. Se esta opção for selecionada, os Avis serão importados no estado Aberto. Em seguida, você pode solicitar uma exceção ou marcar o AVI como falso positivo. ○ Para manter o estado de origem, ou seja, o estado importado do scanner, certifique-se de que a caixa de seleção não esteja marcada. **Nota:** . **Marcar como falso positivo** e. **Exceção de solicitação** As opções estão disponíveis somente para Avis que estão sendo triados em ServiceNow.

13. Selecione **Salvar e testar credenciais** .

O que Fazer Depois

Se o seu ambiente exigir importações separadas por domínio, consulte Crie importações separadas por domínio para uma integração.

Na instalação inicial, consulte Como configurar o Resposta a vulnerabilidades de aplicações para obter mais instruções.

Após a instalação inicial, para obter modificações, consulte Integrações de vulnerabilidade do Fortify modificação e atividades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exiba Integrações de vulnerabilidade do Fortify status da execução da importação

Use **Execuções de Integração de vulnerabilidades** lista relacionada para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o. Fortify status da execução da importação:

- . Resposta a vulnerabilidades e. Integrações de vulnerabilidade do Fortify as aplicações devem ser instaladas e configuradas.
- . Integrações de vulnerabilidade do Fortify as importações devem ser programadas e em execução.

Função necessária: Gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Selecione uma integração.
3. Clique em **Execuções de Integração de vulnerabilidades** lista relacionada.
4. Verifique se todas as importações foram bem-sucedidas.
5. A partir da v2.3, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as Integrações de itens vulneráveis da aplicação.

Integrações de vulnerabilidade do Fortify modificação e atividades

Configure modificações opcionais especificamente para Integrações de vulnerabilidade do Fortify.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Alterando outro Integrações de vulnerabilidade do Fortify as configurações, diferentes das listadas aqui, exigem avançado ServiceNow e. Resposta a vulnerabilidades de aplicações e está além do escopo da documentação do produto.

Execute um manual Fortify importação de vulnerabilidades da aplicação

Se sua importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho agendado diariamente.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração, por exemplo, Fortify Integração da lista de aplicações.
3. Selecione **Executar agora**.

Nota: Para uma recuperação de dados completa, execute as integrações de vulnerabilidade da aplicação FORTIFY em sequência.

Importar dados usando Integrações de vulnerabilidade do Fortify

Importe dados do scanner FORTIFY para mapear itens vulneráveis à aplicação (Avis), enriquecendo os dados em sua instância.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, Fortify as integrações de vulnerabilidades fazem uma importação delta sempre que são executadas, recuperando os dados mais recentes. Consulte Execute um manual Fortify importação de vulnerabilidades da aplicação para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Tudo** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da execução de integração.
Ativo	Opção para ativar uma integração.
Executar	Frequência da execução da integração.
Hora	
Aplicação	Aplicação que contém este registro.
Integração de origem	Integração de origem para esta integração.
Instância de origem	Instância de origem desta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Próxima integração	Integração Next-in-sequence, a ser executada após a execução da integração atual.
Hora de início	Data e hora de início da última execução de integração bem-sucedida. A hora é calculada como horas no horário local. O tempo padrão para a execução inicial é 00:00:00.
Detalhes de Integração	
Script de integração	Inclusão de script que estende o. `VulnerabilityIntegrationBase`a ser executado quando a integração for executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Script que define como construir a inclusão de script selecionada para o script de integração.
Estratégia do processador de relatórios	Estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração é executada.

4. Selecione **Executar agora** para executar a integração.

Incluir itens vulneráveis da aplicação FORTIFY sob demanda encerrados

Por padrão, **Encerrado** AVITs (Application Vulnerable Items, itens vulneráveis à aplicação) não são criados durante Fortify Importações de integração de item vulnerável. Se você quiser criá-los, altere uma propriedade do sistema.

Antes de Iniciar

. Integrações de vulnerabilidade do Fortify deve estar instalado e em execução.

Função necessária: Gerenciador de apps-sec

Procedimento

1. Na navegação à esquerda **Navegador de filtros** caixa de texto, digite `sys_properties.list` .
2. Em **Nome** caixa de pesquisa da lista, insira `sn_vul.create_closed` .
3. Clique duas vezes em **Valor** e definido como **Verdadeiro**
4. Clique no ícone de marca de seleção verde para salvar.
   Registros no **Encerrado** estado no próximo Fortify As importações são criadas como AVITs em Resposta a vulnerabilidades de aplicações.

Integrações de vulnerabilidade de aplicação do GitHub

. Integrações de vulnerabilidade de aplicação do GitHub Importa dados de teste de segurança de aplicações estáticas (SAST) e Análise de composição de software (SCA) para ajudar você a exibir alertas de vulnerabilidade nos repositórios do seu GitHub ambiente.

Integrações de vulnerabilidade de aplicação do GitHub

. Integrações de vulnerabilidade de aplicação do GitHub coleta dados do scanner e disponibiliza esses dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao ServiceNow® Resposta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades para mapear vulnerabilidades de terceiros e. GitHub alertas em sua instância.

. GitHub o ambiente oferece suporte a várias organizações. Essas organizações, tanto no local quanto no Enterprise, podem conter vários departamentos, como Engenharia, Qualidade, Documentação e assim por diante. Cada organização, por sua vez, pode oferecer suporte a vários repositórios. Depois de importar os dados da aplicação com GitHub Integração de repositórios, você pode importar dados de vulnerabilidade e alertas desses repositórios. Os dados importados são processados como uma aplicação no Resposta a vulnerabilidades de aplicações aplicação. Quando os scanners detectam vulnerabilidades e geram alertas para os repositórios, as vulnerabilidades são criadas em Resposta a vulnerabilidades de aplicações.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Versões disponíveis

Versão de lançamento	Notas de versão
Integrações de vulnerabilidade de aplicação do GitHub v1.2, v1.1, 1,0	Resposta a vulnerabilidades de aplicaçõesnotas da versão Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações do GitHub

Integração	Descrição
GitHub Integração de repositórios	A partir da v1.1, importe todos os dados da aplicação para seu GitHub Contas no local e na nuvem (Enterprise). A integração importa aplicações dos repositórios que você configurou para uma organização (no local) ou do seu ambiente empresarial (nuvem). Execute esta integração antes de executar a outra GitHub Integrações, porque dependem dos dados da aplicação atual importados da Integração de repositórios.
GitHub Integração do CodeScan	Recupera alertas de vulnerabilidade de verificação de código de GitHub repositórios para vulnerabilidades de segurança e erros de codificação. Os dados importados são mapeados para os resultados do SAST em sua instância.
GitHub Integração dependente	Recupera alertas dependentes para dependências com vulnerabilidades conhecidas de repositórios. Os dados importados são mapeados para os resultados do SCA em sua instância.
GitHub Verificação secreta	Recupera segredos do código da sua organização junto com os resultados do teste de segurança da aplicação. Os dados são mapeados para os resultados do SCA em sua instância.
GitHub Local de verificação secreta	Recupera o local e os números de linha dos segredos verificados no código da sua organização para ajudar os desenvolvedores a corrigir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Carregando SBOM arquivos para ServiceNow AI Platform® do seu GitHub repositórios

Determine se SBOM Os arquivos gerados em seus pipelines de IC/CD (integração contínua e entrega/implantação contínua) foram enfileirados com sucesso em seu ServiceNow AI Platform® instância.

- Proteja seus ambientes contra componentes potencialmente prejudiciais durante os ciclos de desenvolvimento de software com GitHub Ações que você inicia a partir de GitHub ambiente.
- Obtenha qualquer necessário GitHub Ações para SBOM Carregue no GitHub Marketplace.

. SBOM as aplicações são necessárias para carregar SBOM arquivos. Para obter mais informações, consulte Explorando Lista de materiais de software.

Exibindo dados importados

Dados da aplicação importados do GitHub A integração de repositórios é exibida na tabela Aplicações descobertas [sn_vul_app_release]. Execute esta integração primeiro.

A Integração de repositórios importa marcadores e tópicos que você configurou para um repositório no GitHub Conta no menu Configurações. Todas as propriedades personalizadas estão localizadas no menu em seu repositório. Os valores definidos para as propriedades são importados como pares de chave-valor. Para obter mais informações sobre onde exibir essas informações em sua instância, consulte Exiba Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e dados importados do repositório.

Dados importados (descobertas) do GitHub A Integração dependente é exibida nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary].
- Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item].
- Pacotes [sn_vul_app_package].

Os dados importados da integração do GitHub CodeScan são exibidos nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary].
- Entradas de vulnerabilidade da aplicação [sn_vul_app_vul_entry].
- Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item].

Preparando para Integrações de vulnerabilidade de aplicação do GitHub

Prepare-se para a integração executando essas tarefas. . Integrações de vulnerabilidade de aplicação do GitHub Presume que você esteja familiarizado com o produto e a API do GitHub.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Funções necessárias:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- administrador para baixar, instalar e ativar aplicações e atribuir funções.
- Administrador do GitHub para obter credenciais e gerar tokens no console do GitHub.
- para configurar conexões e registros de alias em sua instância.

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se o Integrações de vulnerabilidade de aplicação do GitHub está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instale o. ServiceNow Integrações de vulnerabilidade de aplicação do GitHub.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários do Gerenciador de apps-sec. • O Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados. • sn_vul_github_config_integration é herdado pelo grupo de usuários do Gerenciador da App-Sec. Esta função contém as funções connection_admin e oauth_admin.
Obtenha suas credenciais do GitHub e informações de conta.	As informações da conta são necessárias nos registros que você cria para autenticação. Consulte Criando credenciais do OAuth 2,0 para GitHub JWT para Integrações de vulnerabilidade de aplicação do GitHub Para obter mais informações sobre os detalhes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
	de que você precisa e como configurar os registros necessários para autenticação OAuth.
Verifique se você está importando dados de CWE (Common Weakness Enumeration, enumeração de pontos fracos comuns).	A integração Common Weakness Enumeration (CWE) também é usada por Resposta a vulnerabilidades de aplicações E devem estar em execução antes de instalar e configurar a Integração de vulnerabilidades do GitHub. Ele é instalado com Resposta a vulnerabilidades, por padrão. **Nota:** Os dados do NIST Vulnerability Database (NVD) não são necessários para instalar a Integração de vulnerabilidades do GitHub, no entanto, eles fornecem aprimoramento e seriam úteis. Para obter informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Criando credenciais do OAuth 2,0 para GitHub JWT para Integrações de vulnerabilidade de aplicação do GitHub

Execute as etapas a seguir para integrar seu GitHub Aplicativos que usam o token do portador JWT para Integrações de vulnerabilidade de aplicação do GitHub.

Funções necessárias:

- sn_vul.app_sec_manager e admin para registros em seu ServiceNow AI Platform.
- Nenhuma função de instância necessária para tarefas em seu GitHub conta.
- Para obter mais informações sobre o contexto das etapas desta configuração, consulte Protocolo OAuth 2,0 .

Crie e configure o. GitHub aplicação para Integrações de vulnerabilidade de aplicação do GitHub

Criar um personalizado GitHub Aplicativo do seu GitHub Conta para ativar a autenticação OAuth 2,0 com seu Integrações de vulnerabilidade de aplicação do GitHub em sua instância.

Antes de Iniciar

Função necessária: Nenhuma função de instância necessária

Por Que e Quando Desempenhar Esta Tarefa

Conclua estas etapas no seu GitHub conta. Confira Construção GitHub Apps em GitHub Site do desenvolvedor para obter instruções sobre como criar e configurar aplicações personalizadas.

Procedimento

1. Do seu GitHub, crie sua GitHub Navegando até **Configurações do desenvolvedor** > **GitHub Apps**.
2. Em **URL da página inicial** campo, insira `https://<instance-name>.service-now.com` .
3. Em **URL de retorno de chamada de autorização do usuário** campo, insira `https://<instance-name>.service-now.com/oauth_redirect.do` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Em **Identificar e autorizar usuários** desmarque **Tokens de autorização do usuário expirados** campo.
5. Em **Webhook** , selecione **Ativo** campo.
6. Em **URL do webhook** campo, insira `https://instance-name>.service-now.com/` .
7. Deixe os campos restantes em branco (padrão).
8. Em **Permissões do repositório** defina as seguintes configurações.

Verificação de código	Somente leitura
Conteúdos	Somente leitura
Propriedades personalizadas	Somente leitura
Alertas dependentes	Somente leitura
Metadados	Somente leitura

Nota: Se você já estiver usando um aplicativo GitHub e atualizar qualquer uma das permissões, revise e aceite essas permissões para o seu aplicativo GitHub Você pode navegar até seu app e selecionar **Revisar solicitação > Aceitar novas permissões** .

9. Deixe as permissões restantes como `Sem acesso` (padrão).
10. Em **Assinar eventos** , selecione **Regra de proteção de implantação** opção.
11. Clique com o botão direito do mouse no cabeçalho para salvar as mudanças.
12. Instale o recém-criado GitHub Nas contas de sua escolha.
    a. Na página de configurações do GitHub Apps, selecione seu app.
    b. Na barra lateral esquerda, selecione **Instale o app** .
    c. Selecione **Instalar** ao lado da organização ou da conta pessoal que contém o repositório correto.
    d. Instale o app em todos os repositórios ou selecione repositórios.
    Para obter mais informações, consulte Instalando aplicações do GitHub .
13. Após a instalação, selecione as configurações (ícone de engrenagem) da sua aplicação e anote ou anote as seguintes informações.

    Esses detalhes são necessários quando você cria o registro da aplicação em seu ServiceNow AI Platform instância.

    - ID de app
    - ID de cliente
    - Segredo do cliente.
    - Anote o token no URL. Este é o ID do token que você insere no URL do token em sua instância.
14. Role a página para baixo, gere uma nova chave privada e salve-a em sua máquina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gere o certificado JKS para Integrações de vulnerabilidade de aplicação do GitHub

Gere um certificado JKS para a autenticação JWT para Integrações de vulnerabilidade de aplicação do GitHub.

Antes de Iniciar

Anote a senha que você usa para gerar o arquivo .jks (senha do armazenamento de chaves).

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Crie um certificado assinado por CA usando GitHub Chave privada da aplicação:

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. Insira os detalhes necessários.
3. Crie o arquivo PKCS 12 usando GitHub Chave privada da aplicação e certificado assinado por CA:

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. Forneça a senha de exportação.
5. Crie o arquivo JKS:

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. Forneça as senhas do armazenamento de chaves de destino e de origem.

Anexe o. GitHub Java Key Store para sua instância para Integrações de vulnerabilidade de aplicação do GitHub

Ative a autenticação de token de concessão do portador JWT anexando o certificado do GitHub Java KeyStore (JKS) válido à sua instância.

Antes de Iniciar

Um certificado Java KeyStore válido.

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Certificados**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos do formulário da certificação X.509

Campo	Descrição
Nome	Nome para identificar exclusivamente o registro. Por exemplo, Meu certificado de app GitHub para AVR .
Notificar no vencimento	Opção para especificar os usuários a serem notificados quando o certificado expirar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aviso emitido antes do vencimento (em dias)	Número de dias para enviar uma notificação antes que o certificado expire.
Ativo	Opção para habilitar o certificado.
Tipo	Opção para selecionar o tipo de certificado. Selecione **Armazenamento de chaves Java**.
Dias até o vencimento	Número de dias até o certificado expirar.
Senha do armazenamento de chaves	Senha associada ao certificado (dica: A senha do armazenamento de chaves de destino criada anteriormente).
Descrição resumida	Resumo sobre o certificado.

4. Selecione o ícone Anexos e anexe um certificado JKS.
5. Selecione **Validar armazenamentos/certificados** .
   Uma mensagem key_store válida é exibida para arquivos de certificado válidos.

Crie uma chave de assinatura JWT para GitHub Certificado JKS para Integrações de vulnerabilidade de aplicação do GitHub

Crie uma chave de assinatura JSON Web Token (JWT) para atribuir ao seu GitHub Java KeyStore certificado.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **OAuth de Sistema** > **Chaves de JWT**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos do formulário de chaves de JWT

Campo	Descrição
Nome	Nome para identificar exclusivamente a chave de assinatura JWT. Por exemplo, Minha chave JWT da aplicação GitHub para AVR .
Armazenamento de chaves de assinatura	Selecione o certificado JKS válido anexado na tarefa anterior.
ID de chave	Deixe esse campo em branco.
Algoritmo de assinatura	Deixe este valor como RSA 256.
Senha da chave de assinatura	Senha associada à chave de assinatura. Esta é a senha que você usou para gerar o arquivo JKS.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Opção para habilitar a chave.

4. Clique com o botão direito do mouse em qualquer lugar no cabeçalho cinza da página e selecione **Salvar** .

Crie um provedor JWT para seu GitHub chave de assinatura do Integrações de vulnerabilidade de aplicação do GitHub

Adicione um provedor JSON Web Token (JWT) ao seu ServiceNow instância para GitHub.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **OAuth de Sistema** > **Provedores JWT**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos de formulário do Provedor JWT

Campo	Descrição
Nome	Nome para identificar o provedor JWT de forma única. Por exemplo, Provedor JWT da aplicação GitHub para AVR .
Intervalo de Vencimento (s)	Número em segundos para definir a vida útil dos tokens do provedor JWT. Você pode deixar essa configuração no padrão.
Configuração de Assinatura	Selecione a chave JWT que você criou nas etapas anteriores.

4. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.
5. Insira seu GitHub Aplicação **ID da aplicação** para o valor de **iss** Declaração, na lista relacionada Declarações padrão.
   Este é o ID da aplicação do GitHub Em seu GitHub console que você criou nas etapas anteriores.
6. Sair **aud** e. **sub** valores em branco (padrão).
7. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.

Registre-se GitHub Como um provedor OAuth (JWT) para Integrações de vulnerabilidade de aplicação do GitHub

Use as informações geradas durante GitHub Configuração da conta da aplicação a ser registrada GitHub Como um provedor OAuth e permitir que a instância solicite tokens OAuth 2,0.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **OAuth de Sistema** > **Registro de aplicações**.
2. Selecione **Novo**.
   . **Que tipo de aplicação OAuth?** a mensagem é exibida.
3. Selecione **Conecte-se a um provedor OAuth de terceiros** .
4. No formulário, preencha os campos.

Campos do formulário Registro de aplicações

Campo	Descrição
Nome	Nome para identificar exclusivamente o registro. Por exemplo, insira `Meu provedor de aplicações GitHub para AVR` .
ID de cliente	ID do cliente do seu GitHub Aplicação O ID do cliente é do GitHub aplicação em seu GitHub console que você criou nas etapas anteriores. Este ID está disponível em **Sobre** . GitHub Configuração da aplicação em GitHub.
Acessível	Deixe esta configuração em seu valor atual.
Segredo do cliente	Segredo do cliente do seu GitHub Aplicação O segredo do cliente é do GitHub aplicação em seu GitHub console que você criou nas etapas anteriores. Este ID está disponível em **Sobre** . GitHub Configuração da aplicação em GitHub.
Ativo	Opção para habilitar a chave. Deixe selecionado.
URL de Autorização	Este URL é gerado automaticamente.
URL do token	O local do endpoint do token que a instância usa para recuperar e atualizar tokens. Insira o Token do URL em seu GitHub Aplicação Este é o token exibido no URL depois que seu app é instalado em GitHub. Na seção Instalar aplicativo na configuração do aplicativo GitHub em GitHub, selecione a engrenagem. O token é exibido no URL da página da web. ○ Para nuvem: https://api.github.com/app/installations/49374672/access_tokens . ID de instalação: 9374672. ○ No local: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
Script da API OAuth	Opção que permite que você faça referência a uma inclusão de script OAuthUtil corrigida. Selecione **OAuthGitHubJWTHHandler** .
Tipo de concessão padrão	Tipo de concessão associada ao registro da aplicação. Selecione **Portador JWT**.

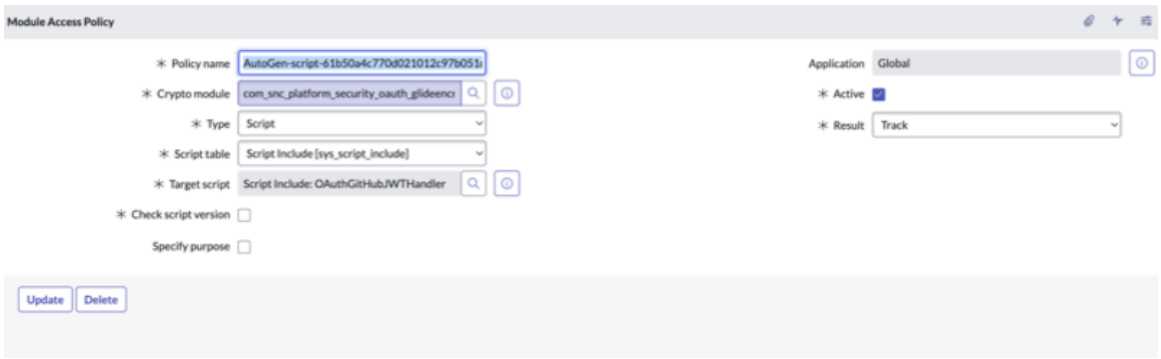
5. Deixe o restante dos campos do formulário como padrão.
6. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.
7. Role até **Perfis de entidade OAuth** lista relacionada, selecione-a e abra o perfil padrão que foi criado na lista.
8. Preencha **Provedor JWT** Campo com o provedor JWT criado anteriormente e salve o formulário.
9. Retorne ao arquivo de registro da aplicação e salve-o.
10. Navegar até **Gestão de chave** > **Políticas de Acesso ao Módulo** > **Tudo**.

Tradução automática

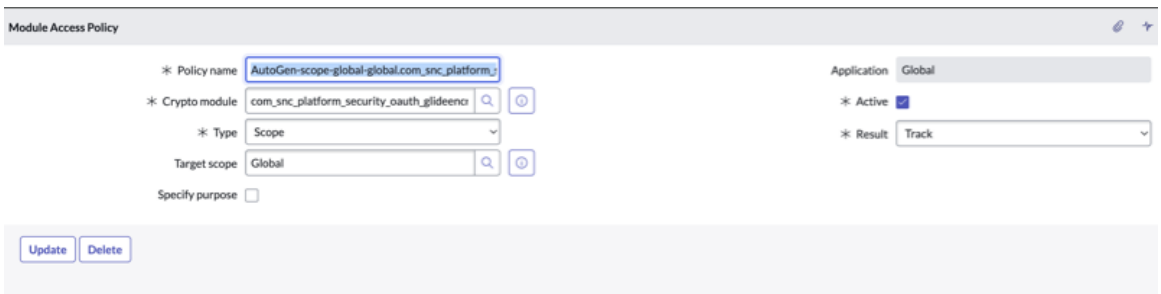
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Selecione a política para que com_snc_platform_security_oauth_glideencrypter é exibido como **Módulo de criptografia** valor do campo, e. OAuthGitHubJWTHHandler É a inclusão de script no **Script de destino** campo.

    Na imagem a seguir com_snc_platform_security_oauth_glideencrypter selecionado como o valor para **Módulo de criptografia** campo. . **Tabela de scripts** o campo é exibido Inclusão de script [sys_script_include] e **Script de destino** o valor do campo é OAuthGitHubJWTHHandler .



12. Selecione **Atualizar**.



    Como mostrado na imagem anterior, o valor em **Nome da política** mudanças de campo e **Tabela de scripts** e. **Script de destino** os campos não são mais exibidos.

13. Verifique **Resultado** o campo está definido como Rastrear e salve suas mudanças.

Criar credenciais e conexões para Integrações de vulnerabilidade de aplicação do GitHub

Crie um registro de credencial para GitHub Provedor de app criado anteriormente para autorizar ações.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Credenciais e conexões** > **Credenciais**.
2. Selecione **Novo**.
3. Selecione **Credenciais OAuth 2.0**.
4. Selecione **Novo** e preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome exclusivo do registro.
Aplica-se a	Selecione as Credenciais do OAuth 2,0 na lista.
Perfil de Entidade OAuth	Selecione o ícone de pesquisa e localize o perfil de entidade que você criou nas etapas anteriores.
Outros campos	Deixe esses campos em seus padrões.

5. Clique com o botão direito do mouse em qualquer lugar no cabeçalho da página e selecione **Salvar** .
   A lista Credenciais é exibida.
6. Abra o registro que você acabou de criar e selecione **Obter token OAuth** link relacionado.
   É exibida uma mensagem informando que o token OAuth foi importado com sucesso.
7. Navegar até **Credenciais e conexões** > **Conexões**.
8. Selecione **Novo**.
9. Selecione **Conexão HTTP(s)**.
10. Selecione **Novo** e preencha os campos.

Campo	Descrição
Nome	Nome do registro.
Aplicação	Somente leitura.
Alias primário (opcional)	Selecione o ícone de pesquisa e escolha um na lista.
Tipo	Conexão e credencial.
Tipo de conexão	HTTP.
Suporte a várias conexões ativas (opcional)	Desativado.
Política de nova tentativa padrão	Política de novas tentativas HTTP padrão
Modelo de configuração	Deixe em branco.

11. Selecione **Enviar**.
    A lista Conexões e Aliases de credencial é exibida.
12. Abra seu registro e, na guia da lista relacionada Conexões, selecione **Novo** E preencha os campos no registro de conexão HTTP.

Campo	Descrição
Nome	Nome do registro.
Ativo	Ativado.
Credencial	Selecione o registro de credencial que você criou nas etapas anteriores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Alias de conexão	Seu registro é exibido.
Construtor de URL	Desativado.
URL de conexão	Este é o URL base: https://api.github.com Para empresas. O local é o URL do end-point do GitHub.
Usar MID Server (opcional)	O MID Server é necessário para no local. É opcional para Enterprise.
Tempo limite de conexão	Insira um valor.

13. Selecione **Enviar**.
    A lista Conexões e Aliases de credencial é exibida. Agora você está pronto para concluir as etapas para Configure o Integrações de vulnerabilidade de aplicação do GitHub. No campo Conexão, insira as credenciais que você criou nas etapas anteriores.

Instale o. ServiceNow® Integrações de vulnerabilidade de aplicação do GitHub

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Integrações de vulnerabilidade de aplicação do GitHub integra-se corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar Integrações de vulnerabilidade de aplicação do GitHub ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Integrações de vulnerabilidade de aplicação do GitHub aplicação.
4. Selecione o bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Selecione **App de solicitação** e insira seu Now Support credenciais de login.
6. Selecione **Obter** .
7. Insira **Nome da instância** e. **Motivo da instância** e selecione **Validar instância** .
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e selecione **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o Integrações de vulnerabilidade de aplicação do GitHub

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto GitHub se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Funções necessárias:

- Grupo de usuários do gerenciador de apps-sec
- sn_vul.app_sec_manager necessário para a configuração do OAuth

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade do GitHub** > **Configuração**.
2. Escolha **Autenticação básica** ou **OAuth** Para Tipo de autenticação.
   - A autenticação básica requer um MID Server para instâncias no local. Gere o token de API necessário para a autenticação básica do seu GitHub conta.
   - OAuth requer a aplicação OAuth, a credencial e a configuração de conexão descritas em Criando credenciais do OAuth 2,0 para GitHub JWT para Integrações de vulnerabilidade de aplicação do GitHub.
3. Preencha os campos com base no tipo escolhido.
   Autenticação básica

Campo	Descrição
URL da API	Apropriado GitHub URL da API para empresa ou no local. O URL padrão é https://api.github.com . No local é seu GitHub URL do endpoint.
Token de API	Token gerado a partir de GitHub console.
Tipo de API	Selecione um: **Organização** Escolha esta opção se quiser importar dados de uma organização específica por nome. . GitHub o ambiente oferece suporte a várias organizações. Cada organização pode oferecer suporte a vários repositórios. Se você inserir uma organização, somente os dados dessa organização serão importados. **Empresa** O ambiente Enterprise oferece suporte a várias organizações. Escolha esta opção se quiser importar dados de vulnerabilidade de todas as organizações em seu ambiente Enterprise (nuvem).
Nome da organização	Nome do GitHub Repositório. Somente os dados da organização inserida são importados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
MID Server	Para instâncias no local para autenticação básica, um MID Server é necessário.
Selecione opções para gerenciar a gestão de exceções e Falsos positivos.	Selecione as opções para gerenciar a gestão de exceções e o Falso positivo para itens vulneráveis a aplicações (Avis) com ServiceNow fluxos de trabalho automaticamente após a importação. **Gerencie exceções em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de Avis importados marcados para **Adiado** estado. Avis com **Origem** estados que normalmente são mapeados para um **Adiado** em vez disso, o estado em sua instância é mapeado para **Aberto** . Você **Solicite uma exceção** Do registro AVI. **Gerencie falsos positivos em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de Avis importados com **Origem** estados marcados como **Falso-positivo** ou **Possível falso-positivo** . Avis com estes **Origem** estados que normalmente são mapeados para um **Encerrado** o estado em sua instância está mapeado para **Aberto** . Você solicita um **Falso-positivo** Do registro AVI. ○ Desative uma ou ambas as caixas de seleção se quiser preservar o. **Origem** estados importados do scanner. ○ . **Exceção de solicitação** e. **Falso-positivo** As ações não estão visíveis no Avis.
Instância de Integração	Instância para a qual você está importando dados.

OAuth

Campo	Descrição
URL da API	Apropriado GitHub URL da API para empresa ou no local. O URL padrão é https://api.github.com . No local é seu GitHub URL do endpoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Conexão	A conexão que você criou descrita em Criando credenciais do OAuth 2,0 para GitHub JWT para Integrações de vulnerabilidade de aplicação do GitHub.
Tipo de API	Selecione um: **Organização** Escolha esta opção se quiser importar dados de uma organização específica por nome. . GitHub o ambiente oferece suporte a várias organizações. Cada organização pode oferecer suporte a vários repositórios. Se você inserir uma organização, somente os dados dessa organização serão importados. **Empresa** O ambiente Enterprise oferece suporte a várias organizações. Escolha esta opção se quiser importar dados de vulnerabilidade de todas as organizações em seu ambiente Enterprise (nuvem). **Nota:** GitHub As aplicações não são compatíveis com APIs de nível empresarial.
Nome da organização	Nome da organização para seu GitHub repositórios. Somente os dados dos repositórios na organização que você insere são importados.
Selecione opções para gerenciar a gestão de exceções e Falsos positivos.	Selecione as opções para gerenciar a gestão de exceções e o Falso positivo para itens vulneráveis a aplicações (Avis) com ServiceNow fluxos de trabalho automaticamente após a importação. **Gerencie exceções em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de Avis importados marcados para **Adiado** estado. Avis com **Origem** estados que normalmente são mapeados para um **Adiado** em vez disso, o estado em sua instância é mapeado para **Aberto** . Você **Solicite uma exceção** Do registro AVI. **Gerencie falsos positivos em ServiceNow**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Deixe esta opção ativada se quiser fazer a triagem de Avis importados com **Origem** estados marcados como **Falso-positivo** ou **Possível falso-positivo** . Avis com estes **Origem** estados que normalmente são mapeados para um **Encerrado** o estado em sua instância está mapeado para **Aberto** . Você solicita um **Falso-positivo** Do registro AVI. ○ Desative uma ou ambas as caixas de seleção se quiser preservar o. **Origem** estados importados do scanner. ○ . **Exceção de solicitação** e. **Falso-positivo** As ações não estão visíveis no Avis.

4. Selecione **Credenciais Salvar e testar** .
5. Execute o. GitHub Integração de repositórios antes de executar as outras integrações.
   O outro GitHub As integrações dependem dos dados da aplicação atual importados da Integração de repositórios. Os dados da Integração de repositórios são armazenados na tabela Aplicações descobertas [sn_vul_app_release]. Para obter mais informações, consulte Exiba Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e dados importados do repositório.

Exiba Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e dados importados do repositório

Use **Execuções de Integração de vulnerabilidades** lista relacionada para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Antes de Iniciar

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidades do GitHub** > **Integrações**.
2. Selecione uma integração.
3. Selecione **Execuções de Integração de vulnerabilidades** lista relacionada.
4. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns para uma execução com falha incluem:

   ○ Interrupção de rede.

   ○ Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você encontrar qualquer uma dessas condições, selecione **Executar agora** e execute novamente a integração.

5. Para exibir repositórios importados, navegue de volta para a lista de integrações e selecione GitHub Registro de integração de repositórios.
6. Selecione **Execuções de Integração de vulnerabilidades** lista relacionada e abra um registro.
   O número de repositórios importados com uma execução de integração é exibido na coluna Itens importados.

   Marcadores e tópicos que você configurou para um repositório em seu GitHub As contas do menu Configurações são importadas. Todas as propriedades personalizadas importadas estão localizadas no menu em seu repositório.

   Marcadores, tópicos e propriedades personalizadas serão importados para sua instância somente se estiverem configurados em seu GitHub conta.

   Se importado, este GitHub As informações são exibidas em sua instância na coluna Informações adicionais de origem na tabela Aplicações descobertas [sn_vul_app_release] e nas informações adicionais de origem. seção em um registro de aplicação descoberto. As propriedades personalizadas são exibidas como pares de chave-valor, e marcadores e tópicos são exibidos em matrizes.

Exibir Integrações de vulnerabilidade de aplicação do GitHub conjuntos de importação

Exibir detalhes das informações de importação do Integrações de vulnerabilidade de aplicação do GitHub.

Antes de Iniciar
Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegue até **Integração de vulnerabilidades do GitHub** > **Tabelas do conjunto de importação**.
2. Selecione um registro para uma integração.
3. Selecione um link relacionado para exibir as seguintes informações:
   - Conjuntos para importação
   - Mapas de transformação
   - Histórico de Transformações

Integração de vulnerabilidade do Invicti

. Integração de vulnerabilidade do Invicti Usa dados da aplicação importados do produto Invicti para ajudar você a determinar o impacto e a prioridade de falhas no seu código.

Integração de vulnerabilidade do Invicti

. Integração de vulnerabilidade do Invicti coleta dados do scanner e disponibiliza esses dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao ServiceNow® Resposta a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades para mapear informações importadas de vulnerabilidade de aplicações de terceiros para sua instância.

A integração importa os seguintes tipos de dados verificados.

- DAST (Dynamic Application Security Testing, teste dinâmico de segurança da aplicação)
- Teste interativo de segurança de aplicações (IAST)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre DAST e IAST, consulte Explorando Resposta a vulnerabilidades de aplicações.

Versões disponíveis

Versão de lançamento	Notas de versão
Integração de vulnerabilidade do Invicti `v1.1` Integração de vulnerabilidade do Invicti `1.0`	Resposta a vulnerabilidades de aplicaçõesnotas da versão Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações

As integrações a seguir estão incluídas no sistema de base. As integrações são encadeadas para que, depois que uma integração for concluída com sucesso, a próxima integração seja iniciada. As integrações são executadas na ordem listada na tabela a seguir.

Todos os dias, os trabalhos agendados são encadeados para executar essas integrações automaticamente em ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Integrações de vulnerabilidade da aplicação Invivice

Integração	Descrição
Aplicação da lista de aplicações Invicti	Importa aplicações verificadas pela Invivice para a tabela Aplicações descobertas [sn_vul_app_release] ou a tabela Aplicação verificada [sn_vul_app_scan_application] com base em como `sn_vul.use_product_model`A propriedade do sistema é definida para os registros de regra de pesquisa de IC. • Se a propriedade do modelo de produto estiver definida como verdadeira, uma aplicação será inserida na tabela de versão da aplicação descoberta. • Se a propriedade do modelo de produto estiver definida como falsa, uma aplicação será inserida na tabela Aplicação verificada. Você pode optar por ativar regras de pesquisa com itens de configuração (ICs) como os destinos de pesquisa modificando a propriedade do sistema. Se você modificá-lo, também deverá ativar as regras de Pesquisa de IC para corresponder

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de vulnerabilidade da aplicação Invivice

Integração	Descrição
	ao destino da pesquisa. Para obter mais informações, consulte: • Configure o Integração de vulnerabilidade do Invicti • Crie uma regra de pesquisa de IC • Reaplicando regras de Pesquisa de IC em Resposta a vulnerabilidades de aplicações
Integração da lista de verificação Invicti	Esta integração é iniciada depois que a integração da lista de aplicações é concluída com sucesso. Esta integração importa dados sobre a data e a hora em que uma verificação foi executada.
Integração de item vulnerável da aplicação Invicti	Esta integração é iniciada depois que a integração da lista de verificação é concluída com sucesso. A partir da v1.1, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de Item vulnerável da aplicação. Cada vulnerabilidade no Inviviti tem um tipo, por exemplo, **DirectoryListing** . Este tipo é mapeado como um ID exclusivo em sua instância e exibido como parte do valor no campo Vulnerabilidade no registro de item vulnerável à aplicação (AVI): **Invicti-DirectoryListing** . Para obter mais informações sobre mapeamento, consulte Integração de vulnerabilidade do Invicti mapeamento de estado.

O limite superior de itens por página para todas as três integrações é 200.

Prepare-se para Integração de vulnerabilidade do Invicti

Uma integração bem-sucedida requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Integração de vulnerabilidade do Invicti Presume que você esteja familiarizado com o produto e a API Invicti.

A integração Common Weakness Enumeration (CWE) também é usada por Resposta a vulnerabilidades de aplicações E devem estar em execução antes de instalar e configurar a Integração de vulnerabilidades Invicti.

Nota: Os dados do NIST Vulnerability Database (NVD) não são necessários para instalar a integração, no entanto, eles fornecem aprimoramento de vulnerabilidades e são úteis.

Para obter informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Nota: Antes de executar a integração, faça qualquer mudança de configuração necessária com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis à aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente. A função de administrador é necessária para instalar e configurar aplicações no ServiceNow AI Platform instância.

Obtenha suas credenciais de API e token de API no console Invicti. Revise as informações disponíveis no site do produto Invicti em Visão geral da API .

Instale o. ServiceNow® Integração de Resposta a vulnerabilidades com Invivicti

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Integração de vulnerabilidade do Invicti a aplicação se integra corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar Integração de vulnerabilidade do Invicti ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Integração de vulnerabilidade do Invicti aplicação.
4. Selecione o bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Selecione **App de solicitação** e insira seu Now Support credenciais de login.
6. Selecione **Obter** .
7. Insira **Nome da instância** e. **Motivo da instância** e selecione **Validar instância** .
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
10. Localize a aplicação, selecione-a e selecione **Instalar** para ativá-lo.
    Sua aplicação é instalada automaticamente em sua instância.

Configure o Integração de vulnerabilidade do Invicti

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Integração de vulnerabilidade do Invicti funciona corretamente com Resposta a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades.

Antes de Iniciar
Funções necessárias:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- administrador para instalar e ativar aplicações
- Grupo de usuários do gerenciador da App-Sec para configurar a integração

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se o Integração de vulnerabilidade do Invicti está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Invivicti.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo Gerenciador de apps-sec. • O Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.
Para o Inviiti Vulnerability Integration, tenha seu **ID do usuário** e. **Token de API** pronto.	Entre em contato com o administrador Invicti para obter o. **ID do usuário** e. **Token de API** se você não os conhece. Para obter mais informações, consulte o site do produto Invicti em Visão geral da API .

Procedimento

1. Navegar até **Tudo** > **Invicti** > **Configuração do Invicti**.
2. Preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL da API	URL da instância do Inviticti do usuário. Estas são as informações obtidas de Prepare-se para Integração de vulnerabilidade do Invicti.
ID do usuário	ID de usuário exclusivo.
Token de API	Token de API que você gerou no console Invicti. Estas são as informações obtidas de Prepare-se para Integração de vulnerabilidade do Invicti.
Escolha o tipo de verificação. Você deve selecionar pelo menos um.	
Importar DAST	Opção para incluir vulnerabilidades de verificações DAST. As verificações DAST encontram vulnerabilidades para uma aplicação dinamicamente enquanto ela está em execução. Esta abordagem pode imitar um ataque externo.
Importar IAST	Opção para incluir vulnerabilidades de verificações IAST. As verificações do IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.
Formato de data	Parâmetro que converte a hora de início para o formato compatível com a API Invivice usada pela Integração de item vulnerável da aplicação Invivice. Este parâmetro deve corresponder ao formato definido ou selecionado na sua conta Invicti, por exemplo, **dd/MM/aaaa** . Verifique se os formatos de data e hora no console Invicti correspondem aos que você inseriu para o formato de data no seu ServiceNow AI Platform instância. Para mudar este formato na consola Invicti: **a.** Faça login em Invicti Sign in . **b.** Selecione **Nome de usuário** no canto superior direito. **c.** Navegar até **Configurações do usuário** > **Formato de data e hora**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Importações com falha podem ocorrer se você inserir um formato de data inválido em seu ServiceNow AI Platform instância. Se você inserir um formato válido em sua instância que seja diferente do formato de data no console Invicti, o Invicti retornará uma carga vazia.
Gerenciar exceções no ServiceNow	Selecione um: **Ativado (selecionado)** AVIT (Application Vulnerable Items, itens vulneráveis à aplicação) da Invicti com estados como **Presente** e. **AcceptedRisk** que podem ser adiados em sua instância são mapeados para **Aberto** automaticamente. **Desativado (não selecionado)** os estados de origem dos itens vulneráveis à aplicação (AVITs) importados da Invicti são preservados. Você deve gerenciar exceções para esses AVITs (adiá-las) dos registros AVIT. Para obter mais informações sobre estados de origem e campos de destino Invicti, consulte Integração de vulnerabilidade do Invicti mapeamento de estado.
Gerenciar falsos positivos no ServiceNow	Selecione um: **Ativado (selecionado)** AVITs com estados de Invicti como **Presente** e. **Falso-positivo** que pode fazer a transição para **Encerrado** em sua instância são mapeados para **Aberto** automaticamente. **Desativado (não selecionado)** os estados AVIT importados da Invicti são preservados. Você deve gerenciar falsos positivos ou possíveis falsos positivos para esses AVITs de registros AVIT.

3. Selecione **Salvar e testar credenciais** .
4. **Opcional:** Modifique suas regras de pesquisa para que elas sejam baseadas em itens de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Por padrão, o **sn_vul.use_product_model** a propriedade do sistema está ativada (definida como verdadeiro Para suas regras de pesquisa listadas na tabela [sn_sec_cmn_ci_lookup_rule] com base no modelo do produto. Quando esta regra é ativada:

- Esta regra identifica correspondências entre os dados importados e os dados em seu Configuration Management Database (CMDB) com base no modelo do produto.
- Registros são criados ou atualizados na tabela Aplicações descobertas [sn_vul_app_release].
- Quando você cria ou edita suas regras de pesquisa para Invicti, **Modelo do produto** é exibido em **Destino de pesquisa** campo no formulário de regra.

Para modificar suas regras para que elas sejam baseadas em itens de configuração, você deve desativar manualmente (defina como falso . **sn_vul.use_product_model** propriedade do sistema.

a. Navegar até **Tudo** > **Propriedades do sistema** e localize **sn_vul.use_product_model** Registre e defina o valor como falso .

b. Selecione **Atualizar**.

c. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Regras de pesquisa**.

d. Localize o nome da aplicação e as regras de ID da aplicação de origem que têm o destino de pesquisa como **Item de configuração** .

e. Marque a caixa de seleção Ativo para essas regras.

f. Selecione **Atualizar**.
Ao criar ou editar suas regras de pesquisa para Invicti, observe isso **Item de configuração** é exibido em **Destino de pesquisa** campo no formulário de regra. Registros são criados ou atualizados na tabela Aplicações verificadas [sn_vul_app_scan_application].

Exibindo o. Integração de vulnerabilidade do Invicti status e registros de execução de importação

Use **Execuções de Integração de vulnerabilidades** lista relacionada para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Exibição de status de importação, conjuntos de importação e registros

Para exibir o status de suas importações, como um usuário no grupo de usuários do Gerenciador da App-Sec, navegue até **Tudo** > **Integração da vulnerabilidade do Invicti** > **Integrações** e selecione um registro de integração. Selecione **Execuções de Integração de vulnerabilidades** lista relacionada.

A partir da v1.1, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de Item vulnerável da aplicação.

Para exibir os conjuntos de importação, navegue até **Tudo** > **Integração da vulnerabilidade do Invicti** > **Integrações** > **Tabelas do conjunto de importação** e selecione uma integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Integração da lista de aplicações cria ou atualiza registros com base no destino de pesquisa:

- Modelo de produto: Tabela Aplicações descobertas [sn_vul_app_release]
- Item de configuração: Tabela Aplicações verificadas [sn_vul_app_scan_application]

A integração da Lista de verificação cria ou atualiza registros na tabela Aplicações verificadas [sn_vul_app_scan_summary].

A Integração de item vulnerável da aplicação cria ou atualiza registros nas tabelas Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item] e CWEs [sn_vul_cwe].

Nota: Cada vulnerabilidade no Invivice tem um "tipo", por exemplo, ProductDirectoryListing. Este tipo é importado mapeado como um ID exclusivo para sua instância e exibido como parte do valor no campo Vulnerabilidade no registro de item vulnerável à aplicação (AVIT). Neste exemplo, o valor é Inviticti-ProductDirectoryListing E este valor também é exibido como o ID exclusivo no registro de entrada de vulnerabilidade da aplicação. Inviti AVITs são compatíveis com várias entradas de CWE (Common Weakness Enumeration, enumeração de pontos fracos comuns), portanto os CWEs não são usados como IDs exclusivos. CWEs também são exibidos no registro AVIT.

Inviti AVITs, se houver tipos duplicados em Invicti para uma vulnerabilidade, a palavra "personalizado" será inserida no valor, por exemplo, Inviticti-custom-ProductDirectoryListing . Se você criar um tipo personalizado para vulnerabilidades, o ID da vulnerabilidade poderá ser Inviticti-Custom- <title of vulnerability>.

Novos campos: Para Invicti , Os parâmetros afetados e os campos personalizados podem incluir dados que podem ajudar você a entender a vulnerabilidade e ajudá-lo a corrigi-la. Se não houver dados, esses campos não serão exibidos no AVIT.

Integração de vulnerabilidade do Invicti mapeamento de estado

Os seguintes estados de origem do Integração de vulnerabilidade do Invicti e seus estados de destino em sua instância estão listados na tabela a seguir.

estados de origem Invicti e seus correspondentes ServiceNow AI Platform estados

estados de origem Invicti	Descrição dos estados de origem	Estado de destino no ServiceNow AI Platform
Present	O problema foi identificado.	Aberto
AcceptedRisk, revivido	O problema foi considerado e está marcado como uma vulnerabilidade de baixo risco.	Adiado
Falso-positivo	O problema foi considerado e está marcado como uma vulnerabilidade não genuína.	Encerrado
FixedNão confirmado, Corrigido Não confirmado	O problema foi corrigido, mas não foi confirmado pela Invicti Enterprise.	Resolvido
Fixo (confirmado), FixedConfirmed, FixedConfirmed, AceptedRisk, FixedConfirmed, falso-positivo	O problema foi corrigido e confirmado pela Invicti Enterprise e nenhuma ação adicional é necessária.	Encerrado
Corrigido (não é possível testar novamente)	O problema foi identificado, mas a Invicti não pode testar novamente	Resolvido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados de origem Invicti e seus correspondentes ServiceNow AI Platform estados

estados de origem Invicti	Descrição dos estados de origem	Estado de destino no ServiceNow AI Platform
	para confirmar se o problema foi corrigido ou não.	
Revivido	O problema foi corrigido em verificações anteriores, mas foi encontrado novamente.	Aberto
Adiado, ignorado	O problema foi ignorado pelo usuário. Em Invivice Enterprise, para ignorar um problema, um usuário atualiza seu status para "Risco aceito".	Risco aceito

Mapeamento de versão da aplicação

Campo de origem	Campo de destino ativado ServiceNow AI Platform
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date
Nome	app_name
RootUrl	Source_additional_info
Descrição	descrição
Marcadores	Marcadores

Mapeamento de vulnerabilidades

Campo de origem	Campo de destino ativado ServiceNow AI Platform
Tipo	Nome da categoria
Detalhe da vulnerabilidade	Resumo
Impacto	Ameaça
Referências de origem	Referências da Web
Recomendação de origem	Solução
Tipo	Source_entry_id/ID
Gravidade	source_severity
Classificação["CWE"]	Lista de CWE
CvssVectorString	Campos CVVS v3

Mapeamento de resumo da verificação

Campo de origem	Campo de destino

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Origem
TotalVulnerabilityCount	Detected_flaw_count
Data de início	Data de verificação dinâmica
id	source_scan_id

Mapeamento de item vulnerável à aplicação (AVIT)

Campo de origem	Campo de destino ativado ServiceNow AI Platform
Tipo	Tipo de verificação
ID do site	ID de aplicação de origem
ID	ID de AVIT de origem
Data da última exibição	Último encontrado
Data da primeira exibição	Primeiro encontrado
Data da última atualização	Data da última verificação
parâmetros	Parâmetro afetado
URL	URL afetada
Gravidade	Gravidade de origem
URL	Link da origem
Detalhe da vulnerabilidade	Resumo da vulnerabilidade de origem
Referências externas	Referências de origem
Referências de solução e solução	Recomendação de origem
Estado	Status da correção da origem
Impacto	Explicação da vulnerabilidade de origem

Integração de Resposta a vulnerabilidades com Veracode

. Resposta a vulnerabilidades Integração com Veracode a aplicação usa dados importados do Veracode produto para ajudar você a determinar o impacto e a prioridade de falhas em seu código.

Integração de Resposta a vulnerabilidades com Veracode

. Veracode O produto coleta testes dinâmicos de segurança de aplicações (DAST), testes estáticos de segurança de aplicações (SAST) e dados do scanner manual e disponibiliza esses dados para o. ServiceNow AI Platform®. Ele se integra facilmente ao Resposta a vulnerabilidades de aplicações recurso de Resposta a vulnerabilidades mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

A partir da v19.0 de Resposta a vulnerabilidades, Você pode importar vulnerabilidades da Análise de composição de software (SCA) e Lista de materiais de software(SBOM) dados de vulnerabilidade para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Explorando Lista de materiais de software.

Uma API compartilhada ingesta dados DAST, SAST, SCA e resultados de testes de invasão manuais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que são listadas. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida da correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Obtenha mais detalhes de Veracode

A partir da v4.2, selecione **Obter mais detalhes** Itens vulneráveis à aplicação (AVITs) que têm Veracode Como a Origem na tabela Item vulnerável à aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir o seguinte Veracode dados.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- Solicitação de origem HTTP, Resposta de origem e Recomendações são exibidas na guia Detalhes na Resposta a vulnerabilidades Resposta a vulnerabilidades espaços de trabalho.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Versões disponíveis

Versão de lançamento	Notas da versão
Veracode v4.3 Veracode v4.2 Veracode v4.1	Resposta a vulnerabilidades de aplicaçõesnotas da versão Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Grupo de usuários e funções

. Integração de Resposta a vulnerabilidades com VeracodeÉ instalado por um administrador do sistema [admin] e configurado por um membro do grupo Gerenciador da App-Sec. Para obter mais informações, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

Integração de Resposta a vulnerabilidades com Veracode

Para exibir o. Veracode integrações de vulnerabilidades, navegue até **Tudo** > **Integração de vulnerabilidade da Veracode** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Resposta a vulnerabilidades com Veracode

Integração	Descrição
A partir da v4.1: Veracode Vincular integração de projetos	Esta integração é ativada por padrão. Recupera todos os projetos associados para cada aplicação de Veracode. As aplicações podem ter vários projetos no Veracode aplicação. Os dados importados desta integração são exibidos nos seguintes registros: • **Data da última verificação do SCA** , **Data de criação da aplicação** e **Data de atualização da aplicação** estão listados em registros em **Aplicações descobertas** . • Nos registros de Resumo de verificação de vulnerabilidades da aplicação e Itens vulneráveis à aplicação (AVITs), o. **Status do SDLC de origem** (Ciclo de vida de desenvolvimento de software) é exibido. • **Exploração da origem** É exibido em registros de item vulnerável à aplicação (AVI).
Veracode Integração da lista de aplicações (JSON)	Esta integração está inativa por padrão. Recupera Veracode dados do scanner de aplicações (vulnerabilidades, metadados) e enriquece os dados da aplicação. Recupera registros de verificação de Veracode Por meio de uma API baseada em JSON.
Veracode Integração da lista de aplicações (XML)	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera Veracode dados do scanner de aplicações (vulnerabilidades, metadados) e enriquece os dados da aplicação. Esta integração está definida para ser executada diariamente às 00:00:00. **Nota:** Uma API baseada em JSON de Veracodeé usado para recuperar a lista de aplicações. Esta API importa a "data da última verificação de conformidade da política" para essas aplicações, o que significa quando essas aplicações foram verificadas pela última vez por Veracode.
Veracode Lista de materiais de software(SBOM Integração	Versão 4,3 do Integração de Resposta a vulnerabilidades com Veracode o inclui os seguintes aprimoramentos com Veracode SBOM arquivos: • Se você instalou o SBOM Response, terá a opção de incluir vulnerabilidades encontradas por Veracode Para os arquivos SBOM que você carrega. • Veracode está mapeado para **Origem** Campo para registros na tabela Lista de materiais [sn_sbom_doc] para Veracode Arquivos SBOM. Esta integração é ativada por padrão. A partir de v4.2, importações Lista de materiais de software Arquivos nos formatos CycloneDX e SPDX gerados por Veracode e os coloca na fila para análise em sua instância. . Você deve ter Lista de materiais de software aplicações instaladas para importar esses dados e exibi-los.
Veracode Integração de resumo de	Esta integração está inativa por padrão. Recupera registros de verificação de Veracode Por meio de uma API baseada em JSON. Esta integração substitui a integração de API baseada em XML. Ele é acorrentado e segue o. Veracode Integração da lista de aplicações quando ativado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Resposta a vulnerabilidades com Veracode

Integração	Descrição
verificação (JSON)	
Veracode Resumo da verificação (XML)	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera registros de verificação de Veracode. Esta integração é encadeada e segue o. Veracode Integração da lista de aplicações quando ativado. **Nota:** Segue automaticamente o. Veracode Integração da Lista de aplicações quando ativada. "Data da última verificação de conformidade da política" para as aplicações de Veracode esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
Veracode Integração JSON de item vulnerável da aplicação	A partir da v4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável da aplicação. Esta integração está inativa por padrão. Recupera resultados da verificação com mais dados de vulnerabilidade do que a integração baseada em XML do Veracode. Ele insere Avis e enriquece seus dados de vulnerabilidade de terceiros.
Veracode Integração de item vulnerável da aplicação (XML)	A partir da v4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável da aplicação. Esta integração está inativa por padrão. Recupera os resultados da verificação de Veracode Insere itens vulneráveis à aplicação (AVITs) e enriquece seus dados de vulnerabilidade de terceiros. Por padrão, se o registro do scanner estiver em **Encerrado** AVITs não foram criados. AVITs existentes ainda estão atualizados. Esta integração é encadeada e segue o. Veracode Integração do resumo da verificação quando ativada. A API baseada em XML foi descontinuada para Veracode Integração JSON do resumo da verificação. **Nota:** Segue automaticamente o. Veracode Integração do resumo da verificação. "Data da última verificação de conformidade da política" para as aplicações de Veracode esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
Veracode Integração de categorias	Esta integração está inativa por padrão. Recupera dados de Categorias aprimorados de Veracode.
Veracode Integração do CWE	Esta integração é ativada por padrão. Recupera Veracode- Dados de enumeração de pontos fracos comuns (CWE) específicos para informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Resposta a vulnerabilidades com Veracode

Integração	Descrição
	de ameaças e recomendações de correção. Esses dados são preenchidos e atualizados nos registros de entrada de vulnerabilidade da aplicação. Esta integração do CWE opera independentemente do trabalho agendado para a Integração abrangente do CWE 2000 que você ativa para Resposta a vulnerabilidades aplicação. Seus dados não serão duplicados se você tiver Veracode Integração do CWE e a Integração abrangente do CWE 2000 ativadas.
Veracode Integração do DevOps	Esta integração está inativa por padrão. A integração pode ser visualizada na lista Integrações de vulnerabilidades da aplicação em Resposta a vulnerabilidades de aplicações. Se você tiver uma licença do DevOps Change Velocity, esse recurso será estruturado para que os usuários do DevOps não precisem de uma licença SecOps para exibir detalhes resumidos de verificações de vulnerabilidades de terceiros. Não há impacto ou mudança para Resposta a vulnerabilidades de aplicações.

Para obter os status de execução de integração, consulte, Exiba Veracode Status da execução de importação da Integração de vulnerabilidades da aplicação.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para Integração de Resposta a vulnerabilidades com Veracode

Bem-sucedida Integração de Resposta a vulnerabilidades com Veracode requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando essas tarefas. . Integração de Resposta a vulnerabilidades com Veracode presume que você esteja familiarizado com Veracode Produto e API.

Antes de Iniciar

A integração Common Weakness Enumeration (CWE) também é usada por Resposta a vulnerabilidades de aplicações e devem estar em execução antes de instalar e configurar o. Integração de Resposta a vulnerabilidades com Veracode. Ele é instalado com Resposta a vulnerabilidades, por padrão.

Nota: Os dados do NIST Vulnerability Database (NVD) não são necessários para instalar o. Veracode Integração de vulnerabilidades da aplicação, no entanto, elas fornecem aprimoramento e seriam úteis. Para obter informações sobre NVD, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Há um usuário de execução configurado para cada registro de integração. O valor padrão para este usuário é **VR.System** . Não mude este valor.

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis à aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Integração de Resposta a vulnerabilidades com Veracode Requer um ID de API e uma chave de API.

Procedimento

Para criar o ID da API e as credenciais de chave:

a. Faça login no Veracode Plataforma.

b. Vá para o menu Conta de usuário e selecione **Credenciais de API** .

c. Clique em **Gerar credenciais de API** .

d. Registre suas credenciais para uso posterior.

Instale o. ServiceNow® Integração de Resposta a vulnerabilidades com Veracode

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Veracode o produto se integra corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não tiver sido atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo Gerenciador da App-Sec. Para obter informações sobre funções de grupo, consulte, Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login na instância em que você deseja instalar Integração de Resposta a vulnerabilidades com Veracode ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, Pesquise Integração de resposta a vulnerabilidades com Veracode aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler o. **Outros requisitos** e. **Dependências** , conforme aplicável.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o. Integração de Resposta a vulnerabilidades com Veracode para o seu ambiente. Consulte Configure o Integração de Resposta a vulnerabilidades com Veracode.

Configure o Integração de Resposta a vulnerabilidades com Veracode

Para executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para Veracode o produto se integra corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se o Resposta a vulnerabilidades Integração com Veracode a aplicação está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Veracode.
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários do Gerenciador de apps-sec. • O Gerenciador da App-Sec supervisiona a configuração e verifica os resultados esperados.
Para Veracode Integração de vulnerabilidade da aplicação, tenha seu **ID da API** e. **Chave de API** pronto.	Contato Veracode para obter o. **ID da API** e. **Chave de API** . Consulte Preparando para Integração de Resposta a vulnerabilidades com Veracode. A partir da versão 4,0, se você estiver usando Integração de Resposta a vulnerabilidades com Veracode, os testes de avaliação de invasão no Integração de Resposta a vulnerabilidades com Veracode são descobertas manuais de Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão que você configura em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre solicitações de teste de invasão em Resposta a vulnerabilidades de aplicações, consulte Configurar testes de invasão.

Função necessária: Grupo de usuários do gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade da Veracode** > **Configuração**.
2. Preencha **ID DA API** e. **Chave de API** campos.
3. Escolha os resultados dos testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Versão 4,0:	**a.** Selecione **DAST** ou **SAST** tipos de dados a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um. **b.** Selecione **SCA** Para importar vulnerabilidades da Análise de composição de software (SCA). **c.** Selecione **Incluir Manual** para importar resultados de testes de invasão manuais de Veracode. AVITs são criados para esses resultados.
Versão 3.0	Selecione **DAST** ou **SAST** tipos de dados a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um.
Versão 1,0:	Os resultados do teste de segurança da aplicação dinâmica são selecionados por padrão.

4. Adicione Veracode **Gravidade** nível para filtrar seus dados importados.
   Este valor é importado de Veracode. Você pode adicionar vários valores ao campo. Se preenchida, a importação reunirá somente dados que correspondam aos níveis de gravidade adicionados.
5. Salve e valide suas escolhas.

Opção	Descrição
Versão 3,0:	Clique em **Salvar e testar credenciais** . **Nota:** A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.
Versão 1,0:	Clique em **Salvar**. Verifique a configuração bem-sucedida clicando em **Credenciais de teste** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.

6. Selecione como você deseja gerenciar exceções e falsos positivos para AVITs na importação.
Opções para gerenciar AVITs na importação com ServiceNow A Gestão de exceções e os fluxos de trabalho falso-positivos são ativados por padrão. Os fluxos de trabalho são acionados com base em como **Origem** os estados nos AVITs são mapeados em sua instância. Para obter um exemplo de caso de uso, consulte Gerenciar mapeamento de estado para adiamentos e falsos positivos em Resposta a vulnerabilidades de aplicações.

Habilitado	**Gerencie exceções em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de AVITs importados marcados para **Adiado** estado. AVITs com **Origem** estados que normalmente são mapeados para um **Adiado** em vez disso, o estado em sua instância é mapeado para **Aberto** . Você **Solicite uma exceção** Do registro AVI. **Gerencie falsos positivos em ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de AVITs importados com **Origem** estados marcados como **Falso-positivo** ou **Possível falso-positivo** . AVITs com estes **Origem** estados que normalmente são mapeados para um **Encerrado** o estado em sua instância está mapeado para **Aberto** . Você solicita um **Falso-positivo** Do registro AVIT.
Desativado	Desative uma ou ambas as caixas de seleção se quiser preservar o. **Origem** estados importados do scanner. Esses AVITs são mapeados para **Destino** e. **Motivo de destino** estados conforme são importados, mas não são triados pelos fluxos de trabalho de exceção e falso-positi–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	vo. . **Exceção de solicitação** e. **Falso-positivo** As ações não estão visíveis em AVITs.

7. A partir da v4.3, escolha ou verifique as configurações dos seguintes parâmetros.

Parâmetro	Descrição
Região da API	Selecione uma região na lista.
Tempo limite da API	O padrão é 30K. Você pode preferir deixar este campo em sua configuração padrão.
Incluir vulnerabilidades de SBOM	Selecione para incluir todas as vulnerabilidades ingeridas pelo Veracode integrações no Veracode SBOM arquivos que você carrega. Deixe o campo limpo Veracode as vulnerabilidades não são analisadas em Veracode SBOM arquivos.

8. Selecione **Salvar e testar credenciais** .

O que Fazer Depois

Se o seu ambiente exigir importações separadas por domínio, consulte Crie importações separadas por domínio para uma integração.

Na instalação inicial, consulte Como configurar o Resposta a vulnerabilidades de aplicações para obter mais instruções.

Após a instalação inicial, para obter modificações, consulte Integração de Resposta a vulnerabilidades com Veracode modificações e atividades.

Exiba Veracode Status da execução de importação da Integração de vulnerabilidades da aplicação

Use **Execuções de Integração de vulnerabilidades** lista relacionada para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o. Integração de Resposta a vulnerabilidades com Veracode status da execução da importação:

- Resposta a vulnerabilidades de aplicações e o. Integração de Resposta a vulnerabilidades com Veracode deve ser instalado e configurado.
- . Integração de Resposta a vulnerabilidades com Veracode as importações devem ser programadas e em execução.

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Selecione uma integração.
3. Clique em **Execuções de Integração de vulnerabilidades** lista relacionada.
4. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns para uma execução com falha incluem:

   - Interrupção de rede.
   - Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

   Se você encontrar qualquer uma dessas condições, clique em **Executar agora** e execute novamente a integração.
5. A partir da v4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as Integrações de itens vulneráveis da aplicação.
   Para obter mais informações sobre como exibir detalhes adicionais importados por Veracode, Consulte Obter mais detalhes em Integração de Resposta a vulnerabilidades com Veracode.

Exibir Veracode resumos de verificação

Exibir detalhes das informações de resumo da verificação para Veracode Integração de vulnerabilidades.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até a tabela Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary_list].
2. Selecione um registro para um Veracode verificação.
3. A partir da v19.0 de Resposta a vulnerabilidades E v4.0 da Integração de vulnerabilidades do Veracode, use o ícone Personalizar lista (ícone de engrenagem) para exibir as seguintes colunas.
   - Tamanho da verificação estática
   - Contagem de biblioteca de terceiros
   - Contagem de biblioteca de vulnerabilidades de terceiros
   - Contagem de falhas de terceiros por gravidade
   - Contagem do problema de biblioteca de terceiros
   - Contagem do problema de licença de terceiros
   - Contagem de falhas mista
   - Contagem de falhas mitigada
   - Contagem de falhas não mitigada
   - Contagem de falhas estáticas por gravidade
   - Nova contagem de falhas por gravidade
   - contagem de falhas não mitigada por severidade
   - Total de contagem de falhas por gravidade
   - Classificação da última verificação de SCA
   - Data da última verificação de SCA
   - Data publicada da verificação
   - Marcadores

Transformação de dados para Veracode Integração de vulnerabilidades

Depois de identificar os dados que você deseja importar, os dados serão recuperados do Veracode processado por meio de um conjunto de fontes de dados e transformado em sua instância.

Veracode Integração de item vulnerável da aplicação

Os dados da API são carregados primeiro no Veracode Importação de item AppVul [sn_vul_veracode_appvul_item_import] e Veracode A transformação de item do AppVul é usada para transformar as informações importadas.

Para acessar este mapa de transformação, navegue até *System Import Sets* > *Transform Maps*e pesquise Veracode Transformação de item do AppVul. A tabela a seguir lista os campos do mapa de transformação por integração.

Veracode Campos do mapa de transformação de item do AppVul

Campo de origem	Campo de destino	Descrição
app_id	source_app_id	ID da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Campos do mapa de transformação de item do AppVul

Campo de origem	Campo de destino	Descrição
issueid	source_avit_id	ID DO AVIT.
app_name	app_name	Nome da aplicação.
versão	app_version	Versão da aplicação.
build_id	source_scan_id	ID de compilação da aplicação.
account_id	account_id	ID da conta.
sandbox_id	sandbox_id	ID da área restrita.
last_update_time	last_scan_date	Hora da última atualização.
app_name e last_scan_date	scan_summary_name	Resumo da verificação.
life_cycle_stage	source_sdlc_status	Status do SDLC de origem.
nível	source_severity	Gravidade da origem.
category_name	categoria	Categoria.
source_severity	source_severity	Gravidade da origem.
Category_id, " cwe-" e cweId	source_entry_id	ID de entrada de origem.
source_vulnerability_summary	source_vulnerability_summary	Resumo da vulnerabilidade de origem.
source_recommendation	source_recommendation	Recomendação de origem.
descrição	descrição	Descrição da origem.
descrição	source_vulnerability_explanation	Explicação da vulnerabilidade de origem.
mitition_status_desc	source_mitition_status	Status de mitigação de origem.
remediation_status	source_remediation_status	Status de correção de origem.
linha	line_number	Linha na qual a falha foi encontrada.
módulo	application_module	Módulo da aplicação.
sourcefile	source_notes	Anotações de origem.
affects_policy_compliance	accomes_with_policy	Os valores podem ser Sim ou Não com base nas informações de origem serem verdadeiras ou falsas.
Sourcefilepath e sourcefile	local	Mapeamento de local no caso de um `static`falha.
URL	local	Mapeamento de local no caso de um `dynamic`falha.
Escopo, tipo, exploitLevel	source_additional_info	Campo Valor do nome preenchido com os valores da origem em caso de falhas estáticas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Veracode tempo e finalidade do script do mapa de transformação

Quando o script é executado	Finalidade
OnComplete (quando um conjunto de importação conclui a transformação)	Script usado para processar a fonte de dados e atualizar a contagem de AVITs criados, atualizados ou inalterados e os importados como parte desta integração de Veracode. Este script é para uso interno e não deve ser modificado ou excluído.

Integração de Resposta a vulnerabilidades com Veracode modificações e atividades

Configure modificações opcionais especificamente para Integração de Resposta a vulnerabilidades com Veracode.

Exibição de dados adicionais importados pelo Integração de Resposta a vulnerabilidades com Veracode

Nota: Alterando outro Integração de Resposta a vulnerabilidades com Veracode as configurações, diferentes das listadas aqui, exigem avançado ServiceNow e. Resposta a vulnerabilidades de aplicações e está além do escopo da documentação do produto.

Obtenha mais detalhes de Veracode

A partir da v4.2, selecione **Obter mais detalhes** Itens vulneráveis à aplicação (AVITs) que têm Veracode Como a Origem na tabela Item vulnerável à aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir o seguinte Veracode dados.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- Solicitação de origem HTTP, Resposta de origem e Recomendações são exibidas na guia Detalhes na Resposta a vulnerabilidades Resposta a vulnerabilidades espaços de trabalho.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Modificar Veracode parâmetros da instância de integração

Após a instalação inicial, você pode modificar os parâmetros do Veracode integrações no Veracode Instância de integração.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Você pode modificar os parâmetros de uma integração de sua instância para determinar que tipo de dados você ingere. Para algumas dessas configurações, você também pode modificar esses parâmetros na página de configuração da integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione **Vulnerabilidade da aplicação Veracode** Na coluna Instância de origem do Veracode integração que você deseja modificar.
3. Selecione **Parâmetros da instância de integração** E clique duas vezes em um campo na coluna Valor para modificar os valores.

   A partir da v19.0 de Resposta a vulnerabilidades e v4.0 do Integração de Resposta a vulnerabilidades com Veracode, você pode configurar os seguintes parâmetros para Veracode integrações.

   importação manual

   Insira verdadeiro para importar resultados de testes de invasão manuais de Veracode. Você também pode modificar esse valor na página de configuração de integração.

   Os testes de avaliação de invasão no Integração de Resposta a vulnerabilidades com Veracode são descobertas manuais de Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão que você configura em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre solicitações de teste de invasão em Resposta a vulnerabilidades de aplicações, consulte Configurar testes de invasão.

   import_sca

   Insira verdadeiro Para importar vulnerabilidades da Análise de composição de software (SCA). Você também pode modificar esse valor na página de configuração de integração.

   status

   Insira Aberto ou Encerrado para importar descobertas para os estados desejados. Se você deixar este campo em branco, a integração importará descobertas para os estados Aberto e Encerrado.

   policy_sandbox

   Insira um política ou sandbox para importar registros que correspondem a uma política ou a uma área restrita. Esses registros podem estar relacionados a como as aplicações são testadas em seu ambiente.

   policy_rule_passed

   Insira verdadeiro ou falso para importar registros aprovados em uma regra de política. Esses registros podem estar relacionados a como as aplicações são testadas em seu ambiente.

4. Selecione **Atualizar** para salvar suas mudanças.

Execute um manual Veracode importação de vulnerabilidades da aplicação

Se sua importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho agendado diariamente.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha e integração, por exemplo, o. Veracode Integração da lista de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Executar Agora**.

   Nota: . Veracode as integrações de vulnerabilidades da aplicação têm como objetivo fornecer a recuperação de dados mais completa. Executá-los fora de ordem requer ServiceNow e. Resposta a vulnerabilidades de aplicações e pode resultar em dados incompletos.

   Quando a importação estiver concluída, as importações programadas serão retomadas.

4. Para obter os status de execução de integração, consulte, Exiba Veracode Status da execução de importação da Integração de vulnerabilidades da aplicação.

5. Se você quiser modificar outros parâmetros de integração, navegue até a instância de integração.

Definido Integração de Resposta a vulnerabilidades com Veracode tempos de importação

Para sua conveniência, você pode redefinir a hora de início do Integração de Resposta a vulnerabilidades com Veracode.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, o Veracode as integrações de vulnerabilidades fazem uma importação completa sempre que são executadas. Consulte Execute um manual Veracode importação de vulnerabilidades da aplicação para obter mais informações sobre como executar importações.

Procedimento

1. Navegar até **Tudo** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha uma integração.
3. Definir o novo **Hora de início** .
   O tempo é calculado como horas no horário local. A hora padrão do Veracode As importações de integração da lista de aplicações são 00:00:00. As outras integrações são **Sob demanda** e acorrentados para serem executados após Veracode Integração da lista de aplicações. Alterando o. **Hora de início** para qualquer um desses, requer avançado ServiceNow e. Gestão de vulnerabilidades de aplicações experiência.
4. Clique em **Atualizar**.
   A nova hora é usada para a próxima importação programada.

Incluir itens vulneráveis da aplicação Veracode encerrados

Por padrão, **Encerrado** Itens vulneráveis à aplicação (Avis) não são criados durante Veracode Importações de integração de item vulnerável. Se você quiser criá-los, altere uma propriedade do sistema.

Antes de Iniciar

. Integração de Resposta a vulnerabilidades com Veracode deve estar instalado e em execução.

Função necessária: administrador

Procedimento

1. Na navegação à esquerda **Navegador de filtros** caixa de texto, digite `sys_properties.list` .
2. Em **Nome** caixa de pesquisa da lista, insira `sn_vul.create_closed` .
3. Clique duas vezes em **Valor** e definido como **Verdadeiro**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no ícone de marca de seleção verde para salvar.
   Registros no **Encerrado** estado no próximo Veracode As importações são criadas como Avis em Resposta a vulnerabilidades de aplicações.

Ingestão manual de vulnerabilidades para Resposta a vulnerabilidades da aplicação

Os profissionais de segurança e testadores de aplicações podem criar e gerenciar as descobertas do teste de invasão da aplicação no Espaço de testes de invasão.

Os formulários de teste de invasão estão disponíveis no Espaço de teste de invasão para documentar as vulnerabilidades identificadas nas principais aplicações de negócios.

Os profissionais de segurança e testadores de aplicações podem importar manualmente descobertas de fontes e plataformas externas usando os modelos fornecidos no formato Excel ou CSV. Todas as descobertas de vulnerabilidade são disponibilizadas no Espaço de testes de invasão.

Para acessar e baixar o modelo para carregar no espaço de teste de invasão, navegue até **Tudo** > **Ingestão manual de AVIT** > **Carregar IU de arquivo**.

Um novo formulário de teste de invasão é criado para cada carregamento de arquivo para a respectiva aplicação. Todas as descobertas de vulnerabilidade nesse carregamento estão associadas ao mesmo formulário de teste de invasão. O Nome da aplicação deve corresponder aos registros em das tabelas:

- Tabela da aplicação
- Tabela de aplicações de negócios
- Tabela da aplicação verificada

O Nome da aplicação é um campo obrigatório presente no modelo para identificar as vulnerabilidades presentes em uma aplicação, associada a um formulário de teste de invasão. Qualquer registro que não tenha o Nome da aplicação não será processado e ignorado durante a criação da vulnerabilidade.

Nota: Campos obrigatórios no modelo são necessários para processar as descobertas do teste de invasão. É necessário garantir que todos os campos no modelo estejam intactos para evitar problemas durante o processamento das descobertas do teste de invasão.

Campos obrigatórios necessários como parte do modelo para criação da descoberta de teste de invasão

Nome da Coluna	Obrigatório(a)	Descrição	Opções disponíveis/ Máximo de caracteres em cadeias de caracteres
Classificação de risco	Obrigatório(a)	Gravidade do item vulnerável da aplicação	Crítico Alto(a) Média Baixo(a) Nenhum (padrão)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos obrigatórios necessários como parte do modelo para criação da descoberta de teste de invasão

Nome da Coluna	Obrigatório(a)	Descrição	Opções disponíveis/ Máximo de caracteres em cadeias de caracteres
Solicitação de	Obrigatório(a)	Solicitação de	151
Categoria CWE	Obrigatório (preencha apenas uma coluna)	ID DO CWE	255
ID de vulnerabilidade	Obrigatório (preencha apenas uma coluna)	ID de vulnerabilidade	255
Aplicação	Obrigatório(a)	Nome da aplicação	255
Finalidade da aplicação	Obrigatório(a)	Finalidade da aplicação	4000
Tipos de dados confidenciais	Obrigatório(a)	Listar tipos de dados confidenciais acessíveis das aplicações	40
Lista de programas de conformidade	Obrigatório(a)	Lista de programas de conformidade	4000
Detalhes das stacks de tecnologia	Obrigatório(a)	Detalhes das stacks de tecnologia	4000
Equipe da aplicação	Obrigatório(a)	Nome da equipe de aplicações; grupo responsável por desenvolver e manter aplicações de software	100
URLs para teste	Obrigatório(a)	URLs para teste	4000
Etapas para reproduzir	Obrigatório(a)	Etapas para reproduzir	1000
Detalhes técnicos	Obrigatório(a)	Detalhes técnicos	1000
Atribuição a	Obrigatório(a)	Atribuído a (indivíduo responsável por conduzir testes de invasão e gerar descobertas de segurança)	151
Grupo de atribuição	Obrigatório(a)	Grupo de atribuição (grupo responsável por conduzir testes de invasão e gerar descobertas de segurança)	151

Tradução automática

Carregue vulnerabilidades da aplicação usando um arquivo de modelo

Use um arquivo de modelo para carregar as vulnerabilidades da aplicação. Para acessar e baixar o modelo, navegue até **Tudo** > **Ingestão manual de AVIT** > **Carregar IU de arquivo**.

Antes de Iniciar

Função necessária: Ethical Hacker **sn_vul.app_pen_tester**

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Ingestão manual de AVIT** > **Carregar IU de arquivo**.
2. Selecione os links do Excel ou CSV e baixe o modelo no respectivo formato.
3. No modelo, insira os dados da vulnerabilidade nos registros.
   Para obter instruções sobre como preencher os dados no modelo, consulte a planilha "Exemplos" no modelo.
4. Selecione Importar arquivo e carregue o modelo atualizado.
5. Selecione Enviar.

   A página Filas de push de integração de vulnerabilidades é exibida. Você pode rastrear o status e exibir anotações de log relacionadas aos envios.

Nota: Para quaisquer erros que ocorram:

- Um **arquivo de log de erros** está anexado diretamente ao relacionado **Fila de push** registro.
- Adicional **detalhes do erro** também pode ser encontrado em **Anotações de log** Mesmo registro da Fila de push.
- Essa abordagem garante que os hackers éticos possam monitorar e solucionar problemas de seus envios sem precisar acessar detalhes mais profundos de integração no nível do sistema.

Verifique a execução da integração

Se a execução da integração for bem-sucedida, revise a contagem de detecções individuais e as descobertas do teste de invasão criadas ou atualizadas.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Ingestão manual de AVIT** > **Integrações**.
2. Selecione o nome da integração com base no tipo de arquivo carregado.
3. Selecione a guia Execuções de integração de vulnerabilidades.
4. Selecione o número de execução de integração.
5. Selecione a guia Itens.
   Revise as informações na guia Itens.

Resultado

Guia Itens

Guia/Campo	Descrição
Guia Itens	Exibe o número total de AVITs importados.
Novos itens	Exibe o número de itens vulneráveis à aplicação que são criados a partir desta execução de integração.
Itens importados	Exibe a soma de todos os campos nesta seção.
Itens duplicados	Exibe itens duplicados. Este campo não está mais preenchido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Itens

Guia/Campo	Descrição
Itens inalterados	Exibe itens vulneráveis à aplicação encontrados durante a execução da integração que existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Nota: Depois de confirmar a execução de integração bem-sucedida, rastreie o status do envio navegando até **Fila de push** registro. O registro da fila de push fornece os seguintes detalhes:

- **Anotações de log** : Consiste em informações de processamento de registro.
- **Arquivos de erro** : Consiste nos detalhes do erro ocorridos durante o envio.

Verifique o status do carregamento

Verifique se a execução da integração de vulnerabilidade foi bem-sucedida, parcialmente bem-sucedida ou uma falha.

Antes de Iniciar

Função necessária: sn_vul.app_pen_tester

Procedimento

1. Navegar até **Tudo** > **Ingestão manual de AVIT** > **Carregar histórico de arquivos**.
2. **Revise o status de carregamento** : Em **Filas de push de integração de vulnerabilidades da aplicação** Examine a coluna Criado para o carimbo de data/hora de carregamento e a coluna Estado para o status de carregamento.
3. **Opcional: Verifique o sucesso** : No campo Anotações, exiba a massagem de sucesso para garantir que todos os registros foram processados com sucesso.
4. **Tratamento de erros (falha/sucesso parcial)**
   - Para carregamentos com um estado "Falha" ou "Sucesso parcial", um arquivo de log de erros é gerado.
   - Os usuários administradores podem exibir este arquivo para entender os motivos da falha no carregamento.
   - Usuários com a função app_pen_tester podem exibir os registros da Fila de push e os detalhes de erro associados.
   - O arquivo de log de erros contém somente as descobertas que falharam no processamento, fornecendo informações específicas para correção e reingestão.
5. **Diretrizes de reingestão** :
   - Reingerir descobertas processadas com sucesso criará registros duplicados.
   - Para evitar duplicatas, reingira somente as descobertas listadas no arquivo de log de erros.

Correção Resposta a vulnerabilidades de aplicações vulnerabilidades

A correção de monitoramento é um processo que começa com a revisão do status e termina com o fechamento de itens vulneráveis à aplicação (AVITs). Resposta a vulnerabilidades de aplicações oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações processo de correção

A correção de item vulnerável da aplicação é feita manualmente.

Uma visão geral do processo:

- Faça login na sua instância Resposta a vulnerabilidades de aplicações.
- Valide se suas regras (Pesquisa de IC, Atribuição) para itens vulneráveis à aplicação estão funcionando conforme o esperado. Para obter informações sobre como revisar regras de pesquisa de IC, consulte Identificar aplicações em Resposta a vulnerabilidades de aplicações automaticamente. Para obter informações sobre regras de atribuição, consulte Atribua itens vulneráveis à aplicação em Resposta a vulnerabilidades de aplicações automaticamente.
- Valide se seus destinos de correção estão corretos. Consulte Automatizar o acompanhamento de destino de correção em Resposta a vulnerabilidades de aplicações para obter informações sobre como funcionam as regras de destino de correção e como revisá-las. Exiba o status de destino de correção de um item vulnerável à aplicação.

  Nota: As regras de destino de correção pertencem aos AVITs. Essas regras são executadas quando o AVIT é importado.

- Revise os painéis ou relatórios. Por exemplo, exiba painéis que mostram o envelhecimento dos AVITs por estados.

  Nota:

  . Performance Analytics para Resposta a vulnerabilidades A aplicação (com.snc.vulnerability.analytics) estiver ativada, os usuários com determinadas funções podem exibir dados de interesse dos membros dos grupos do Gerenciador da App-Sec e do Security Champion.

  Para gerentes da App-Sec, Performance Analytics para Resposta a vulnerabilidades contém o. Resposta a vulnerabilidades de aplicações Visão geral, que pode ajudar você a monitorar áreas de preocupação. Consulte Soluções de análise e emissão de relatórios para resposta a vulnerabilidades da aplicação e. Painel do Application Vulnerability Management [PA] .

  A partir da versão 13,0 do Resposta a vulnerabilidades Aplicação: Para Campeões de segurança, Performance Analytics para Resposta a vulnerabilidades Contém o painel Minhas vulnerabilidades da aplicação, que pode ajudar você a monitorar suas áreas de preocupação. Consulte Meu painel de vulnerabilidades da aplicação .

  A partir da versão 13,0 do Resposta a vulnerabilidades Aplicação: Para limitar a quantidade de dados coletados para relatórios ou listas relacionadas, consulte Defina classificações de serviço para Resposta a vulnerabilidades relatórios e listas relacionadas.

- Revise o estado dos AVITs, em ordem de prioridade, procurando o que mudou.
- Revise o risco dos AVITs, conforme necessário. Para obter mais informações, consulte Crie uma calculadora de vulnerabilidade da aplicação.
- Reatribua o AVIT a um grupo de atribuição para correção, se necessário.
- As novas varreduras são acionadas automaticamente pela programação de importação de terceiros.
- Se o estado for **Corrigido** AVITs são encerrados automaticamente durante a importação.
- Se o estado não for **Corrigido** O AVIT é reaberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obtenha mais detalhes de Veracode

Selecione **Obter mais detalhes** Itens vulneráveis à aplicação (AVITs) que têm Veracode Como a Origem na tabela Item vulnerável à aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir o seguinte Veracode dados.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- Solicitação de origem HTTP, Resposta de origem e Recomendações são exibidas na guia Detalhes na Resposta a vulnerabilidades Resposta a vulnerabilidades espaços de trabalho.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Exibir bibliotecas de vulnerabilidades

Você pode exibir dados de vulnerabilidade importados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou de terceiros para decidir se escalar uma tarefa de correção.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > para **Bibliotecas** .

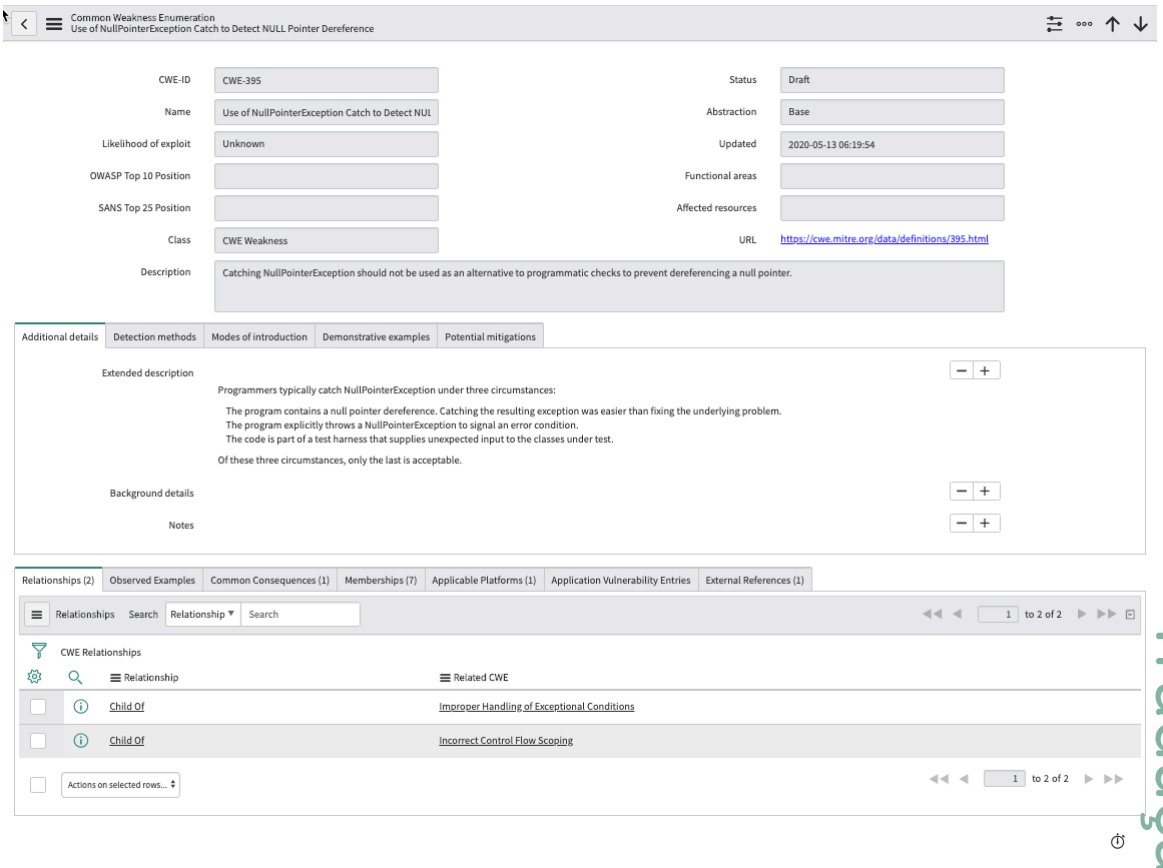
   As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, isso é apenas para referência.
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações, CVEs e CVEs.

2. Escolha uma biblioteca para exibir vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Para obter informações sobre campos específicos, consulte Campos Vulnerabilidade da aplicação.

Campos Vulnerabilidade da aplicação

As vulnerabilidades são criadas automaticamente quando os registros são baixados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou integrações de terceiros. NVD e CWE são armazenados em **Bibliotecas** em Resposta a vulnerabilidades ou abaixo **Vulnerabilidades** em Resposta a vulnerabilidades de aplicações.

Campos de entrada de vulnerabilidade do CWE

Os campos nesta tabela são somente leitura.

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para Categorias e Pontos fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.
Probabilidade de exploração	Qual a probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Baixo(a) • Média • Alto(a)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
10 principais posições da OWASP	Posição numérica desta vulnerabilidade na lista dos 10 principais OWASP.
Posição SANS para 25	Posição numérica desta vulnerabilidade na lista dos 25 principais SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho • Estável • Preterido • Obsoleto • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualização em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivo** . Preenchido somente para 24/862 pontos fracos.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório** . Preenchido somente para 51/863 pontos fracos.
URL	artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.
Execução de integração	A execução de integração na qual este CWE foi importado.
Seções	
Detalhes adicionais	Descrições de conceito de software que explicam melhor o ponto fraco. Inclui: • Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que a fraqueza é introduzida, por exemplo, **Implementação** , **Arquitetura e Design** e assim por diante.
Exemplos demonstrativos	Exemplos de código do ponto fraco com descrições de acompanhamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Mitigações potenciais	Detalhes sobre como evitar a fraqueza, incluindo em qual fase do ciclo de vida da aplicação ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/antecede, requiredby/requer (para pontos fracos compostos), CanAlsoBe, PeerOf, MemberOf.
Exemplos observados	Alguns CVEs que são representativos desta fraqueza.
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: Confidencialidade Impacto: Ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Campos de entrada de vulnerabilidade da aplicação

Os campos nesta tabela são somente leitura.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Origem	Origem da vulnerabilidade - seja um scanner ou teste físico.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de gravidade, consulte Mapeie a gravidade de um item vulnerável à aplicação automaticamente.
Versão 13,0: CWE primário Versão 12,1: Entrada de CWE	Referência ao elemento de enumeração de pontos fracos comuns ao qual esta vulnerabilidade se encaixa melhor. Se houver mais de um CWE associado à vulnerabilidade, o CWE primário será determinado da seguinte forma: • É o CWE mapeado para os 10 principais OWASP. Em caso afirmativo, use este CWE. Caso contrário, continue. • O CWE é mapeado para as 25 principais SANs? Em caso afirmativo, use este CWE. Caso contrário, continue.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• O CWE tem a severidade mais alta? Em caso afirmativo, use este CWE. Caso contrário, continue. • Selecione o mais recente de todos os CWEs. O CWE mais recente é aquele com o mais recente **Atualizado** Valor do campo no registro CWE.
Nome da categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Detalhes da Vulnerabilidade	
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas que podem ser executadas para mitigar a vulnerabilidade.
Lista relacionada	
Versão 13,0: CWEs	Lista de CWEs associados a esta vulnerabilidade. Não aplicável para Integração de Resposta a vulnerabilidades com Veracode.

Campos de entrada de NVD

Os campos importados nesta tabela são somente leitura.

Nota:

Os dados de NVD não são usados em Resposta a vulnerabilidades de aplicações e as entradas representam Resposta a vulnerabilidades somente dados.

CWEs, que são usados em Resposta a vulnerabilidades de aplicações Podem apontar para entradas de NVD, como exemplos de um ponto fraco, e são fornecidos aqui apenas para fins informativos.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Classificação de risco	(Oculto quando não Resposta a vulnerabilidades Itens vulneráveis (VIS) estão associados à vulnerabilidade) Quantificado **Pontuação de risco** Separando VIS em Crítico, Alto, Médio, Baixo e Nenhum.
Pontuação de risco	(Oculto quando nenhum VIS está associado à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade em Resposta a vulnerabilidades. Os mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Resposta a vulnerabilidades de aplicações **Gravidade** derivado de importado **Gravidade da origem** E não NVD. Para obter informações sobre Resposta a vulnerabilidades de aplicações mapeamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de gravidade, consulte Mapeie a gravidade de um item vulnerável à aplicação automaticamente.
Exploração presente	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Nível de habilidade da exploração	O nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque da exploração	Vetor de ataque mais vulnerável das explorações desta vulnerabilidade.
IVs ativos	(Oculto quando nenhum VIS está associado à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado. Se não houver nenhum Avis ativo para esta vulnerabilidade, **Classificação de risco** e. **Pontuação de risco** não são exibidos.
Entrada de CWE	Referência ao elemento de enumeração de pontos fracos comuns em que esta vulnerabilidade se encaixa melhor de acordo com o NVD.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando nenhum VIS está associado à vulnerabilidade) Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Status da Correção (Oculto quando nenhum VIS está associado à vulnerabilidade)	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis à aplicação ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
%Vis corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
V13.0: Forçar importação de vulnerabilidades de software **Nota:** Removido na v13.0	(Descontinuado) Recalcula o mapeamento de produto com Gestão de ativos de software do ITSM Com base nas informações do NVD. Atualiza a biblioteca de software vulnerável.
Atualizar status	Exibe data e hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação de risco e classificação • Métricas como VIS ativo, total de VIS da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando nenhum VIS está associado à vulnerabilidade) Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.
Soluções	(Oculto quando nenhum VIS está associado à vulnerabilidade) Todos Solução de gestão de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Versão 13,0: Pontos fracos	Dados de fraqueza do CWE importados associados a vulnerabilidades e exposições comuns (CVE).
Versão 13,0: Software Vulnerável	(Oculto quando nenhum VIS está associado à vulnerabilidade) Dados de enumeração de plataforma comum (CPE) importados associados à vulnerabilidade.

Identificar aplicações em Resposta a vulnerabilidades de aplicações automaticamente

Quando os dados são importados de uma integração de terceiros, Resposta a vulnerabilidades de aplicações usa automaticamente dados da aplicação para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras identificam aplicações para o registro de item vulnerável à aplicação (AVI) para ajudar na correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

À medida que as aplicações são importadas, uma pesquisa é realizada na aplicação verificada [sn_vul_app_scan_application] t capaz de usar source_app_id e app_name para encontrar correspondências com aplicações de importações anteriores. Quando uma correspondência de ID da aplicação é encontrada, seus valores são usados em **Aplicação** e. **Versão da aplicação** campos no registro de item vulnerável da aplicação.

Se uma correspondência não for encontrada ou o campo ID da aplicação estiver vazio, as regras usarão as outras informações da aplicação para tentar identificar corretamente a aplicação. Se uma correspondência ainda não for encontrada, um registro de aplicação verificado de espaço reservado será criado somente com **Nome da aplicação** e. **ID da aplicação** campos.

. **ID da aplicação de origem** e. **Nome da aplicação** as regras de pesquisa são enviadas com Integração de Resposta a vulnerabilidades com Veracode, por padrão.

Nota: Regras de pesquisa de IC padrão para Resposta a vulnerabilidades de aplicações estão disponíveis somente para Veracode Integração de vulnerabilidades.

Ao tentar uma correspondência, as regras de pesquisa são avaliadas pelo mais baixo **Pedido** valor primeiro. Eles param quando uma regra retorna um único IC como correspondência.

Nota: Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Para facilitar a localização de problemas correspondentes, quando uma correspondência é encontrada, a regra de pesquisa de IC usada para localizá-la é adicionada ao **Regra de correspondência de IC** Campo para aplicações verificadas. Clique na engrenagem Atualizar lista personalizada Ícone na parte superior da exibição da lista de aplicações verificadas para adicioná-lo à exibição.

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

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações se houver suporte. Por exemplo, o. Veracode Integração de vulnerabilidades, pode ter várias implantações do Veracode Integração de vulnerabilidades. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

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

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

Tópicos relacionados

Gestão de configuração e o CMDB

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma regra de pesquisa de IC

. **Regras de pesquisa de IC** o módulo contém regras que definem quais campos têm dados correspondentes em Configuration Management Database (CMDB). Essas regras são usadas para identificar aplicações e versões de aplicações e adicioná-las ao registro de item vulnerável à aplicação (AVI) para ajudar na correção.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Criar regras de pesquisa de IC requer avançado ServiceNow e. Gestão de vulnerabilidades de aplicações experiência. Em vez de modificar uma das regras de pesquisa existentes, considere copiá-la e modificar a cópia. Quando você estiver satisfeito com que a nova regra faz o que você deseja, desative o original.

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

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Regras de pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ○ **Script** Script pré-criado ou personalizado. ○ **Correspondência de campo** : Pesquisa na tabela ou campo no CMDB.
Tipo	Tipo usado com o Script **Método de pesquisa** .
Ordem	Ordem de precedência da regra. Correspondências com a ordem mais baixa são avaliadas primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Origem	Origem usada como entrada para esta regra. Uma vez escolhidos, os filtros de condição são exibidos.
Campo de origem	Campo de origem usado como entrada para esta regra. Os campos devem ser uma cadeia de caracteres ou um número.
Descrição	Texto que descreve a regra.
V19.0: Destino de pesquisa	Abordagem de pesquisa que você deseja seguir. Selecione entre: ○ Item de configuração ○ Modelo do produto
Script	Script de amostra editável, com base em **Tipo** é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão.

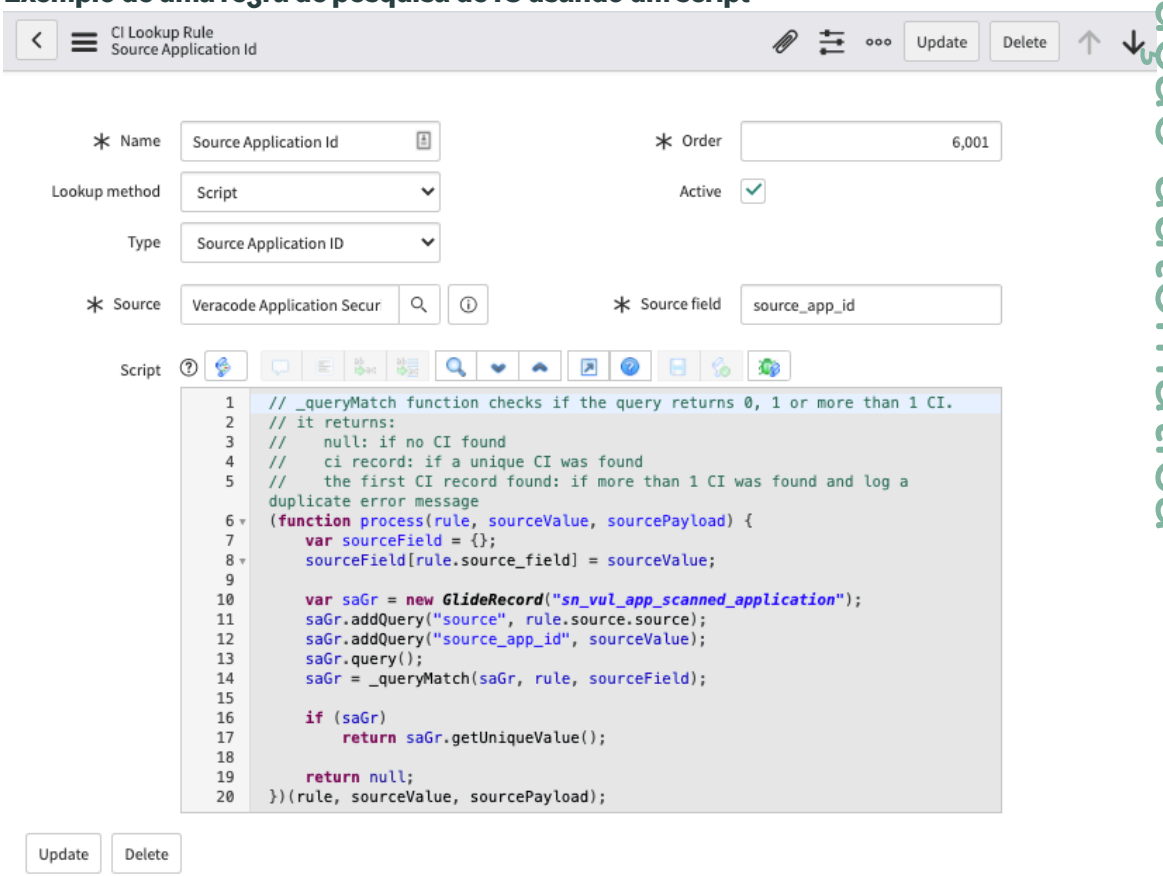
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A função de processo tem três parâmetros: `rule`, `sourceValue`e `sourcePayload`
Pesquisar em IC tabela	Tabela para pesquisar no CMDB. Usado com correspondência de campo **Método de pesquisa** .
V19.0: Pesquisa na tabela de produtos	Se você escolher o Modelo do produto **Destino de pesquisa** , O valor padrão é Modelo de aplicação.
Pesquisar em IC campo	Campo que contém informações que podem ser usadas para localizar um IC. Usado com a correspondência de campo **Método de pesquisa** . Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.
V19.0: Pesquisa no campo de modelo do produto	Se você escolher o Modelo do produto **Destino de pesquisa** , O valor padrão é Nome.

4. Clique em **Enviar**.

Exemplo de uma regra de pesquisa de IC usando um script



Tópicos relacionados

Campos de Item vulnerável da aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reaplicando regras de Pesquisa de IC em Resposta a vulnerabilidades de aplicações

Você pode reaplicar suas regras de pesquisa de item de configuração (IC) para atualizar ICs existentes (aplicações verificadas e modelos de produto) nos registros de aplicações descobertas.

Reaplicando uma regra de pesquisa

"Reaplicar regras de pesquisa" para itens selecionados ou filtrados na tabela Aplicações descobertas.

Se nenhum filtro for aplicado, a opção Reaplicar será desabilitada. Depois de reaplicar, os usuários podem receber um URL de trabalho em segundo plano ou uma mensagem de erro se a integração estiver em execução.

Para reaplicar as regras às aplicações descobertas existentes, navegue até **Tudo** > **Operações de segurança** > **CMDB** > **Regras de pesquisa**.

Nota: A partir da v25.0.3 de Resposta a vulnerabilidades de aplicações Uma nova regra de fechamento automático "IC desativado" é introduzida para fechar os itens vulneráveis e as detecções relacionadas a ICs desativados.

Definir o destino da pesquisa

Por padrão, o *sn_vul.use_product_model*a propriedade do sistema está ativada (definida como **verdadeiro**). Dependendo de como a propriedade do sistema é definida nos registros de regra de pesquisa de IC, os registros da aplicação descobertos são atualizados da seguinte maneira:

- Se o campo Valor estiver definido como **verdadeiro** , O modelo de produto é o destino de pesquisa das regras de pesquisa de IC e as aplicações descobertas são atualizadas com os modelos de produto.
- Se o campo Valor estiver definido como **falso** Item de configuração (aplicativos verificados) é o destino de pesquisa e as aplicações descobertas são atualizadas com os Itens de configuração (aplicações verificadas).

Para modificar *sn_vul.use_product_model*propriedade do sistema para que os itens de configuração sejam usados como destino:

1. Como um usuário com a função sn_vul.app_sec_manager, navegue até **Tudo** > **Propriedades do sistema** > **Tudo**
2. Localizar *sn_vul.use_product_model*.
3. Abra o registro.
4. Defina o campo Tipo como **falso** .
5. Selecione **Atualizar**.

Se você redefinir esta propriedade do sistema, deverá modificar suas regras para que os destinos de pesquisa correspondam à configuração da propriedade do sistema. Por exemplo, se você redefinir a propriedade do sistema para usar o item de configuração como destino, localize as regras que têm o destino de pesquisa como item de configuração.

1. Marque a caixa de seleção Ativo para essas regras e selecione **Atualização** .
2. Localize as regras que usam o modelo de produto como destino e desative-as desmarcando a caixa de seleção Ativo e marcando **Atualização** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você estiver criando uma nova regra de pesquisa, defina o destino de pesquisa para a regra no formulário de regra. Para obter mais informações, consulte Crie uma regra de pesquisa de IC.

Impedir registros duplicados ou órfãos após executar as regras de pesquisa de IC de resposta a vulnerabilidades da aplicação

Tome medidas para impedir registros duplicados ou órfãos resultantes da correspondência de itens de configuração (ICs) em CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em tempos de processamento longos. Testes e depuração completos de scripts de processamento nas regras ajudam a aliviar o potencial de problemas posteriormente no processo.

Evitando registros duplicados ou órfãos

- Use pequenos subconjuntos de dados específicos para a regra de pesquisa de IC que está sendo testada.
  - Definir tudo **Regras de pesquisa de IC** , diferente do que está sendo testado, para **Inativo** .
  - Analise as aplicações importadas e os itens de configuração (ICs) para garantir que você esteja observando o comportamento esperado e a correspondência esteja ocorrendo corretamente.
- Revise estados de IC, como **Descontinuado** .
- Remover dados de teste. Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, comece novamente. Isso pode ser feito por:
  - Excluindo os dados usados para testes: (Consulte **Excluindo dados de tabelas**)
    - Aplicações verificadas
    - Itens vulneráveis à aplicação (Avis)
  - Execute novamente as integrações manualmente.

.

Excluindo dados de tabelas

Às vezes, você importou dados e percebe que algo está errado. Se isso acontecer em um ambiente de desenvolvimento ou desempenho, você poderá clonar novamente de um ambiente melhor, mas isso nem sempre é uma opção.

Nota: Executar essas ações requer avançado ServiceNow experiência.

Há quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** ativado **Configuração da tabela** .
- Configure o. **Limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo **Limpeza automática** registro.
- Trunque gs.truncateTable usando um script em segundo plano.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Nunca use `truncateTable` em um ambiente de produção. Consulte o representante de suporte antes de executar exclusões grandes em ambientes de produção ou compartilhados.

- Crie uma solicitação no HI para excluir os dados.

Atribua itens vulneráveis à aplicação em Resposta a vulnerabilidades de aplicações automaticamente

Atribua automaticamente vulnerabilidades da aplicação com base em marcadores da aplicação ou em qualquer um dos grupos de atribuição no Item de configuração [cmdb_ci] ou nos grupos de atribuição da plataforma para reduzir o tempo médio de atribuição.

Atribuir itens vulneráveis à aplicação automaticamente

Há três maneiras diferentes de atribuir Avis usando **Atribuir usando** :

Nota: O recurso de recomendação de atribuição em Resposta a vulnerabilidades não está disponível para Resposta a vulnerabilidades de aplicações.

- Grupo de usuários: Esta opção permite selecionar qualquer um dos existentes ServiceNow AI Platform® grupos de usuários.
- Campo de grupo de usuários: Esta opção permite que você escolha qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir no menu de lista em **Campo Grupo de usuários** .
  - Nenhum: Indica nenhum valor padrão para este campo obrigatório
  - Item de configuração: Grupo de aprovação
  - Item de configuração: Grupo de atribuição
  - Item de configuração: Grupo de suporte
- Script: Esta opção permite definir as condições usando um script. Esta opção requer codificação ou avançado ServiceNow experiência.

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

Processo de avaliação da regra de atribuição

Quando um novo AVI é criado, importado ou reaberto após ser encerrado, as regras de atribuição são avaliadas em relação a ele. Um AVI só é avaliado uma vez, a menos que seja reaberto após ser encerrado. Você pode reaplicar regras manualmente após as mudanças.

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

- Para cada regra de atribuição de vulnerabilidade, o AVI é comparado ao filtro de atribuição, regra de ordem mais baixa primeiro.
- Quando a condição corresponde, o AVI é atribuído a um grupo de atribuição. A pesquisa é interrompida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando as condições não encontrarem uma correspondência entre todas as outras regras, o AVI será atribuído ao grupo de atribuição padrão, se houver uma regra padrão.

Nota: Se não houver regra padrão, o AVI permanecerá sem atribuição.

Tipo de atribuição se **Manual** ou **Regra** e. **Regra de atribuição** Está disponível no slushbucket de layout do formulário no formulário de item vulnerável à aplicação (AVI). Qualquer AVI que foi originalmente atribuído por uma regra, mas posteriormente reatribuído manualmente contém uma referência à regra original. Usar **Regra de atribuição** e. **Tipo de atribuição** informações para identificar casos em que as regras de atribuição não encontraram uma correspondência correta para o destinatário pretendido. Ou quais regras tiveram mais reatribuições.

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

Reaplicar regras de atribuição

Ao alterar uma regra de atribuição, use **Aplicar mudanças** Botão na exibição de lista Regras de atribuição para executar novamente todas as regras alteradas em todos os Avis abertos ativos (exceto aqueles que foram atribuídos manualmente).

Nota:

. *`Reapply all vulnerability assignment rules`*o trabalho agendado não foi executado antes do primeiro uso **Aplicar mudanças** , Em seguida, ele executa todas as regras de atribuição em todos os AVIS abertos, exceto aqueles que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** execute novamente somente as regras alteradas e todas as regras dependentes. Mudanças em uma regra podem resultar em um AVI correspondente a uma regra não modificada diferente.

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

Criar ou editar Resposta a vulnerabilidades de aplicações regras de atribuição

Você pode criar regras para atribuir automaticamente itens vulneráveis à aplicação (Avis) com base nas condições de filtro. Essas regras atribuem Avis conforme são importadas ou criadas manualmente.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Com as regras de atribuição, você define a condição de atribuição e a ordem de execução. Quando um AVI corresponde a uma condição de regra, a pesquisa de atribuição é interrompida. Para obter mais informações, consulte Filtrando em Gestão de vulnerabilidades de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de atribuição**.
2. Clique em **Nova**.
3. Se **Novo** preencha os campos no formulário, conforme apropriado.

Regra de atribuição de vulnerabilidades da aplicação

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, em que o risco é crítico ou um AVI deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde não há manipulação especial r e você sabe quem deve ser responsável por eles. Por fim, crie uma regra padrão para atribuir Avis ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Descrição	Descrição da regra de atribuição.
Condição	
Campos de condição	Condições que devem ser atendidas.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ○ Grupo de usuários: Selecione um grupo de usuários na tabela de pesquisa. ○ Campo de grupo de usuários: Selecione um campo de grupo de usuários no menu de lista. ○ Script: Crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow experiência.

4. Clique em **Enviar**.
   Regras novas ou atualizadas são avaliadas na próxima importação.

Removendo atribuições de Resposta a vulnerabilidades de aplicações itens vulneráveis e tarefas de correção

Você pode limpar **Atribuído a.** e. **Grupo de atribuição** campos em Resposta a vulnerabilidades de aplicações itens vulneráveis diretamente dos registros de item vulnerável da aplicação e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tarefa de correção que você determina que podem estar atribuídos incorretamente a você ou aos seus grupos.

Visão geral do fluxo de trabalho

Se você determinar isso Resposta a vulnerabilidades de aplicações Itens vulneráveis (AVITs) e tarefas de correção (AVULs) não estão dentro do seu escopo de correção ou, se você acha que registros foram atribuídos incorretamente a você ou aos seus grupos, você pode remover a si mesmo ou aos seus grupos do **Atribuído a.** e. **Grupo de atribuição** Campos nos registros AVIT e AVUL.

O fluxo de trabalho Cancelar atribuição é compatível com as exibições clássica e de espaço para AVITs e AVULs.

Você tem a opção de enviar solicitações para limpar os campos de atribuição para aprovação. Para obter mais informações, consulte Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades.

- . **Cancelar atribuição** O botão é exibido nos registros AVIT e AVUL em qualquer estado diferente de Encerrado ou Resolvido.
- Depois que a solicitação para limpar os campos for aprovada, todos os **Atribuído a.** e. **Grupo de atribuição** Os campos nos AVITs que estão associados a um AVUL que têm o mesmo grupo de atribuição também não são atribuídos. Se algum item vulnerável à aplicação tiver um grupo de atribuição diferente da tarefa de correção associada, ele não será desatribuído. Na maioria dos casos, esses itens vulneráveis à aplicação foram atribuídos manualmente. Para obter mais informações, consulte Removendo atribuições de itens vulneráveis e tarefas de correção.
- Todos os registros que você atualizar com a ação de IU ou manualmente serão exibidos no módulo Não atribuído para Resposta a vulnerabilidades de aplicações.
- Você pode limpar os campos de atribuição de vários AVITs em uma lista. Depois de selecionar os AVITs e selecione **Edição em massa** na caixa de diálogo exibida, selecione **Cancelar atribuição** caixa de seleção.

Consulte Remova atribuições de itens vulneráveis e tarefas de correção para obter mais informações sobre as etapas de como limpar os campos de atribuição.

Propriedades do sistema e notificações de aprovação

Se um responsável pela correção selecionar **Cancelar atribuição** Em um registro, por padrão, a propriedade do sistema sn_vul.unassign_vr.approval_required aciona o fluxo de aprovação e cria um registro de aprovação de mudança de estado no estado Revisão, e a solicitação é roteada para aprovação. A solicitação é exibida na lista Minhas aprovações para usuários com sn_vul_.unassign_approver.

Nota: Como administrador de vulnerabilidades [sn_vul.vulnerability_admin], você pode definir *sn_vul.unassign_vr.approval_required*propriedade do sistema para **falso** para desabilitar o processo de aprovação.

Além disso, você pode alterar o valor em *sn_vul.default_assignment_group*portanto, se os campos de atribuição estiverem limpos, um grupo específico será atribuído. Por exemplo, se um usuário clicar **Cancelar atribuição** Em um registro e você deseja redirecioná-lo para um grupo específico para revisão, você pode adicionar o ID do sistema para o grupo de sua escolha no campo Valor da propriedade do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Consulte Removendo atribuições de itens vulneráveis e tarefas de correção para obter mais informações sobre como alterar as propriedades do sistema.

Calcule o risco em Resposta a vulnerabilidades de aplicações automaticamente

As calculadoras de vulnerabilidade da aplicação automatizam o cálculo dos valores de risco iniciais para os campos em Itens vulneráveis à aplicação (Avis). Os cálculos de risco oferecem informações sobre como priorizar a correção. Cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Calculadoras de vulnerabilidades da aplicação

. Resposta a vulnerabilidades de aplicações o sistema de base inclui duas calculadoras de vulnerabilidade que definem a base **Pontuação de risco** no item vulnerável da aplicação.

- **Calculadora de risco básico**
- **Calculadora do Risco avançado**

Calculadoras de vulnerabilidade da aplicação podem ser criadas para priorizar e classificar o impacto do AVIS com base em qualquer critério usando filtros de condição. Seja o impacto comercial da vulnerabilidade, a classe do item de configuração (IC) ou a idade do AVI, você pode criar calculadoras de vulnerabilidade adicionais para definir outros campos no AVIS. Ou você pode personalizar as calculadoras de vulnerabilidade existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades. Para obter mais informações, consulte Filtrando em Gestão de vulnerabilidades de aplicações.

Os Avis contêm **Pontuação de risco** valor derivado das calculadoras de risco.

Nota: Um AVI é exibido **Gravidade da origem** gravidade normalizada. A gravidade normalizada é usada pelas calculadoras para obter o. **Pontuação de risco** Valor, mas não é mostrado na Avis.

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

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um AVI é criado, quando um IC associado ou uma vulnerabilidade muda.

. **Risco básico** a calculadora calcula **Pontuação de risco** Para AVIS usando a severidade da vulnerabilidade normalizada.

Nota: Apenas uma calculadora por campo de destino (**Pontuação de risco**) pode estar ativo por vez.

. **Risco básico** está habilitado por padrão. . **Calculadora avançada de risco** está inativo por padrão.

Regras da calculadora de vulnerabilidades da aplicação

O sistema de base **Calculadora básica de risco** A calculadora contém regras de calculadora que atribuem a cada nível de gravidade (Nenhum a Crítico) um valor (0-100) para **Pontuação de risco** com base na gravidade. **Gravidade desconhecida** é atribuída automaticamente uma pontuação de risco de 100. Esses valores podem ser ajustados e,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

como **Calculadora avançada de risco** novas regras de calculadora ou novas regras de risco podem ser criadas.

Nota: A partir da v23.0 de Resposta a vulnerabilidades de aplicações Sempre que a pontuação de risco é atualizada em um AVIT, o. **Anotações** a seção é atualizada com os seguintes detalhes:

- Nome do grupo de calculadora
- Nome da calculadora: Dependendo se a regra da calculadora é baseada em um modelo ou script, o nome é anexado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e selecione **Exibição avançada** caixa de seleção. Em **Tipo de valor** caixa suspensa, selecione a opção necessária. Se **Modelo** selecionado, a pontuação de risco é atualizada de acordo com a condição especificada na regra. Se **Script** selecionado, você pode adicionar ou atualizar o script existente. A propriedade do sistema *sn_sec_cmn.risk_score_changes_add_worknotes*Ajuda a preencher a seção de anotações de trabalho. A partir da v25.0.3 de Resposta a vulnerabilidades de aplicações, a propriedade do sistema *sn_sec_cmn.risk_score_changes_add_worknotes*está inativo por padrão. Somente se você habilitá-lo, poderá ver todas as mudanças relacionadas à pontuação de risco de um item vulnerável à aplicação na seção Anotações de trabalho. Além disso, as anotações de trabalho serão atualizadas somente se houver uma mudança na pontuação de risco.

O sistema de base **Calculadora avançada de risco** a calculadora contém uma regra de calculadora de vulnerabilidade especializada chamada **Regra de risco padrão** . Calcula **Pontuação de risco** com base em vários valores:

- Gravidade da vulnerabilidade
- 10 principais da OWASP
- 25 principais da SANS

Você pode personalizar os critérios da regra de risco padrão. Para obter mais informações, consulte Defina campos e pesos para a regra de risco.

Você pode ajustar os valores a serem usados no **Regra de risco padrão** e quanto peso dar a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir **Pontuação de risco** .

Cada regra tem um **Pedido** no entanto, o primeiro a corresponder às condições atualiza o. **Pontuação de risco** Campo no AVI. As regras da calculadora sem script normalmente criam menos impacto no desempenho do que as regras da calculadora com script.

Pesos da pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação de risco e classificação com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *Update Risk Rating from Risk Score*na tabela de item vulnerável é responsável por calcular a classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Versão 17,1 do Resposta a vulnerabilidades(VR), as seguintes classificações de risco foram fornecidas como parte da inclusão de script VulnerabilityUtils , que foram codificados.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

A partir da versão 18,0 do Resposta a vulnerabilidades,

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

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

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

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

Defina campos e pesos para a regra de risco

Personalize os parâmetros e os pesos da regra de risco para que você possa gerar pontuações de risco que usam a vulnerabilidade e os dados de ativos exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vul.app_manage_risk_score_configuration

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Calculadoras de Vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidades, clique em **Calculadora avançada de risco** .
3. Navegar até **Página Calculadora de vulnerabilidades** > **Guia Regras da calculadora de vulnerabilidades** > **Regra de Risco Padrão**.
4. **Opcional:** Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo da pontuação de risco geral.
5. Para desativar a regra, você deve limpar **Ativo** caixa de seleção.
6. Para adicionar campos de regra de risco aos critérios da calculadora de risco, clique em **Adicionar critérios** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir a ponderação da pontuação de risco. Você pode selecionar uma destas opções: ○ **Item vulnerável à aplicação** : Adicione campos que são diretamente passíveis de observação com pontos do item vulnerável (VI). ○ **Item vulnerável da aplicação - Item de configuração** : Adicione campos caminháveis com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci). ○ **Item vulnerável da aplicação - Vulnerabilidade** : Adicione campos passíveis de observação com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, entrada de terceiros. Esses campos não fazem parte da tabela base de Entrada de vulnerabilidades. ○ **Tabela de referência de item vulnerável da aplicação** : Adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Tabela de referência do item de configuração** : Adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Tabela de referência de vulnerabilidade** : Adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos não podem ser visitados diretamente com pontos do VI ○ **Condições personalizadas** : Use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ○ **Item vulnerável da aplicação -> Item de configuração** ○ **Item vulnerável da aplicação -> Vulnerabilidade** ○ **Tabela de referência do item vulnerável da aplicação** ○ **Tabela de referência do item de configuração** ○ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada na tabela Escolher referência. Selecione o valor mínimo ou máximo a ser considerado para cálculos quando Campo for selecionado nas tabelas relacionadas (m2m).
Peso	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Defina Valor ponderado	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1 a 5). Os pesos devem ser inteiros entre 0 e 100. **Nota:** Este campo não aparecerá se a opção Condições personalizadas estiver selecionada na tabela Escolher referência.
Tabela de condição	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Insira um nome para os critérios de risco.
Condição	Campo que aparece somente quando Condições personalizadas é selecionado na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Clique em **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

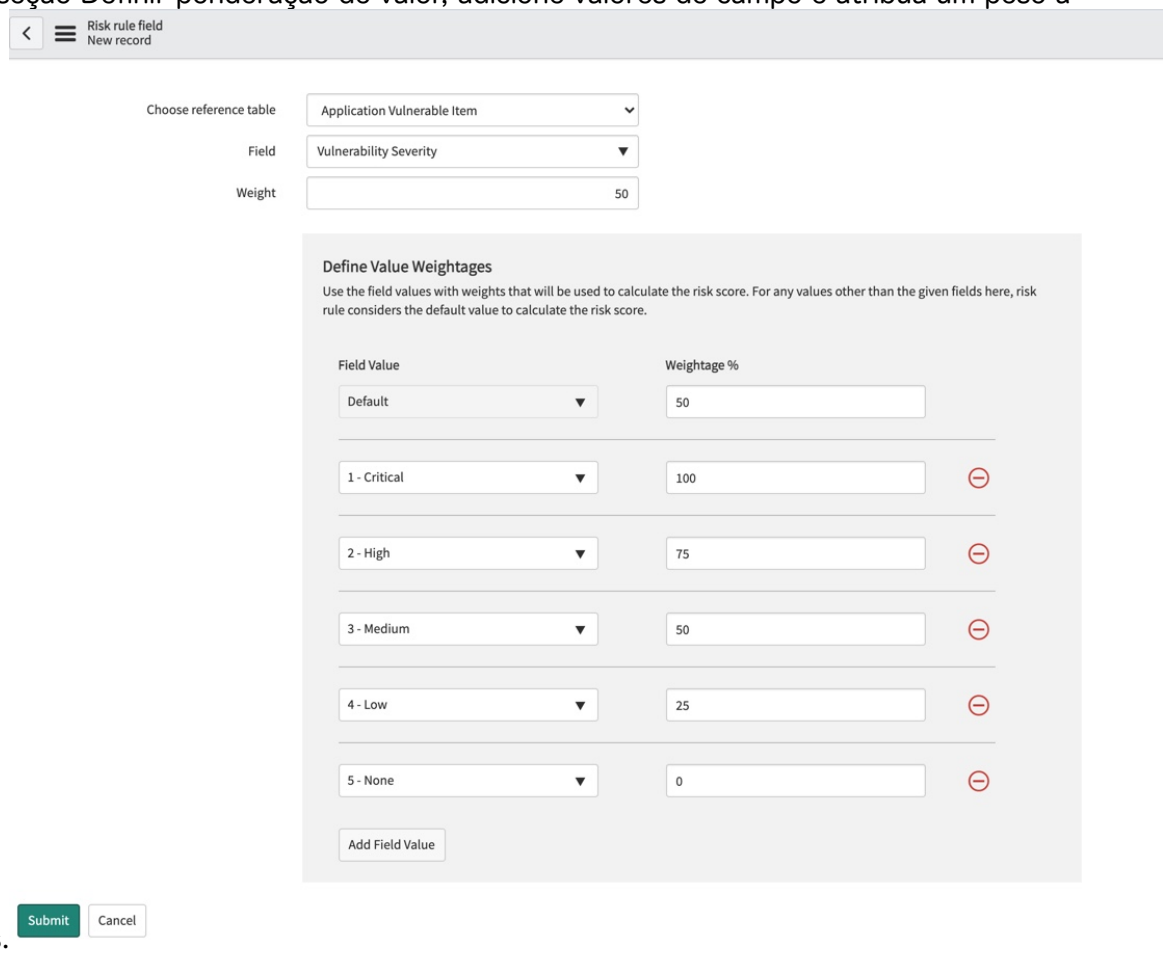
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Adicione a gravidade de origem como um critério para uma regra de risco.

Caso de uso: Fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas em **Gravidade da origem** campo na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, limpe **Ativo** caixa de seleção.
3. Para adicionar campos de regra de risco aos critérios da calculadora de risco, clique em **Adicionar critérios** .
4. Na lista Escolher tabela de referência, selecione **Item vulnerável à aplicação** .
5. Na lista Campo, selecione **Severidade.Vulnerabilidade** .
6. Em **Peso** insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
7. Na seção Definir ponderação de valor, adicione valores de campo e atribua um peso a eles.



8. Clique em **Enviar**.

Tópicos relacionados

Calculadoras de resposta a vulnerabilidades e regras da calculadora de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma calculadora de vulnerabilidade da aplicação

Uma calculadora de vulnerabilidade da aplicação é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. Calculadoras, que calculam o item vulnerável à aplicação (AVI) **Pontuação de risco** , pode conter **Regras de risco** . Os cálculos de risco oferecem informações sobre como priorizar a correção.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Nota: Você pode notar degradação no desempenho ao executar calculadoras de vulnerabilidade da aplicação que contêm scripts.

Ordene suas regras para executar as regras mais simples primeiro. Execute scripts somente nos itens que não podem ser manipulados com um valor de condição e modelo ou uma regra de risco.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Calculadoras de Vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Formulário da calculadora de vulnerabilidades

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidades da aplicação.
Tabela	Preenchido automaticamente com o nome da tabela AVI.
Aplicação	Preenchido automaticamente com Resposta a vulnerabilidades.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Ligar ou desligar a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar** .
. **Regras da Calculadora de vulnerabilidades** a seção é exibida.
5. Clique em para criar uma regra para a calculadora **Novo** .

Nota: Para **Novas Regras de Risco** (disponível somente quando **Campo de destino** . **Pontuação de risco** consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da calculadora de vulnerabilidades

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual executar a calculadora de vulnerabilidades. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionado, as condições de script e os valores de script podem ser selecionados **Tipo de condição** e. **Tipo de valor** .

7. Preencha os campos em **Quando esta condição é atendida** , conforme apropriado.

Quando esta condição é atendida

Campo	Descrição
Tipo de condição	Disponível quando você seleciona **Exibição avançada** . As opções incluem: ○ Filtro: Usa condições de filtro. ○ Grupo de filtros: Consulte criar e definir grupos de filtros para definir os critérios da calculadora. ○ Script: Condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne ao **Calculadoras de vulnerabilidades da aplicação** lista. Explore os registros da calculadora de vulnerabilidades enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. Selecionando **Grupo de filtros** ou **Script** tipos de condição, oculta este campo.

8. Clique em **Defina esses valores** e preencha os campos no formulário, conforme apropriado.

Defina a guia estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona **Exibição avançada** . As opções incluem: ○ Modelo: Defina os valores a serem definidos em cada campo. ○ Script: Usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou **Script** tipo de valor. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora. Selecionando **Script** tipo de valor, oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar **Reaplicar Calculadora** botão. Ele é executado em todos os Avis ativos e, se essa calculadora for usada para definir seu valor, recalcula o valor desses Avis. Reaplicar uma calculadora pode levar muito tempo, um trabalho agendado lida com isso.

10. Para **Novas Regras de Risco** preencha os campos conforme apropriado.

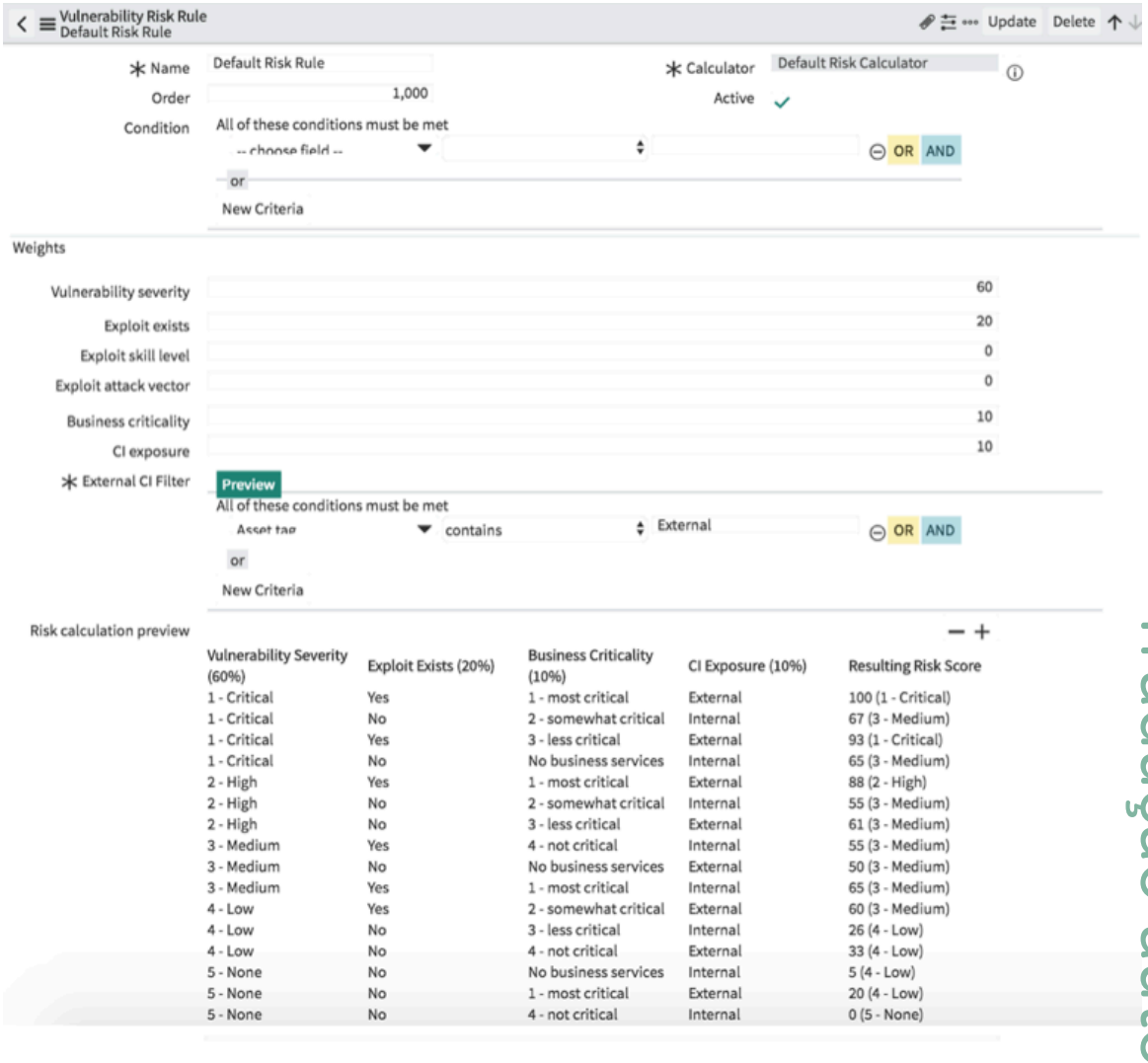
Defina cada ponderação de acordo com a porcentagem do resultado que deve vir desse valor. Para quaisquer dados que o scanner não forneça ou dados que não devem fazer parte da pontuação de risco, defina o peso como zero.

Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os previstos **Pontuação de risco** resultados.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. Selecionando **Grupo de filtros** ou **Script** tipos de condição, oculta este campo.
Pesos	
Severidade da Vulnerabilidade	Percentual do resultado que vem da gravidade.
10 principais da OWASP	Porcentagem do resultado que vem da presença da vulnerabilidade na lista dos 10 principais do OWASP. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
25 principais da SANS	Percentual do resultado que vem da presença da vulnerabilidade na lista das 25 principais SANS. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Total da execução	Totais percentuais calculados automaticamente. Quando esse valor atinge 100, a visualização do cenário mostra pontuações de risco de amostra em diferentes cenários.
Cenários de exemplo	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Clique em **Enviar**.

Mapeie a gravidade de um item vulnerável à aplicação automaticamente

Resposta a vulnerabilidades de aplicações o mapeamento de gravidade transforma campos de gravidade de origem de terceiros em campos reconhecíveis no Resposta a vulnerabilidades.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades de aplicações integrações de terceiros, como Integração de Resposta a vulnerabilidades com Veracode forneça mapeamentos de gravidade na instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Criar ou editar um mapa de severidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente e requer Resposta a vulnerabilidades de aplicações e. ServiceNow experiência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Mapeamento de gravidade normalizado**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de gravidade.
Valor de origem	O valor da gravidade da origem.
Valor de meta	O valor da severidade de destino. As opções são: ○ 1- Crítica ○ 2 - Alta ○ 3 – Médio ○ 4 - Baixo(a) ○ 5 - Nenhum

4. Repita a Etapa 3 para cada nível de gravidade de origem.
5. Clique em **Enviar**.

Filtrando em Gestão de vulnerabilidades de aplicações

Calculadoras e Regras de atribuição usam condições durante a importação, criadas usando o. **construtor de condições** . As mudanças em seus critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

As regras e calculadoras fornecidas com o sistema de base são otimizadas para desempenho. Editar ou criar regras ou calculadoras toma cuidado e pode exigir ambos ServiceNow e. Resposta a vulnerabilidades de aplicações experiência. Dito isso, algumas orientações estão disponíveis.

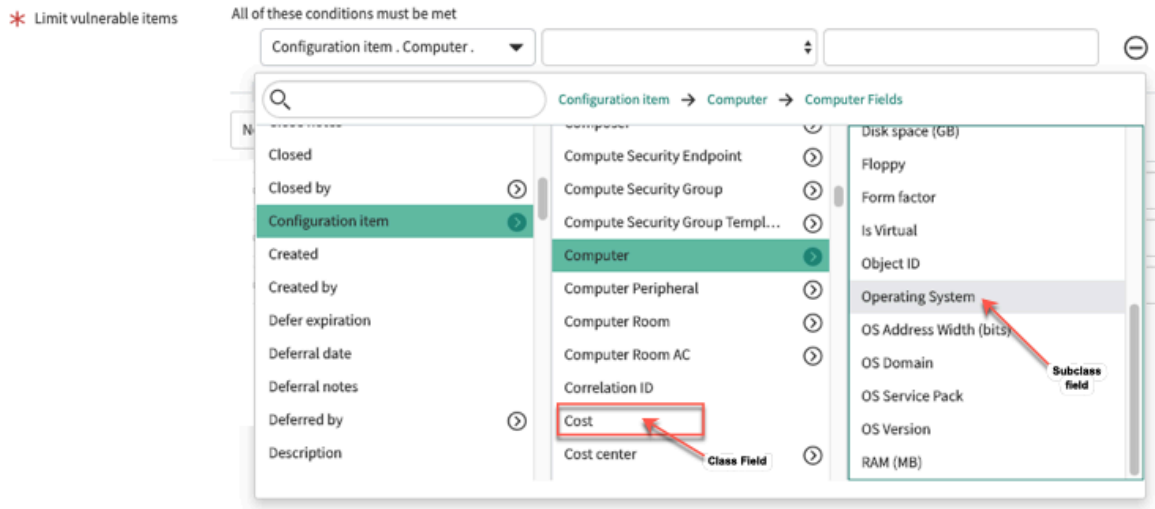
Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão . Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro poderá ser caro para construir e avaliar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Menu suspenso do filtro de condição



Por exemplo, filtrando em **Item de configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de classe e não um campo de subclasse de **Item de configuração**.



Item de configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Esse processo pode levar muitos milissegundos, o que se soma rapidamente, quando milhões de itens vulneráveis estão sendo importados e afetam o desempenho.



Nota: Usar a condição [Contém] é como uma pesquisa curinga e pode causar impacto no desempenho. Usar [IS], sempre que possível, é mais eficiente.

Automatizar o acompanhamento de destino de correção em Resposta a vulnerabilidades de aplicações

As regras de destino de correção da aplicação definem o intervalo de tempo esperado para corrigir itens vulneráveis à aplicação (AVIS), fornecendo um intervalo de tempo para corrigir a vulnerabilidade em si. Por exemplo, se um item vulnerável à aplicação contiver uma classificação de risco crítico, a vulnerabilidade nesse item precisará ser corrigida em 15 dias.

Os gerentes da App-Sec podem criar regras de destino de correção da aplicação definindo:

- O destino de correção.
- O destino do lembrete.

Os gerentes da App-Sec podem ver a data de destino de correção no formulário AVI e nas exibições de lista, no entanto, as datas não são atualizadas para AVIS no **Adiado** , **Resolvido** ou **Encerrado** estado.

. **Data de destino de correção** É codificado por cores na exibição de lista AVI como pontos, da seguinte forma:

- Os Avis que não atingiram a data de notificação são mostrados em verde.
- Os AVIs que se aproximam da data de destino de correção são mostrados em laranja.
- AVIS após a data de destino de correção são mostrados em vermelho.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Regras padrão

Resposta a vulnerabilidades de aplicações vem com três regras padrão que estão inativas por padrão:

- Regra de classificação de risco crítico: Um destino de correção com um **1-Crítico** classificação de risco, uma meta de correção de 15 dias e um lembrete de **7** dias antes da data de destino.
- Regra de classificação de risco médio-alto: Um destino de correção com um **2-Alto** ou **3-Médio** classificação de risco de uma meta de correção de 30 dias e um lembrete de **7** dias antes da data de destino.
- Regra de classificação de risco menos crítico: Um destino de correção com um **4-Baixo** classificação de risco de uma meta de correção de 45 dias e um lembrete de **7** dias antes da data de destino.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de destino de correção atuais para os AVIS às quais ela foi aplicada são apagadas. Se um AVI atender a qualquer regra ativa, essa regra será aplicada, caso contrário, o AVI não terá regra ou data de destino e seu status será **Nenhum destino** .

Quando as regras são excluídas, o **Destino de correção** Os campos Data e relacionados em AVIS encerrados são preservados. . **Destino de correção** Os campos de data e relacionados em AVIS não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário de regra de correção

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

Por exemplo, se um AVI atender à condição de duas regras de destino de correção da aplicação:

Cenário: AVI abriu pela última vez em 03/01/2018 às 10:00:00.

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

Nesse cenário, a regra de destino de correção da aplicação 2 se aplica ao AVI, já que ele tem a data mais restritiva. 10 dias desde que o AVI foi identificado pela primeira vez versus 15 dias.

Nota: Os destinos de correção da aplicação são calculados a partir de **Aberto pela última vez** data mais o número de dias (medido como incrementos de 24 horas). Você pode adicionar este campo ao formulário AVI na caixa de listagem de layout do formulário. É a data em que o AVI foi aberto mais recentemente em sua instância.

A partir da V17.1, os destinos de correção são calculados a partir do **Destino de (data)** . O valor padrão permanece **Data da última abertura** .

Nota: Depois que a regra de destino de correção da aplicação é definida, as datas de destino de correção são calculadas pelo `Evaluate remediation targets` trabalho agendado ou **Aplicar mudanças** Botão na exibição de lista Regras de destino de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sobre o trabalho agendado Avaliar metas de correção

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

Evaluate remediation targets itera por todas as regras de vulnerabilidade ativas, começando com essas regras com a data de destino de correção mais antiga. Todos os Avis são vistos que:

- Não estão em um **Encerrado** , **Adiado** ou **Resolvido** estado.
- Não tem data de destino de correção.
- Ter uma data de destino de correção posterior à data na regra de destino de correção da aplicação.

Evaluate remediation targets adiciona uma data de destino de correção, se não houver uma ou, se esta regra contiver uma data anterior à data no registro, ela atualizará a data de destino existente. Por fim, ele atualiza o. **Data de destino de correção** e. **Status de correção** Campos no formulário AVI. Para regras inativas, **Avalie os destinos de correção** Limpa os campos de correção no AVI.

Reaplicando regras de destino de correção

Ao alterar uma regra de destino de correção, use **Aplicar mudanças** Botão na página de lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os Avis abertos ativos, exceto aqueles em **Encerrado** , **Adiado** ou **Resolvido** estado.

Nota:

Se o trabalho agendado, *Evaluate remediation targets*não é possível iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho agendado for acionado, eles serão executados em paralelo.

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

Criar ou editar regras de destino de correção da aplicação

Conduza a correção de vulnerabilidades de alto risco em tempo hábil configurando uma regra de destino de correção no nível de item vulnerável à aplicação (AVI).

Antes de Iniciar
Função necessária: Grupo do gerenciador de apps-sec

Nota: O sistema de base é fornecido com três regras de destino de correção.

- Regra de classificação de risco crítico
- Regra de classificação de risco menos crítico
- Regra de classificação de risco médio-alto

Essas regras estão inativas por padrão. Se você optar por editar um, em vez de criar um novo, lembre-se de verificar **Ativo** antes de salvar.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de meta da correção**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os Avis devem ser corrigidos, desde a última abertura.
V17.1: Meta de (data)	Data a partir da qual os ANS de destino são calculados. Você pode especificar somente os campos de data ou de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1642413 .
Ativo	Por padrão, o. **Ativo** a caixa de seleção está marcada, o que significa que a regra de destino de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará a novos AVIS criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes do tempo de correção de destino para que um lembrete seja definido. A data de notificação calculada usando este valor é usada para mostrar o status de correção e a codificação por cores. Se a data for anterior à data da notificação, o status da correção será "Em andamento". Se a data de notificação for anterior à data de destino de correção, o status será mostrado como Meta de aproximação. **Nota:** Se este campo estiver definido como 0, somente um **Meta perdida** a notificação está definida.
A regra se aplica a.	Usando o filtro Condição, selecione os critérios para aplicar a regra aos Avis. Para evitar impacto no desempenho, teste suas condições em escala de produção total. O teste permite que você determine por quanto tempo **Avalie os destinos de correção** o trabalho leva para ser executado, dadas as condições e o tamanho do seu Configuration Management Database (CMDB).
Atualizar histórico	
Atividades	Não usado para a criação inicial de uma regra. Em seguida, as anotações de trabalho do sistema são registradas aqui.

4. Clique em **Enviar**.
Esta regra entra em vigor durante a próxima execução do trabalho agendado, *`Evaluate remediation targets`*. O mesmo acontece quando uma regra existente é atualizada ou ao usar o. **Aplicar mudanças** Botão na exibição de lista Regras de destino de correção. O mesmo acontece quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho agendado e. **Aplicar mudanças** consulte, Automatizar o acompanhamento de destino de correção em Resposta a vulnerabilidades de aplicações.

Exiba o status de destino de correção de um item vulnerável à aplicação

Quando um item vulnerável à aplicação (AVI) quase atinge (ou passa) sua data de destino de correção, conforme definido por uma regra de destino de correção, o registro AVI é atualizado com um status. Essas informações podem ajudar você a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar

Função necessária: Grupo do gerenciador de apps-sec

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

. **Avalie os destinos de correção** o trabalho agendado é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de destino de correção associada. Quando a data atual cai no número de dias antes do vencimento da correção, um status de correção é adicionado ao registro de item vulnerável.

Procedimento

Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis**.
Se a data de correção do AVI estiver dentro do intervalo das condições definidas na regra de destino de correção, verifique as colunas Status do destino de correção, visíveis na exibição de lista de Itens vulneráveis. Se a data de destino de correção tiver passado para um AVI, uma anotação será exibida no formulário AVI.

Nota: Para exibir o número de Avis que são **Destino de aproximação** , **Em voo** e. **Destino passado** , consulte Painel do Application Vulnerability Management [PA] .

Tópicos relacionados

Criar ou editar regras de destino de correção da aplicação

Feche uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção da aplicação pode ser encerrado imediatamente sem análise adicional, poderá usar **Fechar** recurso. A partir da v23.0 de Resposta a vulnerabilidades. **Fechar** o botão foi removido para uma tarefa de correção da aplicação.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Em Resposta a vulnerabilidades Espaços de trabalho, uma tarefa de correção passa pelos mesmos estados de uma tarefa de correção anterior em versões anteriores de Resposta a vulnerabilidades. Quando todos os itens vulneráveis (Vits) em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado inativo.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção do Encerrado ou Adiado estados.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione **Fechar** botão.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione o estado como Encerrado.
Motivo	Insira o motivo para encerrar o problema.
Informações adicionais	Insira outras informações relevantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Enviar**.
   A tarefa de correção é marcada **Encerrado** .

Gestão de mudanças para Resposta a vulnerabilidades da aplicação

Crie solicitações de mudança a partir de tarefas de correção na aplicação Resposta a vulnerabilidades da aplicação para agilizar sua investigação de vulnerabilidades da aplicação (AVIT) que exigem intervenção manual.

Crie solicitações de mudança com informações preenchidas previamente para aplicações verificadas que são classificadas como itens de configuração (ICs) para ajudar você a agilizar sua investigação de vulnerabilidades de aplicações (AVITs) que exigem intervenção manual.

- O fluxo de trabalho de solicitação de mudança em Resposta a vulnerabilidades de aplicaçõesé semelhante ao fluxo de trabalho compatível com Resposta a vulnerabilidades.
- Para obter mais informações sobre Resposta a vulnerabilidades fluxo de trabalho de solicitação de mudança, consulte Gestão de mudanças para Resposta a vulnerabilidades.

Crie uma solicitação de mudança para a tarefa de correção da aplicação

Como gerente da App-Sec ou defensor de segurança, você pode criar solicitações de mudança a partir de tarefas de correção na aplicação Resposta de vulnerabilidades da aplicação.

Antes de Iniciar

Funções necessárias:

No Espaço do gerenciador de vulnerabilidades: sn_vul.app_sec_manager.

No Espaço do responsável ITRem: sn_vul.app_sec_champion ou sn_vul.app_developer e função itil.

Por Que e Quando Desempenhar Esta Tarefa

Para criar uma solicitação de mudança no ambiente clássico, siga as etapas listadas abaixo.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente de uma tarefa de correção. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente a partir de uma tarefa de correção:

- Padrão. Uma mudança pré-autorizada que é de baixo risco, relativamente comum e segue um procedimento especificado ou instrução de trabalho.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de serem implementadas, revisadas e encerradas.
- Emergência. Uma mudança para resolver um incidente grave.

Nota: As solicitações de mudança serão compatíveis com a Resposta a vulnerabilidades da aplicação somente se a aplicação descoberta estiver associada a um item de configuração (IC), o que ocorre somente quando você define "Modelo de produto" como "Falso" na propriedade do sistema Usar modelo de produto [sn_vul.use_product_model].

Procedimento

1. Para criar uma solicitação de mudança completa a partir de um registro de tarefa de correção existente, navegue até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**.
   A lista de tarefas de correção atribuídas ao seu grupo de atribuição é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Opcional:** Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Visão Geral da Correção** Para exibir o painel Visão geral da correção e localizar um VUL atribuído a você ou ao seu grupo de atribuição.
3. Como alternativa, na coluna Número, clique em uma tarefa de correção para abrir o registro e exibir os detalhes.
   O registro é exibido.
4. Com o registro APP-VUL exibido para o qual você deseja criar a solicitação de mudança, no canto superior direito do registro, clique em **Criar mudança** .
   O formulário Criar solicitação de mudança é exibido.
5. Preencha os campos.

   a. Na lista de seleção do campo Aplica-se a, escolha um para continuar.

Opção	Descrição
Todos os itens vulneráveis à aplicação ativos neste grupo	Se selecionado, todos os itens vulneráveis à aplicação ativos desta tarefa de correção com um estado diferente de Encerrado serão adicionados automaticamente à solicitação de mudança depois que você clicar em **Criar mudança** .
Todos os itens vulneráveis à aplicação neste grupo correspondem a um conjunto de condições	Se selecionado, o Construtor de condições será exibido conforme mostrado na segunda figura abaixo. Insira critérios de filtro para identificar os itens vulneráveis que você deseja para a nova solicitação de mudança. Um exemplo de filtro pode incluir somente itens vulneráveis que correspondam a critérios de pesquisa específicos: **Estado . Aberto** e. **Pontuação de risco maior que 75** . Depois de inserir suas condições, uma mensagem será exibida com o número de AVITs que correspondem aos seus critérios (10). Um link (**Visualizar itens correspondentes** para visualizar os itens correspondentes é exibido. Se nenhum item corresponder às condições do filtro, uma mensagem será exibida abaixo do construtor de condições instruindo você a ajustar o filtro. Depois de clicar em **Criar mudança** todos os itens vulneráveis à aplicação que correspondem a este filtro de condição são movidos para uma nova tarefa de correção. Esta solicitação de mudança está associada à nova tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar formulário de solicitação de mudança para itens vulneráveis à aplicação em uma tarefa que corresponda a um conjunto de condições

b. Opcional: Se for exibido no formulário, clique em **Visualizar itens correspondentes** Link para obter uma lista de AVITs que correspondem aos seus critérios de filtro.
A visualização da Lista de tarefas de correção é exibida. Você pode selecionar itens nesta lista de visualização e executar ações de IU neles, no entanto, essas ações também são realizadas no APP-VUL. Por exemplo, se você excluir um VI da lista de visualização, esse Avit também será excluído do APP-VUL.

c. Depois de concluir a visualização, feche a janela do navegador para retornar o formulário de solicitação de mudança.

d. Na caixa de seleção Adicionar ICs à CR, escolha uma para continuar.

Opção	Descrição
Caixa de seleção Adicionar ICs à CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem a itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. O APP-VUL é movido automaticamente para Aguardando implementação estado.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos itens vulneráveis da aplicação ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o APP-VUL e o APP-VUL permanece em seu estado atual.

e. Na lista de seleção do campo Tipo de mudança, escolha um para continuar.

Tipo de mudança	Descrição
Emergência	Uma mudança para resolver um incidente grave.
Normal	Um tipo de mudança que é usado para implementar qualquer mudança em um serviço que não seja uma mudança padrão ou de emergência.
Padrão	Uma solicitação de mudança pré-autorizada e de baixo risco que é implementada com frequência. As solicitações de mudança padrão aprovadas podem ser predefinidas em um catálogo de modelos para tornar mais eficiente o acesso e a solicitação de uma mudança padrão. Se selecionado, dois campos serão exibidos. Selecione um de cada lista de seleção para preencher estes campos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de mudança	Descrição
	▪ Categoria de mudança: Selecione uma categoria para a mudança no catálogo existente, por exemplo, Hardware , Mudanças padrão do servidor , Software . Neste exemplo, Patches de mudanças padrão selecionado. ▪ Modelo de mudança: Selecione um modelo disponível para solicitações de mudança com tarefas de suporte predefinidas do seu catálogo. Neste exemplo, Ciclo de aplicação de patches mensal da Microsoft o modelo está selecionado. Para obter mais informações sobre categorias de solicitação de mudança do ITSM, modelos e tipos de mudança, consulte Tipos de mudança .

O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Change Management. Por exemplo, se você mudar o nome das solicitações de Mudança padrão no ITSM de Padrão . Pré-aprovado , Seu novo nome é exibido automaticamente na lista de seleção de tipo de mudança em Criar solicitação de mudança de, conforme mostrado na figura a seguir.

Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações do APP-VUL. Se necessário, esses valores de campo podem ser editados. Por exemplo, revise os valores nos campos na figura a seguir:

Data de término planejada

Esta data (2019-10-10) É o mesmo valor exibido no campo Data de destino de correção do APP-VUL. Este valor é derivado da data de destino de correção mais antiga dos itens vulneráveis da aplicação que pertencem ao APP-VUL. Se você estiver criando uma solicitação de mudança para um problema crítico que requer uma data de correção anterior, você pode preferir editar esse valor e o valor no campo Prioridade.

Justificativa

Este campo exibe o número de ICs adicionados ao CHG. Se você quiser adicionar informações adicionais, você pode preferir editar este texto. Por exemplo, você pode preferir adicionar uma anotação neste campo sobre o filtro usado para criar o novo APP-VUL, por exemplo, Pontuação de risco maior que 75 . Este texto pode ajudá-lo a localizar sua nova solicitação de mudança e tarefa de correção.

Plano de implementação

Este campo exibe a solução preferencial para a vulnerabilidade.

Grupo de atribuição e Atribuído a.

Edite esses campos para mudar o grupo de atribuição ou reatribuir esta solicitação de mudança a um usuário em um de seus grupos de atribuição.

6. Continue a visualizar e editar os campos conforme necessário.
7. Para salvar suas mudanças e permanecer nesta página, na faixa cinza na parte superior do formulário, clique com o botão direito do mouse e selecione **Inserir e permanecer** .
8. Depois de concluir suas edições, escolha uma para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Criar mudança	Sua solicitação de mudança é criada e a nova solicitação de mudança é exibida em Novo estado. Na parte superior, são exibidas mensagens que indicam que a solicitação de mudança foi criada com sucesso com o número de itens vulneráveis à aplicação que foram adicionados. Se a sincronização de estado estiver habilitada e o VUL ainda não estiver em Em investigação , O VUL é movido automaticamente para Em investigação e uma anotação de trabalho é publicada.
Cancelar	A solicitação de mudança não foi criada e o APP-VUL é exibido.

Nota:

Para uma tarefa de correção no Aberto estado Com os campos Grupo de atribuição e Atribuído a não atribuídos (vazio), o usuário conectado atual é atribuído automaticamente à tarefa depois que você clica em **Criar mudança** . Além disso, a caixa de seleção Adicionar ICs à CR deve ser marcada. Na parte superior do VUL, uma mensagem de confirmação azul é exibida indicando esta atribuição.

O que Fazer Depois

Monitore a solicitação de mudança e as tarefas de mudança para verificar se elas foram concluídas e se a solicitação de mudança foi implementada. Depois que este CHG é implementado e movido para Revisão estado, se a sincronização de estado estiver habilitada, o APP-VUL será movido automaticamente para Resolvido .

Associe uma tarefa de correção a uma solicitação de mudança existente

Como gerente de Appsec ou campeão de segurança, evite criar solicitações de mudança duplicadas (CHG) ao trabalhar para resolver suas tarefas de correção associando uma tarefa de correção (APP-VUL) a uma solicitação de mudança que já está disponível em sua instância.

Antes de Iniciar

Funções necessárias:

No Espaço do gerenciador de vulnerabilidades: sn_vul.app_sec_manager.

No Espaço do responsável ITRem: sn_vul.app_sec_champion ou sn_vul.app_developer e função itil.

Por Que e Quando Desempenhar Esta Tarefa

Como responsável pela correção, você pode associar tarefas de correção atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros da tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança a um APP-VUL (VG) existente.

Nota: Você pode associar uma solicitação de mudança existente a um APP-VUL em qualquer estado (Aberto, Em investigação, Aguardando implementação, Encerrado e Adiado). Quando você associa uma solicitação de mudança a um VUL existente, somente os VIS ativos são adicionados à solicitação de mudança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de começar, para evitar a criação de solicitações de mudança duplicadas, você pode preferir exibir todas as solicitações de mudança existentes já associadas a um APP-VUL. Para rastrear facilmente o número de solicitações de mudança relacionadas a um APP-VUL específico, consulte a coluna Contagem de CR na lista Tarefas de correção. Se não for exibido, clique no ícone de configurações () no canto superior direito. Mova a coluna de contagem de CR de Disponível para Selecionado e clique em **OK** .

Para preencher automaticamente a nova coluna, para clientes com dados existentes nesta tabela, execute o trabalho agendado: Preencha a nova coluna Contagem de CR .

Procedimento

1. Para associar uma tarefa de correção a uma solicitação de mudança existente, navegue até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção**.
2. Localize a tarefa de correção com a qual você está trabalhando.
3. **Opcional:** Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Visão Geral da Correção** Para exibir o painel Visão geral da correção e localizar um APP-VUL atribuído a você ou ao seu grupo de atribuição.
4. Na coluna Número, clique em um registro APP-VUL para abri-lo.
   O registro APP-VUL é exibido.
5. Com o registro em aberto exibido, se ainda não estiver sendo exibido, role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas ao APP-VUL são exibidas junto com **Adicionar** botão. Na figura a seguir, não há solicitações de mudança já associadas a este APP-VUL.
6. Para associar o APP-VUL a um CHG existente, clique em **Adicionar** .
   O formulário Adicionar solicitação de mudança existente à tarefa de correção é exibido.
7. No formulário, clique no ícone de pesquisa.
   Uma exibição de lista de solicitações de mudança existentes é exibida em uma nova janela, conforme mostrado na figura a seguir.
8. Selecione um item na lista exibida ou, como alternativa, clique no filtro () e insira condições para limitar os resultados da pesquisa.
9. Na caixa de seleção Adicionar ICs à CR, escolha uma para continuar.

Nota: Esta caixa de seleção é exibida somente para solicitações de mudança existentes no Novo estado.

Opção	Descrição
Caixa de seleção Adicionar ICs à CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem a itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. Quando selecionado, o estado da solicitação de mudança é sincronizado com o APP-VUL. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos itens vulneráveis ativos desta tarefa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o APP-VUL e o APP-VUL permanece em seu estado atual.

10. Com o número da solicitação de mudança que você deseja exibir no campo Pesquisar solicitação de mudança, clique em **Enviar** .
O APP-VUL é exibido. Na parte superior do registro, a mensagem de confirmação azul é exibida indicando que a solicitação de mudança selecionada foi associada com sucesso ao APP-VUL.

Nota: Para um APP-VUL no Aberto estado Com os campos Grupo de atribuição e Atribuído a não atribuídos (vazio), o usuário conectado atual é atribuído automaticamente ao APP-VUL depois que você clica **Adicionar** . Além disso, a caixa de seleção Adicionar ICs à CR deve ser marcada. Na parte superior do APP-VUL, uma mensagem de confirmação azul é exibida indicando que o usuário atual está atribuído.

O que Fazer Depois

Revise o registro APP-VUL. Na coluna Solicitação de mudança na lista relacionada Solicitações de mudança, clique no link para o novo CHG exibir o registro de CR. No registro CHG aberto, você pode monitorar o estado da solicitação de mudança. Os itens de configuração (ICs) afetados e as tarefas de correção são exibidos nas listas relacionadas de ICs afetados e tarefas de correção.

Teste de invasão

Teste de invasão em Resposta a vulnerabilidades de aplicações permite que os proprietários da aplicação avaliem a postura de segurança da aplicação. É o teste manual de uma aplicação pela equipe de hacking ético.

Funções necessárias

O teste de invasão requer as seguintes funções:

App-sec Manager : Contém gerentes de segurança e proprietários de aplicações que gerenciam as solicitações de avaliação de teste de invasão. Ele contém as seguintes funções granulares:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

Hacker ético : Contém membros da equipe de hacking ético que realizam testes de invasão de aplicações. Ele inclui as seguintes funções granulares:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- itil
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Para obter mais informações sobre essas funções, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

A partir da v19.0 de Resposta a vulnerabilidades se você estiver usando Integração de Resposta a vulnerabilidades com Veracode, os testes de avaliação de invasão no Integração de Resposta a vulnerabilidades com Veracode são descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão que você configura em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Integração de Resposta a vulnerabilidades com Veracode.

Ciclo de vida dos testes de invasão

Como proprietário da aplicação, você pode solicitar à equipe de hacking ético uma avaliação de teste de invasão da sua aplicação. A equipe de hacking ético atua nessa solicitação e cria descobertas de teste de invasão. Essas descobertas são itens vulneráveis à aplicação (Avis) criados manualmente.

O fluxo de trabalho de teste de invasão cobre o ciclo de vida do teste de invasão, desde o levantamento da solicitação de teste até a resolução das descobertas da equipe de hacking ético.

Solicitação de uma avaliação de teste de invasão

A partir da v19.0, você pode criar novas solicitações ou copiar solicitações existentes em **Tudo** > **Solicitações de avaliação de teste de invasão** > **Tudo**.

Antes da v19.0, como proprietário da aplicação, você pode solicitar uma avaliação de teste de invasão para sua aplicação usando o catálogo de serviços do ITSM.

Revisando a solicitação de avaliação de teste de invasão

A equipe de hacking ético revisa e avalia a aplicação e o escopo da solicitação de avaliação de teste de invasão e os adiciona ao backlog existente.

Preparando um ambiente

Em seguida, a equipe de invasão ética envia uma solicitação ao proprietário da aplicação para fornecer um ambiente para que eles comecem a testar. Quando o ambiente estiver pronto, o proprietário da aplicação informa a equipe de hacking ético.

Para obter mais informações sobre como configurar solicitações de teste, consulte Configurar testes de invasão.

Testar e relatar as descobertas do teste de invasão

A equipe de hacking ético testa a aplicação e relata as descobertas ao proprietário da aplicação. A equipe de hacking ético também define os acordos de nível de serviço (ANS) para as descobertas do teste de invasão usando a data de destino de correção. Essas descobertas são os AVIS criados manualmente. O proprietário da aplicação, por sua vez,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

revisa o Avis criado pela equipe de hacking ético. Eles planejam as correções e as atribuem à equipe de aplicações.

Nota: As regras de destino de correção não se aplicam às descobertas do teste de invasão.

A equipe de hacking ético pode criar uma biblioteca de entradas de vulnerabilidade da aplicação (AVES) e reutilizá-las ao relatar o AVIS. Eles também podem rastrear o status das descobertas do teste de invasão.

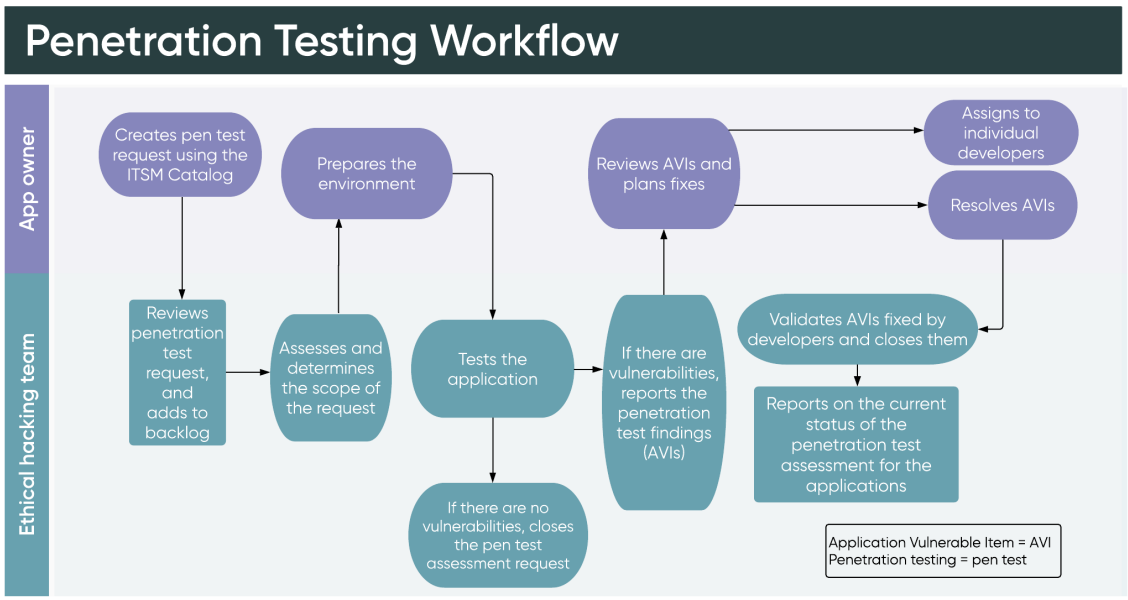
Correção e validação das descobertas do teste de invasão

Depois que as descobertas do teste de invasão são corrigidas e resolvidas pela equipe da aplicação, as correções são validadas manualmente e encerradas pela equipe de hacking ético.

Gestão de vulnerabilidades de aplicações relatórios

Use os relatórios disponíveis no Gestão de vulnerabilidades de aplicações Painel de PA para rastrear as descobertas do teste de invasão.

Ciclo de vida do teste de invasão



Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0)

A partir da v19.0, você cria solicitações de avaliação de teste de invasão diretamente da lista de solicitações existentes. Você também pode copiar solicitações existentes no estado Encerrado nesta lista para criar solicitações.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa

A partir da v19.0 de Resposta a vulnerabilidades se você estiver usando Integração de Resposta a vulnerabilidades com Veracode, os testes de avaliação de invasão no Integração de Resposta a vulnerabilidades com Veracode são descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão que você configura em Resposta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Integração de Resposta a vulnerabilidades com Veracode.

Procedimento

1. Navegar até **Tudo** > **Solicitações de avaliação de teste de invasão** > **Tudo**.
2. **Opcional:** Como alternativa, você pode criar uma solicitação replicando solicitações encerradas. Todos os valores da solicitação original são preservados no novo formulário. Itens vulneráveis à aplicação (Avis) ativos são copiados automaticamente para a nova solicitação. Selecione **Copiar e criar solicitação** De registros no estado Encerrado.
3. Selecione Novo e preencha os campos.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Estado	Selecione um valor com base no status da solicitação.
Solicitação de	Pessoa que solicita a avaliação da aplicação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente da App-Sec. Para configurar grupos, consulte Configurar testes de invasão.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Tipo de aplicação	Selecione uma opção de: ○ Serviço web (conhecido como API anterior à v16.1) ○ Aplicação Web ○ Cliente espesso ○ Mobile (se você selecionar **Mobile** , A guia Mobile é exibida na parte inferior do formulário com campos adicionais)
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo Tipo de avaliação selecionado. Consulte Configurar sprints para teste de invasão e. Configure tipos de avaliação para testes de invasão para obter mais informações sobre

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	como modificar a capacidade de sprint e o escopo de testes.
V19.0: Tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ○ Pequeno ○ Médio(a) ○ Grande ○ Padrão (selecione esta opção se você não tiver certeza do tamanho) Veja mais Configurar testes de invasão mais informações sobre como modificar a capacidade de sprint e o escopo de teste com o tamanho da aplicação e a capacidade de sprint.
Criação em	Data e hora em que a solicitação foi criada.
Tipo de avaliação	Selecione o tipo de avaliação: ○ Teste de invasão completa ○ Teste focado ○ Testar novamente Para obter mais detalhes sobre combinações de teste e escopo de teste, consulte Configure tipos de avaliação para testes de invasão.
Atualização em	Data e hora em que a solicitação foi atualizada pela última vez.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação do produto planejada em	Data planejada para implantar esta aplicação em produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
V19.0: Aplicação de propriedade de um fornecedor terceirizado ou de uma guia de joint venture Se você selecionar Sim para este campo, a guia Informações do fornecedor/Joint Venture será exibida. Preencha os campos adicionais.	
Existe cláusula que nos permite executar testes de caneta?	O termo "cláusula" pode se referir a padrões para testes que incluem quaisquer acordos existentes entre duas ou mais partes que você deseja adicionar. Se você selecionar **Sim** , adicione a cláusula.
A cláusula que cita a permissão para executar o teste de caneta	
Nome jurídico completo e endereço do fornecedor	
Sistema de detecção de intrusão	
Contato técnico do fornecedor	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
As informações registradas foram revisadas de forma de atividade mal-intencionada?	
A aplicação é hospedada por outro fornecedor terceirizado?	
Contato do fornecedor que encerrará o teste de invasão	
Guia Detalhes da aplicação	
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa do front-end ao back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor de terceiros.
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis na aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta algum programa de conformidade, como PCI.
Contatos da equipe de aplicações	Os membros da equipe de aplicações devem ser contatados pela equipe de hacking ético em caso de dúvidas.
Lista de programas de conformidade	
Interfaces ou aplicações de terceiros relacionados	
Endereço IP	
Número aproximado de usuários em produção?	
Existe um script automatizado?	
A versão de produção deste app é externa?	
v 19,0: Impacto nos negócios	
Dano financeiro	Selecione uma opção da lista.
Não conformidade	Selecione uma opção da lista.
Dano à reputação	Selecione uma opção da lista.
Violação de privacidade	Selecione uma opção da lista.
Guia Detalhes do teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada para invasão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Motivo para testar novamente	Motivo para solicitar uma reavaliação de teste de invasão se a aplicação tiver sido testada anteriormente.
Quando a aplicação foi testada?	Intervalo de tempo em que a aplicação foi testada para invasão.
Detalhes da conta de teste	Detalhes da conta de teste que pode ser usada pela equipe de hacking ético para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções mais usadas na aplicação.
Guia Comentários adicionais	
Anotações de trabalho	

4. Selecione **Salvar** para salvar suas edições ou **Enviar** para iniciar a solicitação.

Criar uma solicitação de avaliação de teste de invasão (anterior à v19.0)

Inicie uma solicitação de avaliação de teste de invasão para suas aplicações Web ou APIs. Essas solicitações são enviadas para a equipe de hacking ético, que, em seguida, procede ao teste dessas aplicações e relata manualmente as descobertas do teste de invasão.

Antes de Iniciar
Função necessária: Gerenciador de apps-sec

Por Que e Quando Desempenhar Esta Tarefa
O proprietário da aplicação gera uma solicitação de avaliação de teste de invasão para verificar manualmente sua aplicação ou APIs. A equipe de hacking ético testa a aplicação e cria manualmente as descobertas do teste de invasão. Essas descobertas são itens vulneráveis à aplicação (Avis) criados manualmente.

O grupo de atribuição padrão para a descoberta do teste de invasão é o grupo configurado no campo "Equipe da aplicação" da solicitação de avaliação de teste de invasão associada. O tipo de atribuição da descoberta do teste de invasão é Manual. As regras de atribuição não podem substituir a atribuição dessas descobertas do teste de invasão.

A partir da v19.0, você pode criar solicitações de avaliação de teste de invasão diretamente na tabela Solicitações de avaliação de teste de invasão [sn_vul_pen_test_assessment_request_list]. Para obter mais informações, consulte Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0).

Procedimento

1. Anterior à v19.0, navegue . **Tudo** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitação de avaliação de teste de invasão**.
2. **Opcional:** Como alternativa, você pode criar uma solicitação replicando solicitações encerradas. Todos os valores da solicitação original são preservados. Itens vulneráveis à aplicação (Avis) ativos são copiados automaticamente para a nova solicitação.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Solicitação de	Pessoa que solicita a avaliação da aplicação.
Solicitação de avaliação primária	Solicitação de avaliação de teste de invasão original usada para criar a solicitação secundária. Ele é criado usando uma solicitação de avaliação fechada. Visível somente no formulário de solicitação de avaliação secundária.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Tipo de aplicação	Selecione uma opção de: ○ Serviço Web (conhecido como API anterior à v16.1) ○ Aplicação Web ○ Cliente espesso ○ Mobile (se você selecionar Mobile, a guia Mobile será exibida na parte inferior do formulário com campos adicionais)
V19.0: Tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ○ Pequeno ○ Médio(a) ○ Grande ○ Padrão (selecione esta opção se você não tiver certeza do tamanho)
Tipo de avaliação	Selecione o tipo de avaliação: ○ Teste de invasão completa ○ Teste focado ○ Testar novamente Para obter detalhes, consulte Configure tipos de avaliação para testes de invasão.
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa do front-end ao back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor de terceiros.
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis na aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta algum programa de conformidade, como PCI.
Contatos da equipe de aplicações	Os membros da equipe de aplicações devem ser contatados pela equipe de hacking ético em caso de dúvidas.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação do produto planejada em	Data planejada para implantar esta aplicação em produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
V19.0: Aplicação de propriedade de um fornecedor terceirizado ou uma joint-venture	Se você selecionar Sim para este campo, a guia Informações do fornecedor/empreendimento conjunto será exibida com campos adicionais. O termo "cláusula" pode se referir a padrões para testes que incluem quaisquer acordos existentes entre duas ou mais partes.
Estado	Selecione um valor com base no status da solicitação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo Tipo de avaliação selecionado.
Criação em	Data e hora em que a solicitação foi criada.
Data de início dos testes	Data e hora em que o teste começa.
Atualização em	Data e hora em que a solicitação foi atualizada pela última vez.
Detalhes do teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada para invasão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Motivo para testar novamente	Motivo para solicitar uma reavaliação de teste de invasão se a aplicação tiver sido testada anteriormente.
Quando a aplicação foi testada?	Período em que a aplicação foi testada para invasão.
Detalhes da conta de teste	Detalhes da conta de teste que pode ser usada pela equipe de hacking ético para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções mais usadas na aplicação.

4. Selecione **Enviar**.
   Uma notificação por e-mail é enviada para a equipe de hacking ético informando que a solicitação foi criada para a aplicação relevante.

Replique uma solicitação de teste de invasão no estado Encerrado

Crie uma solicitação de avaliação de teste de invasão replicando uma solicitação no estado Encerrado. Itens vulneráveis à aplicação (Avis) ativos são copiados para a nova solicitação.

Antes de Iniciar

Função necessária: Equipe de aplicações

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Solicitações de avaliação de teste de invasão** > **Tudo**.
2. Selecione uma solicitação no estado Encerrado.
3. Selecione **Copiar e criar solicitação** .
   Uma nova solicitação é criada e os Avis ativos são copiados para esta solicitação com dados atualizados. Para exibir o estado original dos Avis da solicitação primária, navegue até **Snapshot das descobertas do teste de invasão** guia.

Criar descobertas de teste de invasão com base em solicitações de avaliação (anteriores à v19.0)

Crie descobertas do teste de invasão com base na solicitação de avaliação do teste de invasão. Essas descobertas são itens de vulnerabilidade da aplicação (Avis) criados manualmente.

Antes de Iniciar

Função necessária: Ethical Hacker

Procedimento

1. Navegar até **Tudo** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitações de avaliação de teste de invasão**.
2. Para criar um AVI para uma solicitação de avaliação de teste de invasão, selecione a solicitação relevante.
3. Na seção Itens vulneráveis da aplicação, selecione **Novo** .
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de item vulnerável da aplicação (exibição de teste de invasão)

Campo	Descrição
Número	Identificador AVI gerado automaticamente para este registro.
Solicitação de avaliação	Solicitação de avaliação de teste de invasão à qual este AVI está associado.
Vulnerabilidade	Vulnerabilidade selecionada na tabela Entradas de vulnerabilidade usando a opção de pesquisa.
Classificação de risco	Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Calcule o risco em Resposta a vulnerabilidades de aplicações automaticamente. A partir da V16.1, por padrão, o valor é igual à gravidade da vulnerabilidade.
Impacta algum programa de conformidade?	Confirma se há impacto em algum programa de conformidade. As opções são Sim e Não
Lista de programas de conformidade afetados	Este campo é exibido quando o valor do campo "Impacto em qualquer programa de conformidade" é definido como `Yes`. Lista os programas de conformidade afetados.
Versão planejada de liberação/correção	Liberar por quando as descobertas do teste de invasão precisarem ser resolvidas.
Estado	O valor padrão é **Aberto** Quando o AVI é criado. Consulte estados de item vulnerável à aplicação (AVI) para obter mais informações sobre como os estados são mapeados.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVI. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Meta da correção	Data em que os Avis devem ser corrigidos, desde que identificados pela primeira vez. Este campo aparece somente quando aplicável. Para obter mais informações sobre destinos de correção, consulte Automatizar o acompanhamento de destino de correção em Resposta a vulnerabilidades de aplicações.
Criação em	Carimbo de data/hora em que o item vulnerável à aplicação (AVI) foi criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atualização em	Carimbo de data/hora em que o item vulnerável à aplicação (AVI) foi atualizado.
Aberta por	Usuário que criou esta descoberta de teste de invasão.
Contato da equipe de segurança	Ponto de contato na equipe de hacking ético.
Descrição resumida	Breve explicação da descoberta do teste de invasão.
Detalhes	
Detalhes técnicos	Detalhes técnicos da descoberta do teste de invasão.
Impacto	Avaliação do impacto da descoberta do teste de invasão.
Etapas para reproduzir	Documente as etapas para reproduzir e revisar a descoberta do teste de invasão.
Recomendação	Registre as ações recomendadas neste campo.
Anotações	
Anotações de trabalho	Adicione anotações para comunicar informações sobre transições de estado e outras atualizações de campo.
V16.1: URLs afetados	Mais informações relacionadas aos URLs afetados.
V16.1: Parâmetros afetados	Mais informações relacionadas aos parâmetros afetados.
V16.1: Funcionalidades afetadas	Mais informações relacionadas às funcionalidades afetadas.

5. Para salvar o formulário, selecione **Enviar** .

Crie uma entrada de vulnerabilidade da aplicação

Crie uma entrada de vulnerabilidade da aplicação para a vulnerabilidade especificada para a descoberta do teste de invasão. Vulnerabilidades da aplicação são vulnerabilidades nas aplicações de software personalizadas.

Antes de Iniciar

Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades de aplicações relaciona uma vulnerabilidade a uma aplicação para criar a descoberta de teste de invasão. Essas descobertas são itens vulneráveis à aplicação (Avis) criados manualmente. Você pode reutilizar uma entrada existente ou criar uma manualmente para cada vulnerabilidade durante o teste de invasão.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Bibliotecas** > **Terceiros**.
2. Na página Entradas de vulnerabilidade da aplicação, selecione **Novo** .
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de entrada de vulnerabilidade da aplicação (exibição de teste de invasão)

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para NVD e com integrações de terceiros da ServiceNow. Para obter mais informações sobre como criar ou ajustar mapas de gravidade, consulte Mapeie a gravidade de um item vulnerável à aplicação automaticamente.
CVE primário	Referência ao elemento de enumeração de pontos fracos comuns ao qual esta vulnerabilidade se encaixa melhor.
Nome da categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Detalhes da Vulnerabilidade	
Vetor de ataque	Vetor de ataque mais vulnerável para esta vulnerabilidade.
Complexidade de ataque	Métrica que descreve as condições além do controle do invasor que devem existir para explorar a vulnerabilidade.
Escopo	Métrica para medir a capacidade de uma vulnerabilidade de software de afetar recursos além de seus meios.
Integridade	Métrica para medir o impacto na integridade de uma vulnerabilidade explorada com sucesso.
Vetor CVSS	Estrutura aberta para capturar as características e a gravidade das vulnerabilidades de software.
Privilégios necessários (PN):	Nível de privilégios que um invasor deve possuir antes de explorar a vulnerabilidade com êxito.
Interação do usuário	Requisito de interação humana para explorar com sucesso uma vulnerabilidade.
Confidencialidade	Impacto na confidencialidade dos recursos de informação devido a uma vulnerabilidade explorada com sucesso. Esses recursos são gerenciados por um componente de software.
Disponibilidade	Impacto na disponibilidade do componente afetado resultante de uma vulnerabilidade explorada com sucesso.
Pontuação base de CVSS	Representação numérica (0-10) da gravidade de uma entrada de vulnerabilidade da aplicação.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas para mitigar a vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para salvar o formulário, selecione **Enviar** .

> **Nota:** AVES são criadas na tabela Entrada de vulnerabilidade da aplicação (sn_vul_app_vul_entry). A tabela Entrada de vulnerabilidade da aplicação é secundária da entrada de vulnerabilidade (`sn_vul_entry`). Portanto, as aves criadas também são adicionadas à tabela Entrada de vulnerabilidade.

Espaço de teste de invasão

O espaço de teste de invasão no Application Vulnerability Response ajuda os clientes a solicitar uma solicitação de avaliação de teste de invasão e rastreá-la usando o fluxo de trabalho. Ele permite que os proprietários da aplicação avaliem a postura de segurança da aplicação. É o teste manual de uma aplicação pela equipe de hacking ético.

Funções necessárias

O teste de invasão requer as seguintes funções:

sn_vul.app_pen_tester: Representa um testador de caneta que é responsável por criar descobertas de teste de caneta como parte do teste de invasão da aplicação.

sn_vul.app_pen_test_requester: selecione o registro para a ação: sn_vul.app_pen_test_requester.

Ciclo de vida do teste de invasão

Como proprietário da aplicação, você pode solicitar à equipe de hacking ético uma avaliação de teste de invasão da sua aplicação. A equipe de hacking ético atua nessa solicitação e cria descobertas de teste de invasão. Essas descobertas são itens vulneráveis à aplicação (Avis) criados manualmente.

O fluxo de trabalho de teste de invasão cobre o ciclo de vida do teste de invasão, desde o levantamento da solicitação de teste até a resolução das descobertas da equipe de hacking ético.

Criar uma nova solicitação de avaliação de teste de invasão

Inicie uma solicitação de avaliação de teste de invasão para suas aplicações web, aplicações móveis ou APIs. Essas solicitações são enviadas para a equipe de hacking ético, que, em seguida, procede ao teste dessas aplicações e relata manualmente as descobertas do teste de invasão.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Procedimento

1. Navegar até **Espaço do teste de invasão**.
2. Em **Solicitação de avaliação de teste de invasão** preencha os campos.
3. Selecione **Enviar**.
   Uma notificação por e-mail é enviada para a equipe de hacking ético informando que a solicitação foi criada para a aplicação relevante.
4. Uma vez que o formulário é enviado, a equipe de hacking ético pode **Iniciar o escopo** .
5. Após o escopo, o proprietário da aplicação prepara o ambiente de teste e a equipe de hacking ético pode **Iniciar o teste** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Caso você precise verificar os detalhes na solicitação de, marque a fase de teste em espera selecionando **Colocar em espera** botão.
7. Quando o teste estiver concluído, você poderá exibir os AVITs na guia Descobertas do teste de invasão.

Nota: Você pode duplicar uma solicitação de uma solicitação existente. Uma vez duplicados, os AVITs anexados à solicitação primária são movidos (não copiados) para a solicitação duplicada.

Crie descobertas de teste de invasão com base em um questionário de avaliação

Alinhe o teste com os padrões reconhecidos do questionário MASVS no fluxo de trabalho de teste de invasão. Esses resultados são itens de vulnerabilidade da aplicação (Avis) criados manualmente.

Antes de Iniciar

Função necessária: Gerenciador de apps-sec

Procedimento

1. Navegar até **Descobertas do teste de invasão** guia.
2. Selecione o questionário publicado com base em sua aplicação.
3. Revise os testes e marque a fase de teste como concluída.
4. Após a conclusão da etapa acima, feche a solicitação.

Nota: As etapas anteriores podem ser realizadas por um membro da equipe de hacking ético.

Publique o questionário de avaliação

Para testar um aplicativo para celular, existem determinados padrões desenvolvidos pela comunidade OAS para ajudar os testadores a identificar os bugs em seus produtos. Navegue até o espaço de avaliação para criar o questionário de sua escolha. Publique-os para poder exibi-los no formulário de solicitação de avaliação.

Antes de Iniciar

Função necessária: sn_vul.app_pen_test_requester

Funções necessárias para Solicitante e Testador de Teste de invasão:

sn_vul.app_manage_pen_test_request:

contém: sn_smart_asmt.assessment_reader sn_smart_asmt:assessment_admin sn_smart_asmt.ator.

sn_vul.app_pen_tester

contém: sn_smart_asmt.assessment_reader sn_smart_asmt:ator.

Nota: Como parte do recurso Mecanismo de avaliação inteligente, adicionamos as funções acima. Essas funções são essenciais para que o solicitante e o testador do teste de invasão possam exibir e enviar os questionários.

Procedimento

1. Navegar até **Espaço de avaliação**.
2. Cada questionário contém diretrizes. Revise os questionários e, se necessário, mude para atender às necessidades de teste da sua organização. Depois, você pode concluir o teste.
   Por padrão, o questionário segue os padrões MASVS. Para obter mais informações, visite:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Publique os questionários e selecione o questionário publicado na lista na seção Detalhes do teste do formulário de solicitação de avaliação de teste de invasão.

   Nota: Publique o questionário para poder exibi-lo no formulário de solicitação de avaliação de solicitação de teste de invasão.

4. A persona que executa o teste pode marcar os testes como aprovados ou reprovados ou não aplicáveis na guia Avaliação do formulário de solicitação de teste de invasão.

Use um questionário de avaliação

Após a criação do questionário de avaliação, você pode usar esses questionários para fins de teste.

Antes de Iniciar
Função necessária: sn_vul.app_pen_tester

Procedimento

1. Navegar até **Solicitação de teste de invasão** formulário.
2. Siga as diretrizes mencionadas no formulário.
3. Selecione um **Solicitação de teste de invasão** .
4. Navegue até **Guia Avaliação** .
5. Abra a guia, responda ao questionário e. **Enviar** .

   Nota: A persona atribuída à solicitação de teste de invasão pode enviá-la.

Painel de testes de invasão

Obtenha uma visão geral de suas solicitações de teste de invasão e descobertas manuais em seu Painel de teste de invasão pessoal. Você pode exibir o andamento da sua equipe com no Espaço de teste de invasão. O painel fornece uma visão geral das descobertas do teste de invasão, exibe e prioriza testes que precisam de sua atenção, rastreia descobertas do teste e exibe atribuições.

O gerente de teste de caneta/líder da equipe de hacking ético pode identificar e analisar as principais métricas, como monitorar as solicitações de teste de invasão e exibir o andamento geral da equipe no espaço de teste de invasão. O gerente de teste de caneta/líder da equipe de hacking ético também pode exibir as seguintes informações:

- Visão geral das descobertas manuais categorizadas por estado e tipo de avaliação para informar a tomada de decisões estratégicas.
- Distribuição de testes de invasão atribuídos entre indivíduos para melhor planejamento de capacidade
- Priorize descobertas atrasadas com base em seu andamento para melhorar a eficiência da resolução.
- Entenda o cenário de descobertas de teste interativo com base na distribuição crítica.

Componentes do Painel de invasão

Analise visualmente o progresso e os dados da sua equipe e gere resultados de negócios com a ajuda dos componentes do seu painel pessoal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores de itens importantes

Exiba a versão de emergência não atribuída, os testes após a data de visão geral, os testes não atribuídos e qualquer validação crítica pendente.

- **Versão de emergência não atribuída** : Indica a contagem total de solicitações de teste de invasão não atribuídas para o tipo de avaliação "versão de emergência".
- **Testes atrasados** : Indica a contagem total de testes após a data de vencimento.
- **Testes não atribuídos** : Indica a contagem total de testes não atribuídos à equipe.
- **Validação crítica pendente** : Indica a contagem total de AVITs para todas as solicitações no estado "Validação pendente".

Nota: Selecione cada bloco para exibir a lista de itens e executar as tarefas necessárias.

Solicitações de teste de invasão

Exiba as solicitações de teste por estado, testes atrasados e testes por aprovações de versão.

- **Solicitações de teste por estado** : Indica o número de solicitações de teste nesses diferentes estados do ciclo de teste de invasão. Você pode exibir e navegar até a lista de solicitações de teste em diferentes estados clicando em cada bloco colorido. Você também pode exibir o estado desses testes para os seis meses seguintes selecionando o mês no menu suspenso de filtro na seção superior direita da guia. A seguir estão os diferentes estados de solicitação de teste:
  - Aberto: Número de solicitações de teste em aberto.
  - Escopo em andamento:
  - Escopo concluído:
  - Preparação do ambiente:
  - Ambiente pronto para teste:
  - Teste em andamento:
  - Teste de invasão total:
  - Programas de recompensa por bugs: Incentiva os hackers éticos com recompensas para encontrar e relatar vulnerabilidades de segurança.
  - Teste focado:
  - Relatório sobre o compromisso e o suporte da gestão sênior para projetos críticos dentro da organização.
  - Revisões únicas: Avalie projetos específicos fora dos ciclos regulares de desenvolvimento e versão para avaliar o desempenho e implementar melhorias.
  - Versão de emergência: Oferece suporte a versões de emergência necessárias para atualizações rápidas de software para resolver problemas críticos, como vulnerabilidades de segurança.
- **Testes atrasados:** : Indica o teste pendente de um determinado período. Você pode selecionar a linha do tempo para a qual deseja exibir os testes de vencimento. As opções suspensas são: **Vencimento ontem** , **Vencimento esta semana** , **Vencimento na semana passada** , **Vencimento no mês passado** e **Vencimento antes do mês passado** .
- **Testes por aprovações de versão** : Indica estados de aprovação para testes concluídos prontos para liberação. Verifica se todas as verificações necessárias foram concluídas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

antes de implantar um novo software. Você também pode exibir o estado desses testes para os seis meses seguintes selecionando o mês no menu suspenso de filtro na seção superior direita da guia.

Descobertas

Indica o número de descobertas de teste de invasão em aberto (AVITs) relatados junto com o número de AVITs com validação pendente. Você pode exibir e navegar até a lista de descobertas em diferentes estados selecionando cada bloco colorido. Você pode exibir os seguintes dados nesta seção:

- **Descobertas em aberto (AVITs) por classificação de risco**
- **Validação pendente de descobertas (AVITs)**

Visão geral da equipe

Indica os testes atribuídos aos membros da equipe para o período de seis meses seguinte. A seguir estão os diferentes estados:

- **Escopo em andamento**
- **Abrir**
- **Escopo concluído**
- **Ambiente pronto para teste**
- **Testes em andamento**
- **Preparação do ambiente**

Soluções para Análise da plataforma e relatórios para Resposta a vulnerabilidades de aplicações

Soluções para Análise da plataforma e relatórios contém pré-empacotado Análise da plataforma conteúdo para uso com outros ServiceNow AI Platform produtos. Isso Solução para Performance Analytics e relatórios Apresenta métricas importantes para analisar o processo de Gestão de vulnerabilidades da aplicação.

Visão geral

O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades está disponível no ServiceNow® Store como uma assinatura separada. A aplicação não é instalada automaticamente com a aplicação Resposta a vulnerabilidades. O pacote de conteúdo Resposta a vulnerabilidades da aplicação faz parte do pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades.

Para obter mais informações sobre como configurar, instalar e configurar sua aplicação Performance Analytics for Vulnerability Response, consulte Instale e configure a aplicação Performance Analytics for Vulnerability Response [PA] .

Termos principais

Análise de desempenho (PA)

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde às principais perguntas de negócios para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável à aplicação (AVI)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma vulnerabilidade da aplicação relatada por um verificador de vulnerabilidades de terceiros que está presente em um item de configuração (IC).

Indicador de PA

Define uma medição de desempenho feita em intervalos regulares de uma atividade ou comportamento organizacional, por exemplo, 10 principais aplicações com os itens vulneráveis à aplicação mais críticos.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, AVI Ativo.

- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.
- Exiba as taxas de realização da meta de correção e determine com eficiência quais itens vulneráveis à aplicação (AVIS) apresentam o maior risco para sua organização.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

- ServiceNow AI Platform Administrador (administrador): Instale e ative esta Solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Os painéis a seguir fornecem uma exibição gráfica da atividade de AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

- O painel do Application Vulnerability Management (PA) comunica KPIs para risco e prevalência de vulnerabilidade, aplicações afetadas, tendências de correção e andamento de correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dia, um mês, 3 meses, 6 meses, YTD, 1 ano ou todos.
- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.

> **Nota:** O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e está disponível somente quando um membro do grupo de usuários do Security Champion faz login em uma instância. Para obter mais informações sobre o painel Minhas vulnerabilidades da aplicação, consulte Meu painel de vulnerabilidades da aplicação .

Gestão de vulnerabilidades de aplicações Painel (PA)

Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise e detecção iniciais até a contenção ou correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos de uso

Usuário	Uso do painel
Gerenciadores de vulnerabilidades	Com Gestão de vulnerabilidades de aplicações A gestão de vulnerabilidades pode determinar quais itens vulneráveis à aplicação (AVIS) apresentam mais risco para suas organizações. Esses painéis fornecem uma exibição gráfica da atividade de AVI para ajudá-los a determinar os planos de correção e o andamento do status. Concentre-se nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

Obrigatório ServiceNow AI Platform funções, configuração e as guias do painel

O painel do Application Vulnerability Management (PA) está incluído como parte do pacote de conteúdo do Performance Analytics for Vulnerability Response. O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com o. Resposta a vulnerabilidades aplicação. Está disponível no ServiceNow® Store como uma assinatura separada.

Para obter mais informações sobre como configurar, instalar e configurar sua aplicação Performance Analytics for Vulnerability Response, consulte Instale e configure a aplicação Performance Analytics for Vulnerability Response [PA] .

Para exibir o painel, como um usuário atribuído a grupos de usuários de Campeão de segurança, Gerente da App-Sec ou Desenvolvedor, navegue até **Resposta a vulnerabilidades de aplicações** > **Visão geral**.

Nota: O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e está disponível somente quando um membro do grupo de usuários do Security Champion faz login em uma instância. Para obter informações sobre o painel Minhas vulnerabilidades da aplicação, consulte Meu painel de vulnerabilidades da aplicação.

A partir da versão 19,0 de Resposta a vulnerabilidades de aplicações Este painel também pode ser exibido na IU da Nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Página Painéis em Espaço do gerente de vulnerabilidade e Página Painéis em Espaço de correção de problemas de TI.

O painel Visão geral comunica KPIs para risco e prevalência de vulnerabilidade, aplicações afetadas, tendências de correção e andamento de correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dia, um mês, 3 meses, 6 meses, YTD, 1 ano ou todos.

Detalhar os dados em Gestão de vulnerabilidades de aplicações painel por **Tipo de verificação** , **Aplicação** ou **Unidade de negócios** . Cada uma dessas opções tem um filtro adicional, **Selecione elementos** , para refinar suas seleções. A partir de Resposta a vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de aplicações As aplicações de IC e de negócios v15.0 foram adicionadas às opções do **Aplicação** filtro.

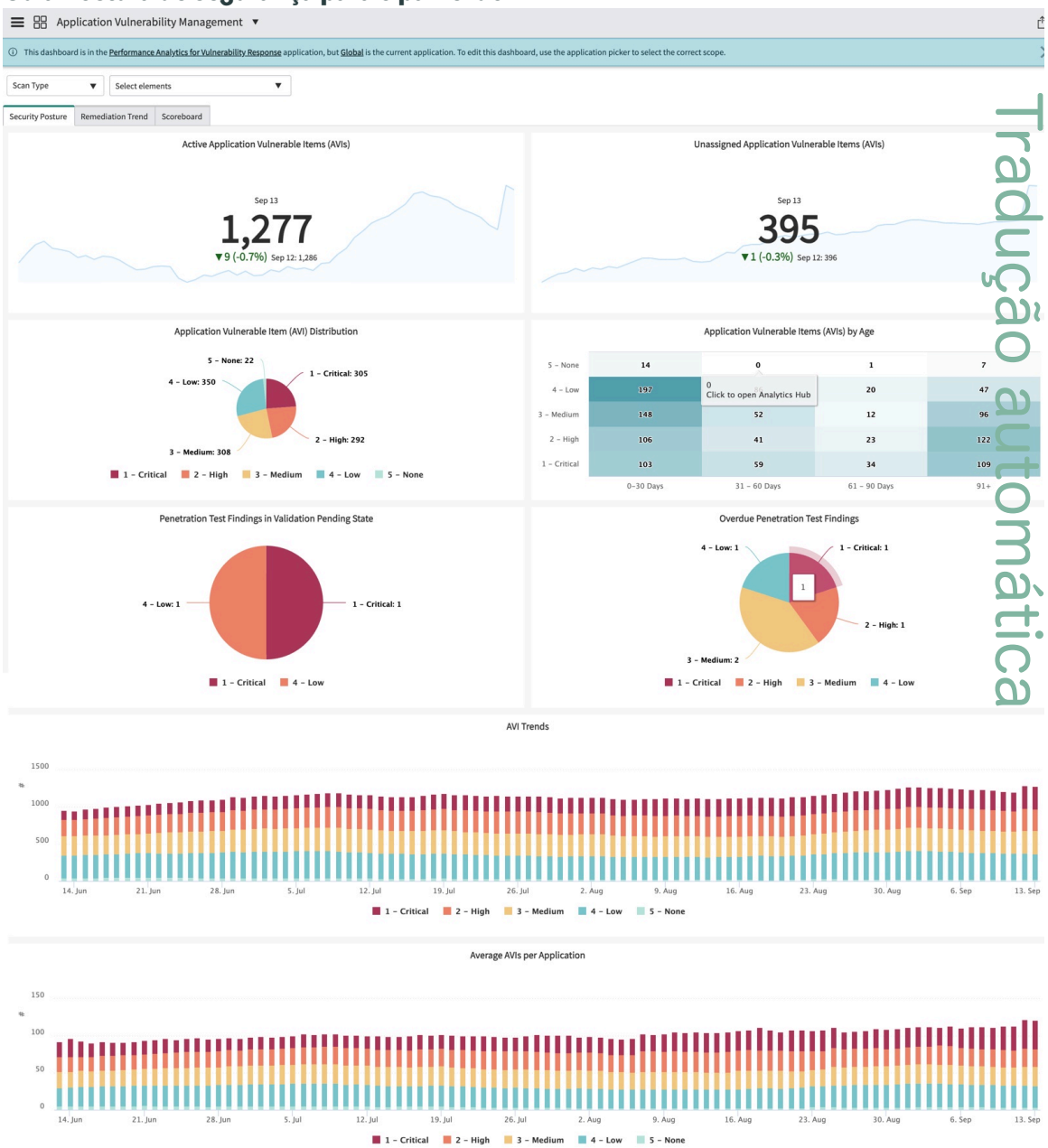
Guia Postura de segurança

A guia Postura de segurança ajuda você a entender sua postura de segurança e o andamento de suas ações de correção.

A partir de Resposta a vulnerabilidades de aplicações v15.0, você pode exibir os relatórios de descobertas do teste de invasão. As descobertas do teste de invasão são itens vulneráveis à aplicação (AVIS) criados manualmente com base nas solicitações de avaliação do teste de invasão.

Nota: O Tipo de verificação desses widgets é Manual.

Guia Postura de segurança para o painel do AVM



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

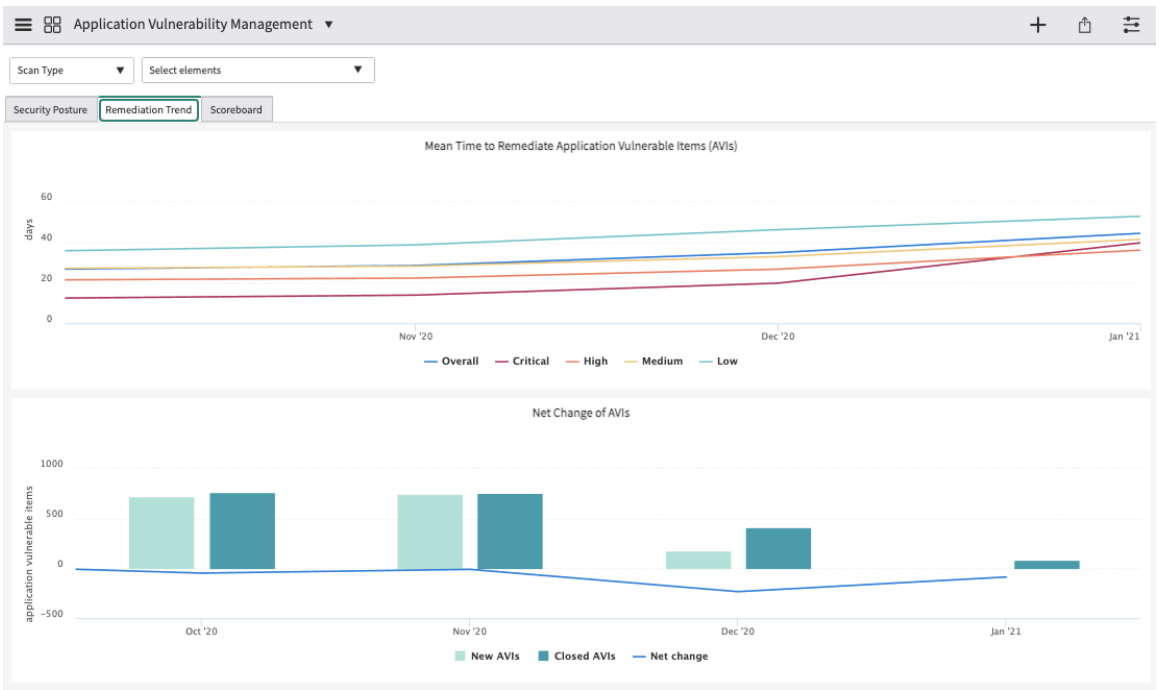
Guia Exceções

Este painel ajuda você a entender onde sua organização está assumindo riscos devido a adiamentos potencialmente excessivos e a reconsiderar as opções de correção.

Você pode exibir itens vulneráveis da aplicação adiados por motivo, Solicitações de adiamento expirando para AVIS, Exceções para itens vulneráveis da aplicação crítica por grupo de atribuição, Solicitações de exceção de AVI por solicitante.

Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento de suas ações de correção.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

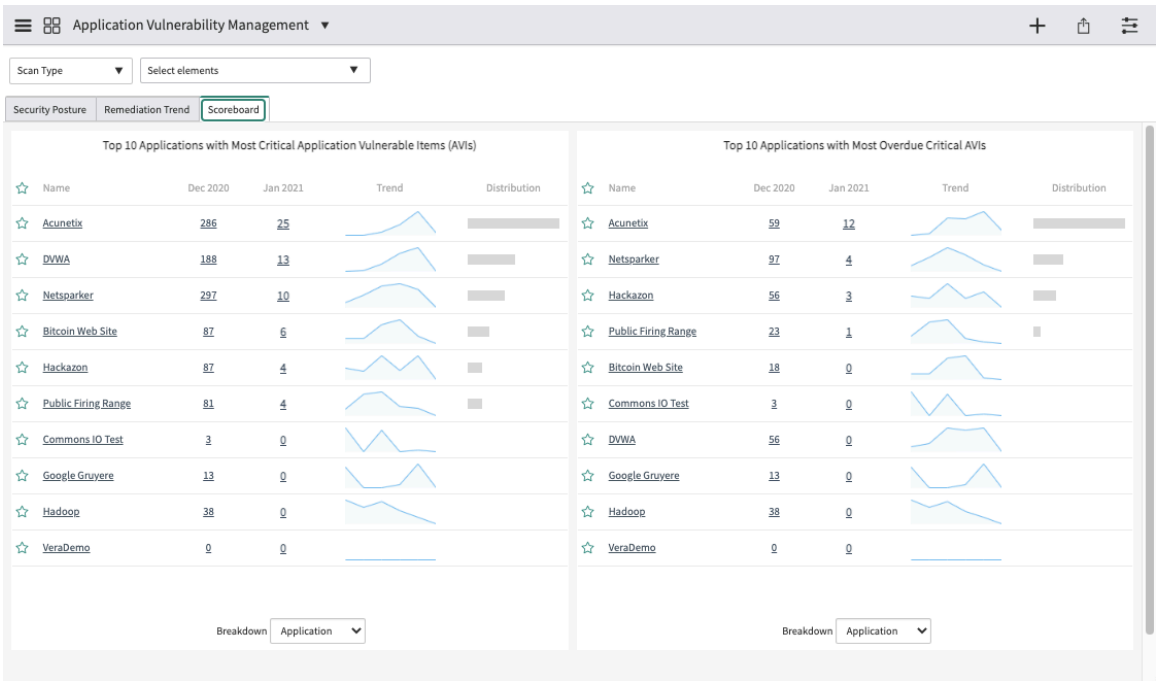
Guia Painel de pontuação

A guia Quadro de pontuação ajuda você a entender o andamento de suas ações de correção e quais Avis precisam de mais assistência com sua conclusão.

Elementos do tipo de verificação:

- Dinâmico: Use somente métricas da importação de dados dinâmicos
- Estático: Use somente métricas da importação de dados estáticos

Você pode escolher um ou ambos.



Indicadores

Tempo médio para corrigir IVAs baixos

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 4 - Baixa]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 4 - Baixa]] . O objetivo é minimizar.

Versões da aplicação

É a contagem distinta em aplicações de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem nos itens do app vul AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

[Itens vulneráveis da aplicação ativa]] / [[Versões da aplicação]] . O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[[Soma da duração dos itens vulneráveis da aplicação encerrados]] / [[Itens vulneráveis da aplicação encerrados]] . O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 2 - Alta]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 2 - Alta]] . O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco 1 - Crítica]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 1 - Crítica]] . O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 3 - Média]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 3 - Média]] . O objetivo é minimizar.

Mudança líquida em IVs

[[Novos itens vulneráveis da aplicação]] - [[Itens vulneráveis da aplicação encerrada]] . O objetivo é minimizar.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem em aplicações de origem do indicador com AVIS ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de negócios
- Pontuação de risco
- Tipo de Verificação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Personalizar o cálculo de Idade e Idade de encerramento para itens vulneráveis à aplicação (AVIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para Avis, consulte KB1703270 artigo da base de conhecimento.

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
V15.0: Descobertas do teste de invasão no estado de validação pendente	Gráfico de pizza	Descobertas do teste de invasão no estado Resolvido, mas com validação pendente, agrupadas por classificação de risco.
V15.0: Descobertas atrasadas do teste de invasão	Gráfico de pizza	Descobertas críticas do teste de invasão que perderam a data de destino de correção, agrupadas por classificação de risco.
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação única	Número de itens vulneráveis da aplicação ativos (não encerrados).
Itens vulneráveis de aplicação (IVAs) não atribuídos	Pontuação única	Número de itens vulneráveis de aplicação (IVAs) sem um atribuído ou grupo de atribuição.
Distribuição de item vulnerável da aplicação (IVA)	Gráfico de pizza	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Itens vulneráveis de aplicação (IVAs) por idade	Mapa térmico	Número de itens vulneráveis à aplicação (AVIS) ativos agrupados por classificação de risco e idade (em dias). **Nota:** Personalizar o cálculo de Idade e Idade de encerramento para itens vulneráveis à aplicação (AVIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para Avis, consulte KB1703270 artigo da base de conhecimento.
Tendências de AVI	Tendência	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	Tendência	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis à aplicação (AVIS)	Linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de Avis	Tendência	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

Placar

Nome	Tipo	Descrição
10 principais aplicações com itens vulneráveis da aplicação (IVAs) mais críticos	Cartão de pontuação e Barra de distribuição	Aplicações com o número maior de itens vulneráveis da aplicação (IVAs).
10 principais aplicações com itens vulneráveis a aplicações críticas (AVIS) mais atrasados	Cartão de pontuação e Barra de distribuição	Aplicações com o maior número de itens vulneráveis à aplicação (Avis) ativos que passaram das datas de destino de correção.

Meu painel de vulnerabilidades da aplicação

Este painel apresenta métricas importantes para analisar o processo de Gestão de vulnerabilidades da aplicação, como exibir as taxas de cumprimento da meta de correção.

Obrigatório ServiceNow AI Platform e exibição do painel

Nota:

- Este painel faz parte do pacote de conteúdo Resposta a vulnerabilidades da aplicação. O pacote de conteúdo Resposta a vulnerabilidades da aplicação faz parte do pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades.
- O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades está disponível no ServiceNow® Store como uma assinatura separada.
- O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com a aplicação Resposta a vulnerabilidades.

O painel Minhas vulnerabilidades da aplicação está disponível somente quando um membro do grupo de usuários do Security Champion faz login em uma instância. Para obter informações sobre o painel Visão geral, consulte Painel do Application Vulnerability Management [PA] .

Para exibir o painel, navegue até **Resposta a vulnerabilidades de aplicações** > **Minhas vulnerabilidades de aplicações**.

A partir da versão 19,0 de Resposta a vulnerabilidades de aplicações Este painel também pode ser exibido na IU da Nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Página Painéis em Espaço do gerente de vulnerabilidade e Página Painéis em Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exiba relatórios que mostram dados de tendências ao longo do tempo. Exiba tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

O painel Vulnerabilidades de Minhas aplicações está incluído com o pacote de conteúdo Análise de desempenho para Resposta a vulnerabilidades. O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com o. Resposta a vulnerabilidades aplicação. Está disponível no ServiceNow® Store como uma assinatura separada.

Casos de uso

Usuário	Uso do painel
Especialistas DE TI, responsáveis pela correção ou analistas que corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem.	Um Campeão de segurança usa o painel Minhas vulnerabilidades da aplicação para rastrear o volume, o desempenho e o andamento da correção de vulnerabilidades da aplicação. Determine com eficiência quais itens vulneráveis à aplicação (AVIS) apresentam o maior risco para sua organização. Esses painéis fornecem uma exibição gráfica da atividade de AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade. Obtenha rapidamente informações sobre sua exposição a vulnerabilidades e postura de segurança. Rastreie desde a análise e detecção iniciais até a contenção ou correção.

Tradução automática

Minhas guias do painel Vulnerabilidades da aplicação [PA]

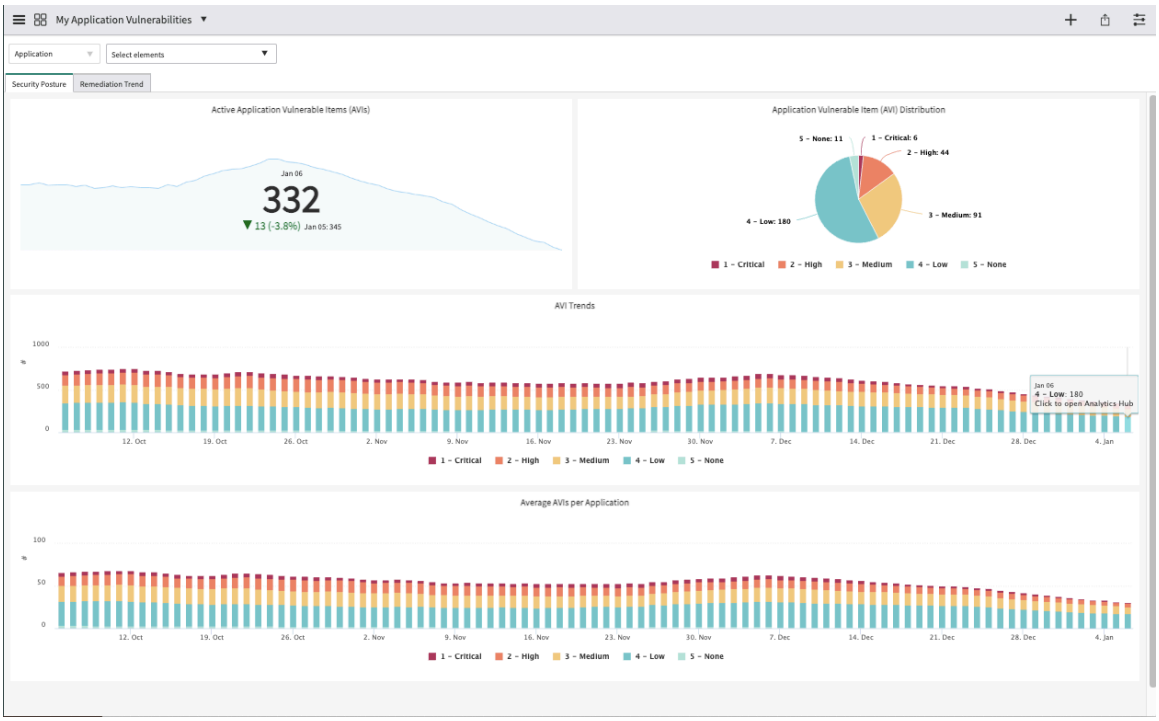
O painel Minhas vulnerabilidades da aplicação comunica KPIs para risco e prevalência de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dia, um mês, 3 meses, 6 meses, YTD, 1 ano ou todos.

Os dados são divididos no painel por **Aplicação** . Use **Selecione elementos** para refinar suas seleções.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

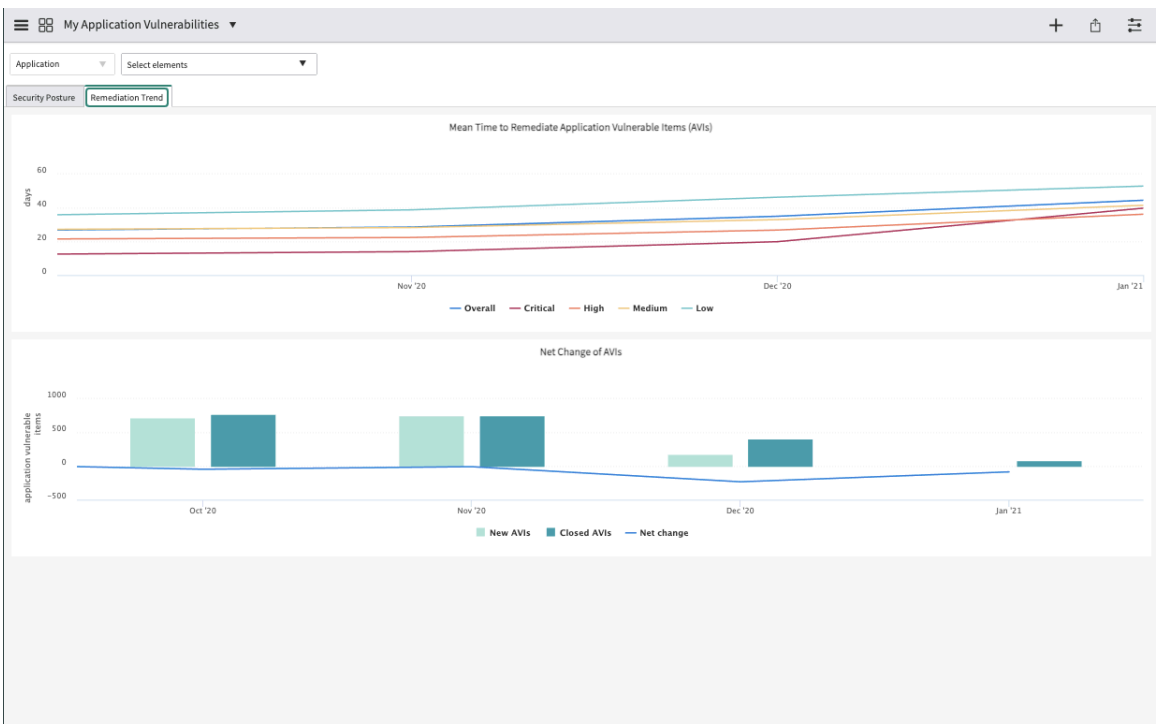
Guia Postura de segurança

A guia Postura de segurança ajuda você a entender sua postura de segurança e o andamento de suas ações de correção. Detalhar os dados no painel Gestão de vulnerabilidades da aplicação por **Tipo de verificação, aplicação** ou **Unidade de negócios** . Cada uma dessas opções tem um filtro adicional, **Selecione elementos** , para refinar suas seleções.



Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento de suas ações de correção.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Tempo médio para corrigir IVAs baixos

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 4 - Baixa]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 4 - Baixa]] . O objetivo é minimizar.

Versões da aplicação

É a contagem distinta em aplicações de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem nos itens do app vul AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

[Itens vulneráveis da aplicação ativa]] / [[Versões da aplicação]] . O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

[[Soma da duração dos itens vulneráveis da aplicação encerrados]] / [[Itens vulneráveis da aplicação encerrados]] . O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 2 - Alta]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 2 - Alta]] . O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco 1 - Crítica]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 1 - Crítica]] . O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco 3 - Média]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco 3 - Média]] . O objetivo é minimizar.

Mudança líquida em IVs

[[Novos itens vulneráveis da aplicação]] - [[Itens vulneráveis da aplicação encerrada]] . O objetivo é minimizar.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem em aplicações de origem do indicador com AVIS ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de negócios
- Pontuação de risco
- Tipo de Verificação

Nota: Personalizar o cálculo de Idade e Idade de encerramento para itens vulneráveis à aplicação (AVIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para Avis, consulte KB1703270 artigo da base de conhecimento.

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação única	Número de itens vulneráveis da aplicação ativos (não encerrados).
Distribuição de item vulnerável da aplicação (IVA)	Gráfico de pizza	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Tendências de AVI	Tendência	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	Tendência	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis à aplicação (AVIS)	Linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de Avis	Tendência	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estrutura de relatórios agregados para Resposta a vulnerabilidades de aplicações

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas dinâmicas complexas e de longa execução para melhorar o desempenho.

A estrutura de relatórios agregados melhora o desempenho ao:

- usando menos recursos e renderizando relatórios mais rapidamente,
- Agregação de dados e reutilização de agregações e detalhamentos (Agrupar por) e.
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis à aplicação (AVITs), use a estrutura de relatórios agregados junto com os relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- ServiceNow AI Platform Administrador (admin): Instale e ative isso Solução para Performance Analytics e relatórios e fazer as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Sn_vul_cmn.admin): Criar agregações.
- VR write(sn_vul_cmn.write): Edite os dados nas agregações e nos resultados agregados.
- VR read (sn_vul_cmn.read): Revise os dados nas agregações e nos resultados agregados.
- Analista de vulnerabilidades (sn_vul.vulnerability_analyst): Revise os resultados agregados.

Tópicos relacionados

Configure uma agregação para dados de origem

Execute várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Crie um relatório usando uma agregação

referências de Resposta a vulnerabilidades de aplicações

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com o. Resposta a vulnerabilidades de aplicações aplicação.

Para obter detalhes, consulte:

- Resposta a vulnerabilidades de aplicações grupos de usuários e funções
- Componentes instalados com Resposta a vulnerabilidades de aplicações
- estados de item vulnerável à aplicação (AVI)
- Campos da aplicação verificados
- Campos de Item vulnerável da aplicação
- Campos Vulnerabilidade da aplicação
- estados do teste de invasão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações grupos de usuários e funções

Antes que você possa corrigir vulnerabilidades com sucesso com Resposta a vulnerabilidades de aplicações(AVR), você deve atribuir usuários a grupos de usuários.

As funções definem o que você e seus grupos podem ver e fazer no Resposta a vulnerabilidades de aplicações, Performance Analytics para Resposta a vulnerabilidades e integrações de terceiros com Resposta a vulnerabilidades de aplicações.

Grupos de usuários

A seguir estão os grupos de usuários padrão suporte Resposta a vulnerabilidades de aplicações:

- App-Sec Manager: Contém gerentes de segurança. A partir de Resposta a vulnerabilidades de aplicações v15.0, ele também conterá os proprietários da aplicação que gerenciam as solicitações de avaliação de teste de invasão.
- Security Champion: Contém ligações entre o grupo de desenvolvimento e os gerentes de segurança.
- Desenvolvedor: Contém colaboradores individuais.
- V15.0: Hacker ético: Contém membros da equipe de hacking ético que realizam testes de invasão de aplicações.

A função de administrador do sistema [admin] é necessária para atribuir usuários ao Resposta a vulnerabilidades de aplicações Grupos de usuários padrão, usando o módulo Administração de usuários,

Nota:

Atribuir usuários AVR ao Resposta a vulnerabilidades de aplicações grupos de usuários para Resposta a vulnerabilidades de aplicações não está disponível em Resposta a vulnerabilidades Recurso Assistente de configuração. Apenas Resposta a vulnerabilidades funções são atribuídas lá.

A tabela a seguir lista os disponíveis Resposta a vulnerabilidades de aplicações grupos de usuários e as funções associadas a eles. Use esta tabela para determinar quais usuários devem ser atribuídos a quais grupos.

Grupo de Usuários	Funções neste grupo
Campeão de segurança Os membros deste grupo podem: • Itens vulneráveis à aplicação (AVIS) de leitura e gravação atribuídos a você. • Atribua um AVI, atribuído a você, a outro indivíduo ou grupo. • V20.0: Criar, atualizar, excluir e cancelar (desativar) regras de exceção.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
Gerente App-Sec Os membros deste grupo podem:	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
• V20.0: Criar, atualizar, excluir e cancelar (desativar) regras de exceção. • Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação. • Ler e gravar todos os Avis. • Configure o AVR criando e gerenciando regras, calculadoras e mapas de gravidade. • Configurar integrações. • Excluir Avis. • Atribua AVI a indivíduos ou grupos. • Gerenciar aplicações. • Permite acesso ao módulo da aplicação. • Programar, configurar e executar integração. • Ler e executar integrações. • Exibir AVR Performance Analytics painéis e relatórios. • V15.0: Gerenciar solicitações de avaliação de teste de invasão.	• sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations **Nota:** Por padrão, esta função contém funções granulares para configuração de integração de terceiros. Para definir ou editar um grupo de usuários do App-Sec Manager por integrações únicas ou específicas, consulte Resposta a vulnerabilidades personas e funções granulares. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Versão 13,0: sn_vul.app_manage_app_sc • Versão 12,0: sn_vul.app_read_application_release [Removido na v12.1. [Não usar] • sn_sec_int.admin • Versão 13,0: pa_power_user • pa_viewer **Nota:** Começando com Resposta a vulnerabilidades v13.0, pa_viewer está incluído em pa_power_user e não é mais necessário por si só. • V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
Desenvolvedor Os membros deste grupo podem:	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
• Leia e grave registros AVR atribuídos a você. • Atribua um AVI, atribuído a você, a outro indivíduo ou grupo.	• sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0: Hacker ético Os membros deste grupo podem: • Configure o grupo de atribuição padrão e o designado para solicitações de avaliação de teste de invasão. • Gerenciar descobertas do teste de invasão. • Gerencie solicitações de avaliação de teste de invasão. • Exibir itens vulneráveis da aplicação. • Atualizar atribuição de itens vulneráveis à aplicação.	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request • V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits • V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

Atribua usuários a grupos de usuários em Resposta a vulnerabilidades de aplicações

Atribua usuários a grupos usando o módulo Administração de usuários em sua instância.

Antes de Iniciar

Função necessária: administrador

Procedimento

Para atribuir ou remover um usuário de um grupo:

a. Navegar até **Administração** > **Grupos**.

b. Localize e abra o grupo apropriado, por exemplo, **App-sec Manager** .
O registro do grupo é exibido.

c. Selecione **Membros do grupo** guia.
Os membros atuais do grupo são exibidos.

d. Clique em **Editar**.
O formulário Editar membros é exibido.

e. De **Coleção** selecione os usuários para adicionar ou remover do grupo.

f. Depois que todos os usuários tiverem sido adicionados ao **Lista de membros do grupo** ou removido, clique em **Salvar** .
Você retornará ao **Membros do grupo** guia.

g. Clique em **Atualização** Para salvar suas mudanças e retornar à lista de grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Componentes instalados com Resposta a vulnerabilidades de aplicações

Componentes instalados com Resposta a vulnerabilidades de aplicações

Vários tipos de componentes são instalados com a ativação do Resposta a vulnerabilidades de aplicações recurso, incluindo tabelas, funções de usuário e trabalhos agendados.

A partir da v24.0.6 de Resposta a vulnerabilidades de aplicações, as propriedades do sistema usadas com mais frequência agora estão acessíveis em Resposta a vulnerabilidades de aplicações aplicação. Para exibir essas propriedades do sistema, navegue até **Tudo**Resposta a vulnerabilidades de aplicações**Propriedades**.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas

Funções granulares em Resposta a vulnerabilidades de aplicações São atribuídos a grupos de usuários específicos, por padrão.

Nota: Usar funções granulares fora desses grupos de usuários requer codificação e avançado Resposta a vulnerabilidades de aplicações ou ServiceNow experiência.

Título da função [name]	Descrição	Contém as funções
V20.0: sn_vul.app_manage_auto_exception_rule	Criar, atualizar, excluir e cancelar (desativar) regras de exceção.	sn_vul.app_read_auto_exception_rule
sn_vul.app_manage_group_rules	Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação.	• sn_vul.app_read_all • sn_vul.app_read_group_rules
V20.0: sn_vul.app_exception_approver	Aprova regras de exceção e solicitações de extensão de regra de exceção. A partir da v20.0, a função granular, sn_vul.app_read_all, foi removida desta função para que você possa acessar os itens vulneráveis à aplicação e as tarefas de correção atribuídas a você e ao seu grupo em vez de todos os itens vulneráveis à aplicação e as tarefas de correção.	• sn_vul.app_read_auto_exception • sn_vul.view_manager_workspace
sn_vul.app_false_positive_approver	Aprova ou rejeita solicitações de falso positivo.	sn_vul.view_manager_workspace

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
sn_vul.app_read_assigned	Exiba itens vulneráveis à aplicação (Avis) atribuídos a você na IU clássica e na Espaço de correção de problemas de TI. **Importante:** A partir da v24.0 de Resposta a vulnerabilidades, a função sn_vul.app_read_assigned tem o privilégio de acessar o. Espaço de correção de problemas de TI.	sn_vul.view_rem_workspace
sn_vul.app_read_all	Exiba todos os Avis e as informações relacionadas na IU clássica ou Espaço do gerente de vulnerabilidade. **Importante:** A partir da v24.0 de Resposta a vulnerabilidades, a função sn_vul.app_read_all tem o privilégio de acessar o. Espaço do gerente de vulnerabilidade.	sn_vul.view_manager_workspace
sn_vul.app_write_assigned	Atualize os Avis atribuídos a você.	
sn_vul.app_write_all	Atualize todos os Avis e as informações relacionadas.	
sn_vul.app_update_assignment_group	Atualizar grupo de atribuição de AVI.	**Nota:** Quando usado fora do grupo de usuários padrão, requer sn_vul.app_write_all ou sn_vul.app_write_assigned.
sn_vul.app_update_assigned_to	Atualizar designado do AVI.	**Nota:** Quando usado fora do grupo de usuários padrão, requer sn_vul.app_write_all ou sn_vul.app_write_assigned.
sn_vul.app_configure_integrations	Configurar integrações de terceiros.	sn_vul.app_read_all sn_vul.app_read_integrations sn_sec_int.admin sn_vul_veracode.configure_integra sn_vul.configure_nvd_administrati

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
		Nota: Para definir ou editar um gr de usuários do App-Sec Manager por integrações únicas ou específicas, co Resposta a vulnerabilidades personas funções granulares.
sn_vul.app_read_integrations	Exibir todas as integrações de terceiros.	
sn_vul_veracode.configure_integration	Defina, atualize e exclua integrações do Veracode.	
sn_vul.app_manage_assignment_rules	Defina, atualize e exclua regras de atribuição de AVI.	sn_vul.app_read_all sn_vul.app_read_assignment_rules
sn_vul.app_read_assignment_rules	Exibir regras de atribuição.	
sn_vul.app_manage_remediation_target_rules	Defina, atualize e exclua regras de destino de correção de AVI.	sn_vul.app_read_all sn_vul.app_read_remediation_targ
sn_vul.app_manage_risk_score_configurations	Defina, atualize e exclua calculadoras AVR e regras de risco.	sn_vul.app_read_all sn_vul.app_read_risk_score_config sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	Exibir calculadoras AVR e regras de risco.	
sn_vul.app_manage_applications	Exibir, atualizar e excluir registros da aplicação.	
sn_vul.app_manage_app_sc	Fornece a um Campeão de segurança a capacidade de adicionar ou remover a si mesmo da lista relacionada da aplicação verificada.	
sn_vul.app_pa_sc_view	Fornece exibição relevante para o Campeão de segurança específico.	
sn_vul.app_manage_app_vul_permissions	[Interno] Usado por sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Atualize o mapeamento para severidade normalizada.	sn_vul.app_read_normalized_severity
sn_vul.app_read_normalized_severity [Removido na v12.1. Não use.]	Exibir registros de gravidade normalizados.	
sn_vul.app_read_application_release	Exibir registros de versão da aplicação.	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
sn_sec_int.admin	Fornece acesso a integrações.	
pa_power_user	Fornece acesso a relatórios	pa_viewer
sn_vul.app_sec_manager	Prioriza e gerencia itens vulneráveis à aplicação.	
sn_vul.app_developer	Desenvolvedor responsável por corrigir as vulnerabilidades da aplicação.	
sn_vul.app_create_watch_topic	Criar Tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_read_watch_topic	Tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_edit_watch_topic	Editar tópicos de observação para vulnerabilidades da aplicação.	
sn_vul_blackduck.configure_integration	Configurar integrações de terceiros.	sn_vul_blackduck.configure_integration

Trabalhos agendados instalados

Para Resposta a vulnerabilidades trabalhos agendados compartilhados consulte, Componentes instalados com Resposta a vulnerabilidades.

Trabalho programado	Descrição
Associe AVIS existentes à regra de exceção automática	Avalia itens vulneráveis da aplicação em busca de correspondências com regras de exceção.
Preencha a entrada e CVE M2M	Torna os registros existentes consistentes com vários registros CWE. Execute uma vez após o upgrade para preencher e desabilitar.
CWE primário novamente	Para cálculos de CWE primário personalizados. Execute uma vez após o upgrade para ressincronizar e desabilitar.
Acumule valores de item vulnerável da aplicação para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis à aplicação. **Nota:** A partir da v23.0 de Resposta a vulnerabilidades de aplicações, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de multithreading. Este upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.
Integração da lista de projetos Black Duck	Extrai e ingere dados na tabela Projetos do Black Duck.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Integração da lista de aplicações Black Duck	Importa aplicações para a tabela Aplicações descobertas para todas as versões de projeto disponíveis com a integração do Black Duck na tabela Projetos.
Integração de item vulnerável da aplicação Black Duck	Ingere itens vulneráveis na aplicação da ServiceNow com base nas vulnerabilidades detectadas pelos scanners para cada aplicação descoberta no sistema.

Tabelas instaladas

Tabela	Descrição
Versão da aplicação [sn_vul_app_release]	Contém informações da versão da aplicação.
Versão 13,0: Campeões de segurança da aplicação [sn_vul_app_m2m_app_sc]	Contém o. Resposta a vulnerabilidades de aplicações Registros do grupo de Campeão de segurança.
Entrada de vulnerabilidade da aplicação [sn_vul_app_vul_entry]	Contém entradas de vulnerabilidade da aplicação.
Integração de vulnerabilidade da aplicação [sn_vul_app_integration]	Contém Resposta a vulnerabilidades de aplicações registros de integração.
Localização de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_location]	Contém informações de local de verificação de terceiros.
Resumo de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary]	Contém informações resumidas da verificação de terceiros.
Item vulnerável da aplicação [sn_vul_app_vulnerable_item]	Contém registros AVI. A partir da v19.0, as seguintes colunas são adicionadas à Lista de materiais do software: • sn_sbm_config_rule • sn_sbom_component • vex_justificação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	• vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Aplicação escaneada [sn_vul_app_scan_application]	Contém informações da aplicação.
Mapa de Estado [sn_vul_app_state_map]	Contém mapeamento de estado de integrações de terceiros para estados de item vulnerável à aplicação (AVI).
CWEs de vulnerabilidade [sn_vul_m2m_entry_cwe]	Vincula dados CVE a entradas vulneráveis da aplicação.
Manifesto de tarefa de correção da aplicação sn_vul_app_rt_manifest	Todas as atualizações na tarefa de correção são feitas usando esta tabela de manifesto por trabalhos agendados.
Tarefa de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.
Item da tarefa de correção da aplicação sn_vul_app_m2m_vul_group_item	Tabela M2M entre AVI e tarefas de correção da aplicação.
Versão 21,0: Itens vulneráveis da aplicação sn_vul_app_vulnerable_item	Contém registros AVI.
Versão 21,0: Pacote [sn_vul_app_package]	Contém detalhes do pacote da aplicação.
Versão 21,0: Licenças sn_vul_app_license	Contém licenças de aplicação.
Versão 21,0: Tarefas de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.
sn_vul_blackduck_config	Contém detalhes da configuração de integração do Black Duck.
sn_vul_blackduck_project	Contém detalhes dos projetos provenientes do Black Duck.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
sn_vul_blackduck_project_import	Tabela do conjunto de importação para a ingestão do projeto Black Duck.
sn_vul_blackduck_app_import	Tabela do conjunto de importação para a ingestão da aplicação Black Duck.
sn_vul_blackduck_avit_import	Tabela do conjunto de importação para ingestão do Black Duck Avit.

estados de item vulnerável à aplicação (AVI)

Resposta a vulnerabilidades de aplicações Oferece um modelo de estado para o status dos itens vulneráveis da aplicação (Avis) a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda você a determinar quando e como corrigir seus Avis.

estados do item vulnerável da aplicação

Entender como os estados funcionam ajuda a criar ou editar regras de AVI (item vulnerável à aplicação). Os Avis têm vários estados possíveis que são mapeados do status de correção importado da integração de terceiros. Em um AVI, o **Estado** o campo é somente leitura.

Resposta a vulnerabilidades de aplicações fluxograma de estado

Estado	Descrição
Aberto	Estado após a criação. A partir deste estado, você pode: **V16: Obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do FORTIFY: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **V16: Marcar como falso positivo** Marque um item como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas, na realidade, não houver vulnerabilidade. **V16: Exceção de solicitação** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data até a qual uma exceção é solicitada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações fluxograma de estado

Estado	Descrição
	V15: Fechar Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. **V15: Resolver** Marque um AVI aberto como Resolvido para movê-lo para um estado Resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Adiado	**V15:** Isso é acionado pelo **Exceção de solicitação** opção. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser encerrado até ser aprovado. A partir deste estado, você pode: **V16: Obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do FORTIFY: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **Reabrir** Faz a transição de um AVI encerrado ou resolvido de volta para um estado aberto. **Fechar** Selecione o estado Encerrado, um motivo e forneça informações adicionais. Fecha o AVI.
Sob Investigação	Selecione esta opção em **Estado** lista. A partir deste estado, você pode: **V20.0** Faça a transição manual de uma tarefa de correção ou registro AVI para **Aguardando implementação** . **V16: Obter mais detalhes**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações fluxograma de estado

Estado	Descrição
	Obtenha as seguintes informações sobre um AVI importado do FORTIFY: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **V16: Marcar como falso positivo** Marque um item como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas, na realidade, não houver vulnerabilidade. **V16: Exceção de solicitação** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data até a qual uma exceção é solicitada. **V15: Fechar** Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. **V15: Resolver** Marque um AVI aberto como Resolvido para movê-lo para um estado Resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Aguardando Implementação	Você só pode fazer a transição de registros para este estado manualmente selecionando Aguardando implementação de AVI e registros de tarefa de correção no estado Em investigação. A partir deste estado, você pode: **Aberto** O AVI é transferido de volta para um estado aberto. **Sob Investigação**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações fluxograma de estado

Estado	Descrição
	Obtenha mais informações para resolução. Transições para Em investigação. **Resolver** Marque um AVI aberto como Resolvido para movê-lo para um estado Resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação. **Fechar** Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. Neste estado, faça a transição de um registro para Aguardando implementação quando sua pesquisa e trabalho em uma tarefa estiverem concluídos e, embora uma correção esteja pronta para implementação, ela ainda não está disponível. Defina **Data do compromisso de correção** e. **Plano de correção** campos. Após a implementação, você resolve ou fecha os registros.
Resolvido	Acionado a partir do botão Resolver. A partir deste estado, você pode: **V16: Obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do FORTIFY: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **Reabrir** Transições de volta para um **Aberto** estado. **Fechar**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações fluxograma de estado

Estado	Descrição
	Selecione **Encerrado** declare, um motivo e forneça informações adicionais. Fecha o grupo. Anotações e informações de resolução aparecem em **Anotações** guia.
Encerrado	Acionado a partir do botão Fechar. A partir deste estado, você pode: Reabrir: Faz a transição de volta para um estado aberto.

Nota: Consulte Integração da Resposta a vulnerabilidades da aplicação Com outras aplicações para entender diferentes integrações que originaram o AVI.

estados da tarefa de correção da aplicação

Da criação ao fechamento de uma tarefa de correção de aplicação, a tarefa de correção de aplicação faz a transição por vários estados durante todo o processo de correção.

A precedência de estado é a seguinte:

Encerrado > **Adiado** > **Resolvido** > **Em revisão** > **Aguardando Implementação** > **Sob Investigação** > **Aberto**

A transição de estado acontece conforme você executa várias ações, como adiar, abrir, fechar etc.

As ações que você pode executar em uma tarefa de correção de aplicação em um estado específico são semelhantes às de uma tarefa de correção de host. Para obter mais informações, consulte Resposta a vulnerabilidades estados da tarefa de correção e. Cenários de roll-up e roll-down de estado em Resposta a vulnerabilidades documentação.

Nota: A partir da v23.0 de Resposta a vulnerabilidades. **Fechar** O botão foi removido para garantir que o fechamento da tarefa de correção seja orientado pelo scanner.

Resposta a vulnerabilidades de aplicações exemplos de regra de tarefa de correção

Um exemplo de um exemplo de regra de tarefa de correção usando o construtor de condições.

Uma regra de tarefa de correção que usa vulnerabilidade, modelo de produto, endereço IP e grupo de atribuição

1. No construtor de condições em um novo registro, defina a condição como **Vulnerabilidade** > **é** e insira uma vulnerabilidade conhecida.

   As vulnerabilidades são importadas das integrações do banco de dados de vulnerabilidades da nação (NVD) e da enumeração de pontos fracos comuns (CWE), conforme descrito em Como configurar o Resposta a vulnerabilidades de aplicações.

2. Na seção Agrupar por, selecione **Item vulnerável à aplicação** para **Agrupar itens vulneráveis da aplicação de** campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No campo Usando, selecione **Grupo de atribuição** .

   Use Regras de atribuição para definir automaticamente **Grupo de atribuição** campo para uso em sua regra de tarefa de correção. Você pode usar uma regra fornecida com a aplicação ou configurar suas próprias regras de atribuição. Para obter mais informações, consulte Atribua itens vulneráveis à aplicação em Resposta a vulnerabilidades de aplicações automaticamente.

4. Selecione outra condição, por exemplo, item de configuração de item vulnerável à aplicação em **Item vulnerável da aplicação do grupo de** E endereço IP ou modelo de produto no **Usando** campo.
5. Na seção Atribuição, para Atribuir tarefa de correção campo por campo, selecione **Agrupar por campo** .
6. No campo Agrupar por, selecione **Grupo de atribuição** .

   Conforme descrito nesta seção, esta seleção atribui itens vulneráveis a vários grupos com base nas condições definidas na seção Agrupar por. Embora os Avis compartilhem a vulnerabilidade, eles são atribuídos a diferentes grupos com base no modelo de produto de IC ou por endereço IP.

7. Selecione **Enviar** para salvar sua regra.

Campos da aplicação verificados

As aplicações são armazenadas durante a importação em **Administração** > **Aplicações descobertas** in Resposta a vulnerabilidades de aplicações.

Campos da aplicação verificados

Os campos importados nesta tabela são somente leitura, a menos que especificado de outra forma. **Departamento** e. **Grupo de suporte** As entradas podem ser adicionadas ou editadas manualmente por um gerenciador da App-Sec.

Campo	Descrição
Nome	Nome importado da aplicação.
Versão	Versão importada da aplicação, quando aplicável.
Status operacional	Status operacional importado da aplicação.
Departamento	Departamento importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Unidade de negócios	Unidade de negócios importada à qual o departamento pertence. . **Departamento** Preenchido, este campo é preenchido automaticamente com a unidade de negócios à qual o departamento pertence. Caso contrário, ele será deixado em branco e somente leitura.
Grupo de suporte	Grupo de suporte importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Descrição	Descrição importada da aplicação.
Data da última verificação de conformidade com a política	Data em que a aplicação foi verificada pela última vez pela Veracode quanto à conformidade com a política. Ele é usado nas integrações encadeadas da integração da Lista de aplicações, em que o suporte está disponível para ingestão delta para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	aplicações, comparando essa data com a hora de início delta das respectivas integrações. **Nota:** Os dados recuperados para aplicações são extraídos da Veracode, cujo valor "Data da última verificação de conformidade da política" é maior ou igual à "Hora de início" (delta_start_time) das integrações encadeadas.
Lista relacionada (visível somente para um gerente da App-Sec ou um campeão de segurança)	
Campeão de segurança	Lista as aplicações associadas a um campeão de segurança. Os gerentes da App-Sec podem adicionar ou remover membros da lista.

Campos de Item vulnerável da aplicação

AVITs (Application Vulnerable Items, itens vulneráveis à aplicação) são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos de item vulnerável da aplicação

Exceto para **Grupo de atribuição** , **Atribuído a.** campos e. **Anotações** Todos os outros campos no AVIT são somente leitura.

Campo	Descrição
Número	Identificador AVIT gerado automaticamente para este registro.
Tipo de verificação	Tipo de scanner que encontrou este AVIT. As opções são: • Dinâmico • Estático • SCA
Classificação de risco	Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte, Calcule o risco em Resposta a vulnerabilidades de aplicações automaticamente.
Pontuação de risco	Valor calculado de risco que o AVI representa para o seu ambiente. Para obter mais informações, consulte Calcule o risco em Resposta a vulnerabilidades de aplicações automaticamente.
Data do compromisso de correção	As datas em que as AVITs devem ser corrigidas após serem movidas para **Em investigação** . Este campo aparecerá somente se o AVIT estiver em **Em investigação** .
Meta da correção	Data em que os AVITs devem ser corrigidos, desde que identificados pela primeira vez. Aparece somente quando aplicável. Para obter mais informações sobre destinos de correção, consulte Automatizar o acompanhamento de destino de correção em Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status da correção	Status da correção do AVIT. Determinado pelo AVIT com a data de vencimento mais próxima, quando aplicável. Os estados incluem: • Em andamento • Perto da meta • Destino passado
Nome da categoria	Nome da categoria da vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável da aplicação.
Versão da aplicação	Versão da aplicação.
Módulo da aplicação	Aplicação afetada na verificação DAST. Oculto para varreduras SAST.
Local Versão 14,0: SAST	DAST: Local da URL da vulnerabilidade na aplicação. SAST: Caminho do arquivo e número de linha da vulnerabilidade na aplicação.
Estado	O padrão deste campo é **Aberto** quando criado. Consulte estados de item vulnerável à aplicação (AVI) para obter mais informações sobre como os estados são mapeados.
Motivo	[Visível somente quando o AIV está em **Encerrado** estado.] Explicação do Estado.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVIT. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente da App-Sec
Primeiro encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela primeira vez.
Último encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela última vez.
Encerrado	[Visível somente quando o AVIT está em **Encerrado** estado.] Data em que o AVI foi encerrado.
Encerrado por	[Visível somente quando o AVIT está em **Encerrado** estado.] Entidade que fechou o AVIT.
Resumo	Descrição importada da vulnerabilidade.
Descobertas Dados somente leitura importados da integração de terceiros.	
ID de AVIT de origem	Identificador importado para o AVIT de origem.
Gravidade de origem	Gravidade importada da aplicação de origem.
Data de correção de destino da origem	Data importada em que a origem espera que o AVIT seja corrigido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status de mitigação da origem	Status de mitigação importado da aplicação de origem.
Status da correção da origem	Status de correção importado da aplicação de origem.
Status de descoberta da origem	[Visível somente quando preenchido] Status do problema importado da aplicação de origem.
Status SDLC	Status do ciclo de vida de desenvolvimento de software importado.
Em conformidade com a Política	Status de conformidade importado. Se nenhum status for fornecido, este campo será definido como **Não aplicável** .
Link da origem	URL para o AVIT de origem.
Anotações da origem	Anotações importadas da origem.
Resumo da vulnerabilidade	Resumo importado da origem.
Explicação da vulnerabilidade	Explicação importada da origem.
Recomendação	Recomendação importada da origem.
Referências	Referências importadas da origem.
Solicitação/resposta HTTP (visível somente para verificações DAST)	
Solicitação de origem	Solicitação HTTP
Resposta de origem	Resposta HTTP
Anotações	
Plano de correção	Detalhes de como os AVITs serão corrigidos. O plano deve ser implementado pelo **Data do compromisso de correção** . Este campo aparecerá somente se o AVIT estiver em **Em investigação** .
Anotações de trabalho/comentários adicionais	Qualquer informação relevante. Selecione a caixa de texto das anotações de trabalho para adicionar informações. Começando com Resposta a vulnerabilidades V20.0, você pode adicionar anotações de trabalho na seção Anotações para um item vulnerável da aplicação adiada.

Cálculos de idade para um AVIT:

- A coluna Idade na lista AVIT exibe a duração (formato: Dias HH:MM:SS) para a qual um AVIT está ativo. O valor Idade é zero para um AVIT encerrado.
- A coluna Idade fechada na lista AVIT exibe a duração (formato: Dias HH:MM:SS) durante a qual um AVI está ativo antes de ser encerrado. Para AVITs, que não estejam no estado Encerrado, o valor Idade Encerrada é zero.

Para obter mais informações sobre como personalizar o cálculo de Idade e Durações de Encerramento de Idade, consulte KB1703270 artigo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados do teste de invasão

Os proprietários da aplicação podem solicitar avaliação de teste de invasão para suas aplicações e monitorar o andamento da equipe de invasão ética até que a solicitação seja resolvida.

A solicitação de avaliação de teste de invasão passa pelos seguintes estados de transição até ser resolvida.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
estados do teste de invasão	
Aberto	Estado quando a solicitação de avaliação é criada pelo proprietário da aplicação.
Escopo	A equipe de hacking ético avalia a solicitação e o escopo da aplicação.
Preparação do ambiente	O proprietário da aplicação cria um ambiente com funções e outras informações e as fornece à equipe de hacking ético para testes.
Testando	A equipe de hacking ético testa manualmente a aplicação para identificar as descobertas do teste de invasão.
V16.1: Teste em andamento	A equipe de hacking ético indica que o teste está em andamento no momento. Se este estado for selecionado, o **Teste em espera** a opção se torna disponível no formulário.
V16.1: Teste em espera	Este campo é exibido somente quando o estado Teste em andamento é selecionado. A equipe de hacking ético controla os acordos de nível de serviço (ANS) das solicitações de avaliação de teste de invasão selecionando este estado, se necessário. Isso garante que SLAs precisos sejam relatados.
V16.1: Teste em revisão	A equipe de hacking ético indica que o teste está concluído e está sendo revisado por um especialista no assunto.
Encerrado	A equipe de hacking ético encerra as solicitações de avaliação do teste de invasão após as descobertas do teste de invasão serem relatadas. **Nota:** A partir da V16.1, você pode usar **Copiar e criar solicitação** Opção no formulário para replicar a solicitação no estado Encerrado e criar uma nova solicitação. Para obter detalhes, consulte Replique uma solicitação de teste de invasão no estado Encerrado.
V16.1: Cancelado	O proprietário da aplicação cancela a solicitação de avaliação de teste de invasão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
V16.1: Rascunho	O proprietário da aplicação cria uma solicitação e a salva como rascunho antes de enviar a solicitação.
estados do item vulnerável da aplicação	
Aberto	Quando a equipe de hacking ético identifica e cria as descobertas do teste de invasão, seu status é Aberto.
Resolvido	Quando a equipe da aplicação resolve as descobertas do teste de invasão, seu status é movido para Resolvido. **Nota:** Se a descoberta do teste de invasão tiver sido resolvida, mas ainda não tiver sido validada pela equipe de hacking ético, o subestado será `Validation Pending`.
Encerrado	A equipe de hacking ético valida que as descobertas do teste de invasão foram resolvidas e move o status para Encerrado.

Gerenciar mapeamento de estado para adiamentos e falsos positivos em Resposta a vulnerabilidades de aplicações

Você pode gerenciar como **Origem** Itens vulneráveis à aplicação (Avis) importados pelo Integração de Resposta a vulnerabilidades com Veracode e. Integrações de vulnerabilidade do Fortify são mapeados em sua instância após a importação.

A partir da v20.0 de Resposta a vulnerabilidades, Você tem mais opções para fazer a triagem de seus Avis importados com ServiceNow fluxos de trabalho.

Quando você Configure o Integrações de vulnerabilidade do Fortify ou Configure o Integração de Resposta a vulnerabilidades com Veracode, as páginas de configuração de integração fornecem duas opções para ajudá-lo a gerenciar exceções e falsos positivos em sua instância.

- Gerencie exceções em ServiceNow
- Gerencie falsos positivos em ServiceNow

Função necessária: Gerenciador de apps-sec.

Caso de uso para gestão de exceções

Os Avis são importados dessas integrações com **Origem** estados. Na importação, esses estados são mapeados para **Destino** e. **Motivo de destino** em sua instância, porque, em alguns casos, não há correspondências exatas entre os estados de origem do scanner e os estados usados pela instância.

Por exemplo, estados de origem como **Não Corrigirá** , **Correção adiada** , **Risco aceito** e **Risco mitigado** em Integrações de vulnerabilidade do Fortify são mapeados para **Adiado** estado com um subestado de **Risco aceito** ou **Mitigação do controle em vigor** em sua instância.

Você tem as seguintes opções nas páginas de configuração para essas integrações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção marcada	Descrição
Gerencie exceções em ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar exceções de registros AVI. Avis importados marcados para **Adiado** os estados são triados com ServiceNow Fluxo de trabalho da Gestão de exceções. Avis com **Origem** estados que normalmente são mapeados para um **Adiado** os estados são mapeados para **Estado de triagem de destino** em **Aberto** estado.
	N	Se você desativar a caixa de seleção, preservará **Origem** estados importados do scanner. Esses Avis são mapeados para **Estado de destino** . **Adiado** e para um **Motivo de destino** em sua instância. Eles não são triados pelo fluxo de trabalho de exceção porque não são mapeados para **Triagem de destino** estado e. **Motivo da triagem de destino** estados. . **Exceção de solicitação** A ação de IU não está disponível no registro AVI, porque o registro já está no **Adiado** Estado de destino.

Caso de uso para falso positivo

Para falsos positivos do Integração de Resposta a vulnerabilidades com Veracode como exemplo, estados de origem como **Falso-positivo** ou **Possível falso-positivo** são mapeados para **Encerrado Estado de destino** com um subestado de **Falso-positivo** .

Opção	Caixa de seleção marcada	Descrição
Gerencie falsos positivos em ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção marcada	Descrição
		um **Falso-positivo** De registros AVI. Avis importados marcados para **Falso-positivo** ou **Possível falso-positivo** os estados são triados com ServiceNow Fluxo de trabalho da Gestão de exceções. Avis com **Origem** estados que normalmente são mapeados para um **Encerrado Estado de destino** são mapeados para um **Triagem de destino** estado em **Aberto** . . **Falso-positivo** A ação de IU está disponível no registro AVI.
	N	Se você desativar a caixa de seleção, preservará **Origem** estados importados do scanner. Esses Avis são mapeados para **Estado de destino** . **Encerrado** e um **Motivo de destino** estado em **Falso-positivo** em sua instância. Eles não são triados pelo fluxo de trabalho de falso-positivo. . **Falso-positivo** A ação de IU não está disponível no registro AVI, porque o registro já está no **Encerrado** Estado de destino.

referências de Resposta a vulnerabilidades de aplicações

Os termos a seguir são usados em Resposta a vulnerabilidades de aplicações.

Itens vulneráveis à aplicação (Avis)

Emparelhamentos de entradas de vulnerabilidade e aplicações potencialmente vulneráveis no ambiente da sua empresa.

Regras de atribuição

Regras usadas para atribuir Avis com base nos critérios definidos.

Enumeração de plataforma comum (CPE)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um esquema de nomenclatura estruturada NIST NIST NVD para sistemas de tecnologia da informação, software e pacotes.

Vulnerabilidades e Exposições Comuns (CVE)

Dicionário de vulnerabilidades e exposições de segurança da informação conhecidas publicamente.

Enumeração de pontos fracos comuns (CWE)

Lista de tipos de pontos fracos de software desenvolvidos pela comunidade.

Integrações

Trabalhos agendados que extraem dados de relatório do CWE ou de um sistema de terceiros, como Veracode, para recuperar dados de vulnerabilidade.

> **Nota:** Se a integração do banco de dados nacional de vulnerabilidades do NIST no Resposta a vulnerabilidades Está ativado e configurado, o aprimoramento de CVE está disponível para CWEs, mas não é necessário. Para obter informações sobre a integração do NIST National Vulnerability Database, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.

Banco de dados nacional de vulnerabilidades (NVD)

Repositório do governo dos EUA de dados de gestão de vulnerabilidades baseados em padrões representados usando o Security Content Automation Protocol (SCAP).

Regras de destino de correção

Regras usadas para atribuir datas de destino do Avis para correção com base nos critérios definidos.

Calculadoras de Vulnerabilidade

Calculadoras usadas para priorizar e categorizar vulnerabilidades da aplicação com base nos critérios definidos.

Exemplo de regra de exceção para Resposta a vulnerabilidades de aplicações

Um exemplo de regra baseada em uma vulnerabilidade conhecida para uma regra de exceção.

Campo	Descrição
Nome	Um nome exclusivo para ajudar você a identificar sua finalidade e localizar a regra com facilidade, por exemplo, `Exceção Veracode-1 cwe-22` .
Estado	Somente leitura: Rascunho
Válida de	Data em que esta regra está ativa para adiar AVIS.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor mais baixo precede um maior.
Válida até	Data em que a tarefa de correção para de aceitar novos VIS.
Adiado até	Data até quando as tarefas de correção e os AVIS são adiados. Nesta data, o AVUL está encerrado, todos os Avis saem da tarefa e são reabertos. As regras de grupo são reaplicadas a esses AVIS.
Motivo	Motivo para criar esta regra de exceção. Selecione um na lista, por exemplo, **Correção Indisponível** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	Grupo atribuído para rastrear o VIS adiado, por exemplo, gerenciador de segurança da APLICAÇÃO.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção. Neste exemplo, Adie a Avis com a vulnerabilidade - Veracode-1-22.
Condição	Condições de filtro para especificar quais Avis correspondem a esta regra. Para este exemplo, A vulnerabilidade é Veracode-1-22 .
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente pelo trabalho agendado *Associate existing AVIs with Auto Exception Rule*começando com novos dados. Se você habilitar a opção Executar nos dados existentes, um trabalho agendado será executado uma vez nos dados existentes no **Válido de** data.

Exibição de produto do Resposta a vulnerabilidades de aplicações

O produto Application Vulnerability Response (AVR) ingere os pontos fracos e vulnerabilidades detectados por suas ferramentas de teste de segurança de aplicações e fornece um único painel para entender a postura de segurança de todas as aplicações em seu ambiente.

O AVR permite reduzir os riscos com os fluxos de trabalho de correção. O objetivo desta exibição de produto é ajudar você a entender como as entidades-chave do AVR funcionam com a estrutura principal do CSDM.

Terminologia atualizada

A partir do AVR v19.0, a tabela de chaves e os nomes de coluna a seguir foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação.

Lista atualizada de termos, tabelas e nomes de campos para AVR

Anterior ao AVR v19.0	A partir do AVR v19.0
Regras de pesquisa de IC	Regras de pesquisa
Formulário de regra de pesquisa de IC	Formulário de regra de pesquisa
Regra de correspondência de IC	Regra de correspondência
Pesquisar na tabela	Pesquisar na tabela de IC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista atualizada de termos, tabelas e nomes de campos para AVR

Anterior ao AVR v19.0	A partir do AVR v19.0
Pesquisar no campo	Pesquisar no campo de IC
Versão da aplicação	Aplicações descobertas
Tabela de versão da aplicação	Tabela Aplicações descobertas
Criticalidade dos negócios	Criticalidade dos negócios de origem

Pré-requisitos

Instale as versões mais recentes dos seguintes aplicativos:

- Security Support Common
- Resposta a vulnerabilidades
- Framework de integração de segurança
- Orquestração do suporte de segurança
- Integrações de scanner, como Veracode e FORTIFY

AVR e CSDM 4,0

Antes do AVR v19.0, quando as vulnerabilidades da aplicação eram ingeridas, a aplicação para a qual as vulnerabilidades eram ingeridas era pesquisada usando as regras de pesquisa de IC em relação às aplicações verificadas (sn_vul_app_scan_application). Se o registro do nome da aplicação não estiver lá, uma entrada será feita.

A partir do AVR v19.0, para alinhar com a estrutura do CSDM 4,0, as tabelas de Modelo de produto são usadas em vez da tabela Aplicações verificadas. Se a aplicação tiver a versão, a pesquisa será em relação à tabela Modelo de software. Se não houver versão, a pesquisa será comparada à tabela Modelo de aplicação. Modelo de aplicação e Modelo de software são tabelas secundárias da tabela Modelo de produto, que é a tabela de base no CMDB. A captura de tela a seguir explica o Modelo do produto.

Propriedade do sistema

Para usar o processo de pesquisa baseado em modelo de produto CSDM 4,0, defina a propriedade do sistema `sn_vul.use_product_model`. `true`.

Considerações de propriedade do sistema

Nome da propriedade do sistema	Valor da propriedade do sistema	Valor de destino da pesquisa	Considerações
sn_vul.use_product_model	verdadeiro	Selecione o valor **Modelo do produto**	Novos usuários devem selecionar o valor **Modelo do produto** Para usar as regras de pesquisa de modelo de produto da estrutura do CSDM 4,0.
	falso	Selecione o valor **Item de configuração**	Os usuários existentes podem continuar usando o processo de pesquisa de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Considerações de propriedade do sistema

Nome da propriedade do sistema	Valor da propriedade do sistema	Valor de destino da pesquisa	Considerações
			IC e o existente **Regras de pesquisa de IC** .

Nota: Para definir o valor de destino da pesquisa, navegue até **Regra de pesquisa** página > **[Regra de pesquisa de integração do AVR]** > **Destino de pesquisa** campo.

Regras de pesquisa no AVR

Na estrutura do CSDM 4,0, regras de pesquisa baseadas em modelo de produto são usadas em vez de regras de pesquisa de IC para criar entradas nas respectivas classes de modelo de produto. Da mesma forma para scripts, você pode definir as regras de pesquisa na estrutura do modelo CSDM 4,0.

A partir do AVR v19.0, ao criar uma regra de pesquisa, você deve definir se deseja usar o item de configuração ou a abordagem do modelo de produto usando **Destino de pesquisa** campo. Para obter mais informações, consulte Crie uma regra de pesquisa de IC.

Aplicações descobertas

Navegar até **Tudo** > **Aplicações descobertas**. A tabela Aplicações descobertas exibe as aplicações ingeridas dos scanners. Se for a propriedade do sistema `sn_vul.use_product_model`está definido como `true`, você pode ver os modelos de produto correspondentes para as aplicações.

Considerações do AVR

Presença de IC duplicado ou registros de modelo de produto

Verifique se a propriedade do sistema `sn_vul.use_product_model`foi configurado corretamente para o processo de pesquisa. Certifique-se de selecionar um dos dois **Item de configuração** ou **Modelo do produto** Como o destino de pesquisa ao configurar o formulário Regra de pesquisa.

Contêiner de Resposta a vulnerabilidades

. ServiceNow® Contêiner de Resposta a vulnerabilidades a aplicação importa itens vulneráveis do contêiner (CVITs) e, de acordo com as regras, permite corrigir vulnerabilidades de contêiner. Os dados de vulnerabilidade são extraídos de fontes internas e externas, como o National Vulnerability Database (NVD) ou integrações de terceiros.

Solicitar aplicativos na Store

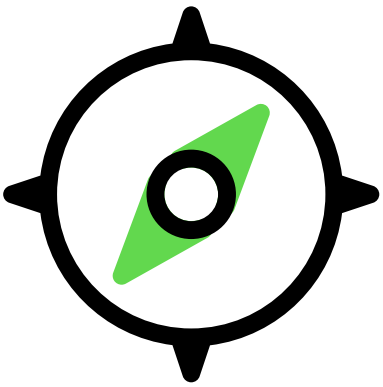
Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

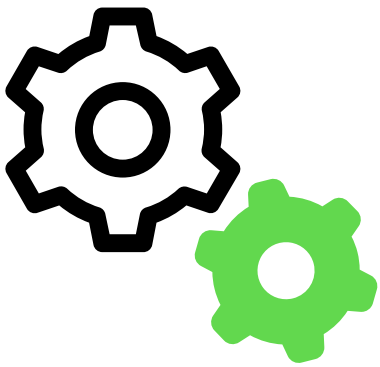
Contêiner de Resposta a vulnerabilidades

Explorar



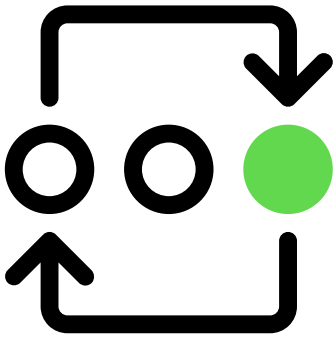
Saiba mais sobre os conceitos e recursos de Resposta a vulnerabilidades de contêiner.

Configurar



Configurar Resposta a vulnerabilidades do contêiner.

Integrar



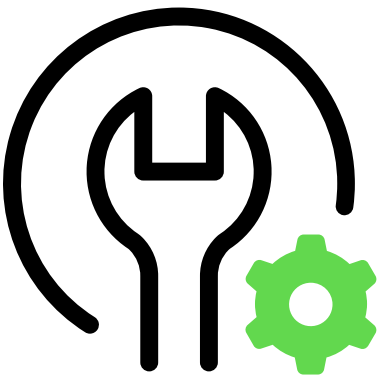
Estenda o contêiner Vulnerability Response integrando-o a outras aplicações.

Use os Espaços de resposta a vulnerabilidades



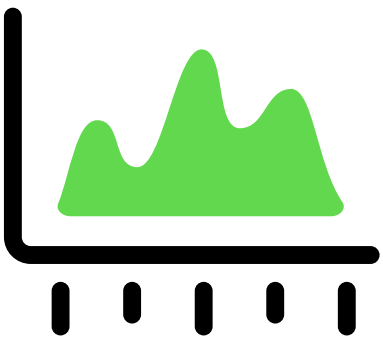
Saiba como monitorar, gerenciar e corrigir CVITs nos espaços de trabalho Gerenciador de vulnerabilidades, Correção de TI e Avaliação de vulnerabilidades.

Corrigir



Saiba como corrigir vulnerabilidades de contêiner.

Análise e emissão de relatórios



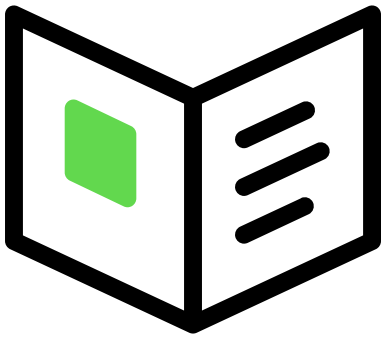
Exibir análise de Resposta a vulnerabilidades do contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contêiner de Resposta a vulnerabilidades

Referência



Obtenha detalhes sobre os componentes de Resposta a vulnerabilidades do contêiner, como campos, tabelas e propriedades.

Benefícios

. Contêiner de Resposta a vulnerabilidades a aplicação oferece os seguintes benefícios:

- Integra-se a produtos de segurança de contêiner de terceiros, como Prisma Cloud Compute da Palo Alto Networks.
- Importa dados de vulnerabilidade para as imagens implantadas no tempo de execução e enriquece os dados de vulnerabilidade com informações contextuais do tempo de execução (hosts, clusters do Kubernetes, serviços e namespaces).
- Fornece uma lista das referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes no Configuration Management Database (CMDB) usando ServiceNow Descoberta do Kubernetes.
- Oferece um painel de emissão de relatórios abrangente, fornecendo informações sobre as tendências de vulnerabilidade e correção.

Principais recursos

. Contêiner de Resposta a vulnerabilidades a aplicação gerencia vulnerabilidades detectadas nos contêineres. Ele fornece os seguintes recursos:

- Aponte para a imagem do Docker de origem dos CVITs em vez de contêineres em execução.
- Configure a granularidade de CVITs para rastrear na imagem, no cluster do Kubernetes, no namespace ou no nível de serviço.
- Rastreie novas versões de imagem para identificar vulnerabilidades corrigidas. Todas as vulnerabilidades relatadas em versões mais antigas são resolvidas automaticamente em ServiceNow quando novas versões de imagem são implantadas no tempo de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Rastreie CVITs em imagens de base separadamente das imagens da aplicação para permitir correção independente.
- Gere solicitações de exceção ou solicitações falso-positivas, que podem ser revisadas por meio de um processo de aprovador multinível.
- Defina regras de exceção para adiar CVITs automaticamente.

Casos de uso

Os contêineres são uma ótima maneira de implantar e dimensionar aplicações em vários ambientes com menos sobrecarga e maior portabilidade. No entanto, as vulnerabilidades nas imagens de contêiner podem representar risco para o host subjacente e, por fim, para a infraestrutura em que os contêineres foram iniciados a partir dessas imagens. Embora existam muitos produtos de segurança de contêiner que verificam vulnerabilidades nas imagens de contêiner, há algumas considerações e problemas associados à correção das vulnerabilidades. Contêiner de Resposta a vulnerabilidades pode ajudar a resolver vários problemas ou casos de uso envolvidos na correção de vulnerabilidades da imagem do contêiner. Explore maneiras de aproveitar o Contêiner de Resposta a vulnerabilidades módulo:

Contexto de tempo de execução

As vulnerabilidades em imagens de contêiner podem ser descobertas verificando a imagem nas fases a seguir do ciclo de vida da aplicação.

- Fase 1: Quando as imagens estão sendo criadas no pipeline de IC/CD.
- Fase 2: Quando as imagens são publicadas no registro
- Fase 3: Quando as imagens são implantadas no tempo de execução.

Embora seja importante identificar vulnerabilidades o mais cedo possível nas fases 1 e 2, executar uma verificação nas imagens implantadas em um ambiente de tempo de execução é igualmente importante. Oferece os seguintes benefícios:

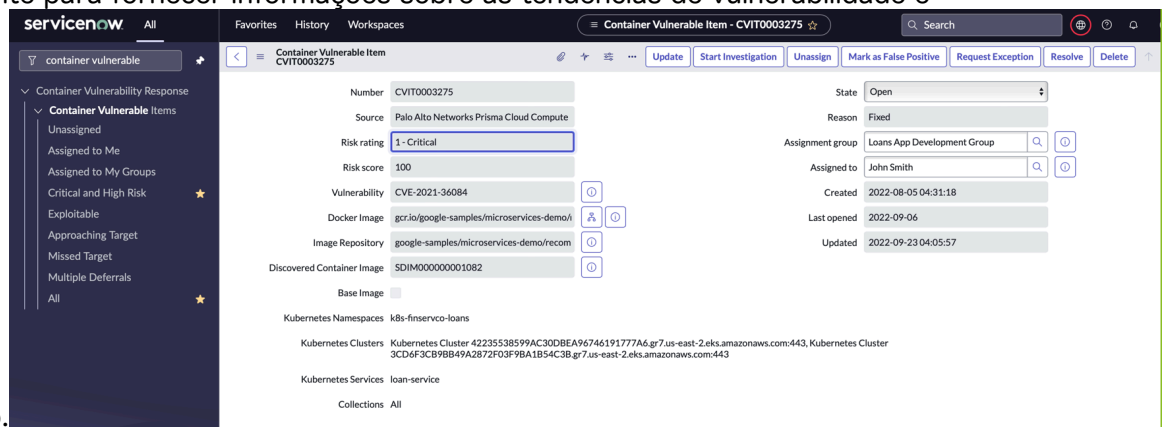
- Identificar todas as novas vulnerabilidades e exposições comuns (CVEs) publicadas.
- Fornecer visibilidade precisa da postura de risco das aplicações implantadas.
- Priorização de vulnerabilidades que devem ser resolvidas. O contexto de tempo de execução em termos de serviços de aplicações ou serviços de negócios afetados devido a uma vulnerabilidade pode ajudar na priorização.

Contêiner de Resposta a vulnerabilidades Integra-se a produtos de segurança de contêiner, como Prisma Cloud Compute de Palo Alto Networks Extrair os dados de vulnerabilidade dessas imagens implantadas no tempo de execução e enriquecer os dados de vulnerabilidade com as informações contextuais do tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces em que essas imagens de contêiner são implantadas. Clientes que usam o. ServiceNow A descoberta do Kubernetes pode ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em Configuration Management Database (CMDB). Além de enriquecer os metadados, ServiceNow também oferece um painel de emissão de relatórios

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

abrangente para fornecer informações sobre as tendências de vulnerabilidade e correção.



Identificar a propriedade

Pré-requisitos

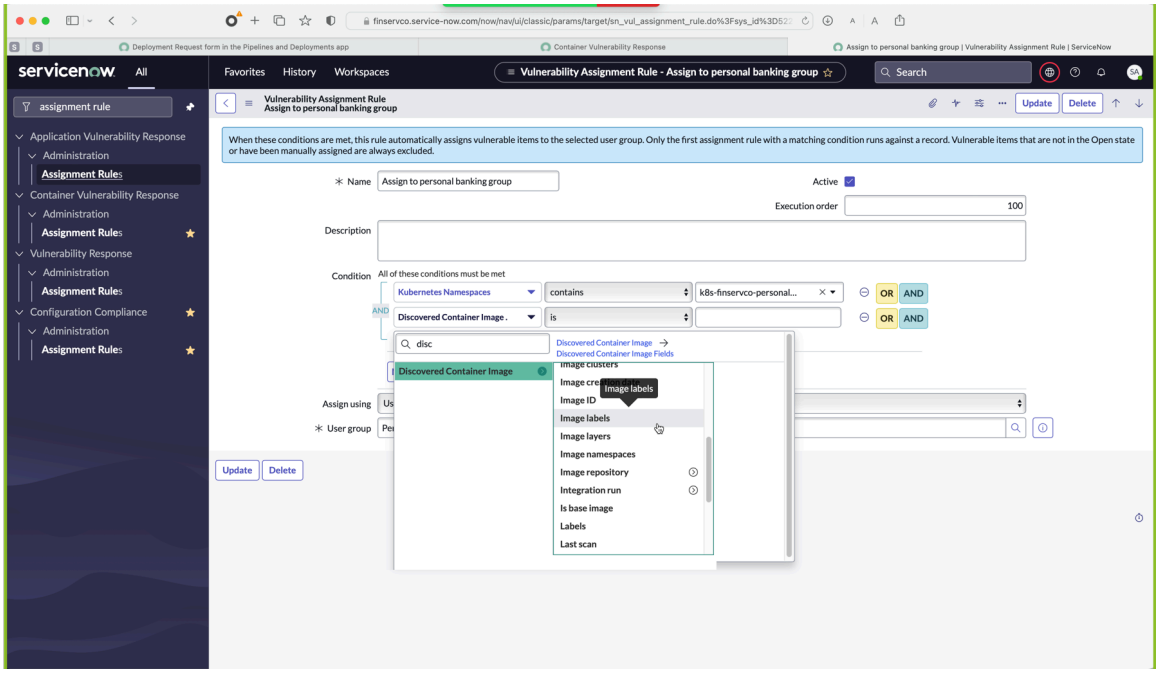
- **Metadados e referências do Kubernetes** : Para Contêiner de Resposta a vulnerabilidades Para preencher metadados do Kubernetes (namespace, cluster e assim por diante) e referências a Configuration Management Database (CMDB), você deve implementar a descoberta do Kubernetes de Information Technology Operations Management(ITOM). A descoberta do Kubernetes preenche a imagem do Docker, os contêineres do Docker, os pods, os clusters do Kubernetes e assim por diante no CMDB. Contêiner de Resposta a vulnerabilidades Identifica a imagem do Docker no CMDB Com base no ID da imagem, e identifica as entidades do Kubernetes relacionadas e preenche as referências a essas entidades de itens vulneráveis.
- **Metadados de nuvem e rótulos de imagem do Docker** : Contêiner de Resposta a vulnerabilidades Também preenche rótulos de imagem do Docker, IDs de conta de nuvem e regiões em que uma imagem é implantada. Esses dados são mantidos no registro "Imagem do contêiner descoberta" associado ao item vulnerável. Esses dados não são pré-requisitos para serem preenchidos. Contêiner de Resposta a vulnerabilidades Usa os dados retornados por produtos de segurança de contêiner (por exemplo, Palo Alto Prisma Cloud Compute) para preencher essas entradas.

A propriedade para corrigir uma vulnerabilidade em uma imagem de contêiner pode variar de organização para organização. Essas informações podem ser capturadas em lugares diferentes. Algumas organizações usam rótulos de imagem do Docker como uma maneira de identificar as equipes de aplicações que possuem uma determinada imagem de contêiner, enquanto outras organizações podem usar o namespace do Kubernetes ou a conta de nuvem em que uma imagem de contêiner é implantada para identificar o proprietário certo.

Contêiner de Resposta a vulnerabilidades Fornece os elementos de modelo de dados necessários para capturar e usar os rótulos de imagem do Docker, os metadados de cluster/serviço/namespace do Kubernetes ou os metadados da conta de nuvem (ID da conta de nuvem, região, provedor e assim por diante) no módulo "Regras de atribuição" e atribuir automaticamente vulnerabilidades à equipe de aplicação certa com base nos metadados da imagem ou do ambiente de tempo de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



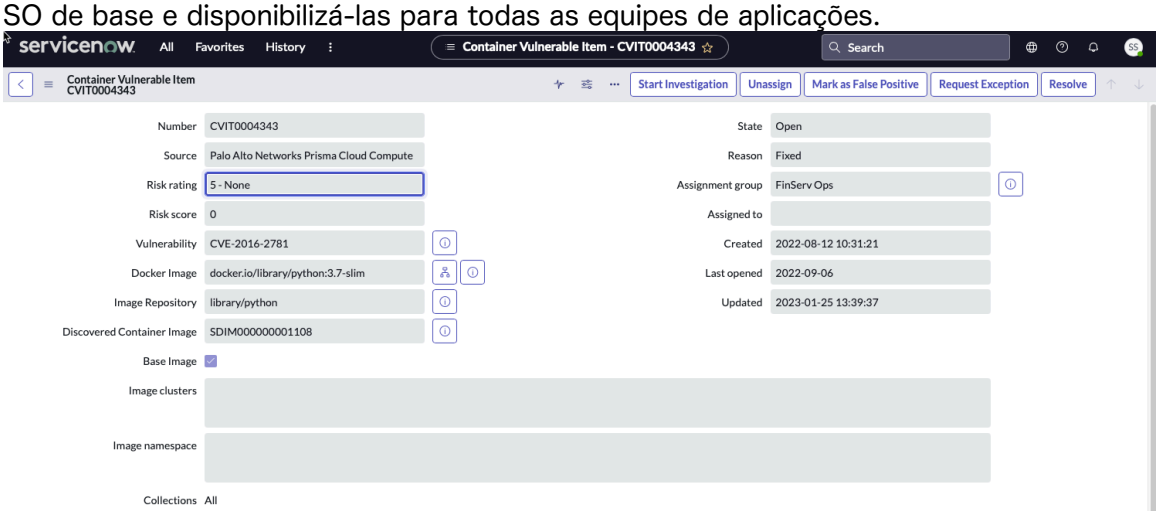
Rastreie vulnerabilidades nas imagens de base

Pré-requisitos

Para a propriedade "Imagem de base" a ser preenchida em Contêiner de Resposta a vulnerabilidades as imagens de base devem ser configuradas explicitamente no Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute console. Para obter mais informações sobre como configurar imagens de base no Prisma Cloud, consulte https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/vulnerability_management/base_images.

Contêiner de Resposta a vulnerabilidades permite a criação de registros de vulnerabilidade separados para uma camada de base para que eles possam ser atribuídos a uma equipe diferente.

Rastreie vulnerabilidades identificadas em uma imagem do SO de base, como Alpine, a partir das vulnerabilidades detectadas em outras camadas da imagem do contêiner. Muitas organizações têm equipes dedicadas que são responsáveis por corrigir imagens do SO de base e disponibilizá-las para todas as equipes de aplicações.



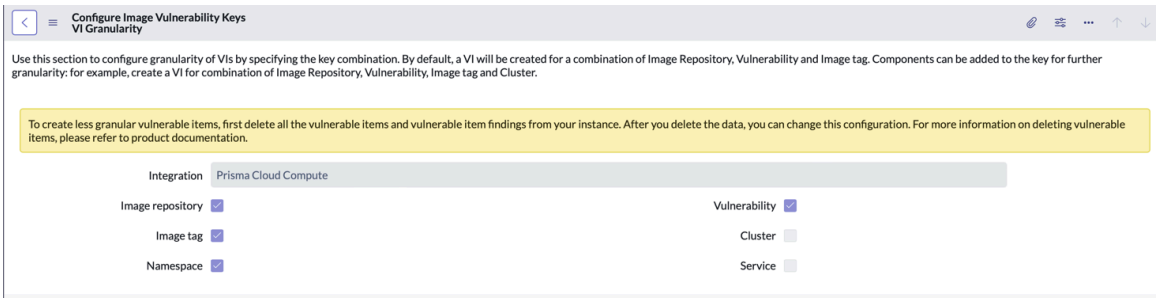
Defina granularidade para itens vulneráveis

Tradução automática

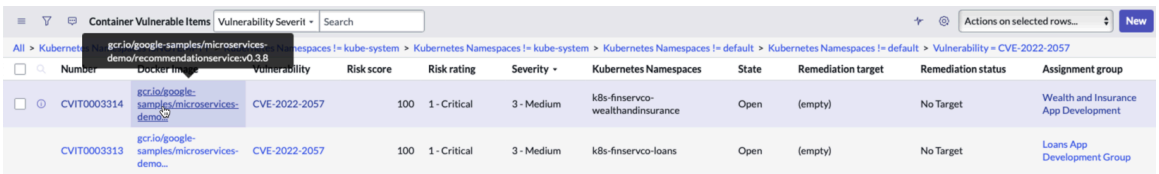
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Para configurar a granularidade dos CVITs navegando até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Configurar granularidade de IV**.



Por padrão, um item vulnerável é criado para cada combinação exclusiva de CVE e a versão da imagem do Docker (referência e marcador). No entanto, algumas imagens do Docker podem ser implantadas em mais de um namespace do Kubernetes e cada namespace pode pertencer a diferentes unidades de negócios ou equipes. Cada equipe pode seguir sua própria cadência para implantar novas versões de imagens de contêiner para corrigir vulnerabilidades. Para acomodar este cenário, Contêiner de Resposta a vulnerabilidades Permite que você defina granularidade para itens vulneráveis: Se um item vulnerável deve ser criado para cada namespace/cluster/serviço do Kubernetes, mesmo para cada combinação exclusiva de versão e vulnerabilidade da imagem do Docker.



No exemplo, você pode ver dois itens vulneráveis criados para a mesma combinação de imagem do Docker e CVE. Um para o namespace do Kubernetes "k8s-finservco-loans" e o outro para "k8s-finservco-wearchandinsurance".

Identifique os serviços afetados usando a identificação de serviço baseada em marcador

Pré-requisitos

- Identifique vários serviços em sua aplicação e defina os pares de marcadores/chave-valor que representam esses serviços.
- Implante imagens do Docker e pods do Kubernetes com esses marcadores ou rótulos.
- Descoberta do Kubernetes do ITOM Defina "Serviços baseados em marcador" com os marcadores ou rótulos corretos.
- Implantar a Descoberta do Kubernetes do ITOM
- Defina "Serviços baseados em marcador" com os marcadores corretos ou os pares de chave-valor.
- Importar dados de vulnerabilidade para ServiceNow usando Contêiner de Resposta a vulnerabilidades

O cálculo de risco para itens vulneráveis pode ser feito analisando o IC (imagem do Docker) e a criticidade dos serviços associados em CMDB. No entanto,

Tradução automática

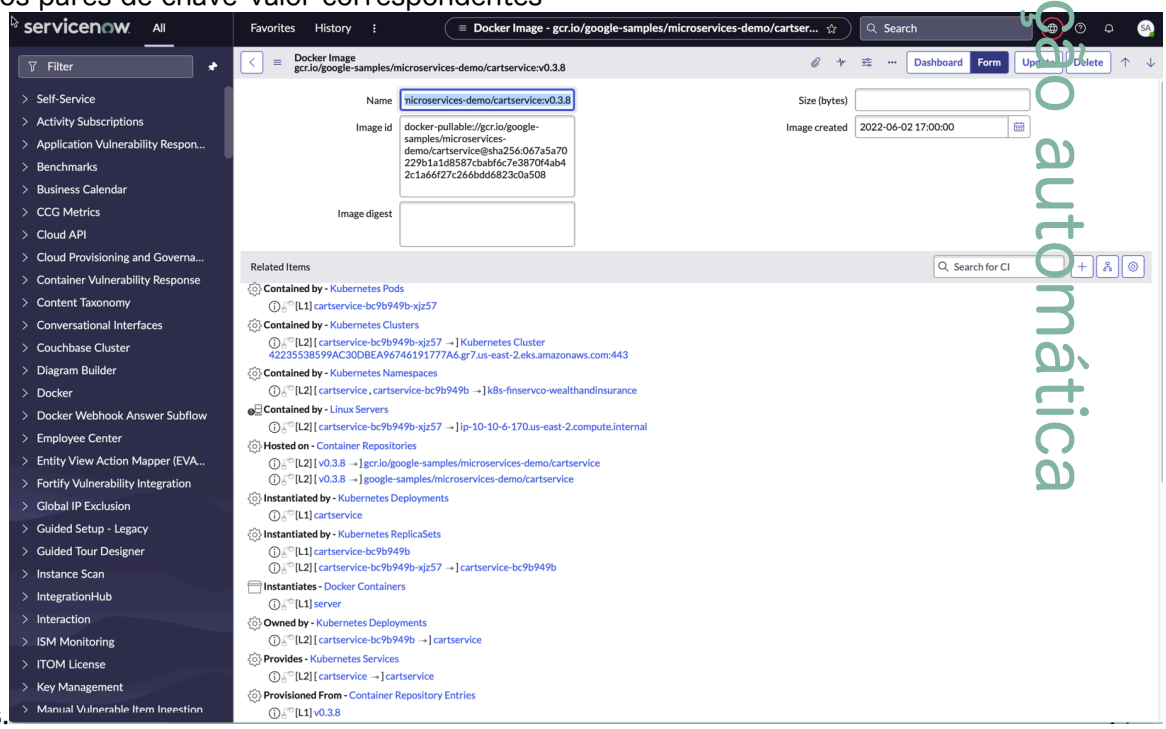
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para facilitar a identificação dos serviços afetados, Contêiner de Resposta a vulnerabilidades oferece identificação de serviço baseada em marcador.

Quando os pods ou entidades do Kubernetes são publicados com valores de chave ou rótulos correspondentes aos valores de chave definidos em qualquer "Serviço baseado em marcador" em ServiceNow, Contêiner de Resposta a vulnerabilidades Estabelece automaticamente o relacionamento entre uma imagem do Docker e o serviço de aplicações afetado e usa a criticidade desse serviço de aplicações no cálculo de risco.

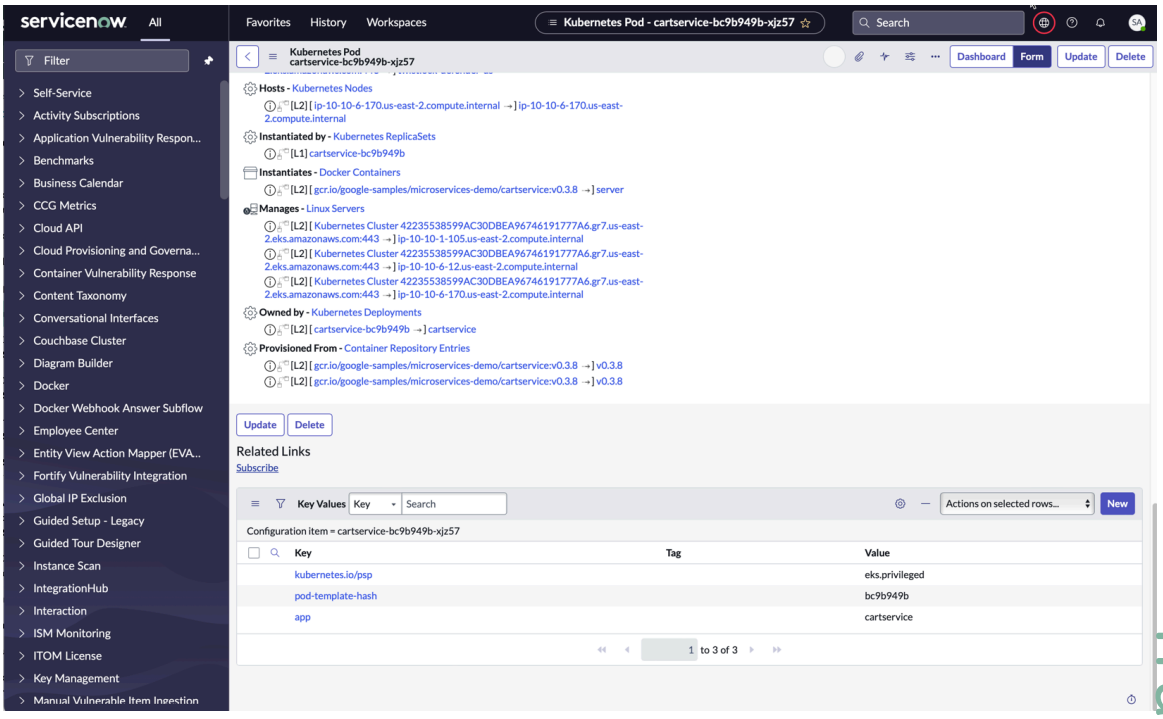
O fluxo é o seguinte:

1. Contêiner de Resposta a vulnerabilidades importa dados de vulnerabilidade do produto de segurança de contêiner.
2. Para cada item vulnerável de contêiner, Contêiner de Resposta a vulnerabilidades Preenche a imagem do Docker de CMDB que tem a vulnerabilidade.
3. Contêiner de Resposta a vulnerabilidades Em seguida, verifica os rótulos de imagem do Docker ou os rótulos/valores de chave publicados com os pods do Kubernetes em que esta imagem está implantada. Esta imagem está disponível em CMDB Se você tiver a descoberta do Kubernetes em execução.
4. Contêiner de Resposta a vulnerabilidades Em seguida, pesquisa "Serviços baseados em marcador" em CMDB com os mesmos pares de chave-valor correspondentes definidos.

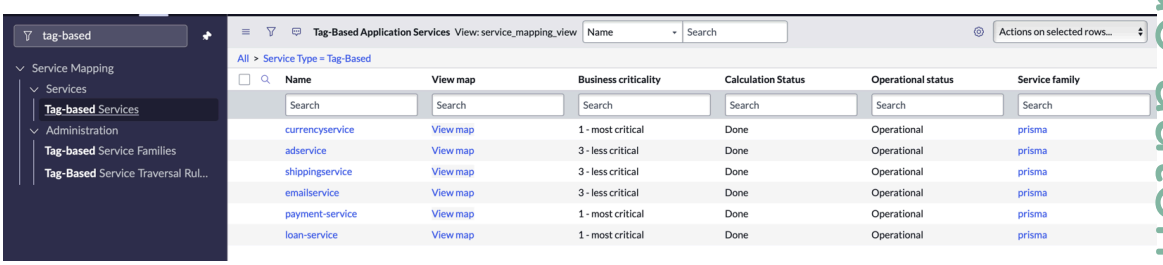


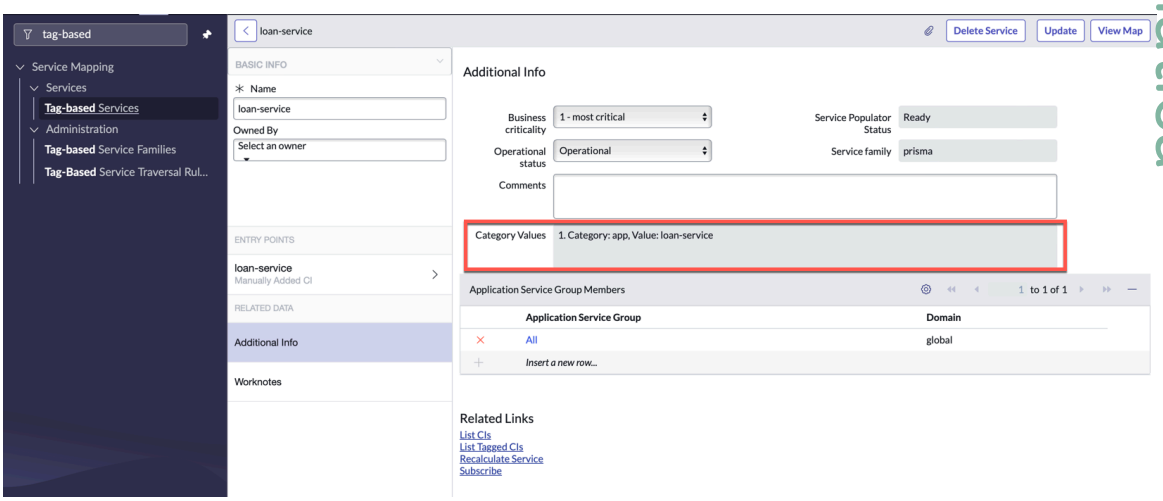
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Contêiner de Resposta a vulnerabilidades Usa a "Criticalidade comercial" do "Serviço baseado em marcador" correspondente (se houver) para calcular o risco de um item vulnerável de contêiner.





Rastreamento de vulnerabilidades

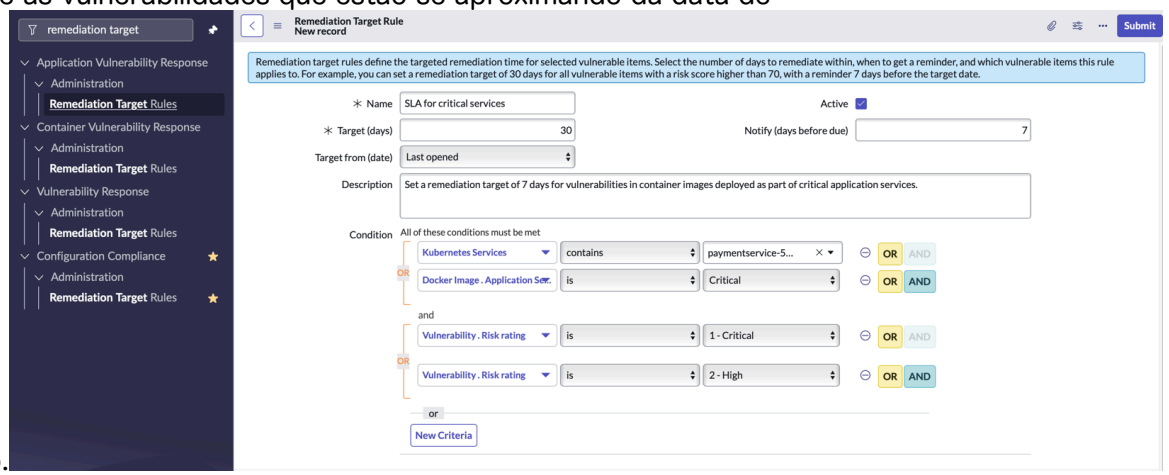
Definir metas de correção

ServiceNow Permite que os gerentes de vulnerabilidades definam "regras de destino de correção" para poder definir acordos de nível de serviço (ANS) para corrigir vulnerabilidades encontradas em imagens de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A data de destino de correção pode ser definida com base em uma condição/critério nos metadados da imagem ou nas informações de vulnerabilidade. Os responsáveis pela correção recebem comunicação por e-mail sobre as vulnerabilidades que estão se aproximando da data de vencimento.



Identificar vulnerabilidades corrigidas

Ao contrário das vulnerabilidades de host que podem ser corrigidas pela aplicação de um patch em um host, as vulnerabilidades de contêiner não podem ser corrigidas. Novas versões de imagens de contêiner devem ser criadas e implantadas para substituir as versões mais antigas. As novas versões têm um identificador (ID de imagem) diferente em comparação com as versões anteriores, o que torna difícil rastrear quais vulnerabilidades já foram corrigidas.

ServiceNow Identifica vulnerabilidades que foram relatadas nas versões anteriores das imagens do contêiner, mas resolvidas na versão mais recente da imagem e move automaticamente essas vulnerabilidades para o estado "Encerrado/Corrigido" para que as equipes de segurança sempre tenham visibilidade precisa da postura de risco mais recente.

Gerenciar exceções

As equipes de aplicações ou responsáveis pela correção das vulnerabilidades podem precisar da capacidade de solicitar uma exceção devido aos seguintes motivos.

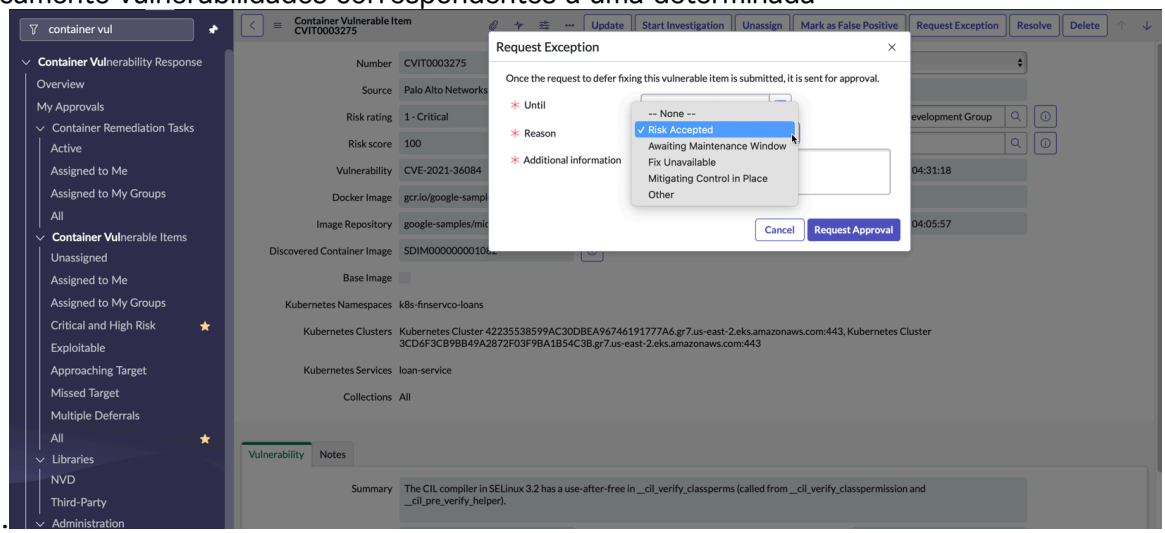
- Um controle de mitigação já está em vigor
- Risco aceito
- Aguardando janela de manutenção para enviar a correção por push.

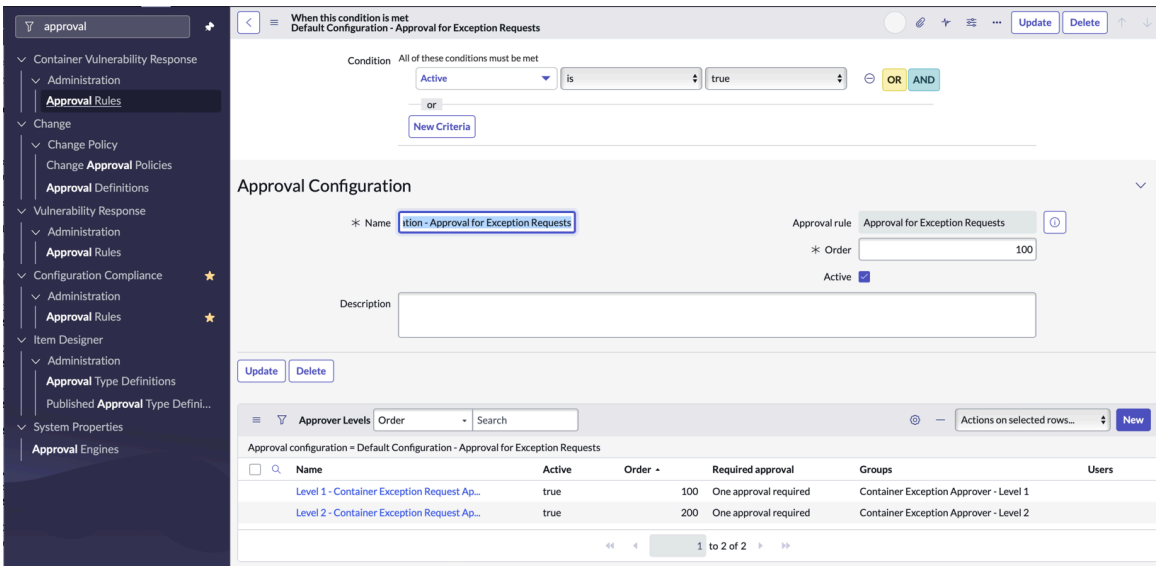
ServiceNow permite que os administradores de segurança definam vários níveis de aprovadores para solicitações de exceção. Você também pode definir regras de exceção automática que podem ser usadas para adiar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

automaticamente vulnerabilidades correspondentes a uma determinada condição.





Tradução automática

Novidades

Para saber mais sobre o que há de novo e o que mudou em Zurich, consulte Zurich notas da versão.

Iniciar

- Para obter uma visão geral sobre Operações de segurança em seu ServiceNow AI Platform instância, consulte Noções básicas sobre Operações de segurança .
- Para obter informações sobre todos os Operações de segurança aplicações disponíveis para download no ServiceNow Store, consulte Operações de segurança e ServiceNow Store .

Explorando Contêiner de Resposta a vulnerabilidades

. Contêiner de Resposta a vulnerabilidades A aplicação importa itens vulneráveis ao contêiner (CVITs). De acordo com as regras, o recurso permite corrigir as vulnerabilidades do contêiner. Contêiner de Resposta a vulnerabilidades está disponível por meio de uma assinatura separada.

Ao contrário das aplicações tradicionais, os contêineres empacotam todos os códigos-fonte da aplicação junto com suas dependências em um arquivo binário chamado imagem

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de contêiner. A imagem é publicada em um registro para fornecer uma opção para executar esta imagem como uma aplicação ou uma instância de contêiner em qualquer plataforma. As fases no ciclo de vida de pré-implantação de um contêiner são as seguintes:

1. Compor a imagem do contêiner: A imagem do contêiner é composta e apontada para um código-fonte ou uma biblioteca dependente.
2. Crie a imagem do contêiner
3. Publicar a imagem do contêiner: O arquivo de imagem do contêiner é publicado em um registro. Cada imagem tem seu próprio ID exclusivo com base no conteúdo da imagem. Essas imagens são extraídas do registro para o ambiente de tempo de execução no modo pós-implantação. Em seguida, as imagens são executadas como instâncias de contêiner no host no ambiente de produção.

Verificando imagens do contêiner

Uma imagem de contêiner pode ser verificada em busca de vulnerabilidades antes ou depois da implantação. Se as imagens de contêiner forem verificadas durante a fase de pré-implantação, você poderá receber muitos alertas de vulnerabilidade, que podem não precisar de atenção imediata. No entanto, a verificação de vulnerabilidades durante a fase de pós-implantação fornece benefícios maiores, como os seguintes:

- Fornecer visibilidade sobre o risco associado às aplicações implantadas.
- Fornecendo uma exibição focada somente nas imagens no ambiente de produção.
- Identificar e priorizar as vulnerabilidades que devem ser tratadas imediatamente.
- Agrupamento e atribuição de vulnerabilidades com base nos metadados da imagem. Por exemplo, um repositório de imagens, um rótulo de imagem e outros atributos relacionados à imagem do contêiner podem ser usados para regras de agrupamento e atribuição.

Cada imagem de contêiner tem os seguintes componentes principais:

- Repositório de imagens ou contêiner: Representa a imagem do docker com um determinado repositório ou nome. Ele hospeda todas as versões da imagem.
- Imagem do Docker: Representa uma versão específica da imagem do docker de compilação.
- Docker Container: Representa uma instância em execução da imagem do docker. Cada versão tem um ID exclusivo e tem várias instâncias dos contêineres em execução no ambiente de produção.

Contêiner de Resposta a vulnerabilidades módulos

. Contêiner de Resposta a vulnerabilidades o módulo fornece detalhes sobre o seguinte:

Itens vulneráveis de contêiner

Os itens vulneráveis ao contêiner (CVITs) são agrupados e listados com base na atribuição, criticidade, exploração e status de correção.

Bibliotecas

Obtenha acesso ao National Vulnerability Database (NVD) e às bibliotecas de terceiros. Embora a biblioteca NVD forneça informações limitadas ao ID do item de vulnerabilidade, a biblioteca de terceiros fornece a maioria dos detalhes sobre um item de vulnerabilidade. As informações na tela NVD são preenchidas somente quando a integração NVD é acionada.

Administração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O módulo Administração fornece informações sobre as regras de atribuição dos itens vulneráveis, regras de destino de correção e integrações de vulnerabilidade do contêiner. Além disso, você também pode configurar a duração após a qual um item vulnerável deve ser encerrado automaticamente. Você pode usar a seção Configurar granularidade de VI para configurar a granularidade de CVITs especificando as combinações de teclas. Por padrão, um CVIT é criado para uma combinação de um repositório de imagens, um marcador de imagem e uma vulnerabilidade. Você pode adicionar componentes adicionais à chave para obter granularidade adicional. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, marcador de imagem, vulnerabilidade e cluster.

Versões disponíveis

Versão de lançamento	Notas da versão
Contêiner de Resposta a vulnerabilidades v2.1 Contêiner de Resposta a vulnerabilidades v 2,06 Contêiner de Resposta a vulnerabilidades v2.0.4	Notas da versão do Resposta a vulnerabilidades do contêiner Para obter informações de compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .

Contêiner de Resposta a vulnerabilidades tarefa de correção e estados de item vulnerável do contêiner

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

estados da tarefa de correção

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

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

Fluxo de estado de Resposta a vulnerabilidades do contêiner

Nota:

- Itens vulneráveis do contêiner não podem ser fechados manualmente.
- Cada formulário de tarefa contém **Seguir** e. **Atualização** botões que são padrão para ServiceNow tarefas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção e transição de estado de CVIT e ordem de precedência

Tarefas de correção e estados de itens vulneráveis podem afetar uns aos outros. Na maioria das vezes, um estado de tarefa de correção atualiza o estado do item vulnerável, com o estado de tarefa de precedência mais alta usado para atualizar os itens vulneráveis no grupo.

Da criação ao fechamento de uma tarefa de correção de contêiner, ela faz a transição por vários estados durante todo o processo de correção.

A precedência de estado é a seguinte:

Encerrado > **Adiado** > **Resolvido** > **Em revisão** > **Aguardando Implementação** > **Sob Investigação** > **Aberto**

A transição de estado acontece conforme você executa várias ações, como adiar, abrir, fechar etc.

As ações que você pode executar em uma tarefa de correção de contêiner em um estado específico são semelhantes às de uma tarefa de correção de host. Para obter mais informações, consulte Resposta a vulnerabilidades estados da tarefa de correção e. Cenários de roll-up e roll-down de estado em Resposta a vulnerabilidades documentação.

Configuração da Contêiner de Resposta a vulnerabilidades

Antes de executar Contêiner de Resposta a vulnerabilidades em seu ServiceNow AI Platform instância, você deve configurá-la.

Instalar Vulnerability Response e Configuration Compliance para contêineres

Antes de executar o. Vulnerability Response e Configuration Compliance para contêineres aplicação em seu ServiceNow AI Platform, você deve obter direito e baixar a aplicação do ServiceNow Store. Instale a aplicação no seu ServiceNow AI Platform E conclua algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Tarefas de configuração	Descrição
Verifique se a aplicação está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte, Instalar Resposta a vulnerabilidades.
Verifique se você tem o necessário ServiceNow funções atribuídas à sua instância.	A função de administrador é necessária para a instalação.

Tradução automática

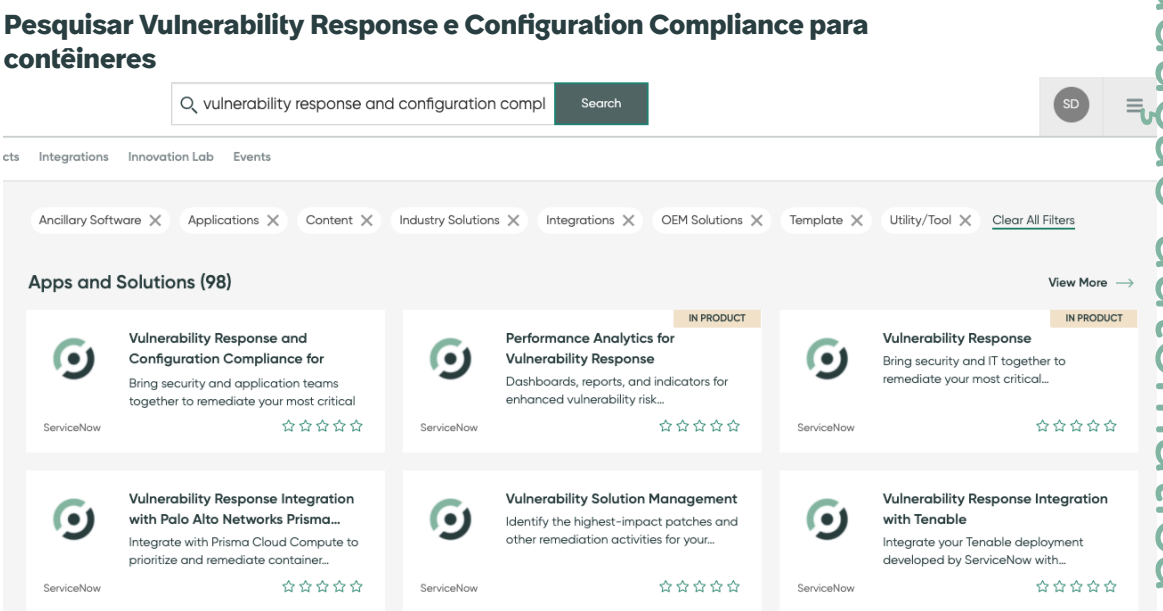
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Se ainda não estiver atribuído, o Administrador do sistema [admin] também atribuirá a função Administrador de vulnerabilidades, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)].

Função necessária: administrador

Procedimento

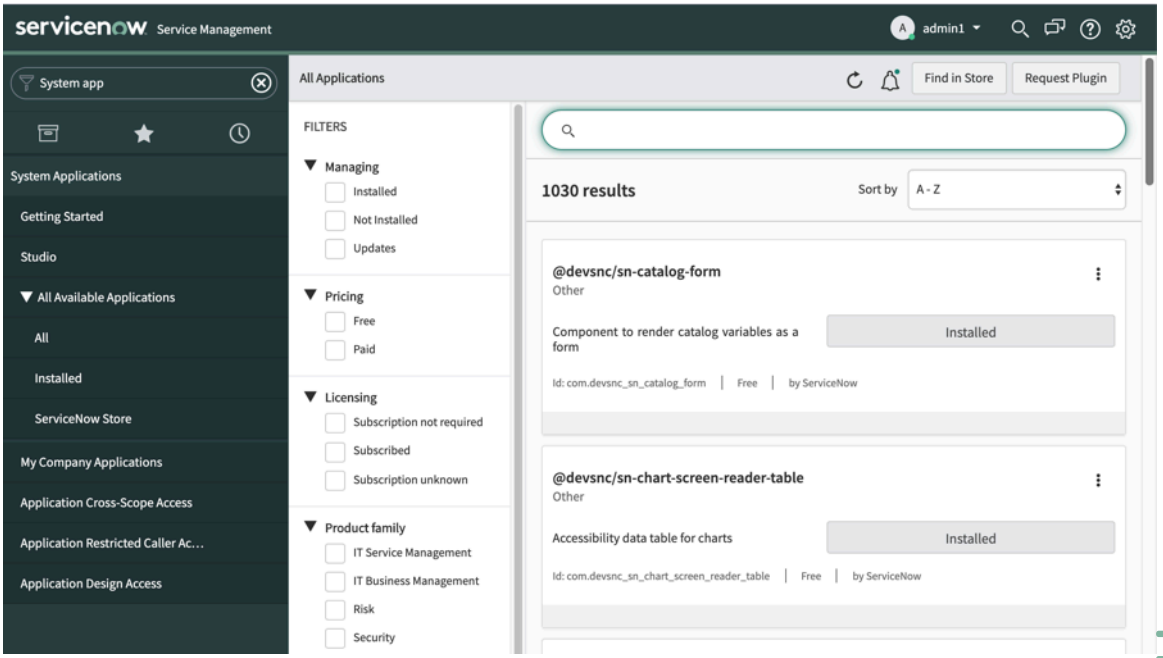
1. Para obter direito e baixar o. Vulnerability Response e Configuration Compliance para contêineres, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Faça login** .
3. Na barra de pesquisa, digite Vulnerability Response e Configuration Compliance para contêineres.
4. Em Aplicativos e soluções, clique em Vulnerability Response e Configuration Compliance para contêineres lado a lado.



5. Clique em **Solicitar instalação** .
6. Faça login no ServiceNow AI Platform instância em que você deseja instalar o. Vulnerability Response e Configuration Compliance para contêineres aplicação em.
7. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Nas aplicações listadas, localize Vulnerability Response e Configuration Compliance para contêineres selecione uma versão na lista e clique em **Instalar** .
   A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências instaladas são exibidas.
9. Clique em **Fechar**.

Definir Contêiner de Resposta a vulnerabilidades notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações falso-positivas. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas para criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultado

A partir de v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para usuários com as funções, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin .
- Links abertos no Espaço de correção de problemas de TI para usuários com funções, sn_vul_container.remediation_owner .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Criar ou editar notificações de destino de correção

Os administradores de vulnerabilidades podem editar a notificação de destino de correção ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo** .
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultado
A partir de v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para os usuários com as funções, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin .
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul_container.remediation_owner .

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configure a Gestão de exceções para Contêiner de Resposta a vulnerabilidades

Limitar a duração de uma exceção solicitada e adicionar um questionário à solicitação de exceção ou falso positivo usando o. Contêiner de Resposta a vulnerabilidades módulo. Por padrão, uma exceção é solicitada usando ServiceNow® Contêiner de Resposta a vulnerabilidades módulo. Você também pode solicitar uma exceção usando GRC: Gestão de políticas e conformidade integração.

Antes de Iniciar
Função necessária: sn_vul_container.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa
Se Contêiner de Resposta a vulnerabilidades habilitado, você pode limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o GRC: Gestão de políticas e conformidade o módulo está instalado, você pode selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite que você solicite uma exceção que especifica o objetivo de Política e controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que levantou a solicitação de exceção ou falso positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos. .

É útil que o aprovador da exceção entenda o motivo da solicitação da exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Gestão de exceção**.
2. Em **Configuração da Gestão de exceções** , selecione como você deseja gerenciar uma exceção selecionando uma opção no **Gerencie exceções usando** lista.
   Você pode selecionar qualquer um Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade.
3. Se você selecionou Resposta a vulnerabilidades insira as seguintes informações:

campos de Resposta a vulnerabilidades

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.

Nota: Ao selecionar GRC: Gestão de políticas e conformidade, Os campos Duração e Unidade desaparecem como Governança, risco e conformidade processa esse fluxo.

4. Selecione **Save** (Salvar).

Configure regras de aprovação para Gestão de exceções

Começando com Resposta a vulnerabilidades v15.0, use o designer de fluxo para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades(VR) Pela primeira vez, o Flow Designer é habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis do contêiner
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso-positivo para itens vulneráveis ao contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação . (dias) A partir da v2.5 de Contêiner de Resposta a vulnerabilidades	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v2.5 de Contêiner de Resposta a vulnerabilidades	Data após a qual o aprovador é notificado para executar uma ação.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Crie configurações para uma regra de aprovação.

> **Nota:** Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Testes de início rápido para Contêiner de Resposta a vulnerabilidades

Valide se Contêiner de Resposta a vulnerabilidades ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em não produção ou produção. Consulte Execute o pacote de testes ATF (Automated Test Framework) para Resposta a vulnerabilidades para obter mais informações sobre como configurar e executar o pacote de testes para Contêiner de Resposta a vulnerabilidades.

Os testes de início rápido do Contêiner de Resposta a vulnerabilidades exigem a ativação da aplicação Contêiner de Resposta a vulnerabilidades (sn_vul_container).

Testes Contêiner de Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
CVR: Regras de atribuição	Determina se um conjunto de regras de atribuição pode atribuir automaticamente itens vulneráveis de contêiner a um grupo de atribuição para correção.	Vancouver
CVR: regra de exceção	Regras de exceção de teste.	Vancouver
CVR: marcar como fluxo falso-positivo	Teste se a opção de marcar como fluxo falso-positivo está funcionando no item vulnerável do contêiner.	Vancouver
CVR: regras de destino de correção	Crie regras de meta da correção.	Vancouver
CVR: fluxo de exceção de solicitação	Teste se o fluxo de exceção de solicitação está funcionando conforme o esperado.	Vancouver
CVR: Calculadoras de vulnerabilidade	Testa as calculadoras de vulnerabilidade do contêiner.	Vancouver

Tópicos relacionados

Testes de início rápido

Execute o pacote de testes ATF (Automated Test Framework) para Contêiner de Resposta a vulnerabilidades

Execute o pacote de testes ATF (Automated Test Framework) depois de instalar ou fazer upgrade do Contêiner de Resposta a vulnerabilidades aplicação.

Antes de Iniciar

Confirme uma instalação bem-sucedida e se sua instância funciona conforme projetado.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em não produção ou produção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para habilitar o teste, siga estas etapas:
  1. Navegar até **Tudo** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
  2. Se não estiver selecionado, selecione **Habilitar execução de pacote de testes/testes** caixa de seleção.
  3. Clique em **Salvar**.
  4. Se o escopo não estiver definido como **Resposta a vulnerabilidades do contêiner** no cabeçalho, ou o escopo não é exibido no cabeçalho, clique no ícone de configurações.
  5. Na janela Configurações do sistema, clique em **Desenvolvedor** .
  6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
  7. Na lista exibida ao lado de Administrador do sistema clique em **Resposta a vulnerabilidades do contêiner** para o campo.

Função necessária: admin ou atf_test_admin

Procedimento

1. Navegar até **Tudo** > **Automated Test Framework (ATF)** > **Testes**.
2. Na lista Pacote, localize **Resposta a vulnerabilidades e Conformidade de configuração para contêineres** .
3. Selecione um teste para abrir o registro.
4. No registro Aberto, selecione **Ativo** caixa de seleção.
5. Na lista relacionada Etapas de teste, selecione Verdadeiro na coluna Ativo.
6. Clique em **Atualizar**.
7. Abra o teste novamente e clique em **Habilite testes e a execução do pacote de testes aqui** .
8. Habilite Propriedades de pacote de testes/testes e Propriedades de depuração de teste.
9. Clique em **Salvar**.
10. . **Executar teste** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar teste** para iniciar o teste.
    Após alguns momentos, a caixa de diálogo Executar teste indica um teste bem-sucedido. Clique em **Ir para Resultado** para obter mais informações.

O que Fazer Depois

Parabéns! Você pode continuar com sua configuração de Contêiner de Resposta a vulnerabilidades.

Para obter mais informações sobre testes automatizados para Contêiner de Resposta a vulnerabilidades e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Integração do Contêiner de Resposta a vulnerabilidades a outras aplicações

Estenda os recursos de Contêiner de Resposta a vulnerabilidades integrando com outras aplicações.

Contêiner de Resposta a vulnerabilidades integra-se a produtos de segurança de contêiner para extrair dados de vulnerabilidade das imagens implantadas no tempo de execução. Em seguida, ele enriquece os dados de vulnerabilidade com as informações contextuais de tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que essas imagens de contêiner são implantadas. Com a descoberta do Kubernetes da ServiceNow, você pode ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em seu Configuration Management Database (CMDB). Além de enriquecer os metadados, a ServiceNow também oferece um painel de relatórios abrangente para fornecer informações sobre as tendências de vulnerabilidade e correção.

Contêiner de Resposta a vulnerabilidades fornece integrações com as seguintes aplicações:

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integração
- Noções básicas do Atlassian Jira integração com Resposta a vulnerabilidades
- Noções básicas sobre a Integração de vulnerabilidades do Tenable
- **Importante:** No Espaço do gerenciador de vulnerabilidades, você pode criar um problema ágil manualmente usando ação de lista e. ação de formulário Rastrear a correção de CVITs e RTS.

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 2.1.2 de Contêiner de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integração

A integração Prisma Cloud Compute permite verificar imagens de contêiner para detectar vulnerabilidades.

A partir da versão 23,0 do Resposta a vulnerabilidades, você pode usar Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute em Contêiner de Resposta a vulnerabilidades aplicação para importar vulnerabilidades nos hosts em execução. As APIs do host Prisma permitem a recuperação de informações abrangentes de vulnerabilidade para um host específico e também fornecem um snapshot das vulnerabilidades do host em um momento específico. Esta API permite a sincronização regular entre a instância Prisma e a ServiceNow. Como o Prisma é oferecido como software como serviço (SaaS) e solução

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no local, é necessário usar um MID Server para invocar APIs Prisma da instância da ServiceNow.

A partir da versão 16,1 do Resposta a vulnerabilidades, você pode usar Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute em Contêiner de Resposta a vulnerabilidades aplicação para importar dados de vulnerabilidade de imagem de contêiner para contêineres implantados. Em seguida, você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis no Resposta a vulnerabilidades painéis. Essas vulnerabilidades podem ser priorizadas e corrigidas.

. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server. Para obter mais informações, consulte Requisitos do sistema DO MID Server .

Exibindo as integrações

Você pode exibir as integrações que fazem parte do Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Para exibir as integrações, navegue até **Tudo** > **Integração do Prisma Cloud Compute** > **Integrações**.

As integrações a seguir estão disponíveis.

Sequência de execução	Agendamento	Integração	Descrição
1	Diariamente	Integração de imagens de base do Prisma Cloud Compute	Recupera as vulnerabilidades das imagens de base da API Prisma e relata as vulnerabilidades das imagens de base separadamente. Ele também cria descobertas de imagem e itens vulneráveis, que apontam para as imagens de base.
2	Diariamente	Prisma Cloud Compute Vulnerabilities Integration	Recupera vulnerabilidades de contêiner. Cria descobertas, itens vulneráveis ao contêiner (CVITs) e imagens do contêiner descobertas.
3	Sob demanda	Prisma Cloud Compute Contêiner Counts Integration	Recupera contagens de contêiner para cada imagem não base.
4	Diariamente	Prisma Cloud Compute Registry Integration	Recupera descobertas de imagem estática obtidas da verificação do registro do Prisma e ingere em Contêiner de Resposta a vulnerabilidades.

Configuração da imagem de base no Prisma

No console do Prisma, você pode configurar o registro e configurar as imagens de base desses registros. Se uma vulnerabilidade estiver presente na imagem de base, quando você executar a Integração de imagens de base de computação em nuvem Prisma, o. **Imagem de base** a caixa de seleção está marcada indicando que as vulnerabilidades estão presentes na imagem de base.

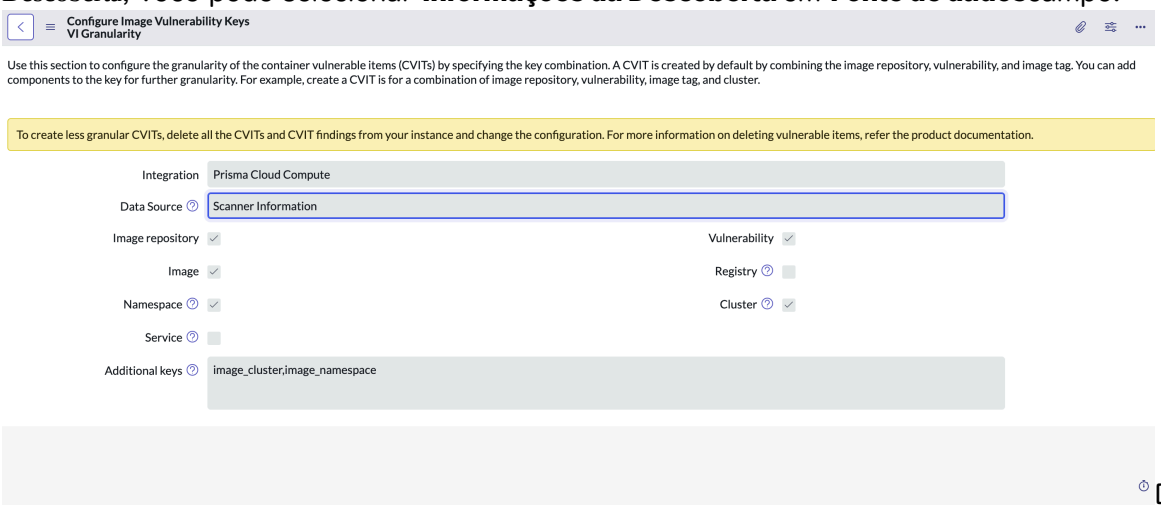
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a granularidade de VI baseada em CVR

Para configurar a granularidade dos CVITs, navegue até **Tudo** > **Integração do Prisma Cloud Compute** > **Configurar granularidade de IV baseada em CVR** e especificam as combinações de teclas. Por padrão, um CVIT é criado para uma combinação de repositório de imagens, imagem e vulnerabilidade. Você pode adicionar componentes adicionais à chave para obter granularidade adicional. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, imagem, vulnerabilidade e cluster.

A partir da v2.12.1 de Contêiner de Resposta a vulnerabilidades Você também pode configurar a granularidade de itens vulneráveis ao contêiner (CVITs) usando informações do Registro e fontes de dados. As informações do namespace e do cluster são recebidas do scanner e do Descoberta. Se você quiser essas informações somente de Descoberta, você pode selecionar **Informações da Descoberta** em **Fonte de dados**campo.



Dependendo da fonte de dados escolhida, você pode exibir as informações da imagem ou do Kubernetes relacionadas a um registro CVIT.



Se **Informações do scanner** Selecionado, o registro CVIT é exibido **Clusters de imagens** e. **Namespace da imagem** campos.

Se **Informações da Descoberta** Selecionado, o registro CVIT é exibido **Clusters do Kubernetes** e. **Namespace do Kuber** campos.

Processo de integração do Prisma

. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud ComputeÉ executado, ele verifica se existe uma CVE (Common Vulnerability and Exposure, vulnerabilidade comum) na

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tabela NVD (National Vulnerability Database, banco de dados nacional de vulnerabilidades). Se já estiver presente, as informações existentes serão usadas. No entanto, se o CVE não for encontrado, registros de espaço reservado serão gerados na tabela NVD. Ao criar esses registros NVD de espaço reservado, inicialmente somente o CVE e seu nome são preenchidos. Outros detalhes não são preenchidos com a suposição de que a integração NVD preenche esses detalhes posteriormente. Se o parâmetro de instância de integração *update_nvd*Definido como verdadeiro, ele atualiza os registros NVD de espaço reservado. Por padrão, o parâmetro de instância é definido como falso. No entanto, pelo menos até que a integração do NVD seja executada e preencha esses detalhes, é necessário entender o CVE, como sua gravidade ou outros detalhes sobre o problema. Para atender a este requisito, use os campos **Existe uma exploração** e. **Anotações de correção** São preenchidos com os detalhes obtidos do Prisma. Essa configuração é personalizável, permitindo que você especifique quaisquer outros campos que deseja preencher na entrada NVD com base nas informações fornecidas pelo Prisma.

Preparando para Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Você pode se preparar para Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute executando tarefas de configuração.

Antes de começar

Para instalar e configurar o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute, você pode imprimir a seguinte check-list. Verifique se os itens listados estão concluídos antes de instalar a aplicação e importar os dados de vulnerabilidade para seu ServiceNow AI Platform® instância.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL de base da API • Nome de usuário e senha. Essas credenciais são usadas para extrair as vulnerabilidades da integração do Prisma Cloud Compute. Para obter mais informações, consulte https://pan.dev/compute/api/ . **Nota:** O MID Server é opcional. A credencial do usuário usada para a integração do Prisma Cloud Compute precisa de permissão para monitorar as imagens. Consulte o seguinte código: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Se ainda não estiver instalado e ativado, instale o. Resposta a vulnerabilidades aplicação antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 16,1 de Resposta a vulnerabilidades ou posterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Obtenha direitos e baixe o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação em seu ServiceNow AI Platform® instância.
☐	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com ServiceNow Suporte técnico.
☐	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir os itens vulneráveis: **administrador** Instale o aplicativo Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade do contêiner (sn_vul_container.vulnerability_admin) e outras funções. **sn_vul_container.vulnerability_admin** Conclui a configuração da integração do Prisma Cloud Compute. Esta função tem acesso completo ao Contêiner de Resposta a vulnerabilidades(CVR) e seus registros. Este administrador configura integrações e regras em Contêiner de Resposta a vulnerabilidades. **Grupo de resposta a vulnerabilidades** Por padrão, o grupo Resposta a vulnerabilidades está disponível. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam sn_vul.read_all, sn_vul_container.read_all. **Grupo do responsável pela correção do contêiner** Por padrão, o grupo Proprietário de correção de contêiner está disponível. Os usuários atribuídos a este grupo herdam sn_vul_container.remediation_owner. O responsável pela correção do contêiner corrige as vulnerabilidades do contêiner atribuídas a ele ou a um grupo ao qual ele pertence. **Analista de vulnerabilidades** Os usuários atribuídos ao grupo Analista de vulnerabilidades de contêiner herdam sn_vul.vulnerability_analyst. O analista de vulnerabilidades monitora a correção de todos os itens vulneráveis. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância. Para obter mais informações, consulte Crie um grupo de usuários .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Instale o. Resposta a vulnerabilidades Integração com NVD e execute a API de integração do banco de dados nacional de vulnerabilidades do NIST - (somente CVE).

Você está pronto para Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.

Instalar o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que o produto Prisma Cloud Compute se integre corretamente com Resposta a vulnerabilidades e. Contêiner de Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ativado.
2. Navegue até ServiceNow Store.
3. Em ServiceNow Store, pesquise Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.
4. Clique no bloco Aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Leia **Outros requisitos** e. **Dependências** seções, se necessário.

5. Clique em **App de solicitação** e insira seu Now Support credenciais de login.
6. Clique em **Obter**.
7. Atualize o. **Nome da instância** e. **Motivo da instância** e clique em **Validar instância** .
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar** .

Resultado

Sua aplicação é instalada automaticamente em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute para o seu ambiente. Consulte Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação.

Configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação

Instale e configure o. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute aplicação. Importe dados do Prisma Cloud Compute. Você pode usar os dados importados para priorizar e corrigir vulnerabilidades para suas imagens e hosts do docker.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Abra o e-mail de ServiceNow que você recebeu sobre a integração.
2. Faça login em sua instância como administrador.
3. Siga as instruções no e-mail para obter Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navegar até **Tudo** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.
   No formulário Configuração de computação em nuvem do Prisma, preencha os campos. Para obter mais informações, consulte Formulário de configuração de computação em nuvem do Prisma.
5. Na lista Projetos, selecione qualquer um **Todos os projetos** ou **Projetos específicos** para configurar todos os projetos ou projetos selecionados, respectivamente.
   Se você selecionar **Projetos específicos** , Você pode selecionar os projetos na lista Disponível.
6. Conclua a configuração selecionando qualquer um **Concluir** ou **Salvar e testar credenciais** .
   - Se você configurou um projeto, selecione **Concluir** .
   - Se você não configurou um projeto, selecione **Salvar e testar credenciais**
7. Exiba a instância recém-criada navegando até **Integração do Prisma Cloud Compute** > **Administração** > **Instâncias de Integração**.
8. Exiba os projetos que você configurou anteriormente selecionando **Parâmetros da instância de integração** .
9. Execute a instância de integração recém-criada para importar os seguintes dados:
   - Imagens do Docker: Lista as imagens do Docker, que são criadas usando um mecanismo de identificação e reconciliação (IRE). Cada imagem do Docker também fornece informações sobre o relacionamento entre os repositórios e as versões instaladas.
   - Imagens de contêiner descobertas: O módulo Imagens de contêiner descobertas fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as informações da camada e as associa à imagem descoberta. Você também pode exibir os projetos e a contagem de contêineres aqui. Para uma imagem de contêiner descoberta, você pode exibir metadados de nuvem, como provedor de nuvem, região de nuvem, ID da conta de nuvem e IDs de recursos de nuvem.
   - Pacotes de imagem do contêiner: Fornece informações sobre os pacotes onde existem as vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgulas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Camadas de imagem do contêiner: Esta tela exibe o registro de cada camada de imagem.
- Descobertas da imagem do contêiner: Esta tela exibe a lista de descobertas junto com informações sobre as vulnerabilidades associadas, camada de imagem, imagem do docker, repositório de imagens e imagem descoberta. Atualmente, as informações de vulnerabilidade estão limitadas apenas ao ID. Informações adicionais são preenchidas quando o National Vulnerability Database (NVD a integração) é acionada.
- Itens vulneráveis do contêiner: Cada descoberta tem uma vulnerabilidade correspondente. As CVITs são criadas com base na granularidade.

10. Configure a granularidade de um item vulnerável.

a. Navegar até **Tudo** > **Integração do Prisma Cloud Compute** > **Configurar chaves de vulnerabilidade de imagem**

b. Configure a granularidade dos CVITs marcando as caixas de seleção necessárias.
Os itens vulneráveis são criados com base nas chaves selecionadas durante a próxima importação.

> **Nota:** Por padrão, um CVIT é criado para uma combinação de Repositório de imagens, Vulnerabilidade e marcador de imagem. Você pode adicionar componentes à chave para obter granularidade adicional. Por exemplo, você pode criar um CVIT para uma combinação de Repositório de imagens, Vulnerabilidade, Marcador de imagem e Cluster. Quando os itens vulneráveis ou as descobertas de itens vulneráveis são criados, as caixas de seleção não são mais editáveis.

Explorar o. Wiz Integração de vulnerabilidade do contêiner

Importe dados de vulnerabilidade do contêiner com Wiz Integração de vulnerabilidade de contêiner incluída com Wiz Resposta a vulnerabilidades Integração.

Wiz Integração de vulnerabilidade do contêiner visão geral

. Wiz A Integração de vulnerabilidades de contêiner importa vulnerabilidades de imagem de contêiner que são identificadas pelo Wiz verificador de vulnerabilidades. Importe dados para ajudar a identificar, priorizar e atribuir vulnerabilidades de contêiner para correção com os fluxos de trabalho automatizados da instância da Plataforma de IA da ServiceNow.

As descobertas são mapeadas para Itens vulneráveis ao contêiner (CVITs) para oferecer suporte à triagem, priorização de risco e fluxos de trabalho de correção direcionados para cargas de trabalho baseadas em contêiner.

Para obter mais informações sobre as outras integrações incluídas com Wiz Resposta a vulnerabilidades Integração e instalação e etapas de configuração, consulte Noções básicas do Wiz Resposta a vulnerabilidades Integração.

Correção de vulnerabilidades de contêiner

A correção de monitoramento é um processo que começa com a revisão do status e termina com o fechamento de itens vulneráveis ao contêiner (CVITs). Contêiner de Resposta a vulnerabilidades oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contêiner de Resposta a vulnerabilidades regras da calculadora

As calculadoras de vulnerabilidade automatizam o cálculo de valores iniciais para os campos em itens vulneráveis do contêiner. Cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Para exibir e criar calculadoras de vulnerabilidade, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Calculadoras de Vulnerabilidade**.

. Contêiner de Resposta a vulnerabilidades O sistema de base inclui duas calculadoras de vulnerabilidade que definem a Pontuação de risco de base no item vulnerável do contêiner. Os seguintes grupos de calculadora estão disponíveis no sistema de base:

- Gravidade da vulnerabilidade: Calcula a pontuação de risco para itens vulneráveis usando a gravidade da vulnerabilidade normalizada.
- Calculadora de risco padrão: Baseia-se na regra de risco.

Nota: A partir da versão 2,10 de Contêiner de Resposta a vulnerabilidades, no caso de:

- **Calculadora de risco padrão** Regra: Sempre que a pontuação de risco em um item vulnerável ao contêiner (CVIT) muda, os seguintes detalhes são documentados na seção Anotações do CVIT:
  - Nome do grupo de calculadora
  - Nome da calculadora
  - Valores de campo que têm uma ponderação maior que 1 e sua contribuição de pontuação de risco.
  - Pontuação de risco final
- **Gravidade da vulnerabilidade** Regra de risco: Sempre que a pontuação de risco é atualizada em um CVIT, o. **Anotações** a seção é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadora
  - Nome da calculadora: Dependendo se a regra da calculadora é baseada em um modelo ou script, o nome é anexado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e selecione **Exibição avançada** caixa de seleção. Em **Tipo de valor** caixa suspensa, selecione a opção necessária. Se **Modelo** selecionado, a pontuação de risco é atualizada de acordo com a condição especificada na regra. Se **Script** selecionado, você pode adicionar ou atualizar o script existente. A propriedade do sistema `sn_sec_cmn.risk_score_changes_add_worknotes`ajuda a preencher a seção de anotações de trabalho. A partir da v2.12.2 de Contêiner de Resposta a vulnerabilidades, a propriedade do sistema `sn_sec_cmn.risk_score_changes_add_worknotes`está inativo por padrão. Somente se você habilitá-lo, poderá ver todas as mudanças relacionadas à pontuação de risco de um item vulnerável de contêiner na seção Anotações de trabalho. Além disso, as anotações de trabalho serão atualizadas somente se houver uma mudança na pontuação de risco.

Pesos da pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação de risco e classificação com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio `Update Risk Rating from Risk Score`na tabela de item vulnerável do contêiner é responsável por calcular a classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis do

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

contêiner. Versão 17,1 do Resposta a vulnerabilidades(VR), as seguintes classificações de risco foram fornecidas como parte da inclusão de script VulnerabilityUtils , que foram codificados.

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

A partir da versão 18,0 do Resposta a vulnerabilidades,

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

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

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

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

Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Contêiner de Resposta a vulnerabilidades regras de atribuição

Defina os critérios pelos quais os itens vulneráveis do contêiner são atribuídos automaticamente a um grupo de atribuição para correção.

Para criar e exibir regras de atribuição para itens vulneráveis ao contêiner, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de atribuição**. Ao criar uma regra de atribuição, você pode definir as condições. Quando essas condições são atendidas, a regra atribui automaticamente os itens vulneráveis do contêiner ao grupo de usuários selecionado. Somente a primeira regra de atribuição com uma condição correspondente é executada em um registro. Consulte Resposta a vulnerabilidades visão geral das regras de atribuição para obter mais informações sobre regras de atribuição.

Funções necessárias: sn_vul_container.manage_assignment_rules para definir e atualizar regras e sn_vul_container.container_reapply para reaplicar regras.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 2,13, os campos para informações do scanner foram adicionados aos registros na tabela Imagem do contêiner descoberto [sn_vul_container_image]. Você pode usar os seguintes valores como condições ao criar ou atualizar suas regras de atribuição para itens vulneráveis à imagem do contêiner (CVITs) para ajudá-lo a rastrear a propriedade em seus ambientes de contêiner.

- IDs da conta de nuvem
- Namespaces das imagens
- Registro
- Hosts
- Rótulos
- Status (status do fornecedor para uma vulnerabilidade resolvida)

Nota: Este valor na tabela Descoberta de imagem do contêiner [sn_vul_container_image_findings] refere-se à versão na qual uma vulnerabilidade foi resolvida, por exemplo, Corrigido em 6.2.1 . Este valor é importado do Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integração.

Nota: Itens vulneráveis ao contêiner (CVITs) que não estão no estado Aberto ou foram atribuídos manualmente são sempre excluídos das regras de atribuição. Se você adicionar valores para esses campos do scanner às suas regras de atribuição e executar novamente suas regras, os itens vulneráveis não serão reatribuídos, a menos que o tipo de atribuição seja Regra . Itens com Tipo manual não são considerados pelas regras de atribuição.

Importante: Como administrador e analista de vulnerabilidades, você pode obter as atribuições mais recentes para CVITs selecionados em Espaço do gerente de vulnerabilidade. Este método é mais eficiente do que reaplicar as Regras de atribuição para todos os CVITs no clássico IU, que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Contêiner de Resposta a vulnerabilidades regras de destino de correção

As regras de destino de correção definem o intervalo de tempo esperado para corrigir um item vulnerável ao contêiner (CVIT). Essas regras são semelhantes à forma como os SLAs fornecem um intervalo de tempo para corrigir a vulnerabilidade em si.

Para criar e exibir regras de destino de correção para vulnerabilidades de contêiner, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de meta da correção**.

As regras de destino de correção definem o tempo de correção de destino para itens vulneráveis ao contêiner (CVITs) selecionados. Defina um prazo para corrigir a vulnerabilidade selecionando o número de dias para a correção. Defina um lembrete para correção e defina os itens vulneráveis ao contêiner aos quais a regra se aplica. Você pode definir uma meta de correção para os dias em que ela precisa ser corrigida e também definir um lembrete antes de se aproximar da data de destino. Para obter mais informações, consulte Resposta a vulnerabilidades regras de destino de correção.

Importante: Como administrador e analista de vulnerabilidades, você pode obter a data de destino de correção mais recente para CVITs selecionados em Espaço do gerente de vulnerabilidade. Este método é mais eficiente do que executar as Regras de destino de correção para todos os CVITs no clássico IU, que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de exceções em Contêiner de Resposta a vulnerabilidades

Quando sua organização não pode cumprir um gerenciamento de vulnerabilidades publicado ou política de segurança, padrão ou diretriz, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável ao contêiner (CVIT) que não pode ser corrigido de acordo com a política.

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

Ciclo de vida de uma exceção

Definição de uma exceção

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

Solicitando uma exceção

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

Aprovando uma solicitação de exceção

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

Nota:

A partir de Resposta a vulnerabilidades V15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

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

- Reabrir
- Excluir
- Atualize o. **Atribuição a.** ou **Grupos de atribuição** campos

Acompanhamento de uma solicitação de exceção

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

Expiração de uma solicitação de exceção

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um único CVIT ou todos os CVITs em um RT forem aprovados no próximo exame, os CVITs e, quando aplicável, o RT **Estado** o campo muda para **Encerrado** com o subestado **Corrigido** .

Configurar regras de aprovação

Exiba e configure regras de aprovação navegando até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de aprovação**. Solicite uma exceção para os CVITs que não podem ser corrigidas ou adiadas imediatamente, identificando as vulnerabilidades afetadas, os itens de configuração (ICs) ou CVITs. Automatizar o processo de adiamento do CVIT. Adie os CVITs correspondentes com base nessas regras quando o sistema identificar esses CVITs.

As seguintes regras de aprovação são enviadas por padrão:

- Aprovação para solicitações de exceção: Uma configuração padrão com dois níveis de aprovação é fornecida no sistema de base. Sempre que houver uma solicitação de exceção em um item vulnerável, a solicitação de aprovação será enviada para os usuários ou grupos presentes no nível 1. Uma vez aprovado pelos aprovadores de nível 1, ele é enviado para os aprovadores de nível 2.

  Nota: Você pode mudar os níveis padrão e editar conforme necessário. A partir de Contêiner de Resposta a vulnerabilidades V2.0.6, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio de fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção ou falso positivo é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Tudo** > **Propriedades do sistema** e selecione *`sn_vul_container.container_exception_approver_L1`*, *`sn_vul_container.container_exception_approver_L2`*ou *`sn_vul_container.container_false_positive_approver_group`*para mudar o valor da propriedade.

- Aprovação para regras de exceção: Ele não tem configuração, mas dois níveis de aprovação.
- Aprovação para falsos positivos: Tem uma configuração com um nível de aprovação.

Nota: A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Solicitando e aprovando uma exceção em Contêiner de Resposta a vulnerabilidades

Você pode solicitar o adiamento da correção de um item vulnerável ao contêiner (CVIT) por um período especificado. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Para solicitar ou aprovar uma exceção, consulte:

- Solicite uma exceção para um item vulnerável de contêiner
- Solicite uma exceção para vulnerabilidades de contêiner usando GRC: Gestão de políticas e conformidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada. A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Solicite uma exceção para um item vulnerável de contêiner

Solicite uma exceção para um item vulnerável ao contêiner (CVIT) que não pode ser corrigido imediatamente. Por exemplo, como responsável pela correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar

Função necessária: Grupo de desenvolvedores

Por Que e Quando Desempenhar Esta Tarefa

Você pode solicitar uma exceção para vários CVITs simultaneamente usando o recurso Edição em massa no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** > **Tudo**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Em investigação.
3. No formulário Item vulnerável do contêiner, clique em **Exceção de solicitação** .

4. a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo reverte para o estado Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 1,2 de Contêiner de Resposta a vulnerabilidades se um item vulnerável foi adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo verificador, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vul.container.auto_defer_cvit_in_active_e* verdadeiro. Além disso, a data Adiado até persiste mesmo depois que o CVIT é encerrado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Defina um mapeamento de motivo de política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Aprovação da solicitação** .
O estado do item vulnerável do contêiner muda para Em revisão. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicite uma exceção para uma tarefa de correção de contêiner

Solicite uma exceção para adiar uma tarefa de correção de contêiner por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções do Resposta a vulnerabilidades Espaços de trabalho. Consulte Solicite uma exceção no Espaço de correção de problemas de TI.

Função necessária:

sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de contêiner no ambiente clássico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Tarefas de correção** > **Tudo**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Em investigação ou Aguardando implementação.
3. No registro da tarefa de correção de contêiner, selecione **Exceção de solicitação** .
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Solicite uma exceção para vulnerabilidades de contêiner usando GRC: Gestão de políticas e conformidade

Solicitar exceções de política usando GRC capacidade de gestão de exceções de política no Gestão de políticas e conformidade aplicação a partir de Contêiner de Resposta a vulnerabilidades.

Antes de Iniciar

Antes de usar a Integração de exceção de política para solicitar exceções de política, você deve baixar o. GRC: Gestão de políticas e conformidade aplicação do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas de correção**)> **Todos** e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Exceção de solicitação** .

   Nota: Se GRC: Gestão de políticas e conformidadeÉ selecionado na tela Gestão de exceções e preencha os campos no formulário Solicitar exceção. Para mais informações sobre campos de formulário, consulte Formulário Solicitar exceção.

   a. Envie a solicitação de exceção clicando em **Aprovação da solicitação** .
   O estado dos itens vulneráveis muda para Em revisão e uma exceção de política é criada. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

   b. Exiba a exceção de política clicando na lista relacionada Exceções de política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique no número da exceção de política.

d. Em **Aprovador** , selecione o nome do aprovador.

e. Clique na guia Origem e selecione um objetivo de controle no **Objetivo de controle** campo.

f. Clique na guia Avaliação de risco e selecione a classificação de risco em **Classificação de risco** campo.

g. Salve o formulário.

h. Clique em **Controles afetados** guia.

i. Adicione os controles clicando em **Adicionar** .

j. Salve o formulário.

Nota: Você pode criar uma revisão de conformidade clicando em **Solicitar revisão de conformidade** .

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicite aprovação adicional clicando em **Solicitar aprovação adicional** .

O estado do registro muda para Adiado. O motivo informado é aquele que você selecionou ao gerar a solicitação de exceção. . **Adiamento** fornece anotações adicionais sobre o registro.

Nota: Se a solicitação for rejeitada, o registro será movido para o estado anterior.

3. Clique em **Enviar**.
Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Defina um mapeamento de motivo de política

Defina as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar

Função necessária: sn_vul.compliance.manager e sn_vul_container.manage_exception_configuration

Procedimento

1. Navegar até **Tudo** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

2. Clique no registro de integração Resposta a vulnerabilidades do contêiner - CVIT.
3. Na lista Opções de motivo, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no ícone de lupa.
5. Adicione uma opção de motivo existente para criar uma nova.
   - Se você quiser adicionar uma opção de motivo existente, selecione um motivo.
   - Se você quiser adicionar uma nova opção de motivo à tabela Opções de motivo, clique em **Novo** e preencha os campos no formulário.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamento do motivo da política para as respectivas aplicações. Para navegar até esta tabela, insira sn_vul_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Pedido para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham **Padrão** o campo selecionado estará disponível.
Ativo	Opção para exibir a opção na lista de opções de motivo.

6. Clique em **Enviar**.

Resultado
A opção de motivo é adicionada. A opção de motivo estará disponível em **Motivo** campo do formulário de solicitação de exceção de política para a aplicação selecionada.

Aprovar uma solicitação de exceção em Contêiner de Resposta a vulnerabilidades

Aprove solicitações de exceção para itens vulneráveis ao contêiner ou tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações de risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você pode aprovar as solicitações de exceção e falso-positivo no Espaço do gerente de vulnerabilidade.

Você também pode aprovar solicitações de exceção no ambiente clássico:

Procedimento
1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adie um item vulnerável de contêiner em Contêiner de Resposta a vulnerabilidades

Se você determinar que o problema associado a um item vulnerável ao contêiner (CVIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, poderá usar **Adiar** recurso.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho agendado é executado todos os dias verificando se há itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do CVIT for definido para expirar, o registro será reaberto.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner**.
2. Abra um item vulnerável.
3. Clique em **Exceção de solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado adiado expira e a tarefa de correção é reativada. **Nota:** A partir da versão 18,0 de Contêiner de Resposta a vulnerabilidades Se um item vulnerável ao contêiner adiado (CVIT) for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do CVIT será revertido para o estado adiado respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema `sn_vul.container.auto_defer_cvit_in_active_ex` verdadeiro. Além disso, a data Adiado até persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação. Se o registro for enviado, se notificações por e-mail são definidos, membros do Contêiner de Resposta a vulnerabilidades o grupo receberá um e-mail quando a data de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado **Em Revisão** . . **Reabrir** o link relacionado é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho em **Aprovações de mudança de estado** guia.

   Começando com Contêiner de Resposta a vulnerabilidades V2.3, você pode adicionar informações relevantes no campo Anotações de trabalho na seção Anotações para um item vulnerável de contêiner adiado.

Solicite uma extensão para um item vulnerável de contêiner adiado

Solicite uma extensão para um item vulnerável de contêiner adiado antes que ele atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner**.
2. Abra um item vulnerável de contêiner adiado.
3. Selecione **Extensão da solicitação** .

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável do contêiner é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até a qual o item vulnerável do contêiner adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Um e-mail é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se um item vulnerável de contêiner adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Trabalhando com uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Você pode solicitar uma exceção para itens vulneráveis ao contêiner (CVITs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de VI, você pode adiar os CVITs correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Crie uma regra de exceção em Contêiner de Resposta a vulnerabilidades
- Aprove uma solicitação de regra de exceção em Contêiner de Resposta a vulnerabilidades
- Ativando uma regra de exceção em Contêiner de Resposta a vulnerabilidades
- Reabra uma regra de exceção em Contêiner de Resposta a vulnerabilidades
- Atualize uma regra de exceção aprovada em Contêiner de Resposta a vulnerabilidades
- Exclua uma regra de exceção em Contêiner de Resposta a vulnerabilidades
- Adie um item vulnerável de contêiner em Contêiner de Resposta a vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Crie uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica para um grupo de itens vulneráveis ao contêiner (CVITs), como uma regra com uma condição baseada na gravidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

A regra é aplicada da data "Válido de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para este VUL é conhecido como regras de exceção. O VUL é criado no estado Adiado. Não é possível fechar, reabrir ou excluir este VUL. CVITs novos e reabertos são adiados e adicionados a este VUL a partir da data "Válido de" até que o grupo expire na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Na página Novo registro de Regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário Regra de exceção, preencha os campos.

   Nota: Para mais informações sobre campos de formulário, consulte Formulário Regra de exceção.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.
6. Para exibir e criar um grupo para gerenciar regras de exceção:

   a. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.

   b. Em uma regra de exceção, clique em **Aprovações solicitadas** para exibir o status da solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um trabalho agendado é executado diariamente, o que executa as regras de exceção nos dados existentes. Todos os itens vulneráveis que correspondem à condição são movidos para o estado Adiado. Se uma regra de exceção aprovada for excluída, todos os itens vulneráveis adiados serão revertidos para o estado anterior. Para obter mais informações, consulte Trabalhar com uma regra de exceção.

Aprove uma solicitação de regra de exceção em Contêiner de Resposta a vulnerabilidades

Avalie solicitações de regra de exceção de usuários para que você possa aprovar ou rejeitar essas solicitações.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Os membros do grupo de usuários de nível 1 do aprovador de exceção podem aprovar as solicitações de regra de exceção de nível 1. Da mesma forma, os membros do grupo de usuários de nível 2 do aprovador de exceção de nível podem aprovar as solicitações de regra de exceção de nível 2. Ambos os grupos de usuários herdam a função de aprovador de exceção por padrão.

Nota:

Se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso positivo, consulte Configure regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com e explique por que você aprovou ou rejeitou a solicitação.
   Depois que uma regra de exceção é aprovada, uma tarefa de correção (RT) é criada no estado Adiado por padrão. A partir da data "Válido de", esta regra é executada em todos os CVITs criados e também nos que são movidos do estado Encerrado para o Aberto. CVITs que correspondem às condições definidas são adicionados ao RT e adiados pelo período especificado.

   Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Ativando uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Uma regra é ativada na data "Válido a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis ao contêiner (CVITs).

A regra de exceção segue este ciclo de vida:

1. Os novos CVITs que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar nos dados existentes ao executar a regra de exceção pela primeira vez, todos os CVITs ativos e não adiados que correspondem à condição da regra de exceção serão movidos para a tarefa de correção recém-criada (RT) e seu estado será alterado para Adiado.
2. Se um CVIT recém-criado corresponder à condição da regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra de grupo não será executada nele.
3. Na data "Válido a partir de", os CVITs existentes serão adicionados se você habilitar a opção Executar nos dados existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. O RT para de aceitar novos CVITs quando a regra expira na data "Válido até". O RT permanece existente até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Reabra uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. Reabrir a regra a move para o estado Rascunho.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode atualizar e reenviar a regra para aprovação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Encontre a regra que você deseja reabrir e clique em **Reabrir** .
3. Atualize o formulário e envie-o novamente para aprovação.

Atualize uma regra de exceção aprovada em Contêiner de Resposta a vulnerabilidades

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de modificar datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis do contêiner (CVITs) sejam movidos para o estado Aberto.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
As regras de grupo são reaplicadas a esses CVITs. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação mais uma vez.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar** .
3. Na caixa de diálogo Cancelar regra, clique em **Regra de cancelamento** .
   A regra retorna para o estado Rascunho e o VUL associado é excluído. Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Exclua uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Exclua uma regra de exceção que não é mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável de contêiner (CVIT) durante a ingestão.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir** .
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Solicite uma extensão para uma tarefa de correção adiada em Contêiner de Resposta a vulnerabilidades

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e o item vulnerável do contêiner é reativado.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Na aprovação da solicitação, as mudanças na tarefa de correção também são transferidas para os itens vulneráveis do contêiner, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis do contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

devem estar no estado Adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicite uma extensão para uma regra de exceção em Contêiner de Resposta a vulnerabilidades

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Regras de exceção**.
2. Selecione uma regra de exceção adiada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até a qual a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nos itens vulneráveis do contêiner. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Marcar e aprovar um item de vulnerabilidade de contêiner falso-positivo

Itens vulneráveis ao contêiner (CVITs) e tarefas de correção (VULs) podem ser marcados como falsos positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

- Marcar como falso positivo em Contêiner de Resposta a vulnerabilidades
- Aprovar um falso positivo

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma tarefa de CVIT ou correção é marcada como falso positivo, o solicitante recebe um e-mail de confirmação. Ao mesmo tempo, o aprovador recebe um e-mail informando que uma tarefa de CVIT ou correção foi marcada como falso positivo.
A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Importante: Como analista de vulnerabilidades e responsável pela correção, você pode solicitar e aprovar falsos positivos do Vulnerability Manager Workspace e. Espaço de correção de TI respectivamente.

Marcar como falso positivo em Contêiner de Resposta a vulnerabilidades

Marque um item vulnerável ao contêiner (CVIT) ou tarefa de correção como falso positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se um CVIT tiver sido desativado, mas o scanner ainda estiver levantando um problema relacionado a ele, marque-o como falso positivo.

Importante: Como analista de vulnerabilidades e responsável pela correção, você pode solicitar falsos positivos do Vulnerability Manager Workspace e. Espaço de correção de TI respectivamente.

Antes de Iniciar

Função necessária: Responsável pela correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner (ou tarefas de correção)** > **Tudo**.
2. Abra o CVIT que você deseja marcar como falso positivo e clique em **Marcar como falso positivo** .
   O CVIT deve estar em um **Aberto** estado.
3. No formulário Falso positivo, insira os detalhes em **Informações adicionais** e clique em **Aprovação da solicitação** .
   A solicitação é enviada para aprovação e o Estado do CVIT muda para **Em Revisão** . O solicitante e o aprovador são notificados por e-mail.

Aprovar um falso positivo

Como um aprovador falso positivo, você pode aprovar solicitações falso-positivas de outros usuários.

Importante: Você pode aprovar ou rejeitar solicitações de falso positivo no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária: False_positive_approver

Você também pode aprovar solicitações de exceção e falso positivo no ambiente clássico:

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Nota: Um falso positivo pode ter um limite de tempo. Somente o aprovador pode definir a data de término.

Tarefas de correção de resposta a vulnerabilidades do contêiner e visão geral de regras de tarefa

Configure tarefas de correção (CVULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis de contêiner (CVIT) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que os CVITs sejam atribuídos automaticamente a tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Removendo atribuições de itens vulneráveis do contêiner e tarefas de correção

A partir da versão 2,13, você pode limpar **Atribuído a.** e. **Grupo de atribuição** Campos em Itens vulneráveis ao contêiner (CVITs) diretamente do CVIT e dos registros de tarefa de correção que você determina que podem estar atribuídos incorretamente a você ou aos seus grupos.

Para obter mais informações, consulte Removendo atribuições de itens vulneráveis do contêiner e tarefas de correção e Remova atribuições de itens vulneráveis e tarefas de correção.

Acompanhamento de contagens de adiamentos para itens vulneráveis ao contêiner e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável à aplicação, item vulnerável ao contêiner ou tarefa de correção é adiado. O trabalho programado Definir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

contagens de adiamento é executado diariamente para publicar contagens para os registros que são adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Noções básicas sobre as regras de tarefa de correção

As regras de tarefa de correção permitem que você defina como os itens vulneráveis do contêiner são agrupados e atribuídos automaticamente. Uma regra padrão **Vulnerabilidade** Está incluído no sistema de base que reúne CVITs com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis no CVIT. Esses valores podem incluir item de configuração (IC), entrada de vulnerabilidade e similares.

Há regras de tarefa para o Resposta a vulnerabilidades do contêiner que estão incluídas com a aplicação Resposta a vulnerabilidades que está disponível quando você a ativa.

Você pode criar várias condições com o construtor de condições. Na seção Agrupar por, depois de definir um par de campos, outra linha será exibida. Você pode ter até seis **Agrupar por** seleções. Você também pode automatizar a atribuição de grupo.

Por exemplo, você pode agrupar os itens vulneráveis do contêiner pelo item de configuração ou pelo modelo do produto. Você pode ter uma regra de tarefa para vulnerabilidades de baixa gravidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades que expõem a empresa a mais riscos. Consulte Criar, editar e excluir regras de tarefa de correção de resposta a vulnerabilidades do contêiner para obter mais informações sobre as opções que você tem disponíveis.

Um conjunto diferente de regras pode ser usado para itens vulneráveis ao contêiner que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado à regra da tarefa de correção **Agrupar por** valores para fazer a descrição resumida do novo registro.

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

O seguinte processo é usado para cada CVIT novo ou reaberto:

- Para cada regra de tarefa de correção, o CVIT é comparado ao filtro de regra de tarefa de correção.
- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados do **Agrupar por** Seleções no CVIT. Ele cria um nome e um campo de grupo. Nesse caso, **QID-32342: Resumo do QID-3242** (Nome: ID da vulnerabilidade: Resumo da vulnerabilidade).

> **Nota:** O campo Descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidades mais longos estão truncados.

A regra verifica se há uma correspondência **Aberto** Tarefa de correção atribuída ao mesmo grupo de atribuição que o CVIT.

- Se a tarefa for encontrada, o CVIT será adicionado à tarefa existente no **Aberto** Estado.
- Se não houver tarefa no **Aberto** encontrado, a regra cria um **Alto risco: QID-32342** A atribui ao mesmo grupo de atribuição que o CVIT e coloca o CVIT na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições da regra

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da tarefa de correção antes de colocá-la em uma tarefa de correção, muitas regras podem afetar o desempenho. Configure suas regras de tarefa para que as condições ajudem a evitar a criação de tarefas de correção duplicadas.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelo **Regras de atribuição** No CVIT ao agrupar os itens e atribuir a tarefa de correção para corresponder aos CVITs.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras em **Regras de atribuição** módulo. Para obter mais informações sobre regras de atribuição, consulte Visão geral das regras de atribuição de Resposta a vulnerabilidades.

Quando uma regra de tarefa é excluída da exibição de formulário ou de lista, você tem a opção de excluir todas as tarefas em aberto criadas por essa regra. Tarefas que não estão no **Aberto** Os estados são excluídos.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use **Reaplicar** botão na página de regra da tarefa de correção para executar novamente a regra alterada em todos os ativos **Aberto** tarefas de correção criadas por essa regra. Exclui e recria tarefas de correção com base na regra alterada automaticamente.

Reaplicar verifica somente as tarefas de correção existentes.

Depois de selecionar **Reaplicar** A seguinte mensagem é exibida: Reaplicar esta regra de tarefa de correção excluirá e recriará as tarefas de correção para esta regra. As tarefas de correção que não estão no estado Aberto não são excluídas.

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

Criação e atualização de regras de tarefa de correção e criação e atualização de CVIT

Se um IC de uma verificação estiver associado a uma vulnerabilidade conhecida, um CVIT será criado. Depois de criado, o CVIT é avaliado em relação às condições das regras de tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o CVIT será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o CVIT.

Se qualquer propriedade capturada nas condições de filtragem da tarefa de correção for atualizada ou alterada em um CVIT, o AVI atualizado também será avaliado em relação às regras da tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o CVIT será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma tarefa será criada para o CVIT.

Rollup de estado e rolldown

Se você atualizar uma tarefa de correção para Aberto ou de Aberto para Em investigação, o novo estado será revertido para todos os CVITs associados. A rolagem de estado ocorre imediatamente depois que você muda o estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O acúmulo de estado de CVITs para a tarefa de correção ocorrerá somente se todos os CVITs na tarefa estiverem em **Adiado** ou **Encerrado- Corrigido** estados. O Rollup é feito com os valores de item vulnerável do contêiner de Rollup para a vulnerabilidade e um trabalho agendado pelo grupo, que é executado a cada 15 minutos. O estado não é acumulado até que o trabalho seja executado. Para que um estado ocorra a partir dos CVITs para a tarefa de correção, todos os CVITs devem estar no mesmo estado.

Criar, editar e excluir regras de tarefa de correção de resposta a vulnerabilidades do contêiner

Você pode criar regras para agrupar automaticamente itens vulneráveis ao contêiner (CVIT) em tarefas de correção (CVUL) com base nas condições de filtro. Essas regras agrupam automaticamente CVITs conforme são importados ou criados manualmente.

Antes de Iniciar

Se você criar uma nova regra, ela não se aplicará aos dados existentes. Depois de enviá-lo, ele será executado em relação às novas importações.

Função necessária: Gerenciador de apps-sec

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras da tarefa de correção.**.
2. Abra a regra ou selecione **Novo** .
3. Preencha os campos no formulário ou edite-os.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra da tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição diferencia maiúsculas de minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. Por padrão, (**Distinção entre maiúsculas e minúsculas** caixa de seleção não marcada), o texto de pesquisa inserido no construtor de condições nos registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefa. Um exemplo de condição é **Vulnerabilidade** > **é** > **VULNENT123451** (uma vulnerabilidade importada conhecida). Qualquer CVIT que

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	tenha esta vulnerabilidade corresponde a esta condição.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Itens vulneráveis do contêiner de grupo de	A tabela que a regra usa para agrupar CVITs. Selecione os elementos na árvore: ○ Item vulnerável do contêiner [sn_vuln_vulnerable_item] ○ Item vulnerável do contêiner - Imagem do Docker ○ Item vulnerável do contêiner - Vulnerabilidade do contêiner **Nota:** Se você escolher uma tabela estendida, o **Usando o campo** é aplicado somente a itens vulneráveis à aplicação que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar CVITs. Selecione Condições na árvore.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir tarefas de correção automaticamente, a opção Atribuição é usada além de **Agrupar por** opções para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para que cada CVIT seja colocado em uma tarefa com um conjunto de grupos de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ○ Agrupar por campo: Se você selecionou qualquer campo de grupo de usuários no **Usando o campo** valores em **Agrupar por** , eles aparecem no menu suspenso. ○ Grupo de usuários: Use a lista de pesquisa para selecionar um grupo de usuários estático.

Nota: Se você excluir uma regra da exibição de formulário ou de lista, terá a opção de excluir todas as tarefas de correção em aberto criadas por essa regra. Os grupos que não estão no estado Aberto são excluídos.

4. Selecione **Enviar** para novas regras.
   Depois de selecionar **Enviar** Sua regra é exibida na lista Regras da tarefa de correção [sn_vul_grouping_rule]. As situações a seguir iniciam sua regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando novos CVITs são criados.
- Ao selecionar **Reaplicar** . Você seleciona **Reaplicar** avaliar regras de tarefa somente em tarefas de correção existentes.
- Quando as CVITs são atualizadas, por você ou pelo sistema.

  Se um CVIT for atualizado, as regras de tarefa serão avaliadas quanto a correspondências com as tarefas de correção existentes. Algumas atualizações comuns que iniciam uma verificação de regras são:

  - Quando o Estado muda de Encerrado para Aberto ou de Encerrado para Em Investigação.
  - O item de configuração (IC) foi alterado.
  - A vulnerabilidade foi alterada.

O sistema verifica se todas as regras de tarefa correspondem ao CVIT atualizado. Se as condições de uma regra corresponderem às condições de uma tarefa de correção, CVITs correspondentes serão atribuídos a ela.

Se nenhuma correspondência for encontrada, uma nova tarefa de correção será criada.

Para obter mais informações sobre acúmulo de estado de CVITs para tarefas de correção e acúmulo de estado de tarefas de correção para CVITs, consulte Tarefas de correção de resposta a vulnerabilidades do contêiner e visão geral de regras de tarefa.

Para obter um exemplo de uma regra de tarefa de correção, consulte Exemplos de regra de tarefa de correção de resposta a vulnerabilidades da aplicação.

5. Para excluir uma regra de tarefa, selecione a regra na lista Regras de tarefa de correção e selecione Excluir. A seguinte mensagem é exibida: A regra de tarefa de correção selecionada criou n tarefas de correção. Das tarefas de correção, n estão no estado Aberto.

Opção	Descrição
Caixa de seleção desativada (padrão).	Exclua somente a regra. Tarefas que não estão no estado Aberto são excluídas.
Caixa de seleção selecionada.	Inclua as tarefas de correção no estado Aberto ao excluir a regra de tarefa de correção. Exclua a regra e todas as tarefas de correção no estado Aberto.

6. Escolha uma opção e selecione **Excluir** .

Criar regras de fechamento automático para Contêiner de Resposta a vulnerabilidades

Use regras de fechamento automático para fechar itens vulneráveis ao contêiner (CVITs) mais antigos automaticamente com base nas condições de filtro definidas.

Antes de Iniciar

Função necessária: sn_vul.container_manage_auto_close_stale_vi

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** > **Regras de fechamento automático**.

   O sistema de base fornece as seguintes regras de fechamento automático: **Vulnerabilidades de contêiner verificadas pela última vez** Vulnerabilidades não relatadas nos últimos 90 dias são transferidas para o estado obsoleto.

2. Selecione **Novo** para criar regra de fechamento automático.
3. No formulário, preencha os campos.

Campo	Valor
Nome	Nome da regra de fechamento automático.
Ativo	Opção para ativar a regra. Se ativado, ele fecha automaticamente todas as detecções que correspondam aos critérios de filtro.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Tipos de integração	Integração de vulnerabilidade do contêiner **Nota:** Para verificar vulnerabilidades do host usando a integração Prisma Cloud Compute, selecione **Integração do verificador de vulnerabilidades** .
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.
   . **Fechamento automático** os trabalhos agendados de regras são executados diariamente. Identifica CVITs com base nas condições especificadas e faz a transição das correspondentes para **Obsoleto** estado. Nos casos em que há CVITs com status Encerrado e obsoleto, o CVIT é encerrado com o subestado definido como Fixo.

Removendo atribuições de itens vulneráveis do contêiner e tarefas de correção

Você pode limpar **Atribuído a.** e. **Grupo de atribuição** itens vulneráveis do contêiner diretamente dos registros de item vulnerável do contêiner e tarefa de correção que você determina que podem estar atribuídos incorretamente a você ou aos seus grupos.

Visão geral do fluxo de trabalho

Se você determinar que os itens vulneráveis ao contêiner (CVITs) e as tarefas de correção (CVULs) não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, poderá remover a si mesmo ou aos seus grupos do **Atribuído a.** e. **Grupo de atribuição** Campos nos registros CVIT e CVUL.

O fluxo de trabalho Cancelar atribuição é compatível com o espaço e nas exibições clássica e do espaço para CVITs e CVULs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de enviar solicitações para limpar os campos de atribuição para aprovação. Para obter mais informações, consulte Aprovar ou rejeitar uma solicitação de cancelamento de atribuição em Resposta a vulnerabilidades e Removendo atribuições de itens vulneráveis e tarefas de correção.

- . **Cancelar atribuição** A ação de IU é exibida nos registros CVIT e CVUL em qualquer estado diferente de Encerrado ou Resolvido.

  Nota: Depois que a solicitação para limpar os campos for aprovada para um CVUL, todos os **Atribuído a.** e. **Grupo de atribuição** Os campos em CVITs que têm o mesmo grupo de atribuição não são atribuídos. Se qualquer CVIT em um CVUL tiver um grupo de atribuição diferente do CVUL associado, ele não será desatribuído. Na maioria dos casos, esses CVITs foram atribuídos manualmente. Para obter mais informações, consulte Tarefas de correção de resposta a vulnerabilidades do contêiner e visão geral de regras de tarefa e Removendo atribuições de itens vulneráveis e tarefas de correção.

- Todos os registros que você atualiza com a ação de IU ou manualmente são exibidos no módulo Não atribuído para Resposta de vulnerabilidade do contêiner.

Consulte Remova atribuições de itens vulneráveis e tarefas de correção para obter mais informações sobre as etapas de como limpar os campos de atribuição.

Propriedades do sistema e notificações de aprovação

Se um responsável pela correção selecionar **Cancelar atribuição** Em um registro, por padrão, a propriedade do sistema sn_vul.unassign_vr.approval_required aciona o fluxo de aprovação e cria um registro de aprovação de mudança de estado no estado Revisão, e a solicitação é roteada para aprovação. A solicitação é exibida na lista Minhas aprovações para usuários com sn_vul_container.unassign_approver.

Nota: Como administrador de vulnerabilidades [sn_vul.vulnerability_admin], você pode definir *`sn_vul.unassign_vr.approval_required`*propriedade do sistema para **falso** para desabilitar o processo de aprovação.

Além disso, você pode alterar o valor em *`sn_vul.default_assignment_group`*portanto, se os campos de atribuição estiverem limpos, um grupo específico será atribuído. Por exemplo, se um usuário clicar **Cancelar atribuição** Em um registro e você deseja redirecioná-lo para um grupo específico para revisão, você pode adicionar o ID do sistema para o grupo de sua escolha no campo Valor da propriedade do sistema.

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

Feche uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção da aplicação pode ser encerrado imediatamente sem análise adicional, poderá usar **Fechar** recurso. A partir da v2.10 de Contêiner de Resposta a vulnerabilidades. **Fechar** o botão foi removido para uma tarefa de correção de contêiner.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Em Resposta a vulnerabilidades Espaços de trabalho, uma tarefa de correção passa pelos mesmos estados de uma tarefa de correção anterior em versões anteriores de Resposta a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades. Quando todos os itens vulneráveis (Vits) em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado inativo.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção do Encerrado ou Adiado estados.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione **Fechar** botão.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione o estado como *Encerrado* .
Motivo	Insira o motivo para encerrar o problema.
Informações adicionais	Insira outras informações relevantes.

4. Selecione **Enviar**.
   A tarefa de correção é marcada **Encerrado** .

IT Operations Management e descoberta de padrão

Quando a descoberta está habilitada, as informações são recebidas do Information Technology Operations Management(ITOM). . ITOM A Descoberta está habilitada, você pode ver namespaces do Kubernetes, clusters do Kubernetes e serviços do Kubernetes ao abrir um item vulnerável de contêiner (CVIT). Caso contrário, você pode ver as informações de carga do Prisma.

Os rótulos de imagem das cargas do Prisma são armazenados como pares de valor de chave na imagem do docker. Os rótulos em uma carga Prisma são armazenados na tabela cmdb_key_value. Para habilitar esse recurso, uma regra de identificação é enviada para cmdb_ci_docker_image pela equipe do ITOM. Abra a imagem do Docker para exibir a lista de itens relacionados. A maioria dos itens é preenchida pelo ITOM equipe. A entrada de identificação de uma imagem do docker é enviada para mostrar os valores como pares de chave-valor.

A criticalidade dos negócios é determinada com base nas informações de criticalidade do serviço recebidas do ITOM equipe. Um trabalho agendado é executado para extrair dados de todos os serviços associados a uma imagem. Calcula a criticalidade dos negócios com base no mapeamento de serviços. Como a pontuação de risco pode depender da criticidade dos negócios, a pontuação de risco também é calculada com base nela.

Soluções de análise e emissão de relatórios para Contêiner de Resposta a vulnerabilidades

Isso Solução para Performance Analytics e relatórios pré-empacotado Análise da plataforma conteúdo para uso com outros ServiceNow AI Platform produtos. Isso Solução para Performance Analytics e relatórios fornece uma exposição sobre como as vulnerabilidades são gerenciadas por meio dos vários gráficos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

- ServiceNow AI Platform Administrador (administrador): Instale e ative esta Solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Análise da plataforma Administrador (pa_admin): Revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Painel do Contêiner de Resposta a vulnerabilidades

As soluções de análise e emissão de relatórios contêm pré-pacotes Performance Analytics e. Emissão de relatórios conteúdo para uso com outros ServiceNow AI Platform produtos. Isso Solução para Performance Analytics e relatórios permite rastrear o volume, o desempenho e o andamento das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

Funções necessárias de ServiceNow AI Platform

- ServiceNow AI Platform Administrador (administrador): Instale e ative esta Solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Acessar os painéis de Contêiner de Resposta a vulnerabilidades

Para abrir o painel, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Visão geral**.

Importante:

A partir da versão 2,2 de Contêiner de Resposta a vulnerabilidades este painel também pode ser exibido no Next Experience IU. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e selecione **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, selecione o menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Página Painéis em Espaço do gerente de vulnerabilidade e Página Painéis em Espaço de correção de problemas de TI.

Nota:

- Se você for um novo usuário, poderá exibir os painéis somente nos espaços de trabalho.
- Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

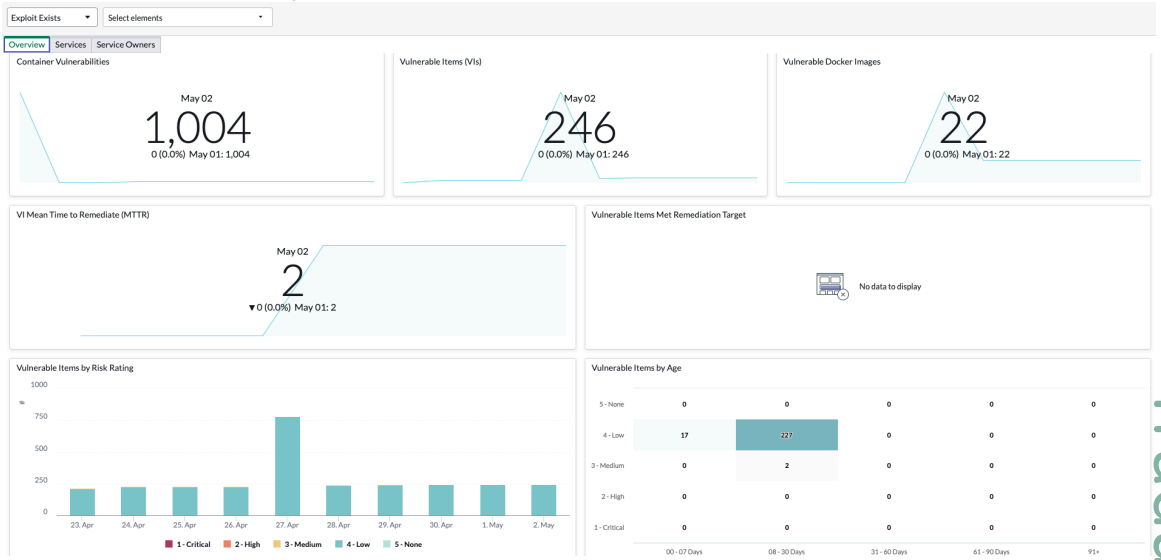
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias Gestão de vulnerabilidades de contêiner

Este painel permite que você veja as vulnerabilidades presentes em contêineres. Você pode exibir as vulnerabilidades e seus dados relacionados por região, idade, serviços e outros detalhamentos.

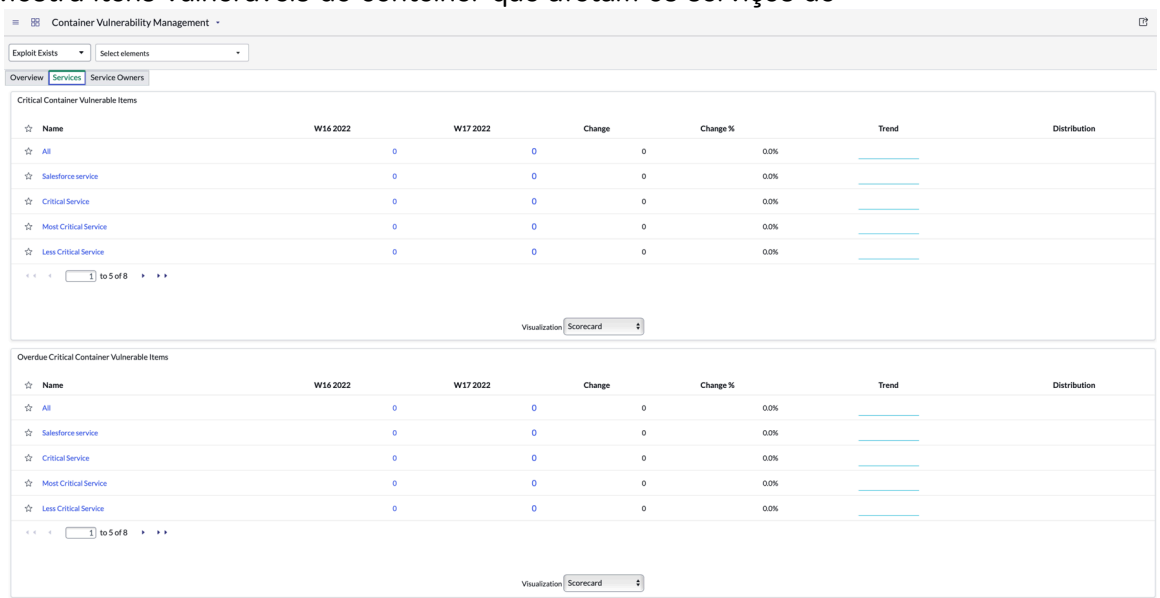
. **Visão geral**Fornece o status geral da Gestão de vulnerabilidades de contêiner no sistema.

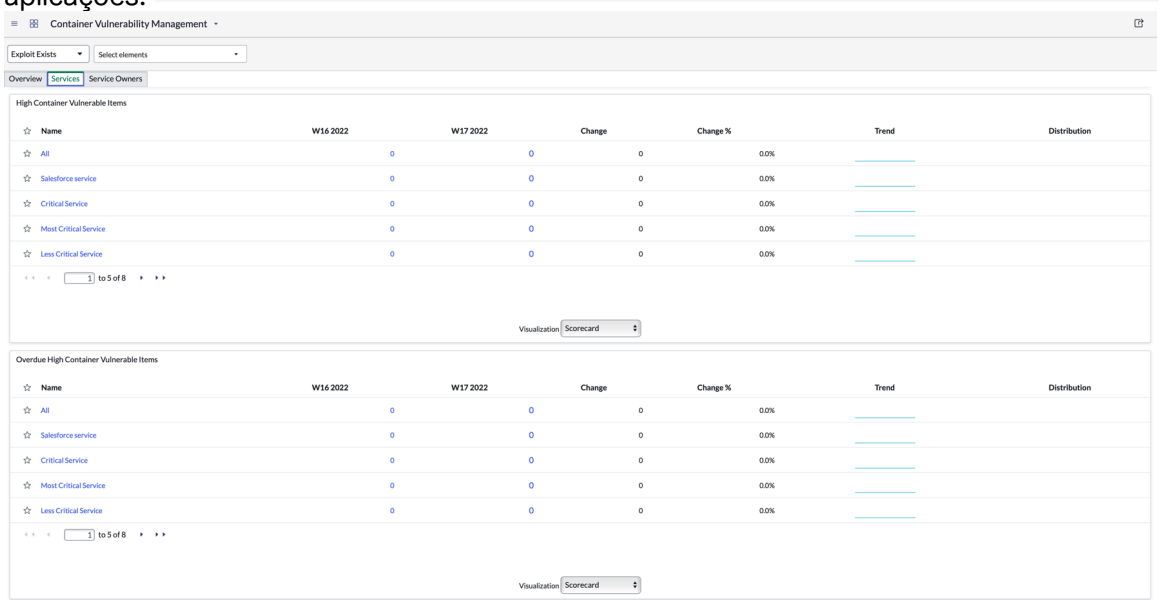


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. **Serviços**Mostra itens vulneráveis do contêiner que afetam os serviços de aplicações.

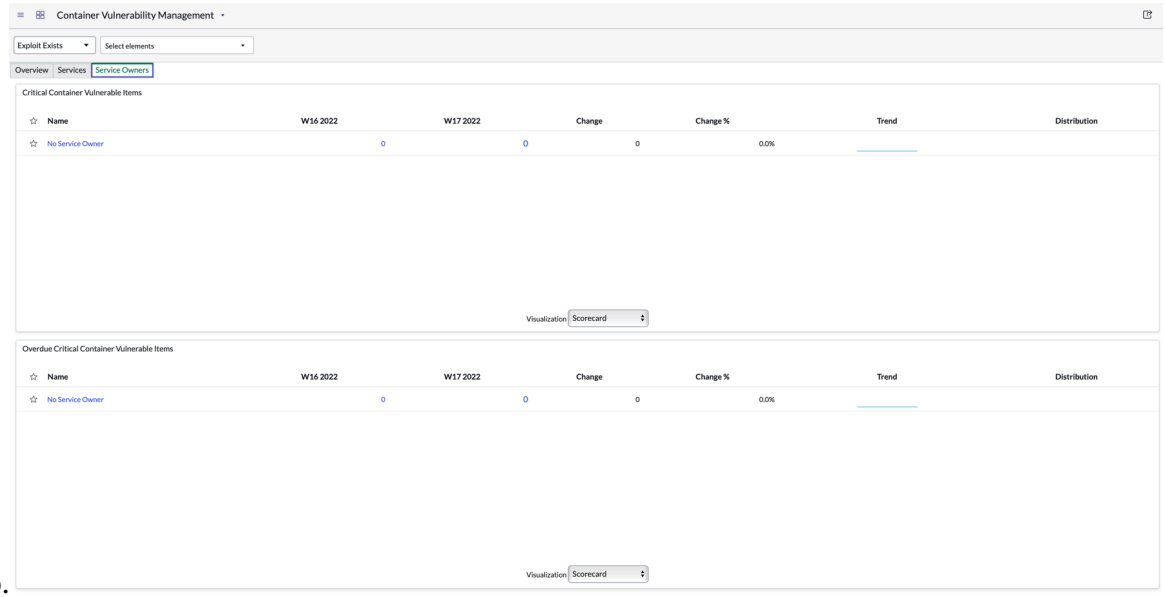




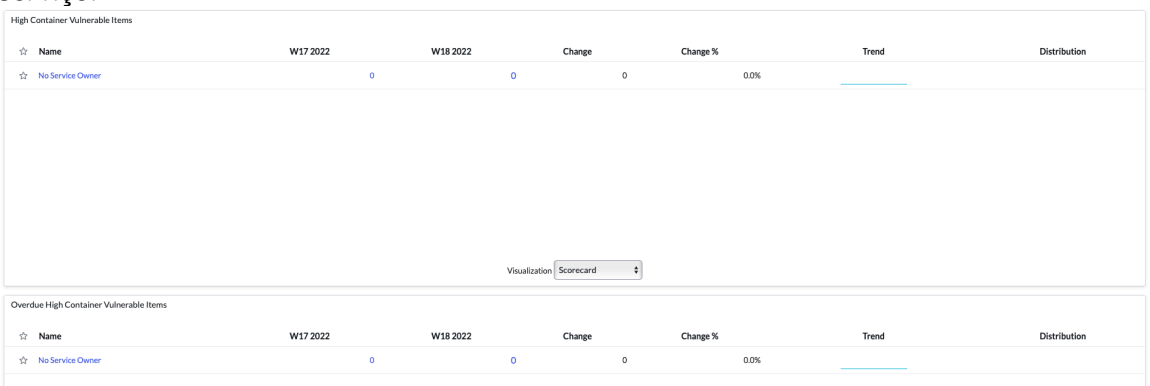
. **Responsáveis pelo serviço**Mostra itens vulneráveis do contêiner que afetam os responsáveis pelo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



serviço.



Detalhamentos

- Explorar Itens Existentes
- Explorar Vetor de Ataque
- Explorar Nível de Habilidade
- Status da meta de correção
- Pontuação de risco
- Estado
- Grupo de atribuição

Tradução automática

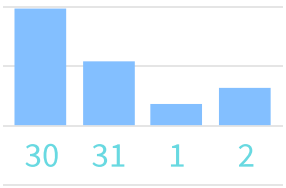
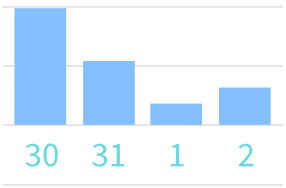
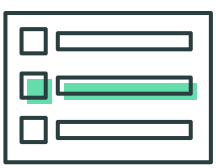
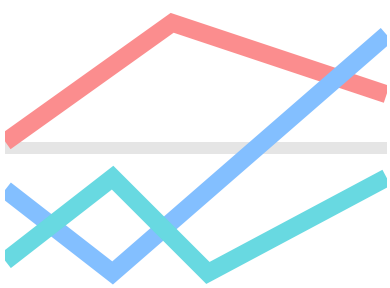
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades do contêiner	Pontuação  única	Número de vulnerabilidades de contêiner associadas a um ou mais itens vulneráveis de contêiner ativos.
Itens vulneráveis (IVs)	Pontuação  única	Número de itens vulneráveis do contêiner ativos (não encerrados).
Imagens do Docker vulneráveis	Pontuação  única	Número de imagens do docker associadas aos itens vulneráveis de contêiner ativos.
Tempo médio de correção do VI (MTTR)	Pontuação  única	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução.
Itens vulneráveis que atenderam à meta de correção	Pontuação  única	Percentual de itens vulneráveis do contêiner encerrado que atenderam às datas de meta de correção nos trimestres atual e anterior. As metas de correção são calculadas a partir da data da última abertura mais o número de dias.

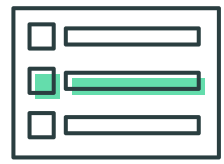
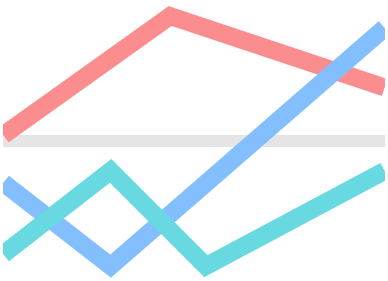
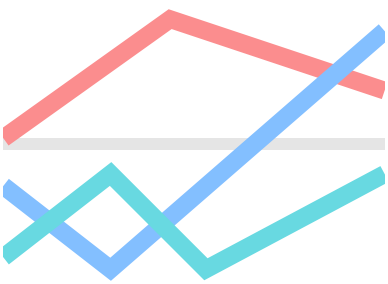
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis por classificação de risco	Barra 	Número de itens vulneráveis de contêiner ativo, agrupados por classificação de risco no período selecionado.
Itens vulneráveis conforme o tempo decorrido	Barra 	Número de itens vulneráveis de contêiner ativos agrupados por classificação de risco e idade (em dias). **Nota:** Personalizar o cálculo de Idade e Idade Encerrada para Itens vulneráveis ao contêiner (CVIS) pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para CVIS, consulte KB1703270 artigo da base de conhecimento.
Itens vulneráveis de contêineres críticos	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítico, agrupados por serviço.

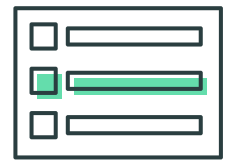
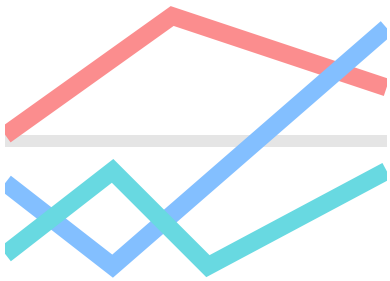
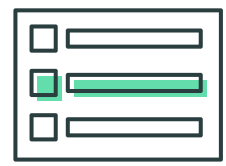
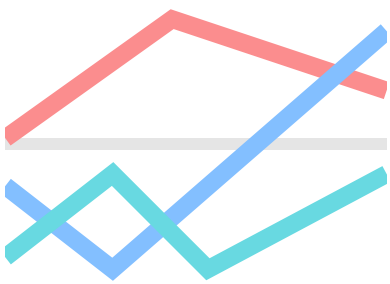
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítico e após as datas de destino de correção, agrupados por serviço.
Itens de alta vulnerabilidade de contêineres	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de alto risco, agrupados por serviço.

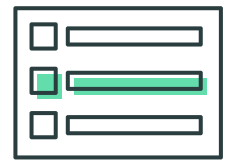
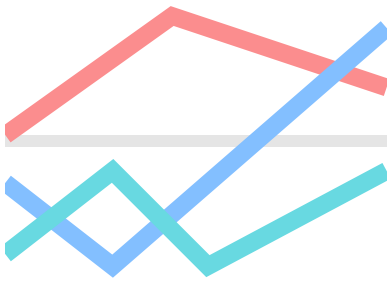
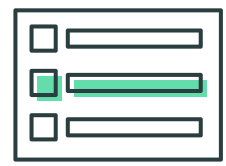
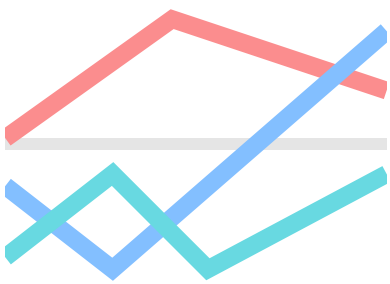
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e Linha  	Número de itens vulneráveis ativos com uma classificação de alto risco e após as datas de destino de correção, agrupados por serviço.
Itens vulneráveis de contêineres críticos	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítico, agrupados por responsável pelo serviço.

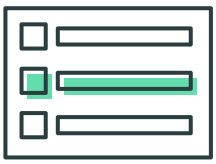
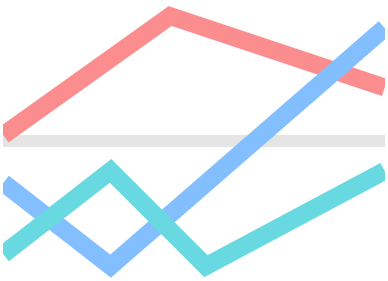
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítico e após as datas de destino de correção, agrupados por responsável pelo serviço.
Itens de alta vulnerabilidade de contêineres	Lista e Linha  	Número de itens vulneráveis de contêiner ativos com uma classificação de alto risco, agrupados por responsável pelo serviço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e Linha  	Número de itens vulneráveis ativos com uma classificação de alto risco e após as datas de destino de correção, agrupados por responsável pelo serviço.

Estrutura de relatórios agregados para Contêiner de Resposta a vulnerabilidades

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas dinâmicas complexas e de longa execução para melhorar o desempenho.

A estrutura de relatórios agregados melhora o desempenho ao:

- usando menos recursos e renderizando relatórios mais rapidamente,
- Agregação de dados e reutilização de agregações e detalhamentos (Agrupar por) e.
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis ao contêiner (CVITs), use a estrutura de relatórios agregados junto com os relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- ServiceNow AI Platform Administrador (admin): Instale e ative isso Solução para Performance Analytics e relatórios e fazer as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Sn_vul_cmn.admin): Criar agregações.
- VR write(sn_vul_cmn.write): Edite os dados nas agregações e nos resultados agregados.
- VR read (sn_vul_cmn.read): Revise os dados nas agregações e nos resultados agregados.
- Analista de vulnerabilidades (sn_vul.vulnerability_analyst): Revise os resultados agregados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

- Configure uma agregação para dados de origem
- Execute várias agregações simultaneamente
- Configure o número de agregações que podem ser executadas simultaneamente
- Crie um relatório usando uma agregação

Referência do Contêiner de Resposta a vulnerabilidades

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com o. Contêiner de Resposta a vulnerabilidades.

Componentes instalados com Contêiner de Resposta a vulnerabilidades

Vários tipos de componentes são instalados com a ativação do Contêiner de Resposta a vulnerabilidades aplicação, incluindo tabelas, funções de usuário e trabalhos agendados.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

A partir da v2.11 de Contêiner de Resposta a vulnerabilidades, as propriedades do sistema usadas com mais frequência agora estão acessíveis em Contêiner de Resposta a vulnerabilidades aplicação. Para exibir essas propriedades do sistema, navegue até **Tudo**Contêiner de Resposta a vulnerabilidades**Propriedades**.

Funções instaladas com Contêiner de Resposta a vulnerabilidades

As funções são adicionadas com a ativação de Contêiner de Resposta a vulnerabilidades.

Persona e funções granulares estão disponíveis para ajudar você a gerenciar o que usuários e grupos podem ver e fazer no Resposta a vulnerabilidades aplicação. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Nota:

Se você for um cliente de upgrade, o acesso para os usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write anteriores a 10.3 não foi alterado. Usuários e grupos permanecem atribuídos com essas funções até que você as altere. No entanto, a partir do 10.3, você pode preferir atribuir funções granulares para obter mais controle sobre o que os usuários e grupos podem fazer e ver no Resposta a vulnerabilidades aplicação. Para obter uma visão geral e mais informações sobre como gerenciar essas funções, consulte Resposta a vulnerabilidades personas e funções granulares e. Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Título da função [name]	Descrição
V2.10: sn_vul_container.delete	Exclui registros de origem. Conte sn_vul_cmn.delete e sn_vul_cont

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição
sn_vul_container.ci_manager	Gerencia a reclassificação de iten configuração (ICs) incompatíveis
sn_vul_container.configure_integrations	Configura integrações de contêin
sn_vul_container.configure_vi_granulity	Configura a granularidade do iten contêiner.
sn_vul_container.create_vi	Pode criar itens vulneráveis de co manualmente.
sn_vul_container.delete_vi	Pode excluir itens vulneráveis de criados manualmente.
sn_vul_container.exception_approver	Aprova exceções, adiamentos e f itens vulneráveis do contêiner. Contém a função sn_vul.view_manager_works A partir da v2.3, a função sn_vul_container.read_all, fo desta função para que voc acessar os itens vulnerávei contêiner e as tarefas de c atribuídas a você e ao seu vez de todos os itens vulne contêiner e as tarefas de c
sn_vul_container.false_positive_approver	Aprova ou rejeita itens vulnerável de fechamento como falso positiv Contém a função sn_vul.view_manager_works
sn_vul_container.manage_assignment_rules	Define e atualiza regras de atribu vulneráveis do contêiner.
sn_vul_container.manage_auto_close_stale_vi	Configure os itens vulneráveis do obsoletos de fechamento automát
sn_vul_container.manage_auto_exception_rule	Gerenciar (criar/ler/atualizar/excl exceção
sn_vul_container.manage_normalized_severity	Pode atualizar o mapeamento par severidade.
sn_vul_container.manage_permissions	Pode atribuir funções de resposta vulnerabilidades de contêiner aos
sn_vul_container.manage_remediation_targ...	Define e atualiza regras de destin contêiner.
sn_vul_contêiner.manage_risk_score_conf...	Define e atualiza Calculadoras de risco, regras de risco e Calculado de vulnerabilidades para itens vu contêiner.
sn_vul_container.read_all	Pode exibir todos os itens vulnera contêiner e informações relaciona

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição
	Contém a função sn_vul.view_manager_works
sn_vul_container.read_assigned	Pode exibir itens vulneráveis do c atribuídos a você ou aos seus gru clássica ou Espaço de correção d TI. Contém a função sn_vul.view_rem_workspace **Importante:** A partir d Resposta a vulnerabilidades sn_vul_container.read_assig privilégio de acessar o. Espa de problemas de TI.
sn_vul_container.read_assignment_rules	Pode exibir regras de atribuição d vulneráveis do contêiner.
sn_vul_container.read_auto_exception_rule	Regras de exceção de leitura
sn_vul_container.read_discovered_image	Pode exibir itens descobertos.
sn_vul_container.read_integrations	Pode exibir resultados de execuçõ integração.
sn_vul_container.read_normalized_severity	Pode exibir o mapeamento de gra normalizado.
sn_vul_contêiner.read_remediation_target...	Pode exibir regras de destino de c
sn_vul_contêiner.read_risk_score_configu...	Pode exibir calculadoras de pontu regras de risco e calculadoras de vulnerabilidades para itens vulne contêiner.
sn_vul_container.remediation_owner	Lê e grava itens vulneráveis do c atribuídos a eles. Os registros de também podem ser lidos por um função.
sn_vul_container.update_assigned_to	Pode atualizar a atribuição vulneráveis do contêiner. Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.update_assignment_group	Pode atualizar o grupo de a para itens vulneráveis do c Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.update_state	Pode atualizar estados de i vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição
	Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.vulnerability_admin	Configura todas as regras, integra por diante para Contêiner de Res vulnerabilidades produto.
sn_vul_container.vulnerability_analyst	Monitora a correção de todos os do contêiner.
sn_vul_container.write_all	Pode atualizar todos os itens vuln contêiner e tarefas de correção.
sn_vul_container.write_assigned	Pode atualizar itens vulneráveis tarefas de correção atribuídas a m grupos.
sn_vul_container.read_watch_topic	Pode ler Tópicos de observação vulnerabilidades de contêiner.
sn_vul_container.create_watch_topic	Pode criar Tópicos de observação vulnerabilidades de contêiner.
sn_vul_container.edit_watch_topic	Pode editar tópicos de observação vulnerabilidades de contêiner.
sn_vul_container.manage_exception_configuration	Pode gerenciar configurações de exceções.

Tabelas instaladas com Contêiner de Resposta a vulnerabilidades

As tabelas são adicionadas com a ativação de Contêiner de Resposta a vulnerabilidades(CVR).

Tabela	Descrição
Descoberta de imagem do contêiner sn_vul_container_image_findings	Armazena informações sobre as vulnerabilidades associadas, camada de imagem, imagem do docker, repositório de imagens e imagem descoberta. A partir da v2.11.3 de Contêiner de Resposta a vulnerabilidades você também pode exibir o caminho onde a descoberta é mostrada.
Camada da imagem do contêiner sn_vul_container_image_layer	Contém as informações de cada camada de imagem. Uma imagem é um arquivo estático com código executável que pode criar um contêiner em um sistema de computação.
Pacote de imagem do contêiner sn_vul_container_image_package	Fornece informações sobre os pacotes em que existem vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgulas. A partir da v2.11.3 de Contêiner de Resposta a vulnerabilidades Você também pode exibir a URL do pacote (PURL).
Item vulnerável de contêiner sn_vul_container_image_vulnerable_item	Contém detalhes de cada descoberta e a vulnerabilidade correspondente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	A partir da v2.11.3 de Contêiner de Resposta a vulnerabilidades você também pode exibir informações sobre a data da última verificação de uma imagem em execução como um contêiner.
Entrada de vulnerabilidade (v2.11.3) sn_vul_entry	Fornece informações sobre a gravidade de um CVE e quaisquer informações adicionais enviadas pelo Prisma.
Imagem do contêiner descoberta sn_vul_container_image	Fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as informações da camada e as associa à imagem descoberta. A partir da v2.11.3 de Contêiner de Resposta a vulnerabilidades Ele também fornece informações sobre Resumo de imagem de uma imagem do docker e a data da última verificação de uma imagem em execução como um contêiner e um registro.
Mapeamentos da descoberta sn_vul_container_finding_m2m_vul_item	Relacionamento M2M das descobertas da imagem do contêiner e os itens vulneráveis do contêiner (CVITs).
Fechar automaticamente itens vulneráveis sn_vul_container_image_auto_close_config	Contém as informações sobre como fechar as descobertas da imagem do contêiner obsoleto e acumular o estado para as CVITs.
Chaves de vulnerabilidade da imagem do contêiner sn_vul_container_image_vulnerability_keys	Contém a configuração de granularidade para criação de CVITs a partir das descobertas da imagem do contêiner.
Serviços relacionados ao Docker sn_vul_container_m2m_ci_services	Contém todos os serviços de negócios relacionados a uma imagem de contêiner.
Contagens de contêineres de VR sn_vul_container_vr_container_counts	Contém a média contínua de instâncias de contêiner descontinuadas de uma imagem de contêiner nos últimos 90 dias.
Item de Tarefa de correção de contêiner sn_vul_container_m2m_vul_group_item	Tabela M2M entre CVIT e tarefas de correção de contêiner.
Tarefa de correção de contêiner sn_vul_container_vulnerability	Contém tarefas de correção de contêiner.
Manifesto de tarefa de correção de contêiner sn_vul_container_rt_manifest	Todas as atualizações na tarefa de correção serão feitas usando esta tabela de manifesto por trabalhos agendados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos agendados instalados com Contêiner de Resposta a vulnerabilidades

Os trabalhos agendados são adicionados com a ativação de Contêiner de Resposta a vulnerabilidades.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Trabalho programado	Descrição
Associe o VIS de contêiner existente à regra de exceção automática	Associa automaticamente a regra de exceção automática aos itens vulneráveis ao contêiner (CVITs) existentes.
Verifique a expiração do adiamento do item vulnerável do contêiner	Envia notificações se itens vulneráveis do contêiner ou vulnerabilidades do contêiner expirarem (e se expirarem em uma semana).
Contagem de contêiner de resposta a vulnerabilidades (aplicação - Resposta a vulnerabilidades e Conformidade de configuração para contêineres)	É executado diariamente para preencher a tabela sn_vul_container_vr_container_counts que calcula a média contínua de 90 dias para contêineres.
Fechar CVITs automaticamente	Fecha automaticamente os itens de vulnerabilidade do contêiner que correspondem à condição definida na configuração de fechamento automático. Seu status é alterado para "Fixo".
Calcular Criticalidade de negócios para CVIT	Processa todos os CVITs ativos e atualiza o campo Criticalidade dos negócios, com base nos serviços afetados da imagem do docker do CVIT.
Cancelar CVITs que não têm uma imagem do Docker associada	Expira automaticamente CVITs que não têm um IC associado a. Seu estado é definido como Encerrado e subestado como Cancelado.
Calcular contagens de VI relacionadas para a tarefa de correção de contêiner	Calcula as contagens nos registros da tarefa de correção de contêiner.
Acumular valores de item vulnerável do contêiner para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis do contêiner. **Nota:** A partir da v2.10 de Contêiner de Resposta a vulnerabilidades, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de multithreading. Este upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.

Contêiner de Resposta a vulnerabilidades glossário

Saiba mais sobre termos e conceitos exclusivos do Contêiner de Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termos principais

Contêiner

Uma unidade de software que empacota o código e todas as suas dependências para que a aplicação seja executada de forma contínua e confiável de um ambiente de computação para outro.

Imagem do contêiner

Um arquivo estático com código executável que pode criar um contêiner em um sistema de computação. Uma imagem de contêiner não pode ser alterada e, portanto, pode ser implantada de forma consistente em qualquer ambiente.

Cluster

Um conjunto de máquinas de trabalho, chamadas de nós, que executam aplicações em contêiner.

Docker

Software para criar, implantar e gerenciar contêineres de aplicações em servidores e na nuvem.

Imagem do Docker

Um arquivo de modelo que contém código, bibliotecas necessárias, configurações e assim por diante. O arquivo é usado para iniciar instâncias de contêiner. Consiste em uma união de sistemas de arquivos em camadas.

Dockerfile

Um arquivo de texto que contém instruções para criar imagens de contêiner adicionando várias camadas. Por exemplo, camadas de Ubuntu base, nginx e código do app.

Docker Compor

Uma ferramenta para definir e executar aplicações complexas com Docker. Com Compor, você pode definir uma aplicação de vários contêineres em um único arquivo.

Contêiner do Docker

Um contêiner do Docker é uma instância de tempo de execução iniciada a partir de uma imagem do Docker.

Camada de imagem

Uma camada é uma modificação em uma imagem. Ele é representado por uma instrução no Dockerfile. As camadas são aplicadas em sequência à imagem de base para criar a imagem final.

Repositório de imagem

Uma coleção de imagens do docker com diferentes marcadores ou versões.

Rótulos de imagem

Um conjunto de pares de chave-valor armazenados com a imagem como metadados.

Namespace

Uma abstração usada pelo Kubernetes para oferecer suporte ao isolamento de grupos de recursos em um único cluster.

Pod

Um conjunto de contêineres em execução (outra abstração em cima de um contêiner).

Registro

Um serviço hospedado que contém repositórios de imagens.

Serviço

Uma maneira abstrata de expor uma aplicação em execução em um conjunto de pods como um serviço de rede.

Marcador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um marcador é um rótulo aplicado a uma imagem do Docker em um determinado repositório de imagens. Marcadores são como várias imagens em um repositório são distintas umas das outras.

Campos do formulário Item vulnerável do contêiner

CVITs (itens vulneráveis ao contêiner) são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos do formulário de item vulnerável do contêiner

Exceto para **Grupo de atribuição** , **Atribuído a.** campos e. **Anotações** Todos os outros campos no CVIT são somente leitura.

Campo	Descrição
Número	Identificador CVIT gerado automaticamente para este registro.
Origem	Scanner que identificou a vulnerabilidade.
Classificação de risco	Quantificado **Pontuação de risco** Separando itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum.
Pontuação de risco	Valor calculado de risco que o CVIT representa para o seu ambiente.
Regra de meta da correção	Regra de destino de correção de acordo com a qual a data de destino de correção é calculada.
Meta da correção	Data em que os CVITs devem ser corrigidos, desde que identificados pela primeira vez. Aparece somente quando aplicável.
Status da correção	Status da correção do CVIT.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável da aplicação.
Imagem do Docker	Arquivo de modelo que contém código, bibliotecas necessárias, configurações e assim por diante. O arquivo é usado para iniciar instâncias de contêiner. Consiste em uma união de sistemas de arquivos em camadas.
Imagem do contêiner descoberta	Registro exclusivo para cada ID de imagem.
Imagem base	Uma imagem básica usada para criar aplicações em contêiner, contendo o sistema operacional e as bibliotecas essenciais. Ele serve como o ponto de partida para criar e personalizar aplicações em ambientes como Docker.
Clusters de imagens	Grupos de imagens relacionadas usados em vários contextos, como agrupar imagens semelhantes em aprendizado de máquina ou imagens de contêiner em um repositório.
Namespace da imagem	Usado para organizar e isolar imagens de contêiner em um registro, permitindo que diferentes equipes ou projetos mantenham coleções separadas.
Estado	O padrão deste campo é **Aberto** quando criado. Consulte estados de item vulnerável à aplicação (AVI) para obter mais informações sobre como os estados são mapeados.
Grupo de atribuição	Grupo selecionado para trabalhar neste CVIT.
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha neste CVIT. Pode ser adicionado ou editado manualmente por um gerente da App-Sec.
Criação em	Data e hora em que um CVIT é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aberto pela última vez	Data e hora mais recentes em que o CVIT é reaberto.
Atualização em	Data e hora em que o CVIT foi modificado pela última vez.
Primeiro encontrado (v2.12.1)	Data em que a vulnerabilidade foi encontrada pela primeira vez. A partir da v2.12.1, você pode ver a data e hora precisas em que foi descoberta pela primeira vez, garantindo clareza e contabilidade para diferentes fusos horários. Para preencher os primeiros detalhes de data e hora encontrados, a integração deve ser executada novamente.
Encontrado pela última vez (v2.12.1)	Data em que a vulnerabilidade foi encontrada pela última vez. A partir da v2.12.1, você pode ver a data e hora precisas em que foi encontrada pela última vez, garantindo clareza e contabilidade para diferentes fusos horários. Para preencher os últimos detalhes de data e hora encontrados, a integração deve ser executada novamente.
Data de resolução (v2.12.1)	Data em que a vulnerabilidade foi resolvida. A partir da v2.12.1, você pode ver a data e a hora precisas em que ela foi resolvida, garantindo clareza e contabilidade para diferentes fusos horários. A data de resolução é preenchida quando o CVIT é resolvido como parte do fluxo de trabalho.
Aberto pela última vez (v2.12.1)	Data em que a vulnerabilidade foi aberta pela última vez. A partir da v2.12.1, você pode ver a data e a hora precisas em que foi aberto pela última vez, garantindo clareza e contabilidade para diferentes fusos horários. O trabalho agendado *`Add default values for last_opened_dt_tm from last _opened`*preenche os dados neste campo. Ele deve ser executado somente uma vez sob demanda.
Vulnerabilidade	
Resumo	Descrição da vulnerabilidade.
Gravidade	Grau normalizado de gravidade desta vulnerabilidade. Os mapas de gravidade são fornecidos para o National Vulnerability Database (NVD) e com integrações de terceiros da ServiceNow.
Pontuação de vulnerabilidade (v3)	Pontuação do Common Vulnerability Score System (CVSS) v3.
Pontuação de vulnerabilidade (v2)	Pontuação do CVSS v2.
Exploração presente	Sim, se pelo menos uma exploração estiver associada às vulnerabilidades associadas a este item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Vetor de ataque da exploração	Vetor de ataque mais vulnerável das explorações das vulnerabilidades associadas a este item vulnerável.
Nível de habilidade da exploração	Nível de habilidade mais baixo necessário para explorar as vulnerabilidades associadas a este item vulnerável.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Ameaça	Informações relevantes sobre a ameaça. Extraído do registro de entrada vulnerável. **Nota:** Todas as mudanças feitas aqui atualizam o registro de entrada vulnerável.
Anotações de correção	Solução relevante para a ameaça, extraída do registro de entrada vulnerável.
Anotações	
Anotações de trabalho	Qualquer informação relevante. Selecione a caixa de texto das anotações de trabalho para adicionar informações.
Descobertas de imagem	Resultados da verificação de vulnerabilidades nas imagens do contêiner.
Aprovações solicitadas	Solicitação de aprovações gerada para o CVIT.
Aprovações de mudança de estado	Solicitação de aprovações de mudança de estado gerada para o CVIT.

Cálculos de idade de um CVIT:

- A coluna Idade na lista de CVITs exibe a duração (formato: Dias HH:MM:SS) para a qual um CVIT está ativo. O valor Idade é zero para um CVIT encerrado.
- A coluna Idade fechada na lista de CVITs exibe a duração (formato: Dias HH:MM:SS) durante a qual um CVIT está ativo antes de ser encerrado. Para CVITs, exceto no estado Encerrado, o valor Idade Encerrada é zero.

Para obter mais informações sobre como personalizar o cálculo de Idade e Durações de Encerramento de Idade, consulte KB1703270 artigo.

Formulário de configuração de computação em nuvem do Prisma

O formulário Configuração de computação em nuvem do Prisma é acessado no módulo Integração de computação em nuvem do Prisma.

Para exibir o formulário Configuração de computação do Prisma Cloud, navegue até **Tudo** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.

Configuração do Prisma Cloud Compute

Campo	Descrição
Instância de Integração	Nome da nova instância de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do Prisma Cloud Compute

Campo	Descrição
	Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da base da API	URL para integrar com o Prisma Cloud Compute.
Nome do usuário	Nome de usuário para acessar o Prisma Cloud Compute.
Senha	Senha para acessar o Prisma Cloud Compute.
MID Server	Uma aplicação Java que é executada como um serviço do Windows ou daemon UNIX em um servidor em sua rede local. O MID Server permite a comunicação e a movimentação de dados entre um ServiceNow instâncias e aplicações externas, fontes de dados e serviços.
Usar projetos	Opção para configurar os projetos. Ao marcar a caixa de seleção, você pode selecionar projetos na página de configuração e executar as integrações com base nos projetos configurados para preencher detalhes específicos do projeto. **Nota:** Se esta caixa de seleção estiver marcada, o **Configurar projetos** a guia está habilitada. Clique em **Próximo** para prosseguir com a configuração dos projetos.

Formulário Solicitar exceção

Solicitar exceções de política usando GRC capacidade de gestão de exceções de política no Gestão de políticas e conformidade aplicação a partir de Contêiner de Resposta a vulnerabilidades.

Para exibir o formulário Configuração de computação do Prisma Cloud, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas de correção**)> **Todos** e abra o item ou grupo para o qual você deseja solicitar uma exceção.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começará. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e quando o estado do item vulnerável ou grupo muda de Adiado para Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	Nota: O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** Que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Formulário Regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica para um grupo de itens vulneráveis ao contêiner (CVITs), como uma regra com uma condição baseada na gravidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Para exibir o formulário Regra de exceção, navegue até **Tudo** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.
Válida de	Data a partir da qual esta regra está ativa para adiar os CVITs.
Válida até	Data a partir da qual a tarefa de correção para de aceitar novos CVITs.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção que foi criada para rastrear os CVITs adiados está atribuída.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição de filtro para os CVITs que podem ser definidos durante o processamento dos CVITs.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.
Estado	Estado da regra de exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de exceção

Campo	Descrição
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando os VULs e CVITs são adiados. Nesta data, o VUL criado é encerrado, todos os CVITs são movidos para fora do grupo e as regras do grupo são reaplicadas.

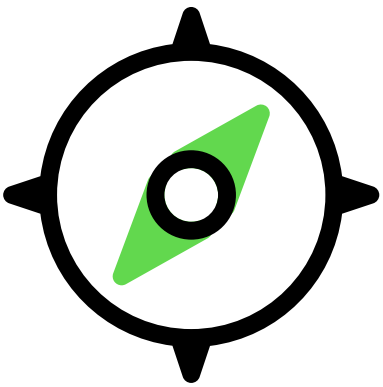
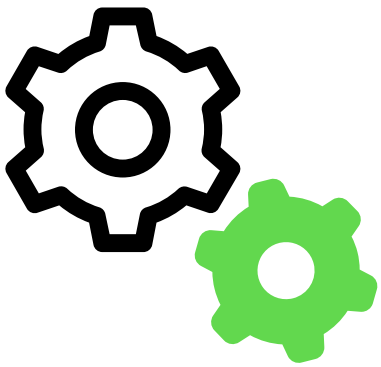
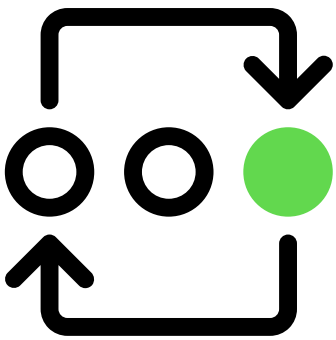
Conformidade de configurações

. ServiceNow® Conformidade de configurações A aplicação é uma aplicação de Avaliação de configuração segura (SCA) que agrega resultados de verificação de integrações com aplicações de verificação de configuração de terceiros. Você pode priorizar problemas de conformidade de configuração usando seu Configuration Management Database (CMDB). Conformidade de configurações Integra-se totalmente ao processo de gestão de mudanças de TI para corrigir suas configurações fora de conformidade.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Conformidade de configurações

Explorar	Instalar, Instalar e Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos de Conformidade de configuração	Configuração Conformidade de configuração	Integre a Conformidade de configuração com outras aplicações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

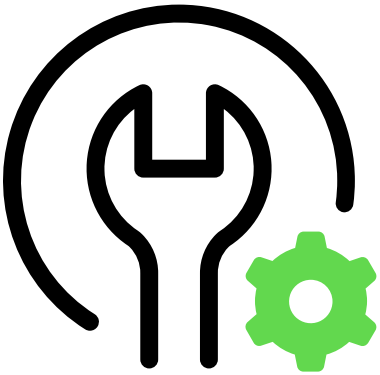
Conformidade de configurações

Use os Espaços de resposta a vulnerabilidades



Saiba como monitorar, gerenciar e corrigir problemas de configuração nos espaços do Gerenciador de vulnerabilidades, Correção de TI e Avaliação de vulnerabilidades.

Corrigir



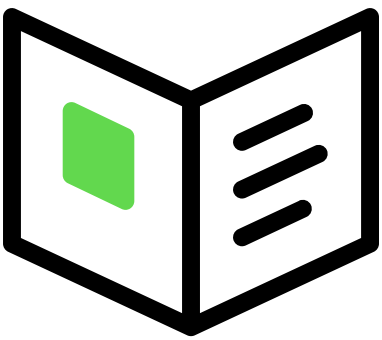
Saiba como corrigir seus ativos fora de conformidade com Conformidade de configuração

Relatórios e análises



Exiba relatórios e painéis em Conformidade de configuração

Referência



Obtenha detalhes sobre os componentes de Conformidade de configuração, como campos, tabelas e propriedades

Tradução automática

Solucionar problemas e obter ajuda

- Biblioteca de recursos de operações de segurança
- Comunidade de Operações de segurança

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorando Conformidade de configurações

Use os resultados de testes obtidos de integrações da Avaliação de configuração segura (SCA) de terceiros para verificar a conformidade com políticas corporativas ou de segurança. Identificar, priorizar e corrigir itens de configuração fora de conformidade.

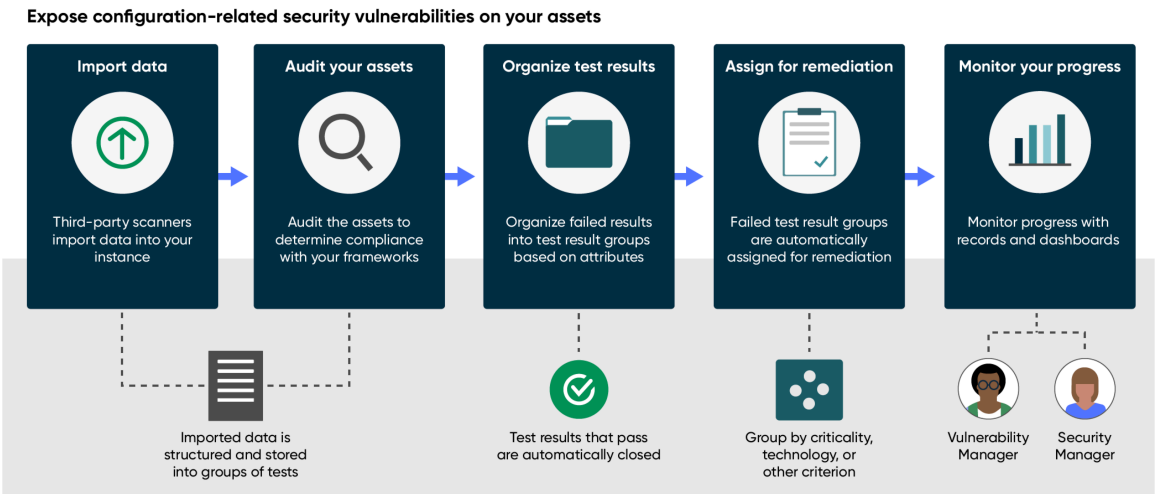
Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

O que é Conformidade de configurações

. ServiceNow® Conformidade de configurações a aplicação permite que você priorize e corrija as vulnerabilidades relacionadas à configuração mais críticas em seu ambiente de forma rápida e eficiente. Conformidade de configurações está disponível por assinatura no ServiceNow® Store.



Principais recursos do Conformidade de configurações

Use Configuration Management Database (CMDB) em seu ServiceNow AI Platform® para ajudá-lo a expor e corrigir suas vulnerabilidades de segurança mais críticas relacionadas à configuração. Concentre seus recursos de correção em atividades com a maior redução de risco. Simplifique o processo de correção entre as partes interessadas de segurança, TI e processo de negócios. . Conformidade de configurações a aplicação inclui os seguintes recursos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Com integrações de terceiros compatíveis, importe automaticamente políticas, testes, fontes autorizadas e tecnologias. Consulte Integrações do Conformidade de configurações para obter mais informações sobre integrações compatíveis.
- Correlacione políticas e testes a itens de configuração (ativos) para identificar vulnerabilidades relacionadas à configuração e ajudar a verificar se seus ativos estão em conformidade com suas políticas e controles.
- Unifique a avaliação de configuração, a atribuição e a correção em todos os seus ativos.
- O conteúdo de verificação de configuração pode ser importado das principais aplicações de integração do ecossistema de Avaliação de configuração segura (SCA).
- Descobertas de configuração, falhas de teste podem ser agrupadas e roteadas automaticamente com base em conjuntos de habilidades especializadas de correção e áreas de responsabilidade. Fluxos de trabalho inteligentes e a integração estreita com a gestão de mudanças fornecem transferências de tarefas suaves entre os grupos.
- Quando usado com ServiceNow Governança, risco e conformidade(GRC aplicação, testes de configuração em Conformidade de configurações Pode ser acumulado para seus controles GRC correspondentes.
- Com o gerenciamento de mudanças aprimorado, crie solicitações de mudança preenchidas previamente para TI diretamente do Conformidade de configurações para ajudá-lo com suas tarefas de correção que exigem recursos adicionais.
- Com os painéis, exiba métricas de status de correção na tarefa de correção, teste de conformidade e registros de política.

Quem usa Conformidade de configurações

Conformidade de configurações as atividades podem envolver muitos níveis de gestão.

- Administradores de sistema
- Administradores de vulnerabilidades
- Gerenciadores de vulnerabilidades
- Analistas de vulnerabilidades
- Administradores de conformidade

Conformidade de configurações as tarefas envolvem as seguintes funções.

- sn_vulc.admin - pode ler, gravar, excluir
- sn_vulc.write - pode ler e gravar
- sn_vulc.remediation_owner - Pode ler e atualizar registros atribuídos

> **Nota:** A função sn_vulc.remediation_owner também é atribuída automaticamente quando qualquer usuário recebe a função itil.

- sn_vulc.read - pode ler

Conformidade de configurações e Operações de segurança

. Qualys Vulnerability Integration e o. Integrações de vulnerabilidade da Tenable estão instalados, acesso a. Resposta a vulnerabilidades fica disponível. Você pode ter várias implantações dessas integrações. Os dados originados de cada implantação são identificados e disponibilizados em uma única instância do GRC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis para Zurich

Versão de lançamento	Notas de versão
Conformidade de configurações v15.4	Notas da versão de Conformidade de configuração . Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão Consulte Instalação e configuração do Conformidade de configurações aplicação para obter mais informações sobre como ativar a aplicação.

Conformidade de configurações dados importados

. Conformidade de configurações a aplicação importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Integrações compatíveis

Integrações de terceiros importam descobertas de avaliação de configuração, grupos de testes, testes, tecnologias, fontes autorizadas, e os resultados de testes em Conformidade de configurações aplicação. Os gerentes de vulnerabilidades ou analistas de vulnerabilidades podem usar esses dados para identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos.

Para obter mais informações sobre integrações compatíveis, consulte Integrações do Conformidade de configurações.

Grupos de teste

Os grupos de teste estão relacionados a documentos autorizados e registros de teste. Um grupo de testes de configuração define grupos de teste. Os grupos de teste normalmente se alinham a uma classe de tecnologia, por exemplo, Windows, Oracle Databases, Cisco IOS, e geralmente são derivados do padrão primário do setor. Grupos de teste podem ser modificados para atender às necessidades da organização. Um único Teste de configuração pode pertencer a vários grupos de teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Qualys Vulnerability Integration	Os grupos de teste são recuperados e os IDs de controle são preenchidos pelo trabalho agendado, **Políticas de PC da Qualys** Às 1:00. Você pode exibir o trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Políticas de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Políticas de PC da Qualys** primeiro.
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io Políticas de importações de integração de resultados de conformidade. Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro da política, navegue até **Tudo** > **Conformidade de configurações** > **Grupos de teste**. Para identificar e criar corretamente os registros do grupo de testes, as informações de auditoria dos grupos de teste são importadas e exibidas no **Descrição resumida** campo.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser governada.

. Conformidade de configurações teste é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de vulnerabilidade. Algumas soluções de verificação de VA de terceiros, como a Qualys, têm bibliotecas muito grandes de testes (até 8 000) que são mapeadas para políticas e "estruturas" de fontes autorizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um Teste pode ter muitos valores, um para muitos, esperado versus real e assim por diante. Um teste é qualquer coisa que pode ser usada para identificar uma classe de ativo de software ou hardware que está fora de conformidade. Por exemplo, uma versão ou número de hardware.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho agendado, **Controles de PC da Qualys** recupera os testes. Você pode exibir o trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Controles de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Controles de PC da Qualys** após **Políticas de PC da Qualys** .
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io A integração de resultados de conformidade importa testes de configuração (testes). Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro Teste de configuração, navegue até **Conformidade de configurações** > **Testes**. No registro, os dados importados são exibidos em **Descrição resumida** Campo e Status de correção, Descrição e Correção. Os dados também são exibidos no **Citações** , **Políticas** e **Resultados do teste** Links relacionados.

Tecnologias

Uma das técnicas usadas por scanners de vulnerabilidades de terceiros para criar grupos de teste de itens de configuração de software e hardware para análise é organizá-los por tecnologia. As tecnologias são uma biblioteca importada de OSes, dispositivos de rede, bancos de dados e aplicativos associados a políticas. Os testes têm várias implementações para diferentes tecnologias. A correção também é específica da tecnologia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exiba as tecnologias aplicáveis para um teste, para entender melhor a quais tipos de ativos de software ou hardware o controle pode ser aplicado. Exemplos de tecnologias que podem ser aplicadas a controles incluem CentOS 7.x, Windows 8,1, Windows 2016 Server e assim por diante. A lista de tecnologias é somente leitura e corresponde às tecnologias definidas em Qualys Cloud Platform aplicação.

As tecnologias são importadas somente para avaliações de configuração relacionadas ao banco de dados. . *db_type*(se não estiver vazio) na importação é usado para criar uma tecnologia. Exiba as tecnologias preenchidas na seção Tecnologias em registros de teste de configuração, registros de resultado de teste, registros de política e em **Conformidade de configurações** > **Dados de suporte** > **Tecnologias**.

Fontes autorizadas

Conformidade de configurações Usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. Fontes autorizadas geralmente são mapeadas para seções de padrões publicados do setor, como "NIST 800-53 versão 3 (2009) 3: 2009, SA-4".

Nota: Em Qualys Vulnerability Integration esta combinação é chamada de estrutura.

Fontes autorizadas e citações (também conhecidas como exigências) são importadas dos verificadores de vulnerabilidades de terceiros.

Os registros de origem autorizada contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas no campo de segurança de computadores. Eles definem requisitos para políticas e procedimentos de segurança. Os testes de configuração podem fazer referência a várias fontes autorizadas por meio de citações. Fontes autorizadas podem relatar a conformidade de um determinado padrão em preparação para uma auditoria.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho agendado, **Detalhe das políticas de PC da Qualys** recupera as fontes autorizadas e as citações. Você pode exibir este trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Detalhe das políticas de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Detalhe das políticas de PC da Qualys** após **Políticas de PC da Qualys** .
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io A integração de resultados de conformidade importa fontes autorizadas como parte dos dados de citações. Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	• Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Os dados são exibidos no **Citações** link relacionado em registros de teste de configuração.

Resultados de testes

Conformidade de configurações não calcula os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando eles estiverem visíveis em Conformidade de configurações, eles são corrigidos usando **Tarefas de correção** . Para obter mais informações, consulte Conformidade de configurações correlação.

Integração	Descrição
Qualys Vulnerability Integration	Você pode recuperar os resultados do teste de uma das seguintes maneiras: O trabalho agendado, **Resultados de PC da Qualys** recupera os resultados do teste. Você pode exibir este trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Resultados de PC da Qualys** após **Políticas de PC da Qualys** e. **Detalhe das políticas de PC da Qualys** . . **Resultados de PC da Qualys** a importação usa `Start Time`parâmetro no **Detalhes da integração** guia . Todos os outros Conformidade de configurações as importações trazem todos os dados disponíveis, independentemente de `Start Time`. . **Resultados de PC da Qualys** a importação está concluída, um evento é disparado para acionar cálculos de fim de importação. Para obter mais informações, consulte Conformidade de configurações estados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	Como alternativa, a partir da V14.5, você também pode executar as seguintes integrações para recuperar os resultados do teste: • Qualys Integração de host da política de PCRS - Recupera os IDs de host para cada política. Para exibir este trabalho agendado, navegue até: Qualys Vulnerability Integration > Integrações primárias > Qualys PCRS Policy Host Integration. **Nota:** Se você optar por executar a integração manualmente, execute a Integração do host da política PCRS da Qualys após as políticas do PC da Qualys e os detalhes das políticas do PC da Qualys. Após a conclusão desse trabalho agendado, ele aciona automaticamente a Integração de resultados de teste PCRS da Qualys. • Qualys Integração de resultados de teste DE PCRS - Recupera os resultados de teste para cada ID de host. Para exibir este trabalho agendado, navegue até Integração de vulnerabilidades da Qualys > Integrações primárias > Integração de resultados de teste de PCRS da Qualys. **Nota:** Se você optar por executar a integração manualmente, execute a Integração de resultados de teste de PCRS da Qualys após as políticas de PC da Qualys, Detalhes de políticas de PC da Qualys e Integração de host da política de PCRS DA Qualys. Esta integração usa o parâmetro Hora de início na guia Detalhes da integração.
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io A integração de resultados de conformidade importa resultados de teste. Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	• Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro Teste de configuração, navegue até **Conformidade de configurações** > **Resultados dos testes**. No registro, os dados importados são exibidos em **Teste** e **Item de configuração** campos. Os dados também são exibidos no **Valores esperados** , **Valores reais** e **Correção** guias. . **Tarefas de correção** e. **Histórico do resultado do teste** Os links relacionados são preenchidos.

Descoberta de Conformidade de configurações

Conformidade de configurações Os dados são importados de aplicações de scanner SCA de terceiros. Eles estruturam grupos de testes de software e hardware em registros de dados para agilizar a realização de avaliações.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Quando uma importação é concluída, um evento é enviado para indicar ações de fim de importação. Para cada tarefa de correção ativa, as seguintes ações são realizadas:

- Tarefas de correção resolvidas com resultados com falha retornam para **Aguardando implementação** estado.
- As tarefas de correção em que todos os resultados foram aprovados são **Encerrado** .
- O estado dos resultados de teste que estão em tarefas de correção ativas é atualizado.
- O sinalizador que indica se um resultado faz parte de uma tarefa de correção ativa é atualizado.

Conformidade de configurações correlação

Conformidade de configurações fornece priorização e agrupamento de resultados de teste (em tarefa de correção) para ajudar na correção de problemas de não conformidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Priorização centrada em ativos

Verificações de configuração podem produzir um grande número de descobertas. Priorize as descobertas para obter maior redução de risco. A prioridade inclui a criticalidade do teste de configuração e a criticalidade do ativo. A prioridade do resultado do teste de configuração é expressa como uma pontuação de risco de escala de 0 a 100. Os grupos de calculadora calculam a pontuação de risco e podem ser personalizados.

Quando a importação de terceiros estiver concluída, Conformidade de configurações envia um evento para indicar ações de fim de importação. Para cada grupo de resultados ativo, as seguintes ações são realizadas:

- Tarefas de correção resolvidas com resultados com falha retornam para **Aguardando implementação** estado.
- Tarefas de correção em que todos os resultados aprovados estão **Encerrado** .
- O estado dos resultados de teste que estão em tarefas de correção ativas é atualizado.
- O sinalizador que indica se um resultado faz parte de uma tarefa de correção ativa é atualizado.

Ordem de precedência das tarefas de correção

Quando os resultados do teste pertencem a mais de um grupo, o. **Estado** de um resultado de teste é derivado de acordo com uma ordem de precedência.

. **Estado** e. **Resolução** campos no **Teste de configuração** e **Resultado** . **Resultado do teste** , são calculados seguindo esta ordem de precedência.

Nota:

A precedência de associação do grupo se aplica somente a itens em que o item não passou no teste de configuração. **Aprovado** os itens estão sempre em **Encerrado-Corrigido** estado.

. **Resultado** o valor determina o estado. Ignoramos as tarefas de correção no **Encerrado-Corrigido** e. **Encerrado-Cancelado** estado. O estado do item é calculado a partir dos estados de todas as outras tarefas de correção às quais ele pertence ou está definido **Aberto** se não houver outro grupo para o item.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Criação de tarefas de correção

Conformidade de configurações As tarefas de correção são criadas manualmente.

Há duas maneiras de criar e preencher **Tarefas de correção** .

- Em **Tarefas de correção** e usando filtros que preenchem automaticamente o. **Resultados do teste** guia.

  Esta forma é boa para quando você sabe qual filtragem deseja usar. Por exemplo, capturar todos os resultados de teste com falha que são de criticidade moderada e maior, afeta a infraestrutura baseada em Windows e se aplica somente à aplicação da cadeia de suprimentos SAP.

- Selecionando resultados de teste em **Resultados do teste** e criação de uma tarefa de correção a partir do **Ações nas linhas selecionadas...** menu.

  Este método é bom para resultados que não são filtrados facilmente ou para situações em que você deseja especificar resultados de teste para correção. Por exemplo, valores atípicos que não têm nada em comum.

Nota: Se você criar uma tarefa de correção do **Resultados do teste** e, posteriormente, você decidir usar um filtro para essa tarefa de correção, suas entradas originais serão removidas e substituídas pelos resultados do filtro.

Resultados de testes não agrupados

Resultados de testes não agrupados conter todos os resultados de testes sem aprovação que não são membros de um ativo (não **Encerrado** tarefa de correção. Este módulo é atualizado após cada importação e sempre que os resultados de teste são adicionados ou removidos de uma tarefa de correção.

Itens descobertos para Conformidade de configurações

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) usando regras de pesquisa de IC quando são importados usando o host e as integrações de resultados de teste. Os itens descobertos fornecem visibilidade de como a identificação de ativos é mapeada para ICs no CMDB.

Itens descobertos são considerados **Correspondido** , **Incompatível** ou **Reclassificado** . Os ICs identificados estão no **Correspondido** estado.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para facilitar a localização de possíveis problemas correspondentes, a Regra de pesquisa de IC que correspondeu ao IC aparece em **Regra de correspondência de IC** campo.

Nota: **Regra de correspondência de IC** o suporte de campo está disponível somente para Qualys integração.

Se uma correspondência não for encontrada, um IC será criado no *IC incompatível* classe [sn_sec_cmn_unmatched_ci] , [cmdb_ci_unclassed_hardware] ou [cmdb_ci_incomplete_ip] de CMDB. Se o IC original incompatível tiver sido reclassificado, os registros do item descoberto serão atualizados para refletir esse estado. Para obter mais informações, consulte ICs incompatíveis e. Exibir e reclassificar itens de configuração incompatíveis para obter mais informações.

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

Para obter uma descrição dos campos em Itens descobertos, consulte Campos do formulário Itens descobertos .

Mudanças de IC para itens descobertos para Conformidade de configurações

O valor padrão da propriedade sn_sec_cmn.update_on_ci_change . verdadeiro . Portanto, quando o item de configuração (IC) de um item descoberto é atualizado, os resultados do teste também são atualizados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

O ID externo do resultado do teste é atualizado e a pontuação de risco, as regras de atribuição, as regras de tarefa de correção e a regra de destino de correção são reavaliadas. Se existir um resultado de teste com o mesmo teste e IC, os resultados do teste serão atualizados com o resultado de teste existente e o resultado do teste atual será encerrado com o subestado InvalidIC . As anotações de trabalho são adicionadas de acordo.

Se você não quiser atualizar o IC para o resultado de teste existente, defina a propriedade como falso. Se um IC mudar, um novo resultado de teste será criado e o existente será encerrado como um InvalidIC .

Reconciliar itens descobertos incompatíveis para Conformidade de configurações

Crie um trabalho de programação para reconciliar itens descobertos incompatíveis. Quando um resultado de teste é criado, o item de configuração (IC) adicionado a ele no momento da criação pode estar desatualizado.

Antes de Iniciar
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se as informações no CMDB mudarem, as informações de IC incompatíveis não serão reconciliadas. Para reconciliar, aplique regras de pesquisa de IC nos resultados de teste que estão em um estado incompatível quando o CMDB é atualizado com os ICs mais recentes.

Um trabalho de programação é executado sob demanda para reaplicar a regra de correspondência de IC aos itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados de testes afetados também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Nota:

Começando com Conformidade de configurações v24, você pode ignorar a reaplicação de regras de pesquisa de IC em itens descobertos com o subestado "IC desativado" habilitando a propriedade do sistema *sn_sec_cmn.skipItemsWithCIDecommissioned*.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação** .
3. No formulário, preencha os campos.

Nota: Você só pode editar o campo Parâmetros.

Trabalho em segundo plano

Campo	Descrição
Número	Número de trabalho exclusivo.
Criada por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis: ○ Número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10 000 itens descobertos serão reconciliados. ○ FirstDiscovereditem: Primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação começará a partir do primeiro item descoberto.
Estado	Estado atual do trabalho em segundo plano.
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis** .
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total necessário para concluir o trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Subestado	Subestado do estado selecionado.
Anotações	Número de registros processados.

4. Clique em **Enviar**.

Nota:

- Para parar a execução do trabalho, clique em **Cancelar** .
- Você não pode reconciliar ICs incompatíveis ou reaplicar regras de pesquisa de IC ao importar hosts ou resultados de testes.

Reaplicar regras de pesquisa de IC nos itens descobertos selecionados para Conformidade de configurações

Reaplicar regras de pesquisa de item de configuração (IC) em itens descobertos selecionados nas ações de seleção de exibição da lista de itens descobertos. O administrador pode precisar editar ou atualizar uma regra de pesquisa por vários motivos. Se a regra de pesquisa mudar, eles poderão reaplicá-las nos itens descobertos.

Antes de Iniciar

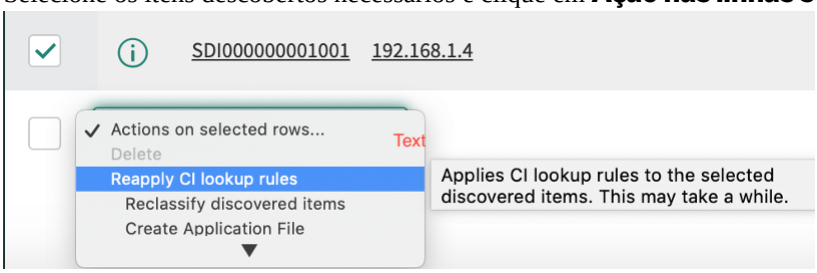
Funções necessárias:

Por Que e Quando Desempenhar Esta Tarefa

Se o IC mudar após a reaplicação das regras de pesquisa de IC, os itens descobertos serão atualizados com o novo IC e os resultados de teste. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **CMDB** > **Itens descobertos**.
2. Selecione os itens descobertos necessários e clique em **Ação nas linhas selecionadas** .



3. Selecione **Reaplicar regras de pesquisa de IC** da lista.

As regras são reaplicadas nesses itens descobertos.

Nota:

Começando com Conformidade de configurações V15.1.5, você pode ignorar a reaplicação de regras de pesquisa de IC em itens descobertos com o subestado "IC desativado" habilitando a propriedade do sistema *sn_sec_cmn.skipItemsWithCIDecommissioned*.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Integrações de vulnerabilidade da Tenable com Conformidade de configurações

. Tenable.io produto do Integrações de vulnerabilidade da Tenable importa políticas, controles (resultados de testes) e testes de configuração para processamento no Conformidade de configurações aplicação.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tenable.io

. Integrações de vulnerabilidade da Tenableé compatível.

Você pode usar dados importados para:

- Identifique vulnerabilidades relacionadas à configuração em seus ativos listados em seu Configuration Management Database (CMDB)
- Verifique se seus ativos estão em conformidade com suas políticas e controles.

Ativos, políticas, controles (resultados de testes) e testes de configuração são importados com as seguintes integrações:

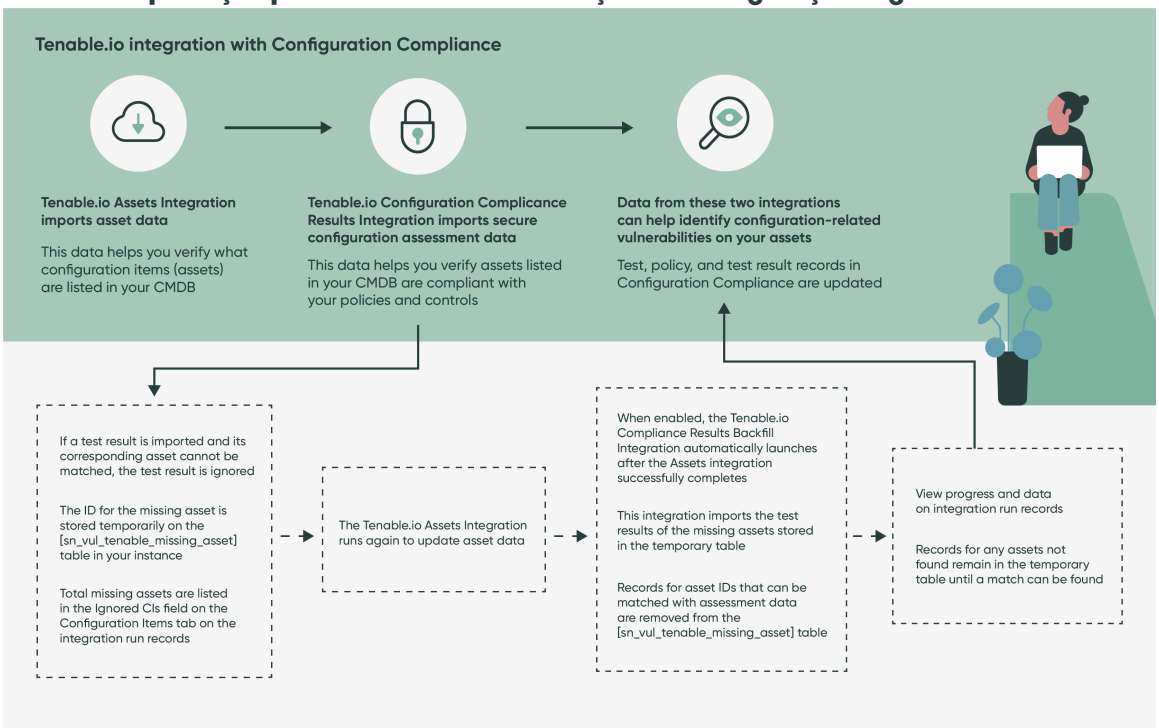
- Tenable.io Integração de ativos
- Tenable.io Integração de resultados de conformidade
- Tenable.io Integração de preenchimento de resultados de conformidade

A imagem a seguir ilustra como as integrações funcionam juntas para importar ativos e dados de avaliação de configuração e reconciliar ICs ignorados ignorados ignorados ignorados ignorados durante uma importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de importação para resultados de avaliação de configuração segura



Os dados são importados, atualizados e exibidos no resultado do teste, na política e nos registros de teste de configuração no Conformidade de configurações aplicação.

Em alguns casos, o número de itens de configuração (ICs) importados é diferente para Tenable.io Integração de ativos e Tenable.io Integração de resultados de conformidade. Quando isso ocorre, registros temporários são criados e armazenados para os IDs de ativos ignorados. Esses registros podem ser correspondidos posteriormente com dados de avaliação importados por importações da Integração de preenchimento de resultados de conformidade.

Por exemplo, digamos que a Integração de ativos importe 80 ativos em uma execução de integração, mas a Integração de resultados de conformidade importe 100.

Nota: Você pode verificar o número de ICs ignorados nas execuções de integração navegando até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**. Clique no nome de uma integração para abrir o registro. Em **Execuções de Integração de vulnerabilidades** Link relacionado, abra um registro de execução de integração e selecione **Itens** para ver o valor em **ICs ignorados** campo. Este campo rastreia o total de ativos ignorados (ausentes) da importação.

Comparando valores em **ICs ignorados** Em cada registro de execução de integração, há uma diferença de 20 ICs ignorados. Como resultado, a integração de preenchimento é executada automaticamente, conforme mostrado na imagem anterior. Esta integração importa as informações de avaliação de configuração para os 20 ativos extras encontrados pela Integração de resultados de conformidade, mas ausentes pela Integração de ativos. Como os dados de avaliação de ativos ausentes não são importados, o. Tenable.io A integração de preenchimento de resultados de conformidade importa até 200 IDs de ativo por execução de integração para reconciliar os ativos ausentes com os dados de avaliação correspondentes. Todos os registros criados para ativos ausentes ou ignorados e listados na tabela temporária são excluídos depois que esses ativos e seus dados são correspondidos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Várias execuções dessas integrações podem ser necessárias para importar todos os ativos ignorados.

Para obter mais informações sobre como habilitar e configurar o. Tenable.io Integração de ativos, consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração. Consulte Noções básicas sobre a Integração de vulnerabilidades do Tenable para obter mais informações sobre a integração.

. Tenable.io Integração de resultados de conformidade e Tenable.io A integração de preenchimento de resultados de conformidade está inativa por padrão.

Para ativá-los:

1. Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações do Tenable, clique em um nome de integração para abrir o registro e selecione **Ativo** marque a caixa para habilitá-la. Você pode preferir deixar as configurações de programação nos valores padrão para que essas integrações sejam iniciadas.

Regras de Pesquisa de IC para identificar itens de configuração a partir de integrações de vulnerabilidade de terceiros do Conformidade de configurações

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

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

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

Um novo item descoberto é criado e mapeado para este IC.

Nota: As regras de pesquisa de IC estão disponíveis somente para Qualys Integração para Operações de segurança.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações. A Qualys pode ter várias implantações da Integração Qualys. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

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

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

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

Alguns dos Qualys As regras de pesquisa de IC enviadas com o sistema de base são:

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

Algumas das regras de pesquisa de IC do Microsoft Defender fornecidas com o sistema de base são:

- Bucket S3
- Nome
- ID do recurso

Algumas das regras de pesquisa de IC do Palo Alto Prisma Cloud fornecidas com o sistema de base são:

- Bucket S3
- Nome
- ID do recurso

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicar novamente as regras de pesquisa de IC atualizadas

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

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

Se o item de configuração (IC) mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados do teste também são atualizados. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Desduplicação de itens de configuração existentes para Conformidade de configurações

O remediador de IC duplicado para tarefas de desduplicação é atualizado com `sn_sec_cmn_src_ci.cmdb_ci` propriedade.

Sempre que uma tarefa de desduplicação é usada para atualizar os itens de configuração (ICs), ela também atualiza os itens descobertos relacionados a esses ICs. Portanto, os resultados do teste são atualizados com o IC. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Criando ICs para Conformidade de configurações Usando o Mecanismo de Identificação e Reconciliação

Começando com Conformidade de configurações11,1, você pode criar itens de configuração (ICs) no Configuration Management Database (CMDB) Usando a API do Mecanismo de identificação e reconciliação (IRE). Ao usar a API IRE para criar ICs, você pode impedir que ICs duplicados sejam criados e pode reconciliar atributos de IC permitindo que somente fontes de dados autorizadas gravem em CMDB.

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

Usando IRE para criação de IC

Antes da versão 11,1, se um IC correspondente não foi encontrado na lista de itens descobertos ou CMDB Um IC foi criado na classe de IC incompatível (`sn_sec_cmn_unmatched_ci`).

Para obter mais informações, consulte ICs incompatíveis .

A partir da versão 11,1, você pode usar a API IRE para criar ICs no CMDB. Em vez de usar a classe de IC incompatível, um IC é criado na classe Hardware não classificado ou Dispositivo identificado por IP incompleto.

Classes de IC do CMDB

Nota: Para usar as novas classes, ative CMDB Plug-in Modelos de classe de IC. Caso contrário, os ICs serão criados na classe de IC incompatível.

A partir da versão 11,1, se o host importado de um scanner de terceiros não puder ser encontrado na lista de itens descobertos ou CMDB, ele é armazenado em um dos novos a seguir CMDB Classes de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classes de IC do CMDB

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

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

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

Tópicos relacionados

Aplicação da Store dos Modelos de classe de IC do CMDB

Mecanismo de Identificação e Reconciliação (IRE)

Conformidade de configurações visão geral das regras de atribuição

Defina os critérios pelos quais os resultados de teste são atribuídos automaticamente a um grupo de atribuição para correção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Uma regra de atribuição padrão, **Atribuir ao grupo de suporte de IC** está incluído no sistema de base que atribui resultados de teste ao **Grupo de suporte de IC** . Inativo por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os grupos de atribuição definidos pelas regras de atribuição são usados por **Regras da tarefa de correção** Para atribuir responsáveis a tarefas de correção (RTS).

Atribuir resultados de teste automaticamente

Há três maneiras diferentes de atribuir resultados de teste usando **Atribuir usando** :

- Grupo de atribuição: Esta opção permite selecionar qualquer um dos existentes ServiceNow AI Platform® grupos de usuários.
- Campo do grupo de atribuição: Esta opção permite que você escolha qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três seguintes campos de grupo:
  - Nenhum: Indica nenhum valor padrão para este campo obrigatório
  - Item de configuração: Grupo de aprovação
  - Item de configuração: Grupo de atribuição
  - Item de configuração: Grupo de suporte
- Script: Esta opção permite definir as condições usando um script. Esta opção requer codificação ou avançado ServiceNow® experiência.

Consulte Criar ou editar Conformidade de configurações regras de atribuição para obter mais informações sobre como criar regras de atribuição.

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar os resultados de teste e as tarefas de correção atribuídas a eles ou aos grupos de atribuição. Para exibir os módulos, navegue até **Tudo** > **Conformidade de configurações** > **Resultados de testes** > **Meus Resultados de testes em Aberto**ou **Conformidade de configurações** > **Tarefas de correção** > **Minhas tarefas em aberto**.

A função sn_vulc.remediation_owner pode ser atribuída diretamente a um usuário ou é atribuída automaticamente quando você atribui a um usuário a função itil.

Processo de avaliação da regra de atribuição

Quando um novo resultado de teste é importado ou reaberto após ser encerrado, as regras de atribuição são avaliadas em relação a ele. As regras de atribuição são avaliadas após a correspondência de IC e os cálculos de pontuação de risco. Um resultado de teste só é avaliado automaticamente após a importação inicial e quando uma regra é alterada, a menos que seja reaberto após ser encerrado. Você pode reaplicar regras manualmente após as mudanças.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de atribuição de resultado de teste, o resultado do teste é comparado com o filtro de atribuição, regra de ordem mais baixa primeiro.
- Quando a condição corresponde, o resultado do teste é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Quando as condições não encontram uma correspondência entre todas as regras, o resultado do teste permanece sem atribuição.

Reaplicar regras de atribuição

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

O trabalho agendado [*Reapply all assignment rules*] está inativo, por padrão. Quando ativado, ele avalia todos os resultados de testes em aberto em relação a todas as regras ativas, exceto as atribuídas manualmente. Pode ser executado diariamente, semanalmente, mensalmente, periodicamente, uma vez ou sob demanda.

Importante: Como administrador e analista, você pode obter as atribuições mais recentes para os resultados de testes selecionados no Espaço do gerente de vulnerabilidade. Este método é mais eficiente do que reaplicar as Regras de atribuição para todos os resultados de teste no clássico IU, que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Atribuição de regras de atribuição e atribuição de tarefa de correção

Normalmente, você atribuiria sua tarefa de correção (RT) ao mesmo grupo de atribuição que os resultados de teste nela. É isso que as regras de tarefa de correção fazem, por padrão.

Por exemplo, se seus grupos de RT por classe de item de configuração, a tarefa de correção criada poderá ser dividida pelos diferentes grupos de atribuição. Um TRG do Oracle Database pode ser atribuído ao Grupo 1 e um TRG do Oracle Database atribuído ao Grupo 2.

Quando o grupo de atribuição é alterado no nível da tarefa de correção, todos os resultados de teste nessa tarefa de correção que têm o mesmo grupo de atribuição são atualizados para o novo grupo de atribuição. Os resultados do teste são marcados como atribuídos manualmente e não estão qualificados para avaliação de regra adicional.

Removendo atribuições de Conformidade de configurações tarefas de correção

Você pode limpar **Atribuído a.** e. **Grupo de atribuição** campos em tarefas de correção e seus resultados de teste associados diretamente dos registros de resultado de teste e tarefas de correção que você determina que podem estar atribuídos incorretamente a você ou aos seus grupos.

Visão geral do fluxo de trabalho

Os responsáveis pela correção podem atualizar registros para reatribuição com **Cancelar atribuição** botão.

Caso de uso para sn_vulc.remediation_owner

Se você determinar que os RTS e os resultados de testes associados não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, poderá remover a si mesmo ou aos seus grupos do **Atribuído a.** e. **Grupo de atribuição** campos nesses registros de tarefa de correção.

Cancelar atribuição do módulo

. **Cancelar atribuição** O botão é exibido nos registros de tarefa de correção e de resultado de teste em qualquer estado diferente dos estados Encerrado ou Resolvido.

Se você selecionar **Cancelar atribuição** , você será solicitado que todos os resultados de teste associados à tarefa de correção sejam reatribuídos e façam a transição para **Não atribuído** tipo de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se algum resultado de teste em uma tarefa de correção tiver um grupo de atribuição diferente da tarefa de correção, ele não terá atribuição cancelada. Na maioria dos casos, esses resultados de teste foram atribuídos manualmente.

Todos os registros que você atualizar com o botão de IU ou manualmente serão exibidos no módulo Não atribuído em Conformidade de configurações.

Para as etapas para reatribuir registros usando *Unassigned*Ação de IU, consulte Remova atribuições de tarefas de correção para você ou seus grupos.

Propriedades do sistema e notificações

Se você for um administrador com a função sn_vulc.vulnerability_admin, ao selecionar **Cancelar atribuição** em um registro, por padrão, a propriedade do sistema, *sn_vulc.unassign_test_result_group.approval_required*Aciona o registro Aprovação de mudança de estado e o registro Aprovação solicitada. Além disso, a solicitação é exibida na lista Minhas aprovações do aprovador.

Nota: Como administrador de vulnerabilidades, você pode definir *sn_vulc.unassign_test_result_group.approval_required*propriedade do sistema para **falso** para desabilitar o processo de aprovação.

- Se o aprovador aprovar sua solicitação, por padrão, a propriedade do sistema, *sn_vulc.default_assignment_group*Limpa os campos Atribuído a e Grupo de atribuição e preenche o campo Tipo de atribuição com **Não atribuído** . Como administrador de vulnerabilidades, você pode alterar o valor em *sn_vulc.default_assignment_group*propriedade do sistema para que os campos de atribuição sejam limpos e um grupo específico seja atribuído. Por exemplo, se um usuário selecionar **Cancelar atribuição** Em um registro e você deseja redirecioná-lo para um grupo específico para revisão, você pode adicionar um ID do sistema para o grupo de sua escolha no campo Valor da propriedade do sistema.
- Se o aprovador rejeitar sua solicitação, o motivo da rejeição será exibido no **Anotações** guia.

Se *sn_vulc.default_assignment_group*Não está configurado para um grupo específico. Por padrão, os usuários que você adiciona ao grupo de usuários de notificação Cancelar atribuição são alertados quando os registros não são atribuídos. A propriedade do sistema, *sn_vulc.default_notification_group*determina as notificações para este grupo.

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

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

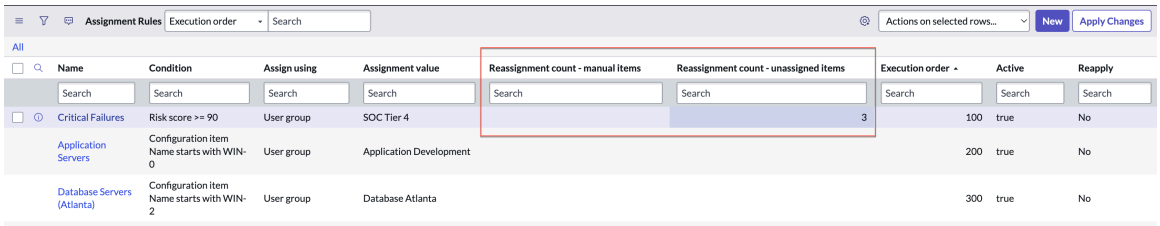
Um trabalho agendado diariamente conta os registros quando eles fazem a transição para **Não atribuído** tipo de atribuição. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar quaisquer regras de atribuição que possam não estar tendo um bom desempenho com base em regras de atribuição que tenham contagens mais altas de RTS não atribuídos.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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



1. Como administrador de vulnerabilidades, você pode exibir essas contagens navegando até **Conformidade de configurações** > **Administração** > **Regras de atribuição**.
2. Selecione o ícone de engrenagem no canto superior direito da lista e selecione **Contagem de reatribuições - itens manuais** e **Contagem de reatribuições - Itens não atribuídos** para exibição.
3. Qualquer RT que foi originalmente atribuído por uma regra, mas posteriormente foi reatribuído automaticamente ou manualmente, contém uma referência à regra original na exibição de lista.

Conformidade de configurações tarefas de correção e visão geral das regras de tarefa de correção

Crie tarefas de correção (RTS) automaticamente para analisar os resultados em massa usando regras de tarefa de correção. Os critérios pelos quais as tarefas são formadas são configurados para que você não precise atribuir manualmente os resultados de teste às tarefas de correção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Noções básicas sobre tarefas de correção

As tarefas de correção representam um conjunto de resultados de teste a serem corrigidos. Agrupar resultados de testes tem muitas vantagens. Você pode mover resultados de teste pelos estados de correção, marcá-los como sob investigação, adiá-los e marcá-los como resolvidos em massa usando grupos. Você pode criar condições para agrupar automaticamente todos os resultados com resultados especificados, tecnologias, pontuações de risco e quaisquer outros dados relacionados aos resultados do teste. Os resultados do teste podem pertencer a mais de uma tarefa de correção, dando a você a flexibilidade de trabalhar ativamente com uma tarefa de correção e monitorar outra. Tudo depende das suas necessidades organizacionais. Por exemplo, você pode agrupar por atribuição e também criar um grupo que contenha tecnologias.

As tarefas de correção são criadas da seguinte forma.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Manualmente, usando uma das duas opções, para adicionar resultados de teste ao grupo.
  - **Manual** cria uma tarefa de correção sem entradas. Os resultados do teste devem ser adicionados manualmente.
  - **Filtro** cria uma tarefa de correção e usa condições para adicionar automaticamente resultados de teste a essa tarefa de correção.

Nota: Os resultados de testes adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições de tarefa de correção.

- Usando regras de tarefa de correção. Esta opção é a opção mais fácil: Depois de configuradas, as regras de tarefa de correção criam todas as tarefas de correção desejadas.

A partir de uma tarefa de correção, o grupo de resultados de teste pode ser atribuído a um usuário, adiado para mais tarde, usado para criar um **Solicitação de mudança** e assim por diante.

Nota:

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar os resultados de teste e as tarefas de correção atribuídas a você ou aos seus grupos de atribuição. Para exibir os módulos, navegue até **Tudo** > **Conformidade de configurações** > **Resultados de testes** > **Meus Resultados de testes em Aberto**ou **Conformidade de configurações** > **Tarefas de correção** > **Minhas tarefas em aberto**.

Quando é determinado que um novo resultado de teste pode ser adicionado a uma tarefa de correção, o resultado do teste é incluído em **Resultados do teste** lista relacionada da tarefa de correção.

Ao atualizar o estado de uma tarefa de correção, os resultados de teste associados podem ter seu estado atualizado para corresponder a esta tarefa de correção. Para obter mais informações sobre mudanças de estado, consulte Conformidade de configurações estados.

Noções básicas sobre as regras de tarefa de correção

As regras de tarefa de correção permitem definir como os resultados de teste são agrupados e atribuídos automaticamente. Uma regra padrão, **Grupo de atribuição, Teste** está incluído no sistema de base agrupando resultados de teste com base em um resultado de teste **Grupo de atribuição** e o. **Teste** campo. Esta regra está desabilitada, por padrão. Você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis a partir do resultado do teste. Você pode usar até seis chaves e qualquer número de condições. Para obter mais informações, consulte Criar ou editar Conformidade de configurações regras de tarefa de correção.

Importante: Como administrador e analista, você pode avaliar as regras da tarefa de correção para resultados de teste selecionados no Espaço do gerenciador de vulnerabilidades. Este método é mais eficiente do que reaplicar as regras da tarefa de correção na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Por exemplo, você pode agrupar os resultados do teste por grupo de atribuição ou tecnologia e item de configuração (IC). Um conjunto diferente de regras pode ser usado para resultados de testes que expõem a empresa a mais riscos. Você pode ter uma regra de tarefa de correção para ICs de baixa gravidade ou baixo risco. Consulte Exibir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações resultados do teste para obter mais informações sobre os campos disponíveis.

Quando um novo resultado de teste é importado ou reaberto após ser encerrado, as regras da tarefa de correção são avaliadas em relação a ele. Um resultado de teste só é avaliado uma vez, a menos que seja reaberto após ser encerrado.

As regras da tarefa de correção são avaliadas após a correspondência de IC, os cálculos de pontuação de risco e as regras de atribuição.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de tarefa de correção, o resultado do teste é comparado com o filtro de condição.
- Para cada regra em que a condição da regra corresponde, ele extrai os dados das colunas de chave do grupo no resultado do teste. A regra verifica se há uma correspondência **Aberto** tarefa de correção atribuída ao mesmo grupo de atribuição que o resultado do teste.

  Se a tarefa de correção for encontrada, o resultado do teste será adicionado à tarefa de correção existente no **Aberto** estado.

- Se não houver tarefa de correção no **Aberto** encontrado, a regra cria uma tarefa de correção e a atribui com base em **Grupo de usuários** ou **Chave** valor na regra e coloca o resultado do teste nela.

Mais de uma regra de resultado de teste pode ser definida para agrupar diferentes tipos de resultados. Como cada resultado é comparado com as condições da regra antes de colocá-lo em uma tarefa de correção, muitas regras podem afetar o desempenho.

Quando uma regra de tarefa de correção é excluída, você tem a opção de excluir todas as tarefas em aberto criadas pela regra. Isso se aplica à exibição do formulário de regra e à exibição de lista.

Quando uma atribuição de tarefa de correção é feita ou alterada, o. **Grupo de atribuição** e o. **Atribuído a.** Os campos são rolados para todos os resultados de teste, exceto aqueles em que o resultado do teste tem um grupo de atribuição diferente do RT. Para obter mais informações sobre regras de atribuição, consulte Conformidade de configurações visão geral das regras de atribuição. Essas atribuições são usadas automaticamente para este grupo na próxima importação.

Rastreie contagens de adiamentos para resultados de testes e tarefas de correção

A partir da v14.3, rastreie o número de vezes que um resultado de teste ou uma tarefa de correção é adiado no módulo de vários adiamentos. Um trabalho agendado, **definir contagens de adiamentos** É executado diariamente para contabilizar contagens de registros que são adiados mais de uma vez na coluna Contagem de adiamentos nos registros listados no módulo Vários adiamentos.

Configurar grupos de calculadoras e calculadoras para Conformidade de configurações

Calculadoras de conformidade de configuração são usadas para atualizar valores de registro quando as condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Calculadoras de conformidade de configuração

A aplicação Conformidade de configuração inclui dois tipos de calculadoras, Calculadoras de risco e Calculadoras de acúmulo de pontuação de risco. Esses grupos de calculadora são habilitados por padrão.

O grupo de calculadoras de Pontuação de risco foi renomeado para Calculadoras de risco.

As Calculadoras de acúmulo de pontuação de risco incluem calculadoras de acúmulo para testes de configuração e tarefas de correção.

Configurar calculadoras de risco e acúmulo para correção de resultados de teste e tarefas de correção inclui as seguintes tarefas:

- Crie uma calculadora de risco
- Crie uma calculadora de acúmulo de pontuação de risco

Depois de criar uma calculadora de risco, ela ficará disponível para cálculos com a próxima ingestão de dados. Depois de criá-lo, você também pode preferir aplicá-lo sob demanda.

Para obter mais informações sobre calculadoras e grupos de calculadoras, consulte Conformidade de configurações grupos de calculadoras.

Conformidade de configurações Visão geral da Gestão de exceções

Quando sua organização não pode cumprir um gerenciamento de vulnerabilidades publicado ou política de segurança, padrão ou diretriz, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções para uma tarefa de correção que não pode ser corrigida de acordo com a política.

Importante: A gestão de exceções é compatível com Vulnerability Manager Workspace e. Espaço de correção de TI .

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

reconhece e concorda com as consequências de não corrigir a vulnerabilidade relacionada à configuração.

Ciclo de vida de uma exceção

Uma exceção é uma solicitação para adiar a correção de uma tarefa de correção por um período especificado.

O ciclo de vida de uma exceção é o seguinte:

- Solicitando uma exceção
- Aprovando uma solicitação de exceção
- Acompanhamento de uma solicitação de exceção
- Expiração de uma solicitação de exceção

Solicitando uma exceção

Como responsável pela correção, você pode solicitar uma isenção para uma tarefa de correção usando o processo de gestão de exceções. Durante o processo de aprovação, a tarefa de correção permanece em **Em revisão** estado. Depois que o aprovador de exceção aprova esta solicitação, a tarefa de correção é movida para um **Adiado** estado.

Importante: Você pode solicitar uma exceção do Espaço de correção de TI. Para obter mais informações, consulte Solicite uma exceção no Espaço de correção de problemas de TI.

Aprovando uma solicitação de exceção

As tarefas de correção que não podem ser corrigidas imediatamente são revisadas, avaliadas quanto a riscos e aprovadas para adiamento até que possam ser corrigidas. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicione um aprovador de exceção para Conformidade de configurações.

Importante: Você pode aprovar ou rejeitar uma solicitação de exceção do Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade.

Nota:

A partir de Conformidade de configurações V13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho.

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

- Reabrir
- Excluir

Nota: Os comentários de rejeição são mostrados nas anotações de trabalho de uma tarefa de correção. Se uma solicitação de exceção for rejeitada, esta tarefa de correção será revertida para o estado anterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

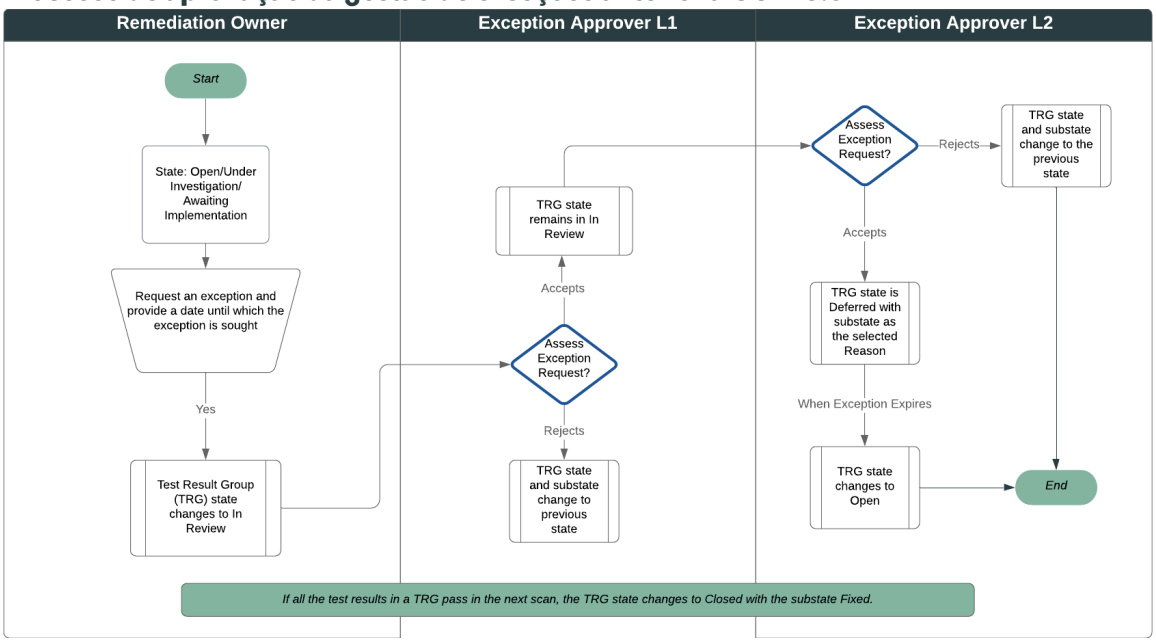
Acompanhamento de uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando **Aprovações de mudança de estado** tarefa de correção. Se uma ação for realizada em uma tarefa de correção, você não poderá rastrear o status dos resultados de teste individuais nessa tarefa de correção.

Expiração de uma solicitação de exceção

Quando uma solicitação de exceção para uma tarefa de correção expira, a tarefa de correção é revertida para sua **Aberto** estado.

Processo de aprovação da gestão de exceções anterior à CC v13.0



Conformidade de configurações gestão de mudanças

Como responsável pela correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente das tarefas de correção (RTS) no Conformidade de configurações aplicação.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Solicitações de mudança e Conformidade de configurações fluxo de trabalho

As solicitações de mudança e a gestão de mudanças fazem parte do processo de correção do Conformidade de configurações fluxo de trabalho. Durante esta fase de correção, você pode usar solicitações de mudança para ajudar a priorizar, rastrear e corrigir os resultados de testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Conformidade de configurações a aplicação funciona com ServiceNow AI Platform® Processo de gestão de mudanças de TI para ajudá-lo a corrigir software e tecnologias fora de conformidade em seu ambiente.

Com gestão de mudanças no Conformidade de configurações, você pode associar resultados de teste a solicitações de mudança existentes ou dividir uma tarefa de correção e criar uma nova tarefa de correção somente para resultados de teste selecionados.

Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações.

Termos principais

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser governada. Um teste é qualquer coisa que pode ser usada para identificar uma classe de software ou um ativo de hardware que está fora de conformidade.

Resultados de testes

Os resultados do teste são importados por integrações de terceiros. Quando eles estiverem visíveis em Conformidade de configurações, eles são corrigidos usando **Tarefas de correção** . Os grupos são atribuídos para correção de acordo com as regras de atribuição.

Nota: A partir da versão 14,9 de Conformidade de configurações o resultado do teste é rotulado, *Descoberta* .

Tarefa de correção

Os resultados do teste são agrupados em tarefas de correção de acordo com as regras de atribuição e atribuídos automaticamente aos responsáveis pela correção.

Nota: A partir da versão 14,9 de Conformidade de configurações o resultado do teste é rotulado *Tarefa de correção* .

Grupos de teste

Os grupos de teste estão relacionados a documentos autorizados e registros de teste. Um grupo de testes de configuração define grupos de teste.

Solicitações de mudança

As solicitações de mudança ajudam a implementar processos controlados para correção. Você pode usar solicitações de mudança com tarefas de correção em Conformidade de configurações para ajudar você a identificar, rastrear e resolver ativos fora de conformidade (itens de configuração) que exigem recursos adicionais ou que você pode direcionar para adiamento.

Para obter mais informações sobre resultados de testes e tarefas de correção, consulte Conformidade de configurações tarefas de correção e visão geral das regras de tarefa de correção.

Quando usar solicitações de mudança em Conformidade de configurações

As solicitações de mudança ajudam a iniciar e rastrear atividades de correção nos resultados de testes. Quando os responsáveis pela correção têm um grande número de resultados de teste não corrigidos ou itens de configuração, eles podem usar solicitações de mudança para identificar resultados de teste para adiamento. Como alternativa, eles podem identificar e reagrupar resultados de teste e itens de configuração que exigem mais recursos do que os inicialmente identificados na tarefa de correção original.

Crie solicitações de mudança a partir de uma tarefa de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma solicitação de mudança diretamente de uma tarefa de correção para todos os resultados de teste na tarefa de correção ou use a filtragem para identificar somente resultados de teste que correspondam a critérios específicos. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de resultados de teste que exigem intervenção manual.

Divida uma tarefa de correção

Em uma tarefa de correção existente, identifique um subconjunto de resultados de teste que você deseja mover para uma nova tarefa de correção. Ao criar um novo TRG, você pode trabalhar com um grupo específico de resultados de teste sem afetar a tarefa de correção original.

Associe resultados de teste a uma solicitação de mudança existente

Associe resultados de teste a tarefas existentes para evitar a criação de solicitações de mudança duplicadas enquanto trabalha para resolver suas tarefas de correção. Ao associar uma tarefa de correção a uma solicitação de mudança que já está disponível em sua instância, você pode usar listas de tarefas existentes.

Tipos de solicitações de mudança para uma tarefa de correção

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente das tarefas de correção atribuídas a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente a partir de uma tarefa de correção:

- Padrão. Uma mudança pré-autorizada que é de baixo risco, relativamente comum e segue um procedimento especificado ou instrução de trabalho.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.
- Emergência. Uma mudança para resolver um incidente grave.

Instalação e configuração do Conformidade de configurações aplicação

Antes de executar a aplicação em seu ServiceNow AI Platform® primeiro, você deve baixar e instalar o. Conformidade de configurações aplicação do ServiceNow® Store. Esta aplicação está disponível como uma assinatura separada.

Conclua as etapas da check-list de configuração a seguir listadas na tabela a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Para obter mais informações sobre as versões lançadas do Conformidade de configurações, bem como de terceiros e ServiceNow aplicações compatíveis com ele, consulte Matriz de compatibilidade de resposta a vulnerabilidades e mudanças no esquema de versão [KB0856498] artigo na Base de conhecimento HI.

Para obter mais informações sobre como obter direitos para apps da Store, consulte Operações de segurança e o ServiceNow Store.

Tarefas de check-list de configuração

Tarefas de configuração	Descrição
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de check-list de configuração

Tarefas de configuração	Descrição
	• Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá a função Administrador de conformidade de configuração [sn_vulc.admin]. • O administrador de conformidade de configuração [sn_vulc.admin] supervisiona a configuração e verifica os resultados esperados. • O responsável pela correção [sn_vulc.remediation_owner] lê e atualiza os registros atribuídos. A função sn_vulc.remediation_owner também é atribuída automaticamente quando qualquer usuário recebe a função itil.
Integrações compatíveis	Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede. Verifique se o Resposta a vulnerabilidades a aplicação é instalada e ativada antes de configurar integrações de terceiros compatíveis. Consulte Instalar Resposta a vulnerabilidades. Para verificar se as aplicações de integração estão instaladas e ativadas, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre integrações de terceiros e uma lista de produtos compatíveis, consulte Integrações do Conformidade de configurações.

Qualys Vulnerability Integration

- . Qualys Vulnerability Integration Já está instalado em seu sistema e suas credenciais de API são diferentes das que você deseja usar para Conformidade de configurações, Vá para Assistente de configuração (em Resposta a vulnerabilidades) e atribua-os a cada um **Qualys PC** integração.
- Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o. **Credenciais de API da Qualys** campo em **Detalhes REST da Qualys** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter informações mais detalhadas sobre Qualys Vulnerability Integration, consulte Noções básicas do Qualys Vulnerability Integration.

Agora você está pronto para instalar o. Conformidade de configurações aplicação. Consulte Instalar Conformidade de configurações.

Instalar Conformidade de configurações

Antes de executar Conformidade de configurações em seu ServiceNow AI Platform® primeiro, você deve baixar e instalar o. Conformidade de configurações aplicação do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Preencha a check-list de configuração descrita em Instalação e configuração do Conformidade de configurações aplicação antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Função necessária: administrador

Procedimento

1. Para aceitar ServiceNow produtos, siga as etapas em Aceite . ServiceNow Store produtos .
2. Para instalar uma aplicação que você comprou do ServiceNow Store, siga as etapas em Instale um ServiceNow Store aplicação .
3. **Opcional:** Se você quiser gerenciar seu direito para Conformidade de configurações aplicação em outro ServiceNow AI Platform, siga as etapas em Gerencie direitos do seu ServiceNow instância .
4. Se você já instalou o. Conformidade de configurações e você está atualizando, consulte Instale uma atualização em um ServiceNow Store aplicação .
5. Instale aplicações compatíveis.

   Aplicações de terceiros separadas adquirem e transformam dados no Conformidade de configurações. Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

   Para obter informações sobre como instalar integrações de terceiros para Conformidade de configurações, consulte Integrações do Conformidade de configurações.

Criar ou editar Conformidade de configurações regras de atribuição

Crie regras para atribuir automaticamente resultados de teste com base nas condições de filtro. Essas regras atribuem resultados de teste à medida que são importados.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O sistema de base é fornecido com um Conformidade de configurações regra de atribuição, **Atribuir ao grupo de suporte de IC** , Que atribui resultados de teste ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra está inativa por padrão. Você pode modificar usando condições de filtro. Com as regras de atribuição, você define uma ou mais condições de atribuição e a ordem de execução. Quando um resultado de teste corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Nota: Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o. **Aplicar mudanças** Botão na lista Regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de atribuição**.
2. Abra o. **Atribuir ao grupo de suporte de IC** ou clique **Novo** .
3. Edite o. **Atribuir ao grupo de suporte de IC** ou se **Novo** preencha os campos no formulário, conforme apropriado.

Regra de atribuição de conformidade de configuração

Campo	Descrição
Nome	Nome da regra de atribuição.
Ordem de execução	Ordem na qual as regras são avaliadas. O menor número é avaliado primeiro. Regras de alta prioridade, resultados de testes que precisam de tratamento especial, em que o risco é crítico ou um resultado de teste que deve ser tratado pela conformidade regulatória, devem ser executados primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário e você sabe quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir resultados de teste ao grupo que descobre a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Ativo	Indica se a regra de atribuição está ativa.
Condição	
Campos de condição	Condições que devem ser atendidas. A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Descrição	Texto que descreve a regra de atribuição.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: Selecione um grupo de usuários na tabela de pesquisa ◦ Campo de grupo de usuários: Selecione um campo de grupo de usuários no menu suspenso. ◦ Script: Crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow experiência.
Campo de grupo de usuários	Selecione o grupo de usuários responsável pela correção de testes que correspondem às condições das regras de atribuição.

4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações regras de destino de correção

Com as regras de destino de correção, você pode definir os intervalos de tempo esperados para corrigir os resultados do teste. Você pode enviar notificações para usuários e grupos quando as datas de destino estiverem se aproximando e quando estiverem vencidas.

Importante: Como administrador ou analista de Conformidade de configuração, você pode obter a data de destino de correção mais recente para um conjunto específico de resultados de teste no Espaço do Gerenciador de vulnerabilidades. Este método é mais eficiente do que executar as Regras de destino de correção para todos os resultados de teste na IU clássica, o que é um processo demorado. Para obter mais informações, consulte Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade.

Funções necessárias: Administrador de conformidade de configuração (sn_vulc_admin) ou um gerente com a função sn_vulc.manage_remediation_target_rules.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Regras de meta da correção

Um trabalho agendado, *`Evaluate and notify remediation targets`*é executado diariamente e usa regras de destino de correção ativas para avaliar registros de resultado de teste ativos. Sempre que os registros de resultado de teste associados a tarefas de correção são atualizados ou alterados, os valores modificados são avaliados pelas regras de destino e as mudanças são acumuladas e exibidas nas tarefas de correção associadas.

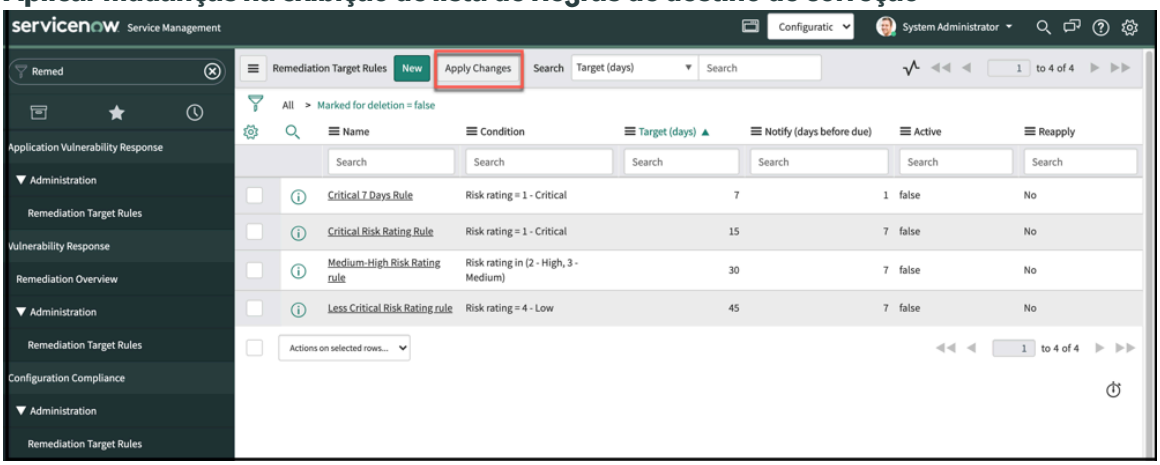
Você pode editar, desabilitar ou excluir regras de destino de correção existentes e criar novas. Ao mudar, desabilitar ou criar uma nova regra, você tem a opção de clicar **Aplicar mudanças** Na exibição de lista Regras de destino de correção e aplique manualmente as mudanças introduzidas antes do próximo trabalho agendado. Com esta opção, você pode reavaliar seus registros de resultado de teste sem precisar esperar. Se você optar por não aplicar suas mudanças manualmente, o próximo trabalho agendado diariamente selecionará suas mudanças e as aplicará.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de meta da correção** para exibir regras de destino de correção.

Aplicar mudanças na exibição de lista de Regras de destino de correção



2. Clique em uma regra na coluna Nome para abrir seu registro.
3. Selecione **Ativo** Caixa de seleção no registro de Regra de destino de correção para habilitar (verdadeiro quaisquer regras desabilitadas (falso).

Sempre que você muda ou adiciona uma regra de destino, independentemente de optar por aplicar as mudanças manualmente ou aguardar o próximo trabalho agendado, suas mudanças são usadas para avaliar todos os resultados de teste ativos junto com outras regras de destino afetadas por suas mudanças. Quando você opta por aplicar manualmente as mudanças, esta avaliação pode levar algum tempo se você tiver um grande volume de resultados de testes ativos, porque todas as regras afetadas por suas mudanças são usadas para uma avaliação.

Por exemplo, o valor padrão para dias de correção de destino é 30. Se você criar uma nova regra que também tenha 30 para dias de correção de destino, esta regra e todas as regras de destino com 30 dias ou mais como datas de destino serão aplicadas aos resultados do teste.

Regras de destino desativadas e excluídas

Quando uma regra está ativa, verdadeiro É exibido na coluna Ativo na exibição de lista Regras de destino de correção. Depois que uma regra é desativada (falso), ele não é mais aplicado a novos resultados de testes. No entanto, o trabalho agendado continua rastreando todos os resultados de teste existentes aos quais a regra foi aplicada. Se a regra ou regras desativadas forem reativadas posteriormente, qualquer resultado de teste com um vazio **Data de destino de correção** o campo é avaliado em relação às regras reativadas. Isso inclui resultados de testes criados enquanto as regras foram desativadas.

Quando as regras são excluídas, o **Data de destino de correção** e os campos relacionados nos resultados de testes encerrados são preservados. . **Data de destino de correção** e os campos relacionados em resultados de testes não encerrados são limpos e todas as regras dependentes são reaplicadas.

Para desativar uma regra, no registro de regra de destino de correção, desabilite a caixa de seleção ativa e clique em **Atualização** . Falso É exibido na coluna Ativo na exibição de lista Regras de destino de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para excluir uma regra, clique em **Excluir** no formulário ou, como alternativa, na exibição de lista, selecione a regra ou regras e clique em **Excluir** em **Ações em linhas** lista. A regra não é mais exibida na lista e a próxima regra na ordem de operação substitui a regra excluída.

Se você desativar ou excluir uma regra e optar por aplicar suas mudanças antes do próximo trabalho agendado, a referência da regra será limpa do campo, mas os dados de data de correção e status serão preservados. Se você não aplicar suas mudanças manualmente, a referência de regra será limpa do campo com o próximo trabalho agendado.

Sobre as regras de destino e o trabalho agendado Avaliar e notificar metas de correção

. *`Evaluate and notify remediation targets`*o trabalho agendado é executado uma vez às 4:30:00 diariamente. Ele seleciona todas as regras de destino de correção ativas e avalia todos os resultados de teste ativos, começando com os resultados de teste com a data de destino de correção mais antiga. Ele avalia todos os resultados de testes que atendem aos seguintes critérios:

- Não estão em um **Encerrado** estado.
- Não tem data de destino de correção.
- Tenha datas de destino de correção posteriores às datas nas regras de destino de correção.
- São criados após a conclusão da importação de um scanner. O trabalho agendado seleciona e avalia todos os novos resultados de teste criados como resultado de uma importação.

Depois que uma regra de destino é definida, as datas de destino de correção são calculadas pelo *`Evaluate and notify remediation targets`*trabalho agendado. O trabalho agendado adiciona uma data de destino de correção, se não existir, ou, se esta regra contiver uma data anterior à data no registro, atualiza a data de destino existente.

Todos os registros expirados e datas de lembrete que correspondam às regras de destino são selecionados pelo trabalho e as notificações são enviadas. Para regras desabilitadas, o trabalho limpa os campos de correção nos registros de resultado de teste e interrompe o envio de notificações.

A propriedade sn_sec_cmn.evaluate_targetmissed_records, quando habilitada, impede o. *`Evaluate and notify remediation targets`*Trabalho agendado de Avaliação de resultados de teste perdidos de destino. Esta propriedade está habilitada por padrão.

Exibição de datas de destino e status nas exibições de lista e formulário

Conformidade de configurações os gerentes podem ver a data de destino de correção no formulário de resultado de teste e nas exibições de lista. As regras de destino de correção também são executadas após a importação de um scanner e executadas novamente se um resultado de teste for reaberto.

O trabalho agendado atualiza o. **Destino de correção** e. **Status de correção** na exibição da lista de resultados de teste, e **Regra de destino de correção** , **Destino de correção** e **Status de correção** campos no formulário de resultado de teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

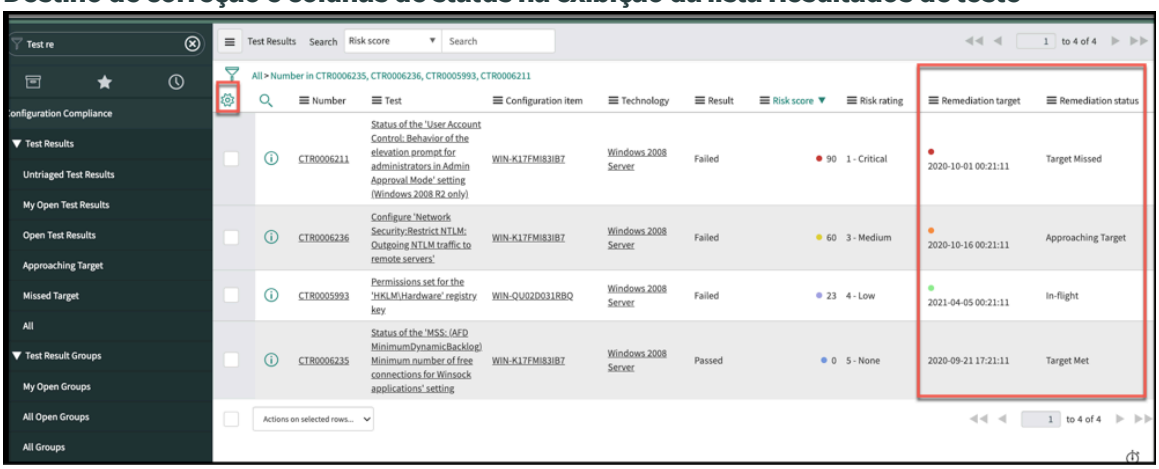
Nota: Por padrão, o **Destino de correção** e. **Status de correção** As colunas não são exibidas na exibição da lista Resultados do teste. Para exibir essas colunas, você também deve adicioná-las à exibição de lista. Da mesma forma, adicione **Regra de destino de correção** , **Destino de correção** e **Status de correção** campos para o formulário de resultado do teste.

Use os slushbuckets nos menus Configurações e Ação adicional, respectivamente, conforme mostrado nas imagens a seguir para exibir essas colunas e campos. Para acessar o menu Ação adicional no registro de resultado de teste, clique no ícone de menu, seguido por **Configurar** e. **Layout do formulário** para exibir o slushbucket e mover os campos de **Disponível** . **Selecionado** .

A data de destino de correção é codificada na exibição da lista Resultados de testes como pontos coloridos:

- Os resultados de testes que não atingiram a data de notificação são mostrados em verde.
- Os resultados de testes que se aproximam da data de destino de correção são mostrados em laranja.
- Os resultados de testes após a data de destino de correção são mostrados em vermelho.

Destino de correção e colunas de status na exibição da lista Resultados de teste

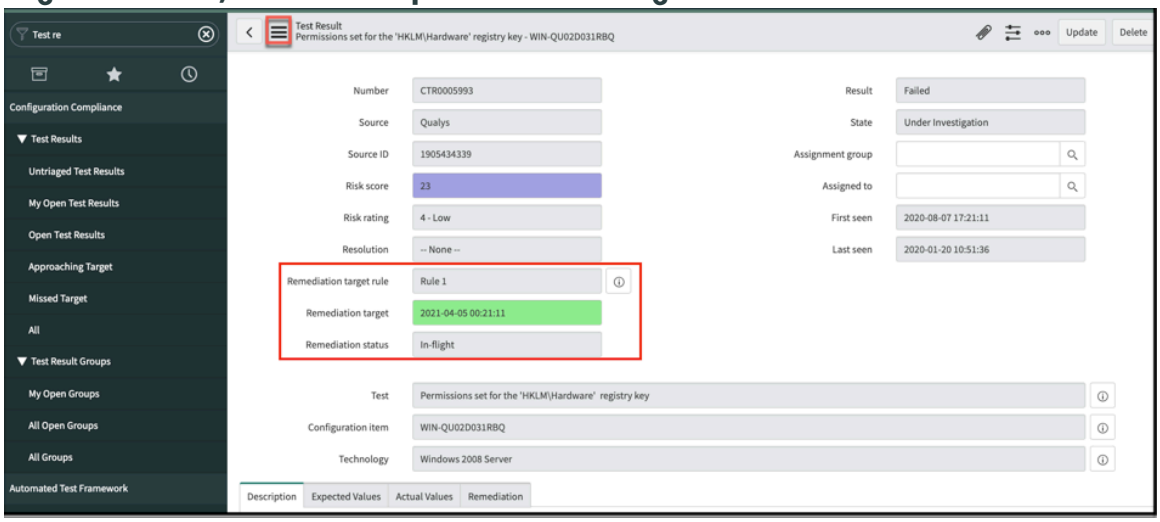


- Meta perdida : a data de destino está atrasada
- Em voo : o resultado do teste está em andamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de destino, destino e campos de status no registro de resultado do teste



Os registros do resultado do teste também são exibidos visualmente no Conformidade de configurações Painel. Navegar até **Tudo** > **Conformidade de configurações** > **Visão geral** e verifique o status do painel. A Visão geral inclui widgets existentes e status de correção. As cores dos gráficos correspondem às cores exibidas na exibição de lista Resultados de teste e no registro de Resultado de teste.

Cenário de regra de destino de correção

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

Por exemplo, se um resultado de teste identificado pela primeira vez em 03/01/2018 atender às condições para duas regras de destino de correção:

- Regra de destino de correção 1: Definida em 07/03/2018; a meta de correção é de 15 dias desde a primeira exibição; a data de meta de correção calculada é 03/16/2018 10:00:00.
- Regra de destino de correção 2: Definida em 10/03/2018; a meta de correção é de 10 dias desde a primeira exibição; a data de meta de correção calculada é 03/11/2018 10:00:00.

Nota:

As metas de correção são calculadas a partir de **Visto pela última vez** data mais o número de dias (medido como incrementos de 24 horas).

A partir da V14.5, os destinos de correção são calculados a partir do **Destino de (data)** . O valor padrão permanece **Último Visto** . A partir da v14.12, o valor padrão é **Última passagem** .

Nesse cenário, a regra de destino de correção 2 se aplica ao resultado do teste, porque ele tem a data mais restritiva: 10 dias desde que o resultado do teste foi identificado pela primeira vez versus 15 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie ou modifique regras de destino e reaplique as mudanças

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de meta da correção** para exibir, editar e criar novas regras de destino de correção.
2. Na coluna Nome, clique em uma regra para abrir uma regra de destino e editar o registro ou, como alternativa, clique em **Novo** para criar uma nova regra de destino.
3. Preencha o formulário para definir o intervalo de tempo de correção esperado, especifique a quais resultados de teste esta regra se aplica com condições e determine quando enviar lembretes para usuários, grupos ou ambos.

Formulário Regra de destino de correção

Campo	Descrição
Nome	Nome da regra.
Ativo	Habilite ou desabilite a regra. A regra é habilitada automaticamente (verdadeira) por padrão e será aplicada aos resultados do teste se você optar por aplicar as mudanças manualmente ou após o próximo trabalho agendado.
Meta (dias)	Defina a data do prazo de destino para correção em número de dias. O valor padrão para dias de correção de destino é 30. Por exemplo, se você criar uma nova regra que também tenha 30 para um valor de destino, sua nova regra e todas as outras regras existentes que também tenham 30 dias ou mais como datas de destino serão aplicadas aos resultados do teste.
Meta inicial (data)	Data a partir da qual as datas de destino são calculadas. Você pode especificar somente os campos de data ou de tipo de data e hora. A partir da v14.12, o valor padrão é *Última passagem* . Selecione uma das seguintes opções: ○ Visto pela última vez ○ Visto pela primeira vez ○ Criação em ○ Última aprovação Se a última passagem estiver vazia, a data de criação será considerada para o cálculo do destino de correção. ○ Aberto pela última vez Para personalizar os valores deste campo, consulte KB1642413 .
Notificar (dias antes do vencimento)	Defina um número de dias antes da data do prazo para lembrar usuários e grupos.
Descrição	Descrição resumida da regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Use o construtor de condições para especificar os resultados de teste aos quais esta regra se aplica. Por exemplo, defina uma data de destino de correção de 30 dias para todos os resultados de teste com pontuações de risco maiores que 70. Envie lembretes para usuários ou grupos, ou ambos, sete dias antes da data de correção. A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário. Antes da versão 12,0, a distinção entre maiúsculas e minúsculas é compatível com o texto de pesquisa inserido no Construtor de condições.
Usuários e grupos de usuários ou ambos	Selecione Usuários ou grupos, ou ambos para enviar notificações sobre as datas de meta de aproximação e vencimento que você definiu.

4. Clique em **Enviar**. Como alternativa, para salvar regras editadas, clique em **Atualização** .

   A exibição de lista é exibida com sua regra atualizada ou nova. As regras na lista são ordenadas e executadas a partir da regra com a data de destino de correção mais baixa. Se você desabilitar ou excluir uma regra, a próxima regra na sequência de pedido substituirá a regra inativa ou excluída.

5. Para aplicar suas novas mudanças agora, clique em **Aplicar mudanças** .

Conformidade de configurações grupos de calculadoras

Conformidade de configurações calculadoras são usadas para atualizar valores de registro quando as condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Conformidade de configurações grupos de calculadoras

No registro da Calculadora de risco padrão, as regras da calculadora podem ser aplicadas a todos os resultados de teste afetados e coleções sob demanda. Os gerentes de vulnerabilidades podem usar este recurso para ajustar a configuração da calculadora de risco. Eles podem experimentar vários esquemas de priorização no início da implantação e aplicar essas mudanças sob demanda para exibir como elas afetam as descobertas de importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O grupo de calculadoras de Pontuação de risco foi renomeado para Calculadoras de risco.

Calculadoras de acúmulo de pontuação de risco estão incluídas com Conformidade de configurações. Existem dois tipos de calculadoras de rollup individuais:

Acúmulo de risco de teste de configuração

Calculadoras que acumulam pontuações de risco para todos os resultados de teste com o mesmo teste de configuração para fornecer uma pontuação de risco geral para o teste de configuração. O valor acumulado é exibido nos campos Pontuação de risco.

Acúmulo de pontuação de risco da tarefa de correção

Essas calculadoras acumulam pontuações de risco para todos os resultados de teste em uma tarefa de correção para fornecer uma pontuação de risco geral para essa tarefa de correção. O valor acumulado é exibido nos campos Pontuação de risco.

O grupo de calculadoras de pontuação de risco e o grupo Calculadoras de acúmulo de pontuação de risco são habilitados por padrão.

Para obter mais informações, revise os seguintes termos-chave para Conformidade de configurações calculadoras:

Resultado do teste

Um resultado de teste é o resultado do teste de configuração em um item de configuração (IC) e a tecnologia associada. Os resultados de testes nos estados Falha, Erro e Desconhecido identificam hardware, software e ativos que estão fora de conformidade com suas políticas.

Tarefa de correção

Os resultados do teste são agrupados no momento da importação de dados com base nas regras de tarefa de correção predefinidas. Essas tarefas de correção são semelhantes aos grupos de vulnerabilidades em Resposta a vulnerabilidades. As tarefas de correção organizam os resultados de testes em grupos para análise em massa e representam um conjunto de itens a serem corrigidos.

Pontuação de risco em um resultado de teste

Um valor calculado por calculadoras de pontuação de risco que é baseado no contexto de negócios de um ativo e na gravidade do teste associado. É a média da criticidade comercial do ativo afetado, conforme definido no CMDB, e a gravidade do teste conforme comunicado pelo scanner.

Cada ativo pode ter vários serviços associados a ele. A criticalidade comercial de um ativo é determinada pelo serviço com a criticalidade mais alta.

O valor calculado é exibido nos campos Pontuação de risco dos resultados do teste. As pontuações exibem valores que variam de 0 a 100. Os campos também são codificados por cores para fornecer uma visão geral da gravidade.

Pontuação de risco na tarefa de correção

Esta pontuação é exibida no registro da tarefa de correção e é o valor acumulado das pontuações de risco para todos os resultados de teste ativos em uma tarefa de correção. Essa pontuação muda conforme os resultados do teste são corrigidos na Tarefa de correção.

Pontuação de risco no teste de configuração

Esta pontuação é exibida nos testes de configuração e é o valor acumulado das pontuações de risco para todos os resultados de testes ativos com esse teste de configuração. Esta pontuação muda conforme os resultados de teste associados a este teste de configuração são corrigidos.

Classificação de risco

A quantidade de risco que um resultado de teste com falha representa para o seu sistema. É baseado em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

riscos como Crítico (1) a Nenhum (5). A pontuação é baseada em um intervalo de pontuações de risco e é exibida nos campos Classificação de risco.

Intervalos de classificação de risco

Classificação de risco	Pontuação de risco
1- Crítica	90 a 100
2- Alto	70 a 89
3- Médio	40 a 69
4- Baixo	1 a 39
5- Nenhum	0

Calculadoras de acúmulo de pontuação de risco

Existem dois tipos de calculadoras de acúmulo:

- Acúmulo de risco de teste de configuração: Essas calculadoras acumulam pontuações de risco para todos os resultados de teste com o mesmo teste de configuração para fornecer uma pontuação de risco geral para o teste de configuração. O valor acumulado é exibido nos campos Pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras.
- Acúmulo de pontuação de risco da tarefa de correção: Essas calculadoras acumulam pontuações de risco para todos os resultados de teste em uma tarefa de correção para fornecer uma pontuação de risco geral para essa tarefa de correção. O valor acumulado é exibido nos campos Pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras. Para obter um exemplo de uma calculadora de acúmulo de pontuação de risco e como ela calcula pontuações, consulte Exemplo de cálculo de acúmulo de risco para Conformidade de configurações(anterior à v15.0).

Pontuação de risco histórico

A pontuação de risco inerente em todos os resultados de teste aprovados em uma tarefa de correção. Este campo exibe a quantidade de risco que foi corrigido por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.

As pontuações são calculadas sempre que a pontuação de risco muda ou quando os resultados do teste são adicionados ou removidos de uma tarefa de correção.

Nota: Para funcionar corretamente, este script requer Mapeamento de serviços plug-in. Mapeamento de serviços está disponível como uma assinatura separada e requer ativação por ServiceNow pessoal.

Crie um Conformidade de configurações grupo de calculadora

Conformidade de configurações os grupos de calculadora são usados para agrupar calculadoras com base em como você deseja usá-las.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

. Conformidade de configurações o sistema de base inclui um grupo de calculadora: **Pontuação de risco** . Ao criar outras calculadoras, você pode adicioná-las a este grupo ou criar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

outros grupos e calculadoras. Em cada grupo, a primeira calculadora que corresponde ao resultado do teste é executada.

Há dois grupos de calculadora incluídos com Conformidade de configurações aplicação:

- Calculadoras de risco
- Calculadoras de acúmulo de pontuação de risco

Calculadoras de risco calculam a pontuação de risco e a classificação de risco de um resultado de teste.

Calculadoras de acúmulo de pontuação de risco acumulam pontuações de risco para todos os resultados de teste e tarefas de correção com o mesmo teste de configuração para fornecer uma pontuação de risco geral.

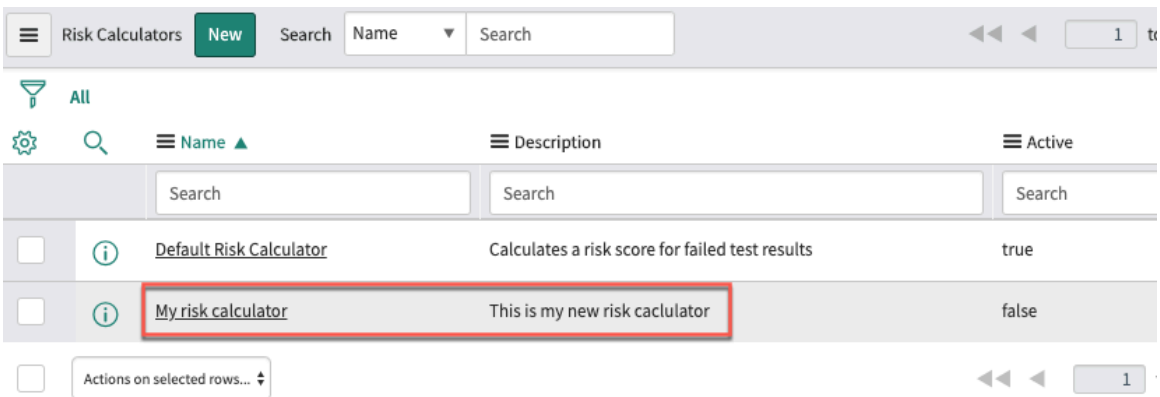
Você também cria novas calculadoras diretamente desses grupos.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Grupos de Calculadoras**.
2. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** e selecione **Calculadoras de risco** ou **Calculadoras de acúmulo de pontuação de risco** .
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora.
Descrição	Uma descrição deste grupo de calculadoras.
Ativo	Habilite ou desabilite o grupo de calculadora.

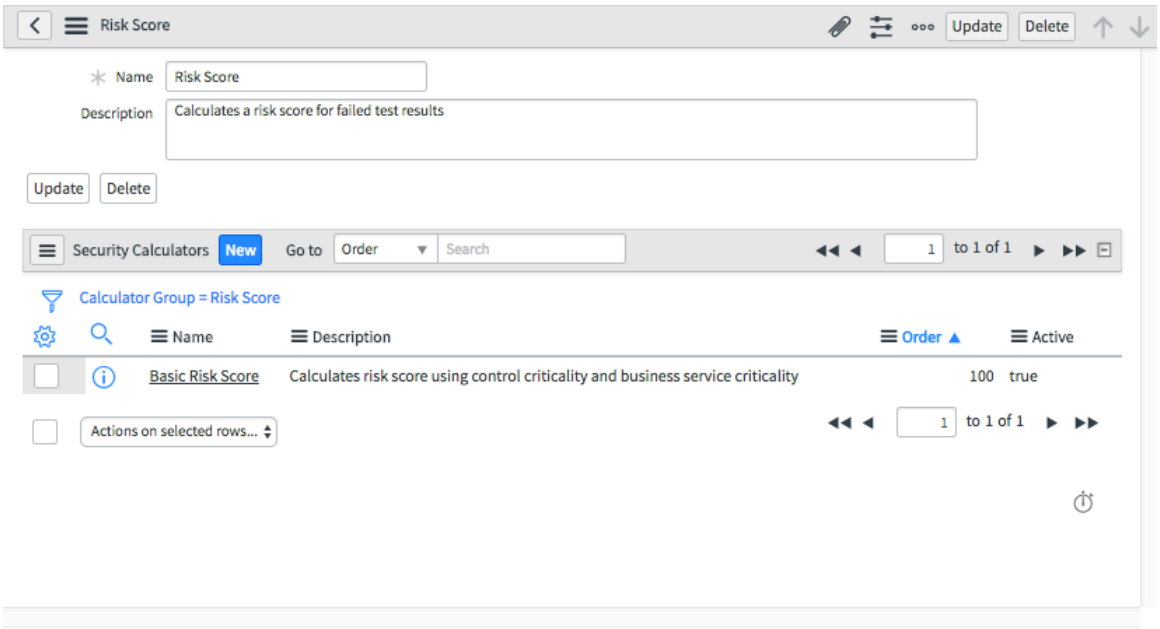
5. Clique com o botão direito do mouse **Salvar** no cabeçalho do formulário ou clique em **Enviar** .
   O novo grupo de calculadoras é exibido na lista de grupos com as outras calculadoras. Clique no nome do novo grupo de calculadora para abrir o registro. Consulte Crie, edite e reaplique calculadoras de risco para Conformidade de configurações para obter mais informações sobre como definir condições e valores exibidos e reaplicar calculadoras.



. **Calculadoras de segurança** a lista relacionada é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Novo** para adicionar calculadoras junto com suas condições ao grupo.

   A distinção entre maiúsculas e minúsculas do texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

Conformidade de configurações calculadoras e regras da calculadora

Conformidade de configurações calcular valores iniciais para os campos nos resultados de testes. Cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Conformidade de configurações calculadoras

O sistema de base de Conformidade de configuração inclui uma calculadora de conformidade de configuração (**Calculadora de risco padrão**) que define a base **Pontuação de risco** no resultado do teste. Calculadoras de conformidade de configuração podem ser criadas para priorizar e classificar o impacto dos resultados de teste com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC), você pode criar calculadoras de conformidade de configuração adicionais para definir outros campos nos resultados de teste ou personalizar as calculadoras de conformidade de configuração existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades.

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

Todas as calculadoras de conformidade de configuração habilitadas definem os campos selecionados sempre que um resultado de teste é criado, quando um IC associado ou Teste de configuração muda ou quando **Calcular pontuação de risco** o link relacionado em um resultado de teste é usado. Por exemplo, a Pontuação de risco é atualizada automaticamente nos registros de resultado de teste quando o valor control.criticality é atualizado em um resultado de teste importado. Depois que uma importação de resultado de teste atualizar uma pontuação de resultado de teste, você pode recalcular a pontuação de risco dos resultados de teste selecionando **Reaplicar Calculadora** botão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

De um resultado de teste existente, se você selecionar **Calcular pontuação de risco** E qualquer uma das calculadoras estiver habilitada, o campo Pontuação de risco no resultado do teste será atualizado.

Nota:

- . **Calcular pontuação de risco** o link relacionado só fica visível quando pelo menos uma calculadora de conformidade de configuração está habilitada.
- A partir da v22.0 de Resposta a vulnerabilidades, Você pode atualizar a pontuação de risco de um resultado de teste no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI selecionando **Calcular pontuação de risco** em sua exibição de registro.
- A partir da versão 14,13 de Conformidade de configurações Sempre que a pontuação de risco em um resultado de teste muda, os seguintes detalhes são documentados na seção Anotações do resultado do teste:
  - Nome do grupo de calculadora
  - Nome da calculadora: Dependendo se a regra da calculadora é baseada em um modelo ou script, o nome é anexado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e selecione **Exibição avançada** caixa de seleção. Em **Tipo de valor** caixa suspensa, selecione a opção necessária. Se **Modelo** selecionado, a pontuação de risco é atualizada de acordo com a condição especificada na regra. Se **Script** selecionado, você pode adicionar ou atualizar o script existente.
  - Valores de campo com sua ponderação e contribuição de pontuação de risco
  - Pontuação de risco final
  - A propriedade do sistema *sn_sec_cmn.risk_score_changes_add_worknotes*ajuda a preencher a seção de anotações de trabalho. A partir da v15.2.1 de Conformidade de configurações, a propriedade do sistema *sn_sec_cmn.risk_score_changes_add_worknotes*está inativo por padrão. Somente se você habilitá-lo, poderá ver todas as mudanças relacionadas à pontuação de risco de um resultado de teste na seção Anotações de trabalho. Além disso, as anotações de trabalho serão atualizadas somente se houver uma mudança na pontuação de risco.

Conformidade de configurações regras da calculadora

Por padrão, um sistema de base **Calculadora de risco padrão** fornecido. Se você quiser criar uma regra de risco para esta calculadora, defina o campo de destino de **Calculadora de risco padrão** . **Pontuação de risco** . Selecione **Nova Regra de Risco** botão para criar uma nova regra de risco . Isso cria uma regra de calculadora de resultado de teste especializada chamada a. **Regra de risco** , que, por sua vez, calcula o. **Pontuação de risco** com base em vários valores. Por padrão, os seguintes valores para calcular a pontuação de risco são considerados :

- Criticalidade dos negócios
- Criticidade

Você pode ajustar os valores a serem usados no **Regra de risco padrão** e quanto peso dar a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a base **Pontuação de risco** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Começando com Conformidade de configurações versão 13,0, você pode personalizar os critérios da regra de risco padrão. Para obter mais informações, consulte Defina campos e pesos para a regra de risco .

Atribuição de uma porcentagem de ponderação

Você também pode atribuir porcentagem de ponderação (0-100) no nível de valor do campo. Por exemplo, você pode atribuir uma porcentagem de ponderação a cada nível de gravidade (Nenhum a Crítico). Se a ponderação de criticidade for 50 para a regra de risco e os seguintes valores de ponderação forem atribuídos para o nível de criticidade:

Atribuir porcentagem de ponderação

Criticidade	Pontuação de Risco
Crítico	100
Alto(a)	50
Médio	20
Nenhum(a)	0

Se a criticidade for crítica, a ponderação correspondente será 50. Se a criticidade for alta, a ponderação será 25 e, se a criticidade for média, a ponderação será 10. Se a criticidade for nenhuma, a ponderação correspondente será 0. Para obter mais informações, Consulte o exemplo de cálculo de pontuação de risco para Conformidade de configuração.

Cada regra tem um **Pedido** no entanto, o primeiro a corresponder às condições atualiza o. **Pontuação de risco** campo no resultado do teste. As regras da calculadora sem script normalmente criam menos impacto no desempenho do que as regras da calculadora com script.

O sistema de base Conformidade de configurações A calculadora contém regras de calculadora que atribuem a cada nível de criticidade (Nenhum a Crítico) um valor (0-100) para **Pontuação de risco** com base na gravidade. Gravidade desconhecida recebe automaticamente uma pontuação de risco de 100. Esses valores podem ser ajustados, como Calculadora de risco padrão, novas regras de calculadora ou novas regras de risco podem ser criadas.

Pesos da pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação de risco e classificação com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio `Update Risk Rating from Risk Score`na tabela de item vulnerável é responsável por calcular a classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Versão 17,1 do Resposta a vulnerabilidades(VR), as seguintes classificações de risco foram fornecidas como parte da inclusão de script VulnerabilityUtils , que foram codificados.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor (classificação de risco)	Peso (pontuação de risco)
4	1 a 39
5	0

A partir da versão 18,0 do Resposta a vulnerabilidades,

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

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

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

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

Defina campos e pesos para a regra de risco

Personalize os parâmetros e os pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de teste e ativos exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Calculadoras de risco**.
2. Clique em **Calculadora de risco padrão** .
3. Selecione o campo de destino como **Pontuação de risco** .
   . **Nova Regra de Risco** O botão é exibido na tabela Regra da calculadora.
4. Clique em **Nova Regra de Risco** botão para navegar até **Regra de risco de conformidade da configuração** formulário.
5. Na seção Critérios da calculadora de risco, defina o peso de cada critério de acordo com sua importância no cálculo da pontuação de risco geral.
6. Limpe **Ativo** caixa de seleção para desativar a regra.
7. Clique em **Adicionar critérios** Para adicionar campos de regra de risco aos critérios da Calculadora de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	A tabela que você usa para definir a ponderação da pontuação de risco. Selecione uma das seguintes opções: ○ Resultado do teste: Adicione campos para os quais você pode fazer a referência com pontos diretamente do Resultado do teste (TR). ○ Item de configuração: Adicione campos passíveis de observação com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela cmdb_ci de base. ○ Teste - Teste: Adicione campos passíveis de observação com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, entrada de terceiros. Esses campos não fazem parte da tabela base de Teste de configuração. ○ Tabela de referência do resultado do teste: Adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao resultado do teste. Esses campos não podem ser rastreados diretamente com pontos do Resultado do teste. ○ Tabela de referência do item de configuração: Adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser rastreados diretamente com pontos do TR. ○ Tabela de referência de teste: Adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vulc_test ou tabelas que têm uma referência a sn_vulc_test. Esses campos não podem ser rastreados diretamente com pontos do TR. ○ Condições personalizadas: Use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Campo	O campo usado para cálculo de pontuação de risco para esta regra.
Peso	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Tabela	○ Resultado do teste > Item de configuração ○ Resultado do teste > Teste ○ Tabela de referência do resultado de testes ○ Tabela de referência do item de configuração ○ Tabela de referência do teste Este campo aparece somente quando qualquer uma das opções listadas é selecionada no campo Escolher tabela de referência.
Agregação	Selecione o valor mínimo ou máximo a ser considerado para cálculos quando o campo for selecionado nas tabelas relacionadas (m2m). Este campo aparece somente quando uma tabela de referência é selecionada no campo Escolher tabela de referência.
Defina a ponderação do valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, defina valores de campo como um intervalo (por exemplo, 1 a 5). O valor deve ser um número inteiro entre 0 e 100. Este campo não aparecerá se a opção Condições personalizadas estiver selecionada no campo Escolher tabela de referência.
Tabela de condição	Selecione uma condição na lista. Este campo aparece somente quando a opção Condições personalizadas é selecionada no campo Escolher tabela de referência.
Nome do campo	Insira um nome para os critérios de risco. Este campo aparece somente quando Condições personalizadas é selecionado no campo Escolher tabela de referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Visualize os itens nesta tabela que correspondem às condições definidas. Este campo aparece somente quando Condições personalizadas é selecionado no campo Escolher tabela de referência.

9. Clique em **Enviar**.

O que Fazer Depois

Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco no resultado do teste ativo.

Editar calculadoras de acúmulo de risco para Conformidade de configurações

Edite uma calculadora de acúmulo de risco existente.

Antes de Iniciar

Função necessária: Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** e selecione **Calculadoras de acúmulo de pontuação de risco** .
2. Com a lista de Calculadoras de acúmulo de pontuação de risco exibida, clique em uma calculadora para abrir o registro e editar o formulário.

Campo	Descrição
Nome	O nome da calculadora de acúmulo de teste de configuração ou tarefa de correção.
Descrição	Uma descrição da calculadora de acúmulo de risco.
Tabela	Tabela na qual a calculadora de rollup é aplicada.
Incluir adiamento	Inclui resultados de testes adiados durante o acúmulo da pontuação de risco.

3. Defina as ponderações de uma das seguintes maneiras:
   - Na seção Ponderações de acúmulo, atribua pesos para o seguinte:

Ponderações de Rollup

Campo	Descrição	Ponderação padrão
Pontuação de risco máximo	Pontuação de risco máximo dos resultados do teste considerados.	85
Pontuação de risco médio	Agregado das pontuações de risco de todos os resultados de testes considerados.	0
Contagem de resultados de testes	Número de resultados de testes.	15

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecione **Exibição avançada** caixa de seleção, e em **Valores de script** editor, edite os valores no script conforme necessário.

  Nota: Editar script requer conhecimento avançado do ServiceNow AI Platform e o. Conformidade de configurações aplicação.

4. Clique em **Atualização** para salvar suas edições.

Calculadoras de acúmulo são trabalhos agendados que são executados por hora para selecionar mudanças. Esses trabalhos agendados também pontuações de risco gerais para testes de configuração e tarefa de correção. Os valores acumulados são exibidos nos campos Pontuação de risco.

Para obter um exemplo de como uma calculadora de acúmulo de risco determina pontuações, consulte Exemplo de cálculo de acúmulo de risco para Conformidade de configurações(anterior à v15.0).

Crie, edite e reaplique calculadoras de risco para Conformidade de configurações

As regras da calculadora podem ser aplicadas a todos os resultados de testes afetados e coleções sob demanda. Os gerentes de vulnerabilidades podem usar esse recurso para ajustar a configuração da calculadora de risco e aplicar mudanças sob demanda para importar descobertas.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Para criar uma nova calculadora de risco, siga estas etapas.

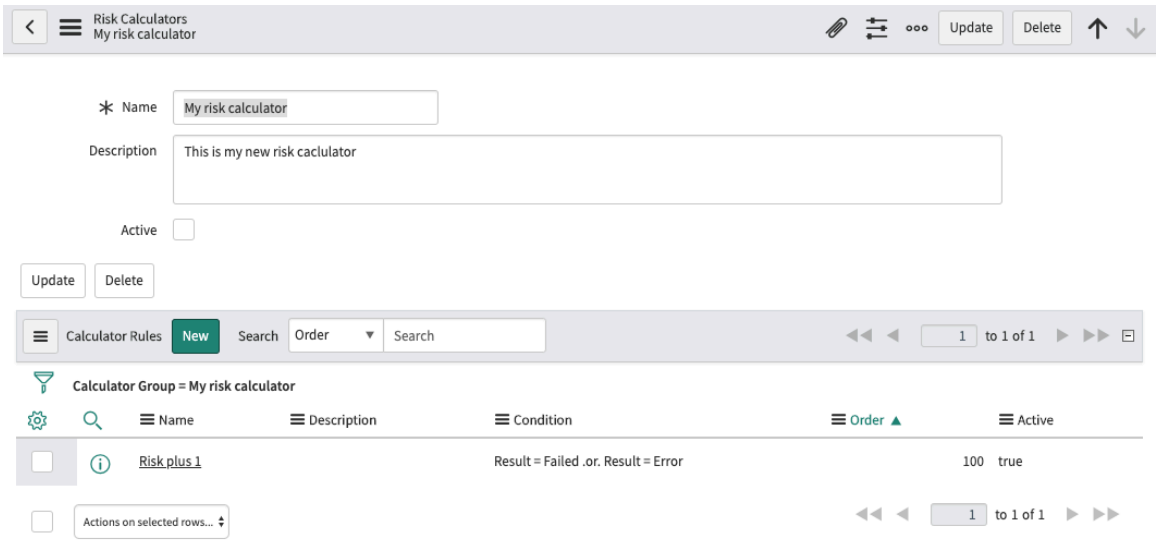
   a. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** e selecione **Calculadoras de risco** .

   b. Na lista Calculadora de risco, clique em **Novo** .

   c. Insira um nome e uma descrição para sua nova calculadora e clique em **Enviar** .
   A nova calculadora é exibida na lista Calculadora de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Na lista, clique na nova calculadora para criar as condições sob as quais a calculadora é executada e especifique os campos e valores que você deseja exibir nos registros de resultado de teste e nas tarefas de correção.

e. No registro exibido, clique em **Novo** .

f. Preencha os campos nas guias conforme apropriado.

Tab	Descrição
Quando esta condição for atendida	Use o construtor de condições para criar as condições sob as quais a calculadora é executada. Um exemplo é: O resultado é Falha ou Resultado é Erro .
Definir estes valores	Use o modelo para selecionar os campos e valores que você deseja exibir.

g. Clique em **Enviar**.
O registro é exibido com as novas regras da calculadora e o grupo ao qual ele pertence.

2. Para reaplicar uma calculadora existente aos resultados de testes ou editar as regras e valores exibidos para uma calculadora de risco existente, siga estas etapas.

a. Nas listas Calculadoras de risco ou Calculadoras de acúmulo de risco, selecione a calculadora que você deseja editar.

b. Para reaplicar uma calculadora de risco aos dados de resultado de teste existentes do registro, clique em **Reaplicar Calculadora** .
Todos os resultados de testes que atendem às condições da calculadora são atualizados.

Nota: Dependendo do número de resultados de testes, esta atualização pode levar algum tempo.

c. Para editar as condições e os valores, no canto inferior esquerdo da coluna Nome, clique no nome da calculadora.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para calculadoras de risco, o registro e o. **Quando esta condição é atendida** e. **Defina esses valores** as guias são exibidas.

d. Preencha o formulário conforme apropriado.

Tab	Descrição de Campo
Quando esta condição for atendida	Use o construtor de condições de filtro para criar as condições sob as quais você deseja que a calculadora seja executada.
Definir estes valores	Escolha um para continuar. ▪ Tipo de valor - Modelo. Escolha os campos da lista e os valores correspondentes. ▪ Script - Insira suas mudanças usando o editor. **Nota:** Editar script requer conhecimento avançado do ServiceNow AI Platform e o. Conformidade de configurações aplicação.

3. Opcional: Para aplicar as novas regras sob demanda aos dados de resultado de teste existentes, siga estas etapas.

a. Com a lista Calculadoras de risco exibida, clique em uma calculadora que você deseja aplicar. O registro é exibido.

b. Clique em **Reaplicar Calculadora** para testar e aplicar suas mudanças sob demanda às descobertas de importação.

4. Exiba suas mudanças nos resultados de testes e continue a editar suas calculadoras conforme necessário.

Exemplos para Conformidade de configurações cálculo da pontuação de risco

A partir da v13.0 de Conformidade de configurações, você pode personalizar os critérios da regra de risco padrão. Use pontuações de risco fornecidas por fornecedores terceirizados, como Qualys e Tenable, para cálculos de pontuação de risco.

Fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo Criticalidade na tabela sn_vulc_test. Use este campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, siga o procedimento:

Adicione criticidade de origem como um critério para uma regra de risco

Use pontuações com base na criticidade fornecida por fornecedores terceirizados para calcular pontuações de risco.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

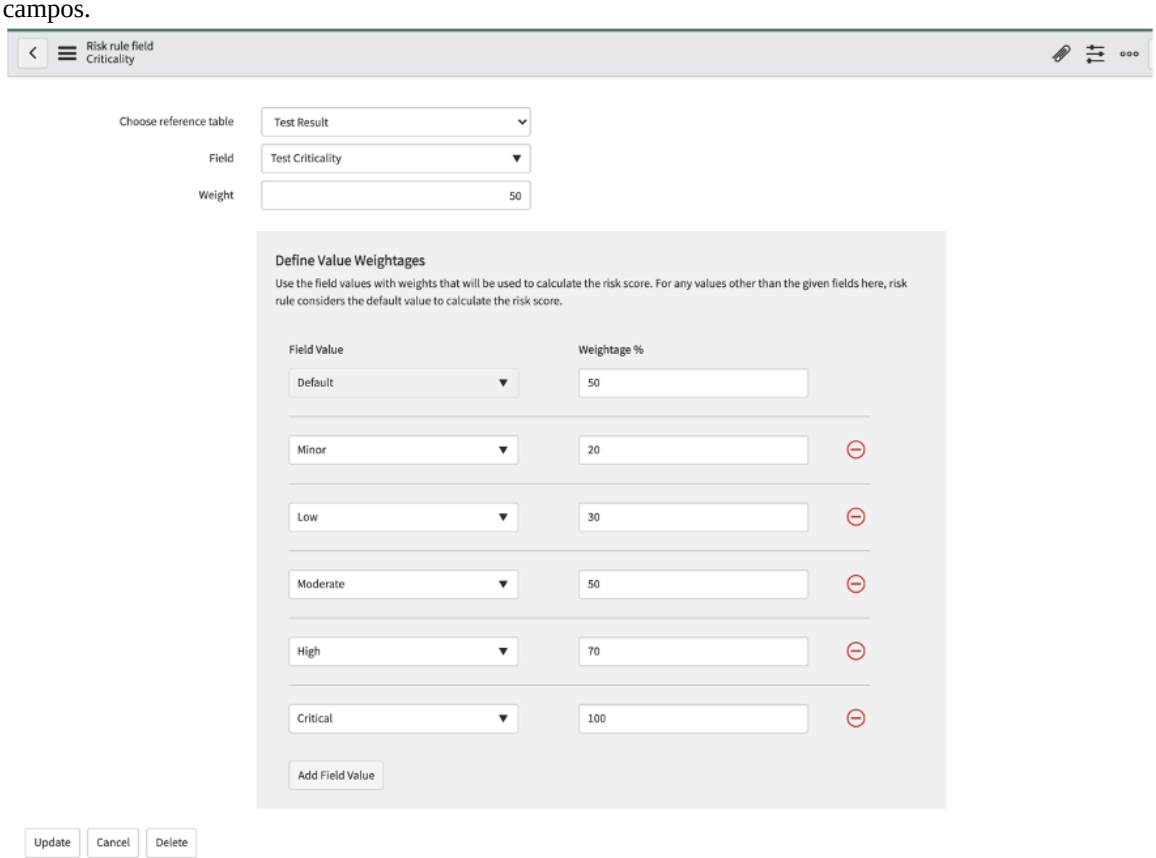
Fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações de risco. Essas pontuações são preenchidas no campo Criticalidade na tabela sn_vulc_test. Use este campo para cálculos de pontuação de risco e calcular a pontuação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Calculadoras de risco**.
2. Navegue até o formulário Regra de risco.
3. Limpe **Ativo** caixa de seleção para desativar a regra.
4. Clique em **Adicionar critérios** .
5. Em **Escolha a tabela de referência** , selecione **Resultado do teste** .
6. Em **Campo** , selecione **Teste.Criticalidade** .
7. Em **Peso** especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
8. Em **Defina pesos de valor** , adicione valores de campo e atribua uma porcentagem de ponderação aos campos.



9. Clique em **Enviar**.

Adicione criticidade de negócios como um critério para uma regra de risco

Especifique um valor de criticidade para os serviços de negócio e use a criticidade de negócios para calcular as pontuações de risco.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Supondo que sua organização tenha muitos serviços de negócios e um item de configuração (IC) esteja sendo usado pelos seguintes serviços:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criticidade dos serviços de negócio

Serviço de negócios	Criticidade
Gestão de nuvem	1 - Mais crítico
E-commerce	2 - Um pouco crítico
Serviços ao cliente	3 - Menos crítico
Viagem e despesa	4 - Não crítico

O mapeamento entre o IC e os serviços é armazenado na tabela Serviços [cmdb_ci_services]. Quando um IC não passa em um Teste de Configuração, um Resultado de Teste (TR) é criado. Você pode usar o valor da criticidade comercial dos serviços afetados para calcular a pontuação de risco para este TR. Siga o procedimento para usar o valor de criticidade desses serviços para calcular a pontuação de risco.

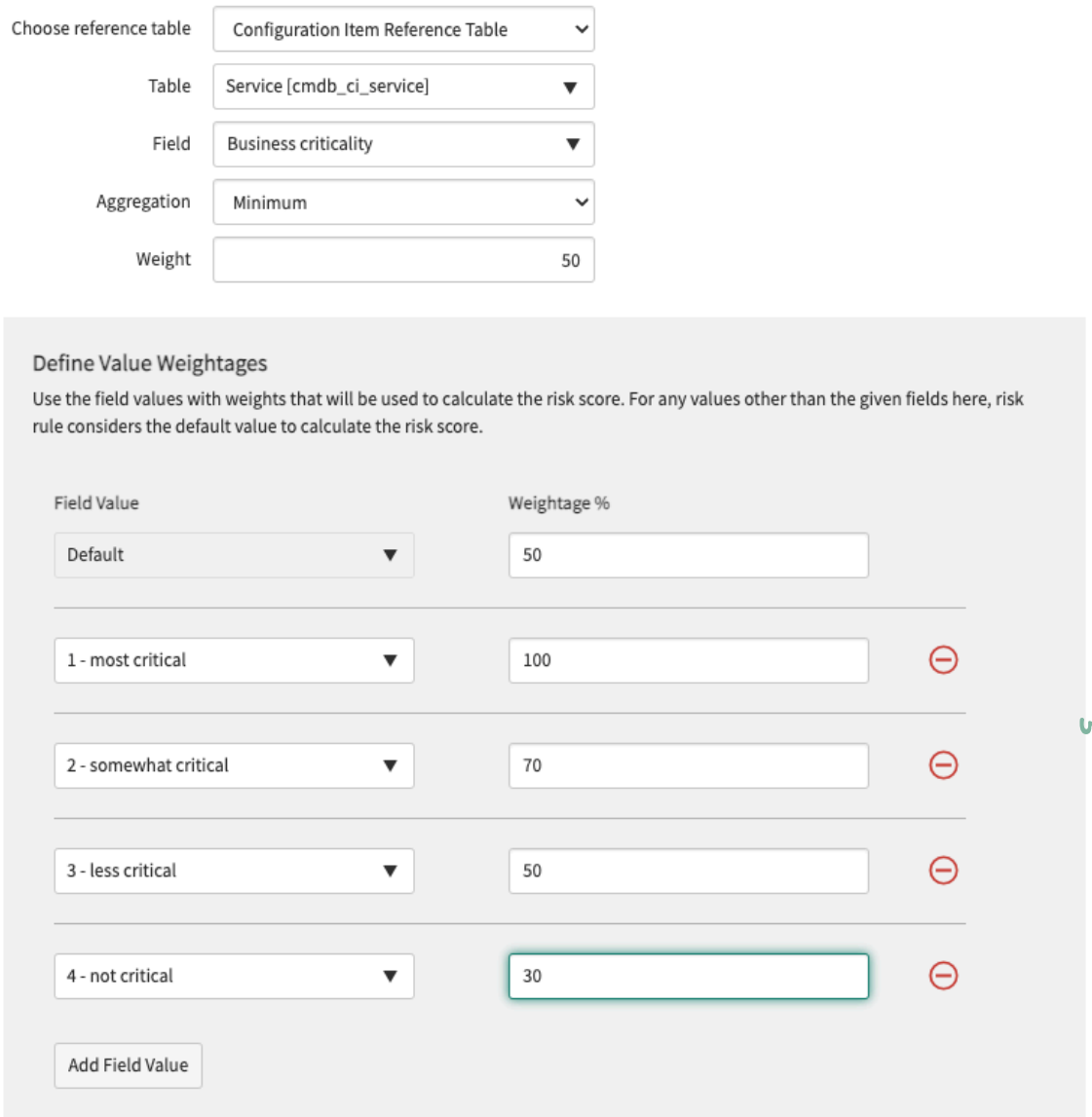
Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Calculadoras de risco**.
2. Navegue até o formulário Regra de risco no **Regras da calculadora** seção.
3. Limpe **Ativo** caixa de seleção para desativar a regra.
4. Clique em **Adicionar critérios** .
5. Em **Escolha a tabela de referência** , selecione **Tabela de referência do item de configuração** .
6. Em **Tabela** , selecione **Serviço [cmdb_ci_service]** .
7. Em **Campo** , selecione **Criticidade dos negócios** .
8. Em **Agregação** campo, selecione **Mínimo** Para recuperar o serviço mais crítico para este caso de uso (1- valor mais crítico) ou **Máximo** Recuperar o serviço menos crítico para este caso de uso (4 – valor não crítico).
9. Em **Peso** especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
10. Em **Defina pesos de valor** adicione valores de campo e atribua ponderações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ponderação da regra de risco de criticalidade comercial personalizada



Tradução automática

11. Clique em **Enviar**.

Adicione critério condicional à calculadora de risco

Use condições personalizadas para a regra de risco para cálculo de pontuação de risco.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Supondo que sua organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar pesos de pontuação de risco para esses ICs externos.

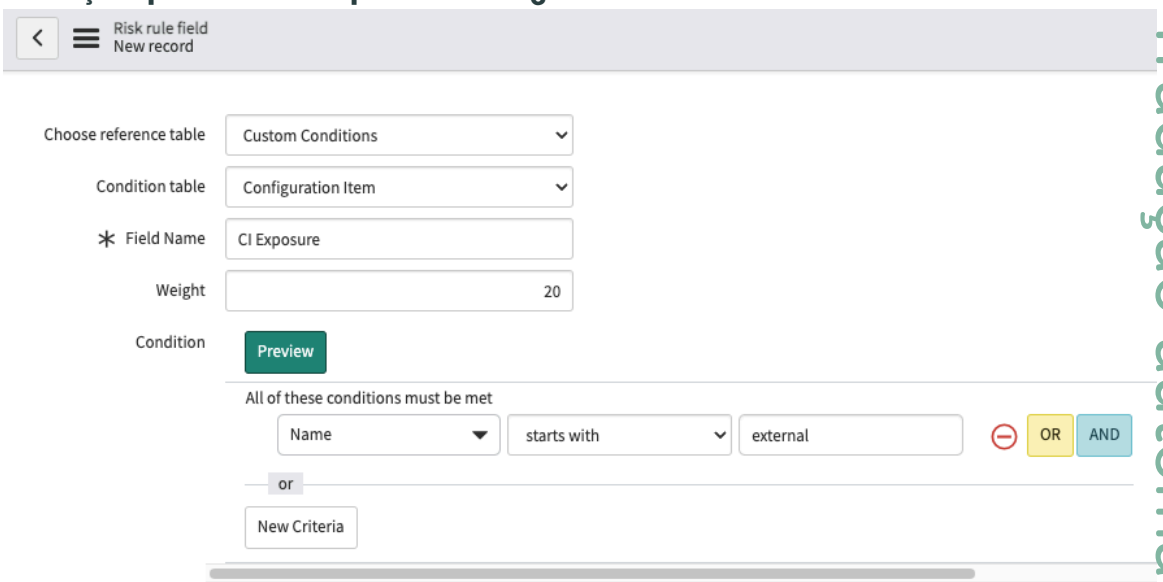
Nota: Você pode identificar esses ICs pelo nome deles. Os nomes começam com "external".

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Calculadoras de risco**.
2. Navegue até o formulário Regra de risco.
3. Limpe **Ativo** caixa de seleção para desativar a regra.
4. Clique em **Adicionar critérios** .
5. Em **Escolha a tabela de referência** , selecione **Condições personalizadas** .
6. Em **Tabela de condições** , selecione **Item de configuração** .
7. Em **Nome do campo** campo, insira `Exposição de IC` .
8. Em **Peso** especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
9. Em **Condição** campo, selecione **Nome > Começa com** especifique o valor como `externo` .

Condições personalizadas para a nova regra de risco



10. Clique em **Enviar**.

Tópicos relacionados

Grupos de calculadora de conformidade de configuração

Exemplo de cálculo de pontuação de risco para Conformidade de configurações

Determine as calculadoras de pontuação de risco para gerar pontuações de risco que usam os dados de teste e ativos específicos da sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas. Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Determine as pontuações da calculadora de regra de risco

Campo	Ponderação	Detalhamento de peso
Criticalidade	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Alto: 70 Crítico: 100
Business_Criticality	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Altura: 70 Crítico: 100

Suponha que os Resultados de teste mostrados nesta tabela estejam presentes no sistema.

Mapeamento de resultados de teste

ID	Criticalidade dos negócios	Criticidade do controle
CTR0000001	1 – Mais crítico	Secundário
CTR0000002	1 – Mais crítico	Baixo(a)
CTR0000003	2 – Um pouco crítico	Secundário
CTR0000004	2 – Um pouco crítico	Moderado
CTR0000005	3 – Menos crítico	Baixo(a)

O cálculo da pontuação de risco para o resultado do teste é calculado com base na fórmula:

Pontuação de risco: (W(control.criticality) * FV (control.criticality). W(business_criticality) * FV(business_criticality)) / 100, em que W é o peso e FV é a porcentagem de peso do valor do campo.

A pontuação de risco resultante para esses resultados de teste é conforme descrito nesta tabela:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco baseada nos resultados do teste

ID	Criticidade dos negócios (50%)	Criticalidade do controle (50%)	Pontuação de risco resultante
CTR0000001	1 – Mais crítico (50% x100)	Secundário (50% x 20)	60
CTR0000002	1 – Mais crítico (50% x100)	Baixo (50% x 30)	65
CTR0000003	2 – Um pouco crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 – Um pouco crítico (50% x 70)	Moderado (50% x 50)	60
CTR0000005	3 – menos crítico (50% x 50)	Baixo (50% x 30)	40

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Resultados da porcentagem de ponderação alterada

Campo	Ponderação	Detalhamento de peso
Criticalidade	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 60 Altura: 70 Crítico: 100
Business_Criticality	50	Padrão: 50 1 – Mais crítico: 100 2 – Um pouco crítico: 70 3 – Menos crítico: 20 4 – Não Crítico: 30

A pontuação de risco dos resultados do teste após a reaplicação da calculadora é mostrada nesta tabela:

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticidade dos negócios (50%)	Criticalidade do controle (50%)	Pontuação de risco resultante
CTR0000001	1 – Mais crítico (50% x100)	Secundário (50% x 20)	60
CTR0000002	1 – Mais crítico (50% x100)	Baixo (50% x 30)	65

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticidade dos negócios (50%)	Criticalidade do controle (50%)	Pontuação de risco resultante
CTR0000003	2 – Um pouco crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 – Um pouco crítico (50% x 70)	Moderado (50% x 60) Valor revisado	65 Valor revisado
CTR0000005	3 – menos crítico (50% x 20) Valor revisado	Baixo (50% x 30)	25 Valor revisado

Exemplo de cálculo de acúmulo de risco para Conformidade de configurações(anterior à v15.0)

O exemplo a seguir demonstra como as pontuações das calculadoras de acúmulo de risco são determinadas.

Para a seguinte calculadora de acúmulo de tarefa de correção, a fórmula para calcular a Pontuação de risco da tarefa de correção é:

(Pontuação de risco máximo/100) * 85 ou mais (fator * 15).

O fator na equação anterior é determinado pelo número de resultados de teste, conforme mostrado na tabela a seguir.

Contagem de Resultado de testes	Fator
Menos de 10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 10000	1

Para a tarefa de correção a seguir, TRG0003066, com três pontuações de risco de resultados de teste, a pontuação máxima é 90.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Reprovado	Aberto
CTR000124	70	TRG0003066	Reprovado	Aberto
CTR000125	40	TRG0003066	Reprovado	Aberto

Para a tarefa de correção, TRG0003066:

A pontuação de risco é 79, (90/100) * 85 * 0,2 * 15: Math.floor (76,5 -3) 79.

A pontuação de risco histórica é nula, porque a Tarefa de Correção ainda está "Aberto".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a ingestão de dados, os resultados do teste são "Passados" e a tarefa de correção muda para "Encerrado", conforme mostrado na tabela a seguir.

Número	Pontuação de risco (anterior a v15.0)	Tarefa de correção	Resultado	Status
CTR000123	0	TRG0003066	Aprovado	Encerrado
CTR000124	0	TRG0003066	Aprovado	Encerrado
CTR000125	0	TRG0003066	Aprovado	Encerrado

O Histórico de resultados do teste é exibido na tabela a seguir.

Número	Pontuação de risco	Último resultado	Resultado
CTRH000111	90	CTR000123	Reprovado
CTRH000112	70	CTR000124	Reprovado
CTRH000113	40	CTR000125	Reprovado

A Pontuação de risco é zero, porque não há resultados de teste ativos na Tarefa de correção.

Para a tarefa de correção, TRG0003066:

A pontuação de risco histórico é 79: (90/100) * 85 * 0,2 * 15: Math.floor (76,5 -3) 79.

Exemplo de cálculo de acúmulo de risco para Conformidade de configurações(v15.0 e posterior)

O exemplo a seguir demonstra como as pontuações das calculadoras de acúmulo de risco são determinadas.

Para a seguinte calculadora de acúmulo de tarefa de correção, a fórmula para calcular a Pontuação de risco da tarefa de correção é:

(Pontuação de risco máxima* 80/100) Mais (Pontuação de risco média* 5/100) Mais (fator * 15)

Em que, os pesos são os seguintes:

- Pontuação máxima de risco: 80
- Pontuação média de risco: 5
- Fator: 15

O peso padrão da pontuação de risco média é 0. Para obter mais informações sobre como definir os pesos, consulte Editar calculadoras de acúmulo de risco para Conformidade de configurações.

O fator na equação anterior é determinado pelo número de resultados de teste, conforme mostrado na tabela a seguir.

Contagem de Resultado de testes	Fator
Menos de 10	0,2
10-99	0,4

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contagem de Resultado de testes	Fator
100-1000	0,6
1001-9999	0,8
> 10000	1

Para a tarefa de correção a seguir, TRG0003066, com três pontuações de risco de resultados de teste, a pontuação de risco máxima é 90 e a pontuação de risco média é 66,67.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Reprovado	Aberto
CTR000124	70	TRG0003066	Reprovado	Aberto
CTR000125	40	TRG0003066	Reprovado	Aberto

Para a tarefa de correção, TRG0003066:

A pontuação de risco é 81, (90* 80/100) (66,67* 5/100) (0,2 * 15) Math.floor (78,3 3) é 81.

A pontuação de risco histórica é nula, porque a tarefa de correção ainda está "aberta".

Após a ingestão de dados, os resultados do teste são "Passados" e a tarefa de correção muda para "Encerrado", conforme mostrado na tabela a seguir. A partir da v15.0 de Conformidade de configurações, A Pontuação de risco de um resultado de teste aprovado é preenchida para determinar o risco mitigado.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Aprovado	Encerrado
CTR000124	70	TRG0003066	Aprovado	Encerrado
CTR000125	40	TRG0003066	Aprovado	Encerrado

O Histórico de resultados do teste é exibido na tabela a seguir.

Número	Pontuação de risco	Último resultado	Resultado
CTRH000111	90	CTR000123	Reprovado
CTRH000112	70	CTR000124	Reprovado
CTRH000113	40	CTR000125	Reprovado

A pontuação de risco da tarefa de correção é zero, porque não há resultados de teste ativos na tarefa de correção.

Para a tarefa de correção, TRG0003066:

A Pontuação de Risco Histórico é 81: (90* 80/100) (66,67* 5/100) (0,2 * 15) Math.floor (78,3 3) 81.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ou editar Conformidade de configurações regras de tarefa de correção

Você pode criar regras para agrupar automaticamente os resultados de teste com base nas condições de filtro. Essas regras agrupam automaticamente os resultados de teste conforme são importados. Use o filtro para limitar os resultados de teste agrupados por esta regra, como selecionar todos os resultados de teste com explorações.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

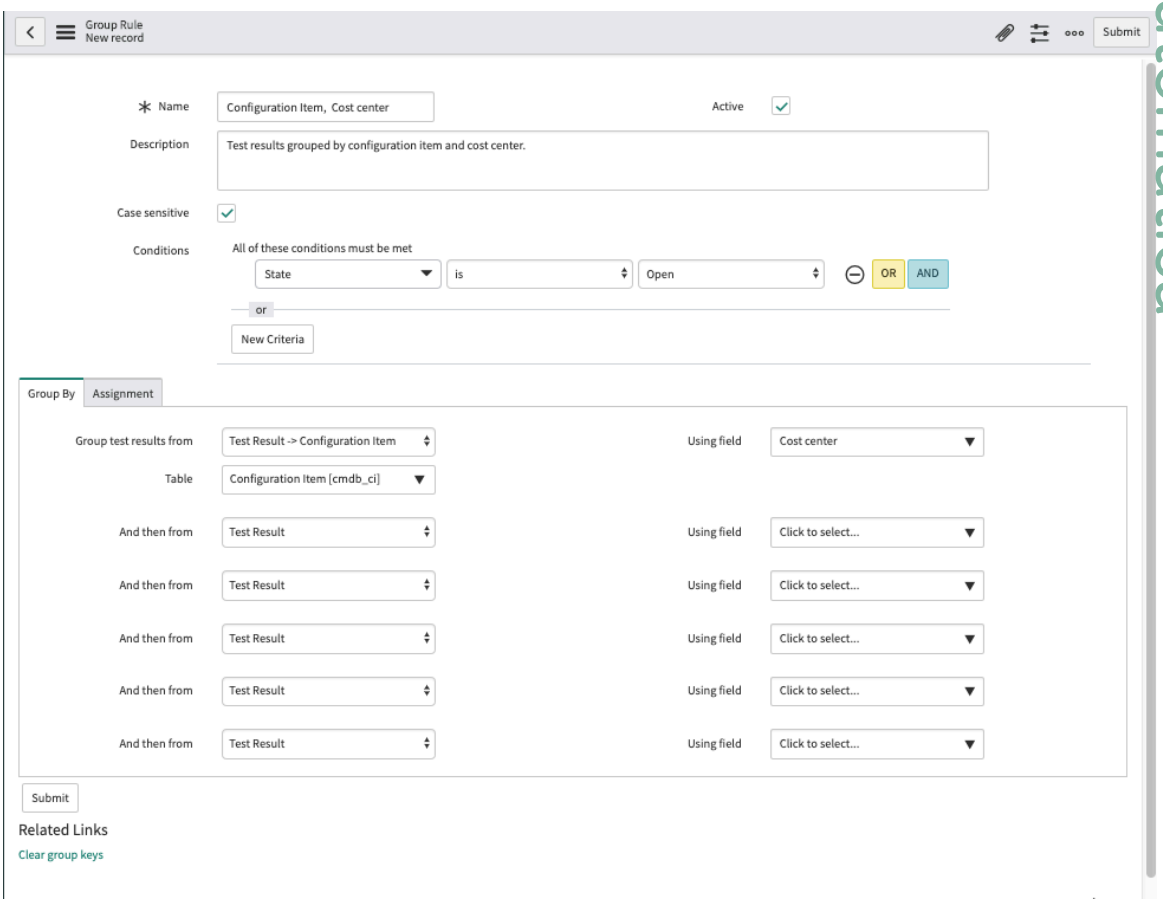
O sistema de base é fornecido com uma regra de tarefa de correção, **Grupo de atribuição, Teste** , que agrupa resultados de teste por grupo de atribuição (preenchido previamente de **Regras de atribuição** e o resultado do teste **Teste** campo. Esta regra pode ser modificada usando condições de filtro e chaves de grupo. Chaves de grupo são colunas na tabela de resultados de testes. Selecione até seis chaves para indicar quais valores devem ser usados para agrupar os resultados do teste.

A partir da versão 14,7 de Conformidade de configurações. **Grupo de atribuição, Teste** a regra da tarefa de correção está desativada para novas implementações.

Nota: Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o. **Reaplicar** Botão no formulário Regra da tarefa de correção.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de tarefa de correção**.
2. Abra o. **Grupo de atribuição, Teste** ou clique **Novo** .



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Se **Novo** preencha os campos no formulário, conforme apropriado.

Conformidade de configurações Regra da tarefa de correção

Campo	Descrição
Nome	Nome da regra da tarefa de correção.
Ativo	Indica se a regra da tarefa de correção está ativa.
Descrição	Descrição de texto desta regra de tarefa de correção.
Diferenciação entre maiúsculas e minúsculas	Determina se a correspondência de regra diferencia maiúsculas de minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condições	Condições que devem ser atendidas. Por padrão, (**Distinção entre maiúsculas e minúsculas** caixa de seleção desabilitada), o texto de pesquisa inserido no construtor de condições nos registros e formulários de regras de tarefa de correção não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de grupo.
Agrupar por	
Agrupar resultados de testes de	Automatizar a criação de grupos com base nesta regra. Escolha uma das opções disponíveis. ○ Resultado do teste | Usando campo ○ Resultado do teste->Item de configuração | Tabela | Usando campo Se for estendido **Tabela** se o campo estiver selecionado, os resultados de teste que não usam a tabela estendida correspondente serão agrupados em uma tarefa de correção separada.
Atribuição	
Atribuir grupos de resultados de teste por	Automatizar a atribuição de grupos criados com base nesta regra. Escolha uma das opções disponíveis. ○ Chave do grupo Quando selecionado, um campo Valor de chave é exibido, os campos disponíveis são listados em um menu suspenso. ○ Grupo de usuários Quando selecionado, um campo de pesquisa de grupo de usuários é exibido.

4. Clique em **Enviar**.

Nota: **Limpar grupo por chaves** O link relacionado remove as chaves de grupo da guia Agrupar por no formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Especifique a duração de uma exceção solicitada para uma tarefa de correção

Use as propriedades do sistema para limitar a duração pela qual uma exceção é solicitada para uma tarefa de correção. A correção da tarefa de correção é adiada pelo período especificado.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
. `sn_vulc.exception_max_request_days` a propriedade é usada para especificar o número máximo de dias para os quais uma exceção para uma tarefa de correção pode ser solicitada. O valor padrão é 365 dias.

Nota: Você pode usar `sn_vulc.exception_approval_required` propriedade para desabilitar o fluxo de trabalho de aprovação de exceção para a tarefa de correção se não for necessário. Por padrão, esta propriedade está habilitada e seu valor é `verdadeiro` .

Procedimento

1. Navegar até **Tudo** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Na página Propriedades do sistema, pesquise `sn_vulc.exception_max_request_days` .
3. Clique no nome da propriedade para abrir o registro de propriedade do sistema.
4. Para poder editar este registro, certifique-se de que Conformidade de configurações selecionado como a aplicação atual.
5. Insira um positivo **Valor** e clique em **Atualização** .
   O registro é atualizado e salvo.

Configure a Gestão de exceções para Conformidade de configurações

Limitar a duração de uma exceção solicitada e adicionar um questionário à exceção usando o. Conformidade de configurações módulo. Por padrão, uma exceção é solicitada usando ServiceNow® Resposta a vulnerabilidades módulo. Você também pode solicitar uma exceção usando GRC: Gestão de políticas e conformidade integração.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Se Resposta a vulnerabilidades habilitado, você pode limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o GRC: Gestão de políticas e conformidade o módulo está instalado, você pode selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite que você solicite uma exceção que especifica o objetivo de Política e controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que levantou a exceção ou a solicitação de falso positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador da exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Resposta a vulnerabilidades

  Nota: A partir de 22,0 de Resposta a vulnerabilidades, você pode configurar o questionário para solicitações de falso positivo para Resposta a vulnerabilidades opção também.

- GRC: Gestão de políticas e conformidade

  Nota: Você deve ativar o. GRC plug-in a ser usado GRC: Gestão de políticas e conformidade para solicitar uma exceção.

Nota: Mudar a configuração não afeta os dados existentes.

3. Preencha os campos no formulário.

Formulário Gestão de exceções de CC

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para uma solicitação falso-positivo é exibido por padrão.

4. Selecione **Save** (Salvar).

Adicione um aprovador de exceção para Conformidade de configurações

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção para uma tarefa de correção em Conformidade de configurações.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Uma solicitação de exceção para uma tarefa de correção é aprovada usando o fluxo de trabalho de aprovação de dois níveis padrão. Adicionar usuários ao grupo de primeiro nível é obrigatório. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada.

Nota: Até Conformidade de configurações v13.0, se não houver aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir de Conformidade de configurações V13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho.

Procedimento

1. Navegar até **Tudo** > **Segurança do sistema** > **Usuários e Grupos** > **Grupos**.
2. Na coluna Nome, pesquise **Exceção** e clique em **Aprovador de exceção - CC de nível 1** .

   Nota: A partir de Conformidade de configurações V14.7.5, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio de fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Tudo** > **Propriedades do sistema** e selecione `sn_vulc.exception_approver_L1_CC`ou `sn_vulc.exception_approver_L2_CC`para mudar o valor da propriedade.

3. No formulário Aprovador de exceção de grupo - CC de nível 1, navegue até **Membros do Grupo** > **Novo(a)** (ou **Editar**).
4. No formulário, preencha os campos.

Formulário de usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário da instância e encerrar todas as sessões ativas do usuário. O sistema impede que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Listas de usuários ○ Lista de seleção em campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário do local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...** .

5. Clique em **Enviar**.
6. **Opcional:** Repita as etapas 1 a 5 para criar um Aprovador de exceção - CC de nível 2.

   Nota: Ao criar um aprovador de segundo nível, selecione **Aprovador de exceção - CC de nível 2**

7. **Opcional:** Se você selecionar **Editar** mover usuários do **Coleção** para **Membros do grupo** e clique **Salvar** .
   O aprovador deve navegar até **Tudo** > **Conformidade de configurações** > **Minhas aprovações** e aprovar solicitações.

Crie um Conformidade de configurações mapa de criticidade

Conformidade de configurações o mapeamento de criticalidade fornece um mapa de transformação para campos de criticalidade de origem de terceiros para campos reconhecíveis em Conformidade de configurações gravidade.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Mapeamento de Criticalidade**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de criticalidade.
Valor de origem	O valor de criticalidade da origem.
Valor de meta	O valor de destino. As opções são: **Crítico** O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. **Alto(a)** O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos críticos da rede. **Moderado** O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. **Baixo(a)** O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor de ICs que estão em maior risco. **Secundário** O problema de configuração associado ao controle é um risco secundário e pode ser ignorado, se necessário.

4. Clique em **Enviar**.

Criar notificações por e-mail

Os administradores de vulnerabilidades podem editar a notificação ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar modelos de e-mail para diferentes tipos de notificações por e-mail. Para obter mais informações sobre como criar modelos de e-mail, consulte Definir Resposta a vulnerabilidades modelos de e-mail.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo** .
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

A partir da v14.11 de Conformidade de configurações, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Espaço do gerente de vulnerabilidade ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Espaço do gerente de vulnerabilidade para os usuários com a função sn_vulc.admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com a função sn_vulc.remediation_owner.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configure regras de aprovação para Gestão de exceções em Conformidade de configurações

Use o designer de fluxo para aprovar solicitações de exceção para gestão de exceções e regras de exceção. Se você estiver implantando Conformidade de configurações pela primeira vez, o flow designer é habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O valor da propriedade do sistema *sn_vulc.flow_designer_activation*definido como verdadeiro. Isso significa que o Flow Designer é ativado por padrão.

Nota: Você não pode reverter para usar o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer em Conformidade de configurações.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Regras de aprovação de exceção para tarefa de correção
- Regra de aprovação para regras de exceção automática

Nota: Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Crie níveis de aprovação para Gestão de exceções em Conformidade de configurações.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de aprovação** > **Regras de aprovação de exceção para Tarefa de correção**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	O valor padrão é Conformidade de configurações.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação . (dias)	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias)	Data após a qual o aprovador é notificado para executar uma ação.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Crie configurações para uma regra de aprovação em Conformidade de configurações.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Crie níveis de aprovação para Gestão de exceções em Conformidade de configurações.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para os mesmos resultados de teste encontrados em diferentes tarefas de correção.

Crie configurações para uma regra de aprovação em Conformidade de configurações

Defina as condições para filtrar tarefas de correção correspondentes para um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Nota: Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Crie níveis de aprovação para Gestão de exceções em Conformidade de configurações.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até **Configurações de aprovação** guia.
3. Selecione uma configuração.
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.

5. Defina uma condição para os resultados de teste ou tarefas de correção de uma das seguintes maneiras:

Campo	Descrição
Condição	Identifica os resultados de teste correspondentes ou as tarefas de correção.
Condição avançada	Script que define a condição para os resultados de teste ou tarefas de correção. **Nota:** Este campo aparece quando você seleciona **Avançado** caixa de seleção.

6. Selecione **Atualizar**.
   Você pode definir condições que contenham vários níveis de aprovação em uma regra. O designer de fluxo herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Crie níveis de aprovação para Gestão de exceções em Conformidade de configurações.

Example:
Você pode definir diferentes caminhos de aprovação para diferentes tipos de tarefas de correção.

Crie níveis de aprovação para Gestão de exceções em Conformidade de configurações

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar
Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até **Configurações de aprovação** guia.
3. Selecione uma configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Em **Níveis de aprovador** selecione um nível de aprovador.
5. No formulário, preencha os campos.

Formulário de nível de aprovador

Campo	Descrição
Nome	Nome do nível de aprovação.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ○ Um aprovador necessário ○ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação. Este campo é somente leitura.
Configuração de aprovação	Contém as configurações de aprovação. Este campo é somente leitura.
Atribuir usando	Selecione uma opção de: ○ Usuário e grupo de usuários ○ Campo da tabela de aprovação ○ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções para gestão de exceções e regras de exceção: ○ sn_vulc.exception_approver ○ sn_vulc.read ○ sn_vulc.read_auto_exception_rule
Usuários	Edite os usuários listados nos grupos.

6. Para salvar as mudanças, selecione **Atualização** .

Nota: Antes da v13.0, o processo de fluxo de trabalho é funcional se houver usuários somente no nível de exceção 1. No entanto, a partir da v13.0, deve haver pelo menos um usuário em cada nível.

Antes da v13.0, no fluxo de trabalho, se não houvesse nenhum usuário no segundo nível, a tarefa de correção era adiada. No entanto, a versão 13.0 em diante, se não houver nenhum usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para tarefas de correção para servidores Linux e Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de gestão de exceções versus Flow Designer em Conformidade de configurações

Começando com Conformidade de configurações(CC) v13.0, se você estiver implantando CC pela primeira vez, o designer de fluxo para aprovar solicitações de exceção no gerenciamento de exceções será habilitado por padrão. Se você for um usuário CC existente, a opção padrão será Fluxo de trabalho.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
Versão	V13.0 de CC.	A partir da v13.0 do CC.
Opção padrão	Opção padrão se você for um usuário CC existente.	Opção padrão para novos usuários CC a partir da v13.0.
Definindo o processo de aprovação	A gestão de exceções inclui solicitações de exceção junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. A gestão de exceções inclui solicitações de exceção junto com regras de exceção.
Atualizando para o Flow Designer	Você pode fazer upgrade para o Flow Designer a partir do fluxo de trabalho. No entanto, as solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	O Flow Designer está habilitado por padrão.
Propriedade do sistema `sn_vulc.flow_designer_activation`	Se você estiver usando o fluxo de trabalho para gestão de exceções antes da v13.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usar o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando CC pela primeira vez para v13.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o. **Habilitar regras de aprovação do módulo** o trabalho agendado é executado em 24 horas. Este trabalho agendado habilita **Regras de aprovação** módulo. Para ativar este módulo instantaneamente, execute este trabalho manualmente.	Se você implantou o CC pela primeira vez do CC v13.0, este módulo estará disponível por padrão.
Níveis de aprovação	Fornece a opção de definir somente dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
		aprovador e adicionar aprovadores dinamicamente para cada regra.

Integrações do Conformidade de configurações

Integrações de terceiros importam descobertas de avaliação de configuração, políticas, testes, tecnologias, fontes autorizadas, resultados de teste junto com outros dados de vulnerabilidade no Conformidade de configurações aplicação.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

. Conformidade de configurações a aplicação oferece suporte às seguintes integrações de terceiros:

- A partir da v14.11, promova a correção de lacunas de segurança em seus ativos empresariais identificados pela aplicação Controle de postura de segurança publicando descobertas como resultados de teste no Conformidade de configurações aplicação. A aplicação Controle de postura de segurança e suas aplicações compatíveis estão disponíveis com assinaturas separadas do ServiceNow® Store. Para obter mais informações, consulte Controle de posturas de segurança.
- Microsoft Defender for Cloud Integration para Operações de segurança
- Palo Alto Prisma Cloud Vulnerability Integration
- Qualys integração com Conformidade de configurações
- . Tenable.io produto do Integração de vulnerabilidades do Tenable

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 de Conformidade de configurações carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Microsoft Defender for Cloud Integration para Operações de segurança

. Microsoft Defender for Cloud Integration o produto é um sistema de gestão de segurança de infraestrutura que aprimora a postura de segurança de seus ambientes em nuvem.

Microsoft Defender for Cloud Integrationpara Operações de segurançaintegra-se ao Conformidade de configurações Aplicação para mapear testes para itens de configuração (ICs) para criar resultados de teste. Ele descobre continuamente novos recursos de nuvem implantados em cargas de trabalho e determina se eles estão configurados de acordo com padrões de segurança, como o Centro de Segurança na Internet (CIS).

A partir da versão 2,2, a Central de segurança do Microsoft Azure é renomeada para Microsoft Defender for Cloud Integration para Operações de segurança.

Versões disponíveis

Aplicação	Versão
Microsoft Defender for Cloud Integration para Operações de segurança	2,3
Conformidade de configurações	14.3
Security Support Common	13.2
Resposta a vulnerabilidades	16,2

Várias implantações do Microsoft Defender for CloudPlataforma

Se você tiver várias implantações do Microsoft Defender for CloudAplicação da plataforma, você pode adicionar uma integração para cada implantação. Os recursos identificados por várias implantações de terceiros são consolidados e reconciliados com seu Configuration Management Database (CMDB). Essa consolidação ocorre mesmo quando os processos de verificação se sobrepõem entre as várias implantações.

ServiceNow Microsoft Defender for Cloud Integrações

. Microsoft Defender for Cloud Integrationpara Operações de segurança aprimora os dados de conformidade em sua instância recuperando dados de Microsoft Defender for Cloud. Uma série de trabalhos agendados invoca as integrações automaticamente. Você também pode executar esses trabalhos agendados manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção dos resultados de teste mantendo a instância sincronizada com Microsoft Defender for Cloud.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há um usuário de execução configurado para cada registro de integração, com o valor padrão **VR.System** . Este valor deve permanecer o mesmo.

Nota: Se você não definir um usuário run-as válido, serão criados anexos duplicados ou vários anexos de recuperação de dados para os registros da fonte de dados. O número de anexos aumenta cada vez que a integração é executada. Isso aumenta o tempo de processamento, resultando em resultados de transformação inconsistentes.

Microsoft Defender for Cloud As tarefas de integração da plataforma envolvem as seguintes funções.

- sn_vul_asc.configure_integration: Capacidade de ler, gravar e excluir registros.
- sn_vul_asc.read_integration: Capacidade de ler registros.

Exibindo o. Microsoft Defender for CloudIntegrações

Navegue até **Tudo** > **Integração com Microsoft Defender para Nuvem** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Integração	Descrição
Integração de definição de política	Recupera políticas e cria entradas de política em sua instância.
Integração de metadados de avaliação	Recupera metadados de avaliação e cria testes em sua instância.
Integração de padrões e controles de conformidade	Recupera padrões e controles e cria a fonte de autorização e as citações. Em seguida, ele os vincula aos testes criados.
Integração de avaliação	Recupera avaliações e as processa em sua instância. A saída desta integração é resultados de testes.

Crie ICs usando o Mecanismo de identificação e reconciliação

Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs, quando um IC existente não puder ser correspondido a um host importado de um scanner de terceiros.

Se um IC não for correspondido no CMDB, um IC será criado no *cmdb_ci_cmp_resource*classe. Mais tarde, quando uma descoberta encontra o mesmo IC, ela enriquece o IC ou cria outro.

Nota: A reconciliação automática não acontece para recursos de nuvem.

Instalar e configurar Microsoft Defender for Cloud Integration para Operações de segurança

Instale e configure o. Microsoft Defender for Cloud Integration para Operações de segurança, para que você possa usar os dados importados de Microsoft Defender for Cloudpriorizar e corrigir quaisquer configurações incorretas em seus ativos.

Antes de Iniciar
Crie um novo registro de aplicativo no Azure Active Directory para Microsoft Defender for Cloud Integration. Para obter mais informações sobre como registrar uma nova aplicação no Azure Active Directory, consulte Documentação do produto Microsoft site. Para obter mais informações sobre as funções do Azure, consulte Funções do Azure .

Função necessária: sn_vulc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise Microsoft Defender for Cloud Integration para Operações de segurança .
3. Selecione **Instalar**.

   Todas as dependências que serão instaladas serão exibidas.
4. Navegar até **Tudo** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Configuração** > **Configuração do Microsoft Defender para Nuvem**.
5. No formulário, preencha os campos.

Microsoft Defender for Cloud Formulário de configuração

Campo	Descrição
URL da API	URL do recurso da instância. Exemplo: https://management.azure.com (Nuvem pública do Azure)
ID de locatário	Identidade do locatário da sua organização.
Instância de integração	Instância padrão. Você também pode criar uma instância para trazer os dados de várias Microsoft Defender locatários ou assinaturas.
ID de cliente	Identidade do cliente que é gerada após Microsoft Defender for Cloud Integration a aplicação está registrada.
Segredo do cliente	Segredo do cliente gerado após Microsoft Defender for Cloud Integrationa aplicação está registrada.
Importar descobertas de	Recursos e avaliações que correspondem aos IDs do grupo de gestão selecionados e IDs de assinatura que serão recuperados.
IDs do grupo de gestão	Recursos e avaliações que correspondem aos IDs do grupo de gestão que serão recuperados. **Nota:** Este campo aparece somente quando você seleciona **Grupos de gestão específicos** em **Importar descobertas de** campo.
IDs de Assinatura	Números de identificação das assinaturas para as quais os recursos e as avaliações serão recuperados. **Nota:** Este campo aparece somente quando você seleciona **Assinaturas específicas** em **Importar descobertas de** campo.
Status de validação	Se as credenciais e o ID de assinatura fornecidos são válidos.

6. Configure ou execute as integrações selecionando **Salve e teste** .

Conformidade de configurações dados importados para Microsoft Defender for Cloud Integration

Conformidade de configurações importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Grupos de teste

Um grupo de testes de configuração constitui um grupo de testes. Os grupos de teste estão relacionados a documentos autorizados e registros de teste e podem ser modificados para atender às necessidades da sua organização. Um teste de configuração pode pertencer a vários grupos de teste.

. Microsoft Defender for Cloud Integrationestá instalado, os grupos de teste são recuperados e preenchidos pelo trabalho agendado, **Integração de definições de política** . Você pode exibir o trabalho agendado navegando até **Tudo** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Integrações** > **Integração de definições de política**.

Nota: Se você optar por executar a integração manualmente, execute o. **Integração de definições de política** primeiro.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como os ativos devem ser governados.

. Conformidade de configurações teste é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de resultados de teste.

. Microsoft Defender for Cloud Integration está instalado, o trabalho agendado, **Integração de metadados de avaliação** recupera os testes. Você pode exibir o trabalho agendado navegando até **Integração** > **Integrações Primárias** > **Integração de metadados de avaliação**.

Nota: Se você optar por executar a integração manualmente, execute o. **Integração de metadados de avaliação** após **Integração de definições de política** .

A partir da v15.0 de Conformidade de configurações, o grupo de testes ao qual um teste pertence é preenchido no **Grupos de teste** Coluna da lista de testes.

Fontes autorizadas

Conformidade de configurações usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente são mapeadas para seções de padrões publicados do setor, como **ISO 27001** e. **PCI DSS 3.2.1** .

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas na área de segurança de computadores. Eles definem requisitos para políticas e procedimentos de segurança.

. Microsoft Defender for Cloud Integration está instalado, o trabalho agendado, **Controles e padrões de conformidade** recupera as fontes autorizadas e as citações. Você pode exibir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

este trabalho agendado navegando até **Tudo** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Integração de padrões e controles de conformidade**.

Nota: Se você optar por executar a integração manualmente, execute o. **Integração de padrões e controles de conformidade** após **Integração de metadados de avaliação** .

Ativos

. **Integração de avaliação** fornece informações vitais, como marcadores de recursos e atributos de nuvem. Essas informações são exibidas no formulário Item descoberto. #Ele é usado principalmente para filtragem em Conformidade de configurações Regras de tarefa de atribuição e correção.

- Marcadores de recurso: Todos os marcadores de recursos de nuvem são importados como marcadores de host como parte do **Integração de avaliação** . Os marcadores de nuvem para qualquer tipo de recurso de nuvem são armazenados aqui, independentemente de o recurso ser um host ou não.
  - O armazenamento de marcador não diferencia maiúsculas de minúsculas. Se um##marcador Tokyo for criado, um **TÓQUIO** #O marcador não pode ser armazenado na tabela de marcadores do host. **Tóquio** e. **TÓQUIO** são considerados o mesmo marcador de host. O marcador que foi importado pela primeira vez vence.
  - Usar marcadores de host como uma chave de grupo em uma regra de grupo pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Atributos de nuvem para ativos: A seguir estão os atributos de nuvem dos quais as integrações recuperam Microsoft Defender for Cloud:
  - Conta de nuvem
  - Região da nuvem
  - Tipo de Recurso de Nuvem
  - Provedor de serviço de nuvem

Resultados de testes

Conformidade de configurações não calcula os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando eles estiverem visíveis em Conformidade de configurações, eles são corrigidos usando **Tarefas de correção** .

. Microsoft Defender for Clouda integração está instalada, o trabalho agendado, **Integração de avaliação** recupera os resultados do teste. Você pode exibir este trabalho agendado navegando até **Tudo** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Integração de avaliação**.

. **Integração de avaliação** a importação é a única integração que usa `Start Time`parâmetro no **Detalhes da integração** guia. Todos os outros Conformidade de configurações as importações trazem todos os dados disponíveis, independentemente de `Start Time`.

. **Integração de avaliação** a importação está concluída, um evento é iniciado para acionar cálculos de fim de importação.

. **Integração de avaliação** extrai as avaliações de dados somente se houver uma mudança de status da última execução de integração bem-sucedida no último dia por padrão. Portanto, se a avaliação falhar continuamente nos últimos dias, a integração não buscará a avaliação, pois não há mudança de status para a avaliação. Para manter os resultados do teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atualizados com as avaliações do defensor, um novo **Integração de avaliação abrangente** adicionado, extrai os dados dos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados de testes, que não foram aprovados.

Regras de pesquisa de IC para identificar ICs de Microsoft Defender for Cloudintegrações

Quando os dados são importados de uma integração de terceiros, Conformidade de configurações usa automaticamente dados de recursos para pesquisar correspondências no Configuration Management Database (CMDB) Usando Regras de pesquisa de IC. Essas regras são usadas para identificar os itens de configuração (ICs) e adicioná-los ao registro do resultado do teste para ajudar na correção. As regras de pesquisa de IC do sistema de base estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre regras de pesquisa de IC, consulte Regras de bloqueio de IC para Microsoft Defender for Cloud Integration para Operações de segurança .

Noções básicas do Vulnerability Response Integration with Palo Alto Prisma Cloud

Prisma Cloud é uma solução de segurança de infraestrutura em nuvem baseada em API. Ele se conecta ao seu ambiente de nuvem e monitora os recursos implantados nos ambientes de nuvem pública, como Amazon Web Services(AWS), Microsoft Azure e assim por diante. Você obtém visibilidade e controle completos sobre os riscos em sua infraestrutura de nuvem pública.

. Vulnerability Response Integration with Palo Alto Prisma Cloud A aplicação facilita a ingestão de políticas e alertas do Prisma Cloud, como testes e resultados de testes, respectivamente, no Conformidade de configurações aplicação. Com a configuração correta, os resultados do teste podem ser gerenciados perfeitamente, atribuindo pontuações de risco apropriadas e agrupando-as e atribuindo-as a usuários e grupos relevantes.

Versões disponíveis

A tabela lista as aplicações que Vulnerability Response Integration with Palo Alto Prisma Cloud depende de, junto com a versão da aplicação.

Aplicação	Versão
Integração do Prisma Cloud para Operações de segurança	2,3
Conformidade de configurações	14.7
Security Support Common	13,5
Resposta a vulnerabilidades	18,0

ServiceNow Prisma Cloud Integrações

. Vulnerability Response Integration with Palo Alto Prisma Cloud A aplicação ajuda a importar os dados do Prisma para seu ServiceNow instância para enriquecer sua instância e melhorar o gerenciamento. Uma série de trabalhos agendados invocam as integrações automaticamente. Você também pode executar esses trabalhos agendados manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção dos resultados de teste, mantendo a instância atualizada recuperando dados periodicamente do Prisma Cloud.

As tarefas de integração do Prisma Cloud envolvem as seguintes funções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_prismacload.configure_integration: Capacidade de ler, gravar e excluir registros.
- sn_vul_prismacloud.read_integration: Capacidade de ler registros.

Exibindo as integrações

Você pode exibir as integrações que fazem parte do Vulnerability Response Integration with Palo Alto Prisma Cloud navegando até **Integração na nuvem do Prisma** > **Integrações**.

As integrações a seguir estão disponíveis no sistema de base.

Sequência de execução	Agendamento	Integração	Descrição
1	Semanalmente	Integração de política do Prisma	• Recupera políticas do Prisma Cloud e cria entradas de teste em sua instância. • Ele não fornece suporte incremental. Se você executar a integração nos últimos 10 dias, ele também mostrará o resultado das execuções de integração anteriores.
2	Diariamente	Integração de Alertas Prisma	• Recupera alertas do Prisma Cloud e cria entradas de resultados de teste em sua instância. • Fornece suporte incremental. A integração é executada diariamente após o último tempo de execução da integração.

Preparando para instalar o. Vulnerability Response Integration with Palo Alto Prisma Cloud

Prepare-se para instalar o. Vulnerability Response Integration with Palo Alto Prisma Cloud executando tarefas de configuração.

Antes de começar

Para integrar o Vulnerability Response ao Palo Alto Prisma Cloud, você deve receber um grupo de permissão no Prisma que forneça acesso somente leitura aos dados de política e alertas. Você pode encontrar mais informações sobre grupos de permissão em Funções de administrador do Prisma Cloud .

Para obter informações detalhadas sobre as funções atribuídas a diferentes grupos de permissão, consulte a página Permissões de administrador do Prisma Cloud .

Chaves de acesso devem ser criadas para permitir a leitura dos alertas. Para obter mais informações sobre como criar chaves de acesso, consulte Criar e gerenciar chaves de acesso .

Para instalar e configurar o. Vulnerability Response Integration with Palo Alto Prisma Cloud, use a seguinte check-list. Antes de instalar a aplicação, verifique se os itens listados estão concluídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL de base da API • ID da chave de acesso • Chave secreta • Nome de usuário e senha para acessar o Prisma Cloud. Essas credenciais são usadas para se conectar à instância do Prisma Cloud do ServiceNow AI Platform® instância. O ID da chave de acesso e a chave secreta devem ser gerados no portal Prisma Cloud após o registro.
☐	Se ainda não estiver instalado e ativado, instale o. Resposta a vulnerabilidades antes de instalar o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte Instalar Resposta a vulnerabilidades. Esta integração requer a versão 15.2.0 de Resposta a vulnerabilidades ou posterior.
☐	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação para seu ServiceNow AI Platform® instância. Consulte .
☐	Certifique-se de ter instalado os seguintes plug-ins para uma execução de integração suave: • Resposta a vulnerabilidades • Conformidade de configurações • Vulnerability Response Integration with Palo Alto Prisma Cloud Os plug-ins a seguir são opcionais, mas podem ser úteis: • Cloud Provisioning and Governance • Padrões de descoberta e mapeamento de serviços
☐	Estime o número de resultados de teste que você espera importar. Verifique se sua instância pode aceitar o número de resultados de teste que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com ServiceNow Suporte técnico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem um administrador para gerenciar as integrações e corrigir os resultados do teste: O administrador instala o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções.

Você está pronto para Instale e configure o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação.

Instale e configure o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação

Instale o. Vulnerability Response Integration with Palo Alto Prisma Cloud Aplicação para usar os dados importados do Prisma Cloud. Use esses dados para priorizar e corrigir configurações incorretas em seus ativos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud .
3. Clique em **Instalar**.

   Todas as dependências que serão instaladas serão exibidas.
4. Navegar até **Tudo** > **Integração na nuvem do Prisma** > **Administração** > **Configuração** > **Configuração do Prisma Cloud**.
5. No formulário, preencha os campos.

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da API	URL para integrar com o Prisma Cloud.
ID da chave de acesso	Chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave depois de fazer login no portal Prisma Cloud.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Chave secreta	Chave privada para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave secreta após fazer login no portal Prisma Cloud.

6. Clique em **Salvar e testar** .

O que Fazer Depois

Depois de concluir a instalação, navegue até **Integração na nuvem do Prisma** > **Configuração** para continuar com a configuração.

Configure o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação

Configure o. Vulnerability Response Integration with Palo Alto Prisma Cloud aplicação. Use os dados importados do Prisma Cloud para priorizar e corrigir configurações incorretas em seus ativos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integração na nuvem do Prisma** > **Configuração**.
2. No formulário, preencha os campos.

Configuração do Prisma Cloud

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da API	URL para integrar com o Prisma Cloud.
ID da chave de acesso	Uma chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave depois de fazer login no portal Prisma Cloud.
Chave secreta	Uma chave privada para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave secreta após fazer login no portal Prisma Cloud.

3. Clique em **Salvar e testar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de concluir a configuração, navegue até **Integração na nuvem do Prisma** > **Integrações** para verificar se a execução da integração foi bem-sucedida.

Verifique Vulnerability Response Integration with Palo Alto Prisma Cloud status da execução da importação

Use Vulnerability Response Integration with Palo Alto Prisma Cloud importe o status da execução para verificar o sucesso das execuções de integração e identificar quaisquer problemas.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 de Conformidade de configurações carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Integração na nuvem do Prisma** > **Integrações**.
2. Clique em **Integração de políticas Prisma** .
3. Clique em **Executar Agora**.
   Quando esta integração é executada, as seguintes tabelas são preenchidas nesta ordem:
   a. sn_vulc_test.list (Testes de configuração)
   b. sn_vulc_auth_src (Fonte autorizada
   c. sn_vulc_citation (citações)
4. Em **Itens** exiba o número de novos testes criados, atualizados e ignorados clicando na execução de integração de vulnerabilidade.

Nota: As políticas são definidas no Prisma Cloud para a instância de nuvem selecionada. A instância é verificada com base nas políticas definidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Integração de Alertas Prisma** .
6. Clique em **Executar Agora**.
   As tabelas a seguir são preenchidas com base na integração:
   - Resultados de testes
   - Itens descobertos: Se os itens de configuração não estiverem disponíveis no sistema, eles serão criados. A classe é sempre Recurso de nuvem. Na página Item descoberto, três novos campos são criados: **Tipo de recurso de nuvem** , **Provedor de serviço em nuvem** e **Categoria do ativo** .

     Em **Itens** clique na execução de integração de vulnerabilidade para exibir o número de novos resultados de testes importados, atualizados e ignorados. . **Itens de configuração** a guia também é preenchida com base no número de resultados de teste criados.

Mapeamento de dados

Os dados do Prisma Cloud são importados no Conformidade de configurações módulo do ServiceNow instância.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Os dados do Prisma Cloud são importados com um nome diferente em Conformidade de configurações conforme mencionado na tabela.

Mapeamento de dados do Prisma Cloud em Conformidade de configuração

Nuvem Prisma	Conformidade de configurações
Política	Testar
Alerta	Resultado do teste
Padrão de conformidade	Fonte autorizada
Seções	Citação
Ativo	Item da Descoberta/Item de configuração (IC)

Testes

Uma política no Prisma Cloud é importada como um teste no Conformidade de configurações. As políticas estão relacionadas a documentos autorizados e registros de teste e podem ser modificadas para atender às necessidades da sua organização. Você pode exibir os testes navegando até **Conformidade de configurações** > **Testes**.

Se **Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud** está instalado, o trabalho de integração, `Prisma Policy Integration`recupera os testes. Você pode exibir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

este trabalho de integração navegando até **Tudo** > **Prisma Cloud Integrações** > **Integração de política do Prisma**.

Resultados de testes

Um alerta no Prisma Cloud é importado como resultado de teste no Conformidade de configurações. Os alertas são corrigidos usando **Tarefas de correção** . Você pode exibir os resultados do teste navegando até **Conformidade de configurações** > **Resultados de testes**.

. Conformidade de configurações importa resultados de teste como parte de uma integração de terceiros. Depois que eles estiverem visíveis no Conformidade de configurações, eles são corrigidos usando tarefas de correção.

Se **Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud** está instalado, o trabalho de integração **Integração de Alerta Prisma** recupera os resultados do teste. Você pode exibir este trabalho de integração navegando até **Tudo** > **Integração na nuvem do Prisma** > **Integrações** > **Integração de Alerta Prisma**.

. **Integração de Alerta Prisma** é um trabalho de integração que é executado diariamente e extrai os resultados do teste com mudança de status após o horário definido em **Hora de início** . **Integração** guia.

Nota: Se você executar o trabalho de integração, **Integração de Alerta Prisma** executá-lo manualmente depois de executar o trabalho de integração, **Integração de política do Prisma** .

. **Integração de Alerta Prisma** conclui a importação dos dados, um evento é iniciado para acionar cálculos de fim de importação. Se o alerta falhar continuamente nos últimos dias, a integração não buscará os alertas, pois não há mudança de status para o alerta. Para manter os dados de resultados de testes atualizados com os alertas do Prisma, um novo trabalho de integração, **Integração abrangente de alertas do Prisma** adicionado, extrai os alertas atualizados nos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados do teste, que não foram aprovados.

Fontes Autorizadas

Conformidade de configurações usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente são mapeadas para seções de padrões publicados do setor, como ISO 27001 e PCI DSS 3,2.1.

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas na área de segurança de computadores. As referências definem requisitos para políticas e procedimentos de segurança. Navegar até **Conformidade de configurações** > **Fontes Autorizadas** para exibir as fontes autorizadas.

Ativos

. Vulnerability Response Integration with Palo Alto Prisma Cloud instalado, o trabalho agendado `Prisma Alerts Integration`Captura as informações relacionadas ao alerta no módulo ou tabela de itens descobertos. Você pode exibir este trabalho agendado navegando até **Integração na nuvem do Prisma** > **Integrações**.

A integração Alertas Prisma importa tipos adicionais de informações, como marcadores de recursos e atributos de nuvem que são armazenados em tabelas. Essas informações são exibidas no formulário Itens descobertos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marcadores do host: Um recurso pode ter vários marcadores. Os marcadores do host estão disponíveis no formato de par de chave-valor. Por exemplo, o sistema operacional é o Windows 10 e a versão do Java é 1,8.
- Atributos de nuvem para ativos: Os seguintes atributos de nuvem estão disponíveis:
  - Conta de nuvem: Fornece o ID da conta da integração. As informações são preenchidas na tabela Contas de nuvem [sn_sec_cmn_cloud_account.LIST].
  - Região da nuvem: Fornece o local onde o recurso foi hospedado. As informações são preenchidas na tabela Regiões de nuvem [sn_sec_cmn_region.LIST].
  - Tipo de recurso de nuvem: Fornece informações sobre o tipo de recurso, como se é uma máquina virtual ou uma instância de banco de dados e assim por diante. As informações são preenchidas a partir da tabela Tipo de recurso de nuvem [sn_sec_cmn_cloud_resource_type.LIST].
  - Provedor de serviço de nuvem: Fornece informações sobre o provedor de serviço de nuvem, seja Amazon Web Services (AWS), Oracle Cloud e assim por diante. As informações são preenchidas a partir da tabela Provedor de serviços em nuvem [sn_sec_cmn_cloud_service_provider.LIST].
  - Grupos de contas na nuvem: Fornece informações sobre os grupos de contas. As informações são preenchidas a partir da tabela Grupos de contas em nuvem [sn_vul_prismacload_account_group.list].

Nota: O atributo Grupos de contas em nuvem está disponível somente para Prisma.

Regras de pesquisa de IC

As regras de pesquisa de IC do sistema de base estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre as regras de pesquisa de IC, consulte Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Operações de segurança e. Palo Alto Prisma Cloud.

Mensagens REST DO Prisma Cloud

As mensagens REST DO Prisma são usadas para fazer chamadas para a Interface de programação de aplicações (API) do Prisma para buscar os dados de conformidade.

As mensagens REST a seguir são enviadas com o sistema de base.

Integrações do Prisma Cloud

Todas as integrações do Prisma Cloud usam o JSON Web Token (JWT) para autenticação e autorização.

Mensagem REST de login do Prisma

Endpoint	Descrição	Método	Corpo da mensagem	Link da documentação da API
/login	Obtém o token JWT para uso em todas as integrações subsequentes.	*POST*	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST do token de atualização do Prisma

Endpoint	Descrição	Método	Corpo da mensagem	Link da documentação da API
/auth_token/extend	Renova automaticamente o token JWT na expiração. A duração padrão da expiração do token é de 60 minutos.	`OBTER`	N/D	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Mensagem REST da Política Prisma

Endpoint	Descrição	Método	Corpo da mensagem	Link da documentação da API
/v2/policy	Recupera todos os dados de política do Prisma.	`OBTER`	N/D	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Mensagem REST do alerta Prisma

Endpoint	Descrição	Método	Corpo da mensagem	Link da documentação da API

/v2/alert	Recupera todos os alertas do Prisma.	`POST`	<pre>{
			"detailed": "false",
			"filters": [
			{
			
			"name": "timeRange.type",
			"operator": "=",
			"value": "ALERT_STATUS_UPDATED"
			}
			],
			"sortBy": [
			"resource.id"
			],
			"pageToken": "",
			"offset": 0,
			"limit": 2000,
			"timeRange": {
			"type": "absolute",
			"value": {
			"startTime": <<Import since at integration level>>,
			"endTime": << Current integration run time>>
			}
			}
			}</pre>
				https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Para integração do Alerta de Compreensão Prisma, os filtros no corpo DA PUBLICAÇÃO acima devem ser substituídos da seguinte forma:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
"filters": [
 {
              "name": "alert.status",
              "operator": "=",
              "value": "open"
           },
           {
              "name": "alert.status",
              "operator": "=",
              "value": "dismissed"
           },
           {
              "name": "alert.status",
              "operator": "=",
              "value": "snoozed"
           },
           {
              "name": "alert.status",
              "operator": "=",
              "value": "pending_resolution"
           },
           {
              "name": "timeRange.type",
              "operator": "=",
              "value": "ALERT_UPDATED"
           }

  ],
```

Qualys integração com Conformidade de configurações

. Qualys A Conformidade de política coleta os dados e os envia automaticamente para Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente como Qualys Integração para Operações de segurança para mapear descobertas de configuração para ICs e serviços de negócios para determinar o impacto e a prioridade de possíveis configurações incorretas.

Se você tiver várias implantações do Qualys Cloud Platform, você pode adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados originados de cada implantação são identificados e disponibilizados em uma única instância do Resposta a vulnerabilidades.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos inativos são desabilitadas por padrão.

Marcadores de host

Todos os marcadores de host são importados como parte do Qualys Integração da lista de hosts. Marcadores de host são usados principalmente para filtragem no Resposta a vulnerabilidades Regras de tarefa de atribuição e correção. Eles são exibidos no formulário Item descoberto.

Nota: . Qualys A integração da Lista de hosts deve ser executada antes da criação das Regras de tarefa de atribuição ou correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Se for um **San Diego** o marcador é criado e, em seguida, um **SAN DIEGO** O marcador não pode ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. O marcador que foi importado pela primeira vez vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags** . Esta propriedade é definida como verdadeira por padrão. Desativar marcadores os desativa em todas as instâncias.

Marcadores de host (também chamados de marcadores de ativo) são usados para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos de host. Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host do Qualys para sua instância em uma base programada.

Associar um teste ao seu grupo de testes

Para preencher o campo Grupo de teste em um formulário de teste, habilite *sn_vulc.add_policy_as_key*propriedade do sistema. Para obter mais informações sobre como um teste é associado a seu grupo de testes, o impacto da habilitação desta propriedade do sistema e os pós-requisitos, consulte KB1644268 artigo.

Aviso: Não é possível desabilitar o. *sn_vulc.add_policy_as_key*uma vez habilitada. Revise a seção Impacto no KB1644268 antes de habilitar esta propriedade do sistema.

Quando você habilita esta propriedade do sistema, após a próxima ingestão, o. **Grupo de teste** O campo é adicionado à tabela Teste e preenche o grupo de testes ao qual um teste pertence. Portanto, você pode facilmente:

- Identifique o grupo de teste ao qual um resultado de teste pertence fazendo referência com pontos de teste para grupo de teste.
- Diferencie registros de teste com o mesmo ID de teste que estão associados a diferentes grupos de teste.

Integração Qualys com ServiceNow® Conformidade de configurações aplicação

. Qualys Vulnerability Integration Já está instalado em seu sistema e suas credenciais de API são diferentes das que você deseja usar para Conformidade de configurações, Vá para Assistente de configuração (em Resposta a vulnerabilidades) e atribua-os a cada um **Qualys PC** integração.

Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o. **Credenciais de API da Qualys** campo em **Detalhes REST da Qualys** guia.

Configure os parâmetros PCRS

A partir da v12.6.3 de Qualys Vulnerability Integration for Security Operations, você pode usar Qualys Integração de host de política de PCRS e Integração de resultados de teste de PCRS da Qualys para importar resultados de teste com novos conjuntos de Qualys APIs. Essas integrações precisam de um URL de gateway para buscar informações Qualys.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Ao instalar o. Qualys Vulnerability Integration for Security Operations para Resposta a vulnerabilidades, você pode configurar **gateway_url** Para as novas integrações DE PCRS em Conformidade de configurações. Para obter mais informações sobre como encontrar o URL de gateway da URL da API, consulte Identifique sua plataforma da Qualys .

O URL do gateway deve ser adicionado em seu ServiceNow instância.

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.

   Nota: Certifique-se de que o escopo em que você está seja Qualys for Security Operations.

2. Abra a instância que é usada pelas integrações DE PCRS.
3. Na guia Parâmetros da instância de integração, adicione o url do gateway para **gateway_url** configuração.

   Nota: A Integração de resultados de teste de PCRS da Qualys depende da Integração do host da política de PCRS da Qualys. Portanto, se você retrodata os resultados do teste de PCRS da Qualys da integração, talvez seja necessário executá-los na mesma ordem novamente.

Componentes instalados com o Qualys Integration for Security Operations

As seguintes funções, trabalhos agendados e tabelas são instalados com o Qualys Integration for Security Operations.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, trabalhos agendados e tabelas instaladas com uma aplicação sejam exibidas. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o Construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **E.** e, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função** , **Trabalho agendado** ou **Tabela** .
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura ao Qualys Vulnerability Integration registros.	
sn_vul_qualys.user	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador de Qualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o. Qualys Vulnerability Integration	sn_vul_qualys.admin

Trabalhos agendados instalado

Trabalho agendado	Descrição
Qualys Políticas de PC	Recupera políticas de Qualys. A saída é armazenada na tabela sn_vulc_policy. A API usada nesta integração não oferece suporte à paginação, portanto, todas as políticas são baixadas em uma única página.
Qualys Detalhe das políticas do PC	Recupera os detalhes completos da política, como tecnologias e seções, por exemplo.
Qualys Controles do PC	Recupera informações de controles de conformidade para diferentes IDs de controle do Qualys.
Qualys Resultados do PC	Recupera registros de postura de conformidade de Qualys. A saída desta integração é Resultados de teste. Por padrão, os detalhes do parâmetro são passados para importar informações do host, datas/horas da última verificação, ID de controle e informações de evidência.
Qualys Resultados abrangentes do PC	Recupera registros de postura de conformidade de Qualys com base na data da última avaliação dos resultados de testes que não foram aprovados. Este trabalho é executado uma vez por semana. A saída desta integração é resultados de testes. Por padrão, os detalhes do parâmetro são passados para importar as informações do host, as datas/horas da última verificação, o ID de controle e as informações de evidência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Qualys Integração do host da política PCRS	Recupera dados do host de Qualys e o processa em sua instância. A saída desta integração é IDs de host de política. . Qualys host dados é importado nesta integração. **Nota:** • Este trabalho agendado aparece somente quando Conformidade de configurações instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. Essas duas integrações serão OOB inativas. Se você ativar qualquer uma dessas integrações, as integrações de resultados do PC serão desativadas. Essas duas integrações são adicionadas com base nas novas APIs de streaming da Qualys.
Qualys Integração de resultados de teste de PCRS	Recupera os resultados do teste para cada ID de host. Esta integração usa o parâmetro Hora de início na guia Detalhes da integração. **Nota:** • Este trabalho agendado aparece somente quando Conformidade de configurações instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. • Se você optar por executar a integração manualmente, execute Qualys Integração de resultados de teste de PCRS após Qualys Políticas de PC, Qualys Detalhe das políticas do PC e. Qualys Integração do host da política PCRS.

Nota: . Qualys Host de política de PCRS e Qualys As integrações de resultados de teste DO PCRS estão inativas por padrão. Essas duas integrações são baseadas nas novas APIs de streaming de Qualys. Se você ativar qualquer uma dessas integrações, a integração de resultados do PC será desativada e vice-versa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instalado

Tabela	Descrição
Qualys Importação de resultado do PC sn_vul_qualys_pc_result_import	Tabela que estende a linha do conjunto de importação. A transformação de mapas de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Id de host de política sn_vul_qualys_policy_host_id	Tabela que armazena o mapeamento entre a Política e o host para o qual esta política foi verificada. Esta tabela é usada no novo Qualys Integração DE PCRS. **Nota:** Esta tabela aparece somente quando Conformidade de configurações instalado.
Qualys Importação de host da política de PCRS sn_vul_qualys_pcrs_policy_host_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete. **Nota:** Esta tabela aparece somente quando Conformidade de configurações instalado.
Qualys Importação de política do PC sn_vul_qualys_pc_policy_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.

Atualize itens de configuração com o identificador de partição de rede para a Integração da Qualys

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão em Resposta a vulnerabilidades Uma maneira de identificar seus ativos é pelo endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (ICs) em seu ambiente podem compartilhar endereços IP, mas têm ids exclusivos de rede e repositório. No entanto, por padrão, esses ativos geralmente são identificados e armazenados como um único IC (IC 1) Durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_ID	Item de configuração
Qualys Vulnerability Integration Integrações de	123.12.12.141	03712	IC 1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_ID	Item de configuração
ativos e vulnerabilidades fixas e abertas			
	123.12.12.141	03713	IC 1

Origem	Endereço IP	REPOSITORY_ID	Item de configuração
Qualys Vulnerability Integration Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para poder identificá-los como ativos distintos. A partir de uma importação de dados nova, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as Integrações Ativos e Vulnerabilidades fixas e abertas para Qualys Vulnerability Integration No Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o Identificador de partição de rede [network_partition_identifier] aos registros de IC existentes de dados importados. ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar seus dados existentes.

A partir da v14.0 de Resposta a vulnerabilidades e v12.1 do Qualys Vulnerability Integration Integração de vulnerabilidades, os modelos de classe de IC do CMDB (1,0.21.) é compatível. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de IRE (Identificação e reconciliação).

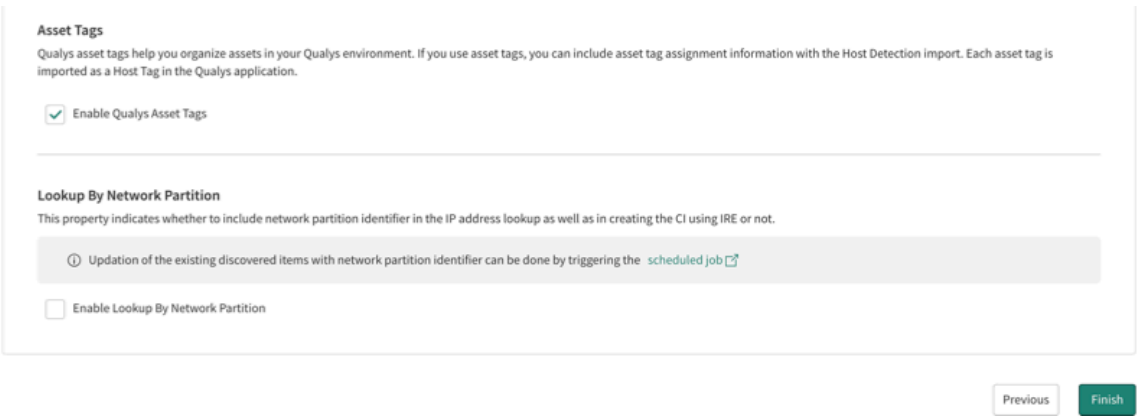
Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. ICs para o seu existente Qualys Vulnerability Integration os dados são criados ou atualizados para incluir a granularidade do identificador da partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são atualizados com os novos ICs.
Aguarde as importações de dados atualizados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Editar** a integração necessária.
4. Escolher **Configuração de detecção do host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITÓRIO _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de endereço IP e de IC de endereço IP incompleto incluem o atributo identificador de partição de rede automaticamente para uma importação de dados das Integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de ativar o trabalho agendado e salvar os registros, você também pode atualizar seus itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos agendados sob demanda. Os ICs no item descoberto existente, item vulnerável e registros de detecção são atualizados automaticamente.

Defina parâmetros de filtro adicionais para Qualys importações

Personalize os parâmetros de filtragem para suas consultas programadas com Qualys Vulnerability Integration para ajudar você a refinar ainda mais os dados de vulnerabilidade importados com o compatível Qualys integrações.

Antes de Iniciar

Casos de uso: Como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você deseja exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou, você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudar você a coletar esses dados, você pode adicionar Qualys parâmetros para ajudá-lo a importar os detalhes específicos da vulnerabilidade de que você precisa.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite personalizar suas informações de solicitação HTTP com Qualys parâmetros em seu ServiceNow AI Platform. Você modifica ou adiciona esses valores no registro do método HTTP no método REST do compatível Qualys integrações do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

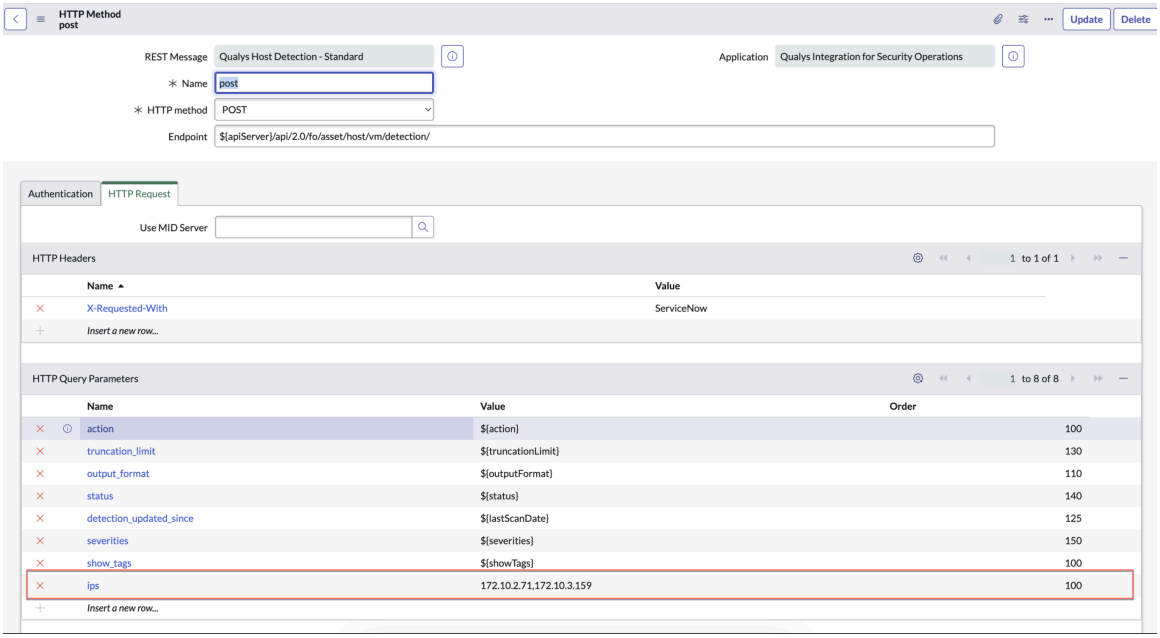
Procedimento

1. Localize os parâmetros compatíveis com Qualys produto no site do desenvolvedor que você deseja usar para filtragem.
   Parâmetros e valores inseridos no Qualys os produtos são compatíveis somente no nível de instância de integração em seu ServiceNow AI Platform. Todos Qualys As integrações oferecem suporte à filtragem usando parâmetros de consulta.
2. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
3. Em Qualys Página de lista de integrações, clique no registro da integração em que você deseja abrir o registro.
4. Com Qualys Guia Detalhes DO REST selecionada, localize e clique no ícone de informações (I) do método REST seguido por **Registro em aberto** Para abrir o registro do método HTTP.
5. Selecione **Solicitação HTTP** guia.
6. Nos Parâmetros de consulta HTTP para o corpo da solicitação, adicione os valores obtidos do Qualys site do desenvolvedor.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços/intervalos IP, *`ips={value}`*foi adicionado. Nesse caso, **valor** É um ou mais IPs/intervalos especificados. Várias entradas são separadas por vírgulas, `172.10.2.71, 172.10.3.159` e um intervalo é especificado com um hífen, `10.10.10.1-10.10.10.100` . Consulte Qualys site do desenvolvedor para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você quiser inserir mais de um parâmetro, consulte Qualys para obter mais informações sobre como separar cada valor.

Nota: Você deve estar ciente dos seus requisitos de API. Pode ser necessário adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

Alguns outros parâmetros que você pode achar úteis no Qualys site do desenvolvedor:

- `ag_ids` - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente as máquinas no seu escopo sejam introduzidas.
- `qids` - Este parâmetro limita os resultados a apenas determinadas vulnerabilidades (QID na tabela de entrada de terceiros). Esta configuração evita inundar seu sistema com registros informativos.

7. Clique em **Atualizar**.

Configurar a granularidade do resultado de teste da Qualys

Configure a granularidade do resultado de teste da Qualys para garantir que o sistema importe resultados em um nível mais detalhado com base nas chaves de configuração selecionadas. Além das chaves padrão, você pode configurar chaves adicionais com base em seus requisitos para aumentar a granularidade. As importações granulares permitem que as equipes gerenciem seus respectivos ativos de forma independente e impedem que os dados sejam substituídos quando vários registros compartilham identificadores comuns.

Antes de Iniciar

Função necessária:

- sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Configurar a granularidade do resultado de teste da Qualys**.

2. No formulário Configuração de chave, confirme que:

- **Integração de origem** . Qualys Cloud Platform .
- **Tabela** está definido como Resultado do teste .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Chave de configuração** escolha o campo para o qual você deseja criar resultados de teste exclusivos. Por exemplo, selecionando `instance` cria resultados de teste exclusivos para cada instância em um banco de dados.

   Nota: Use este recurso com cuidado. Cada chave de configuração adicional aumenta o tempo de integração. Para manter o desempenho ideal, limite o uso a não mais de três teclas extras.

4. Insira *verdadeiro* ao lado de `instance` para habilitar a granularidade, ou *falso* para desabilitá-lo.
5. Selecione **Atualizar** para salvar suas mudanças.

Resolvendo Qualys Problemas de integração de vulnerabilidades

Alguns problemas comumente encontrados, juntamente com soluções alternativas, são discutidos.

Anexos que não aparecem após a importação

Se os anexos não estiverem aparecendo conforme o esperado para fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso de IP podem impedir que anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir anexos em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Os mapas de transformação são fornecidos com configurações básicas e geralmente são suficientes. Você pode modificar mapeamentos de transformação dependendo das necessidades da sua organização.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin e import_admin

Procedimento

1. Navegar até **Tudo** > **Conjuntos para importação do sistema** > **Administração** > **Mapas de transformação** Para exibir as mensagens REST.
2. Filtre a lista resultante por aplicação e limite a lista ao **Integração de vulnerabilidades da Qualys** aplicação.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

   Para obter detalhes sobre os dados fornecidos pela API da Qualys, consulte Documentação da API da Qualys .

Verifique o tamanho da propriedade do anexo XML

Verifica se a propriedade do anexo XML é suficiente para arquivos grandes.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Propriedades do sistema** > **Importação/Exportação**.
2. Role para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.



3. Se necessário, altere o valor para 250 e clique em **Salvar** .

Tópicos relacionados

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados da Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando seu processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection - Padrão/POST** . Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método POST com os seguintes valores:

- Nome: Gravidades
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

A integração da Base de conhecimento da Qualys está falhando

Resolver Qualys Falha na integração da base de conhecimento ao reduzir o tamanho do anexo da carga recebida de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo da carga esteja dentro do limite especificado.
   a. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione **Parâmetros da instância de integração** guia.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys** .
   c. Selecione **Detalhes da integração** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Em **Hora de início** , selecione a data atual para ignorar a execução da execução desse dia.

e. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.

f. Selecione **Parâmetros da instância de integração** guia.

g. Selecione **kb_backfill_full_import** e modificam o valor padrão para verdadeiro.

Resultado

Executar a integração de backpreenchimento da Base de conhecimento da Qualys atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração do Qualys Host Detection cria uma entrada de espaço reservado, a integração de backpreenchimento da Base de conhecimento da Qualys a atualiza.

Qualys gráfico de status de execução de integração

. Qualys O módulo Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

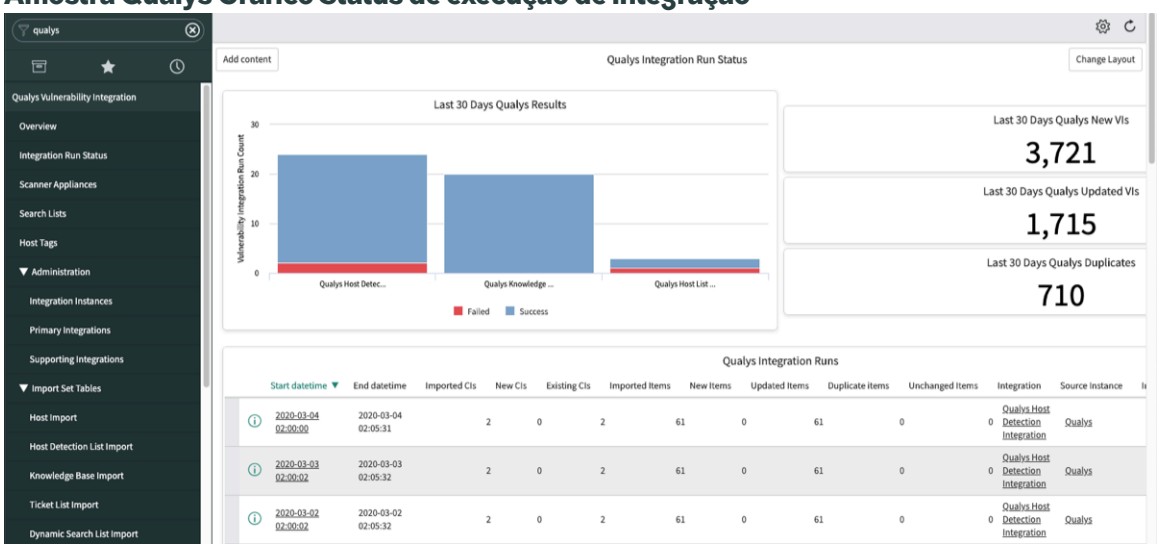
Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

. Qualys Status de execução da integração exibe o status de execução da integração da vulnerabilidade nos últimos 30 dias. A contagem de VIS atualizada da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O VI é atualizado com a nova detecção.

Nota: A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que são definidas como estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Amostra Qualys Gráfico Status de execução de integração



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os valores na coluna Itens importados representam o número total de registros criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos atualizados. Se, por exemplo, um registro é atualizado duas vezes durante a execução da integração, é contado duas vezes e exibido como 2 itens atualizados.
- A coluna Itens inalterados exibe registros encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Nota: A integração é executada com zero resultados para todos os quatro dos seguintes valores: **Novos ICs** , **ICs existentes** , **Novos itens** e **Itens atualizados** são filtrados de **Execuções de integração da Qualys** lista.

Qualys relatórios de gráfico de status de execução de integração

Nome	Descrição
Últimos 30 dias Qualys Resultados	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novo VIS	O número de novos registros importado nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys VIS. Atualizado	O número de registros atualizados importado nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys Duplicatas	O número de registros duplicados importado nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota: V16.1:** Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no `sn_vul_detection`tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Qualys Rendimento de desempenho de	Rendimento diário de ingestão de item vulnerável medido para Qualys Integração de detecção de host nos últimos 30 dias.

Tradução automática

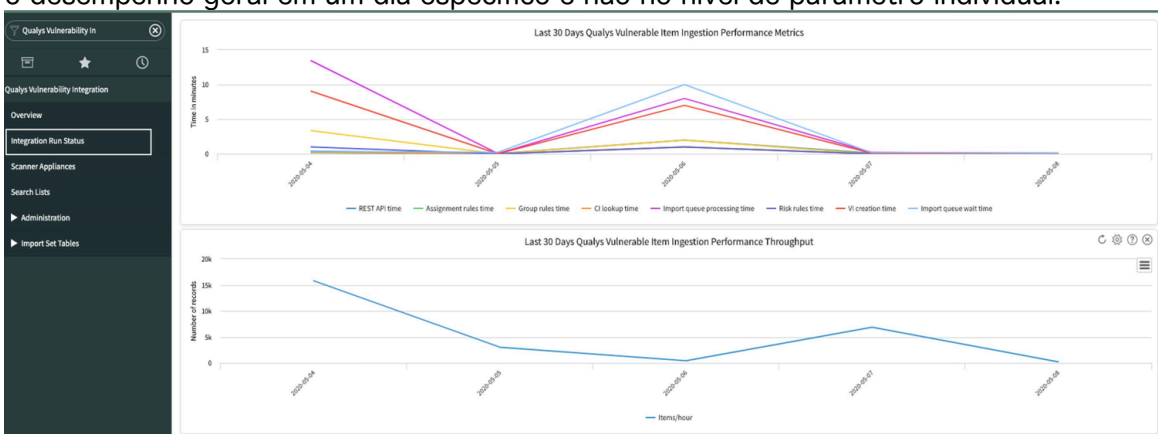
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualys relatórios de gráfico de status de execução de integração

Nome	Descrição
ingestão de item vulnerável	

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

- Qualys Métricas de desempenho de ingestão de item vulnerável: Comparar métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila, e outras estatísticas para itens vulneráveis nos últimos 30 dias, para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo necessário para cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cores para facilitar a identificação.
- Qualys Rendimento de desempenho de ingestão de item vulnerável: Compare o rendimento de ingestão de item vulnerável diário para Qualys Integração de detecção de host. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.



Mensagens REST da Qualys

As mensagens REST da Qualys são usadas para fazer chamadas para a Qualys API para buscar os dados de conformidade.

As mensagens REST a seguir são enviadas com o sistema de base.

Mensagem REST das políticas de PC da Qualys

A mensagem REST de políticas de PC da Qualys recupera dados de política da Qualys. As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações de política.

Parâmetros de mensagem REST das políticas de PC da Qualys

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST das políticas de PC da Qualys

Nome do Parâmetro	Valor	Descrição
detalhes	Tudo	Indica o nível de detalhe mostrado para políticas recuperadas. É seguro para modificar de acordo com sua necessidade.

Mensagem REST dos controles DO PC da Qualys

A mensagem REST de controles do PC da Qualys recupera informações de controles de conformidade para diferentes IDs de controle da Qualys.

O PC da Qualys controla os parâmetros de mensagem REST

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.
detalhes	Tudo	Indica o nível de detalhe mostrado para controles recuperados. É seguro para modificar de acordo com sua necessidade.

Mensagem REST detalhada das políticas de PC da Qualys

A mensagem REST Detalhes das políticas do PC da Qualys recupera os detalhes completos da política, como tecnologias e seções.

Parâmetros de mensagem REST detalhados das políticas de PC da Qualys

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório.
show_user_controls	Booliano	• Defina como 1 para incluir controles definidos pelo usuário (UDCs) na saída XML. • UDCs não especificados não são incluídos. Este é um parâmetro opcional. É seguro para modificar de acordo com sua necessidade.
show_apdency	Booliano	(Opcional) Defina como 1 para mostrar a seção do apêndice na saída XML. Quando não especificado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST DE resultados do PC da Qualys

A mensagem REST de resultados do PC da Qualys recupera registros de postura de conformidade da Qualys.

Parâmetros de mensagem REST DE resultados do PC da Qualys

Campo de origem	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
show_extended_evidence	Booliano	• Defina como 1 para mostrar as informações de evidência estendidas na saída. • Definido como 0 ou quando não especificado, as informações de evidência estendida não são mostradas na saída. **Nota:** • Não é possível especificar `mostrar_extended_evidence: 1` na mesma solicitação que `hide_evidence: 1` . Isso resulta em um erro. A evidência estendida faz parte dos dados de evidência e é mostrada somente quando os dados de evidência são mostrados. • Este parâmetro não é enviado com o sistema de base.
causa_de_falha	Booliano	Se você passar "1", a Qualys retornará a causa da falha. Se você passar "0", a Qualys não retornará esses atributos. **Nota:** Este parâmetro não é enviado com o sistema de base.
policy_id		Mostra registros de informações de postura de conformidade para uma política especificada. Um ID de política válido é necessário.
detalhes	Tudo	Indica o nível de detalhe mostrado para posturas recuperado. É seguro modificar conforme sua exigência.
show_remediation_info		(Opcional) Defina como 1 para mostrar informações de correção na saída XML ou CSV. Por padrão, a saída não inclui as informações de correção. Quando não especificado, as informações de correção não são incluídas na saída.

Mensagem REST DE integração de host da política PCRS da Qualys

A Integração de Host da Política PCRS da Qualys recupera os dados do host da Qualys e os processa em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST DE integração de host da política PCRS da Qualys

Nome do Parâmetro	Valor	Descrição
policyId	(LastRunDatetime)	IDs de política para avaliação de conformidade.

Integração de resultados de testes PCRS da Qualys

A tabela mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST DE integração de resultados de testes PCRS da Qualys

Nome do Parâmetro	Valor	Descrição
Evidência necessária	(LastRunDatetime)	• O valor padrão é 0, o que indica que os dados de evidência não serão recuperados para a postura do host. • Defina o valor como 1 para recuperar os dados de evidência. **Nota:** Mudar o valor para 1 aumenta o tempo necessário para buscar dados de postura.
CompacçãoNecessário		• O valor padrão é 1, o que indica que a saída será compactada. • Defina o valor como 0 se você não quiser que os dados sejam compactados. **Nota:** Não compactar os dados aumenta o tempo necessário para buscar dados de postura.

Noções básicas sobre a Integração de vulnerabilidades do Tenable

. Integração de Resposta a vulnerabilidades com Tenable aplicação desenvolvida por ServiceNow A Engenharia para a Integração de vulnerabilidades do Tenable usa dados importados do Tenable.io, Tenable.sc e Tenable.cs produtos para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. O aplicativo está disponível com uma assinatura separada do ServiceNow® Store.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

A Integração de vulnerabilidades do Tenable emprega três integrações do Tenable, Tenable.io, Tenable.sc e. Tenable.cs, para importar dados do scanner de terceiros sobre seus

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

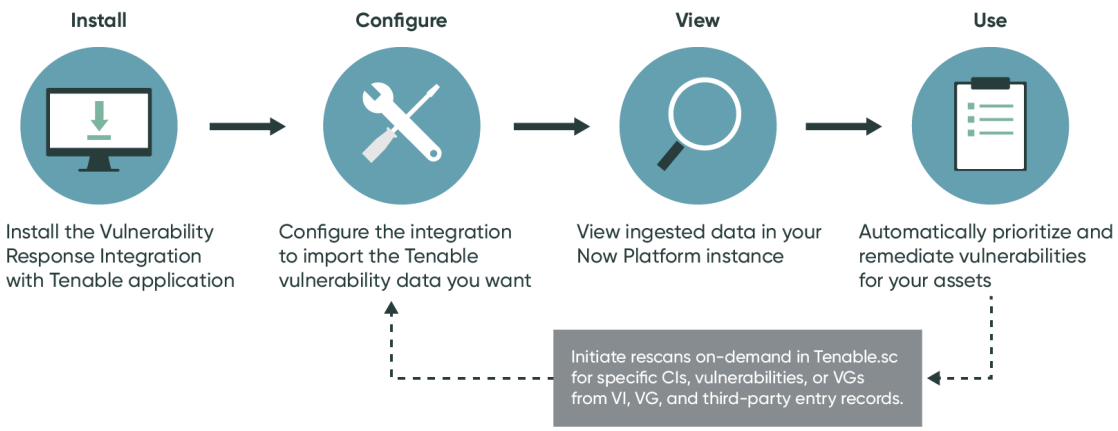
ativos e vulnerabilidades. . Integração de Resposta a vulnerabilidades com Tenable a aplicação oferece suporte ao Tenable.sc produto a partir da versão 5,13 e. Tenable.cs produto a partir da versão 5,0.1.

- Tenable.io é uma integração empresarial baseada em nuvem.
- Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Tenable.sc e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente.
- . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server.
- Tenable.cs é uma integração empresarial baseada em nuvem.

. Integração de Resposta a vulnerabilidades com Tenable a aplicação está disponível no ServiceNow Store com uma assinatura separada.

Para listas e descrições das integrações no Integrações de vulnerabilidade da Tenable, consulte Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações e. Tenable.sc integrações com Resposta a vulnerabilidades aplicação.

Integração com a gestão de vulnerabilidades do Tenable



Versões disponíveis para Zurich

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Tenable v3.13.1, v4.1, v5.0.1	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Principais recursos e termos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em seu ServiceNow AI Platform instância quando:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Uma vulnerabilidade importada de um scanner de terceiros corresponde a um ativo existente (um item de configuração em seu CMDB). O produto Tenable se refere a essas correspondências como **vulnerabilidades** .
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs incompatíveis, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido a um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação.

Entradas de vulnerabilidade de terceiros e plug-ins

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros em seu ServiceNow AI Platform instância. A partir da v24.0 de Resposta a vulnerabilidades, A coluna Softwares na tabela Entradas de vulnerabilidade de terceiros preenche as Enumerações de plataforma comum (CPEs) associadas a um terceiro entrada . Entradas de vulnerabilidade de terceiros do Tenable são ingeridas no Resposta a vulnerabilidades e correspondidos aos ativos existentes listados em seu CMDB. Tenable se refere a entradas de vulnerabilidade de terceiros como **Plug-ins** .

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Item descoberto

Os ativos ingeridos da importação de ativos do Tenable correspondem aos itens de configuração existentes em seu CMDB. Ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in Modelos de classe de IC do CMDB estiver habilitado, o Mecanismo de identificação e reconciliação (IRE) criará ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades Usando o mecanismo de Identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros de item descoberto serão atualizados para refletir o estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados de uma integração de terceiros, o Vulnerability Response usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os Vits são criados para ajudar você na correção.

Nova verificação e correção

Você pode iniciar um comando de nova varredura direcionada em um item de configuração específico, tarefa de correção ou entrada de terceiros diretamente dos registros de item vulnerável, tarefa de correção e entrada de vulnerabilidade de terceiros em seu ServiceNow AI Platform instância. A Tenable se refere a esta nova verificação como um **verificação de correção** .

Fechar automaticamente o VIS mais antigo

Com o módulo Fechar automaticamente itens vulneráveis obsoletos em seu ServiceNow AI Platform, Você pode limpar itens vulneráveis (VI) mais antigos e obsoletos não encontrados recentemente por suas integrações de terceiros. Movendo esses VIS para **Encerrado** ajuda a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração de Resposta a vulnerabilidades com Tenable Para fechar automaticamente o VIS obsoleto.

Instância

Este termo se refere a uma ocorrência distinta do seu ServiceNow AI Platform® aplicação.

Integração

Uma integração é uma referência específica do produto a uma integração, como Tenable.io Integração de ativos ou Tenable.sc Integração de plug-in. Essas são as integrações separadas que pertencem a produtos Tenable específicos na Integração de vulnerabilidades do Tenable em sua instância.

Instância de integração

Este termo se refere às integrações separadas do Tenable listadas por Tenable.io e. Tenable.sc produtos.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação de sua integração. O termo é usado para se referir às integrações e aos produtos em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações do Tenable.io e. Tenable.sc produtos em seu ambiente.

. Tenable.io, Tenable.sc e Tenable.cs as integrações também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas, podem ser importados para o. Conformidade de configurações aplicação com Tenable.io produto. Consulte Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações e. Explorando Conformidade de configurações para obter mais informações sobre como esta integração funciona com Conformidade de configurações aplicação.
- A partir da v2.1 do Integrações de vulnerabilidade da Tenable, Crie itens de configuração (ICs) exclusivos que incluem identificadores de partição de rede diferentes para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todos os Tenable.io, Tenable.sc e. Tenable.cs integrações. Você também pode executar trabalhos agendados manualmente sob demanda.
- Para importações de ativos com Tenable.io, você pode habilitar etiquetas de ativo para organizar e rastrear os ativos listados em seu CMDB em Tenable.io ambiente.
- . Tenable.io, Tenable.sc e. Tenable.cs As integrações permitem que você configure Regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu ServiceNow AI Platform CMDB.
- . Tenable.io, Tenable.sc e. Tenable.cs As integrações permitem que você defina filtros de importação na importação de vulnerabilidades para importar somente as vulnerabilidades desejadas do Tenable. Para Tenable.io, você tem a opção de importar **Corrigido** Vulnerabilidades da Tenable com a importação de vulnerabilidades.
- Para Tenable.sc, você tem a opção de iniciar novas varreduras sob demanda diretamente de um item vulnerável, tarefa de correção e registros de entrada de terceiros em seu ServiceNow AI Platform instância. Se os VIS tiverem sido transferidos para **Encerrado/**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Corrigido mas ainda não foram atualizados em sua instância, você pode verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar uma nova verificação para Tenable.sc integração.

As seções a seguir listam mais detalhes sobre as integrações do Tenable.

Funções necessárias de ServiceNow AI Platform

As tarefas de integração exigem as seguintes funções em seu ServiceNow AI Platform instância.

administrador

O administrador do sistema usa o Assistente de configuração para instalar o. Integração de Resposta a vulnerabilidades com Tenable aplicação. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do Tenable no Assistente de configuração. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações e regras de VR para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Esta função contém a função granular sn_vul_tenable.read_integration e os usuários com esta função podem configurar o. Integração de Resposta a vulnerabilidades com Tenable aplicação.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros do Integração de Resposta a vulnerabilidades com Tenable aplicação.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de tarefa de correção e atribuídos para correção com base em suas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção e Resposta a vulnerabilidades visão geral das regras de atribuição.

Regras de pesquisa de item de configuração (IC)

As regras de pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidades de terceiros.

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

A seguir Tenable.io as regras de pesquisa são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- NetBIOS
- Nome do host
- DNS
- IP

Nota: . Tenable.io As regras de pesquisa de IC priorizam e preenchem os valores de interface de rede não vazios (FDQN, IPV4 e MacAddress) sobre os valores regulares de FDQN, IPV4 e MacAddress para um item descoberto. Quando esses valores de interface de rede estão vazios, os valores regulares de FDQN, IPV4 e MacAddress são preenchidos para um item descoberto.

A seguir Tenable.sc as regras de pesquisa são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Nota: Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando IRE.

. Tenable.cs O ID do recurso em nuvem da regra de pesquisa é enviado com o sistema de base.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, Há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços MAC como parte das regras de pesquisa de IC:

IgnoreIPAddress

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

IgnoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de Item vulnerável do Tenable e das integrações de Ativo do Tenable.

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

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens descobertos.

Etiquetas do ativo

Etiquetas de ativo (também chamadas de marcadores de host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ativos que deseja verificar. O módulo de etiquetas de ativo permite que você baixe dados de etiqueta de ativo do Tenable.io para sua instância em uma base programada. Os dados do ativo que incluem etiquetas de ativo são extraídos de Tenable.io e transformados usando Transformação de ativo do Tenable.io mapas de transformação de integração.

Todas as etiquetas de ativo são importadas como parte do Tenable.io Integração de ativos. As etiquetas de ativo são usadas para filtragem no Resposta a vulnerabilidades Regras de atribuição e Regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Nota: Execute o. Tenable.io Integração de ativos antes de criar Resposta a vulnerabilidades regras de atribuição ou regras de tarefa de correção no Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não diferencia maiúsculas de minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local em San Diego e criar `San Diego` , você também não pode criar um `SAN DIEGO` Marque e armazene-o na tabela Rótulo do ativo. `San Diego` e. `SAN DIEGO` são considerados a mesma etiqueta de ativo pelo sistema. Qualquer marcador importado primeiro é o marcador que será armazenado e reconhecido daqui para frente.
- Usar marcadores de ativo como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas de ativo devem ser usadas somente no Construtor de condições.
- As etiquetas de ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como `verdadeira` por padrão. Desabilitar marcadores os desabilita em todos ServiceNow AI Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para seu ServiceNow AI Platform® instância. Para obter uma lista das configurações mais usadas, consulte Configurações de recuperação de dados para a Integração de vulnerabilidades do Tenable.

Classificação de prioridade de vulnerabilidade (VPR)

A Classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable importado e usado com uma nova calculadora de risco padrão em Resposta a vulnerabilidades. A Regra de Risco do Tenable é instalada com Integração de Resposta a vulnerabilidades com Tenable Aplicação como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidades de Resposta a vulnerabilidades.

Esta regra de risco está inativa por padrão.

Ao habilitar a regra da calculadora de risco do Tenable, os valores de VPR importados são usados para calcular a Pontuação de risco para itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR é 70%, Ativo é 15% e Criticalidade dos negócios é 15%. Habilitar esta regra da Calculadora de risco do Tenable pode afetar o desempenho de ingestão de dados. Para obter mais informações sobre Resposta a vulnerabilidades E a regra da calculadora de risco do Tenable, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Instalação e configuração

Depois de baixar o. Integração de Resposta a vulnerabilidades com Tenable em ServiceNow® Store A instalação e a configuração são compatíveis com o Assistente de configuração em Resposta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a vulnerabilidades. Para obter mais informações, consulte Configurando Resposta a vulnerabilidades Usando o Assistente de configuração.

Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações

. Tenable.io integrações no Integração de Resposta a vulnerabilidades com Tenable as aplicações estão disponíveis no Resposta a vulnerabilidades e. Conformidade de configurações aplicações.

Lista de Tenable.io integrações

O recurso de várias origens é compatível com todos os Tenable.io e. Tenable.sc integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

Tenable.io é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com Tenable.io produto.

. Tenable.io Integração de resultados de conformidade e Tenable.io A integração de preenchimento de resultados de conformidade está inativa por padrão.

Para ativá-los:

1. Navegar até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações do Tenable, clique em um nome de integração para abrir o registro e selecione **Ativo** marque a caixa para habilitá-la. Você pode preferir deixar as configurações de programação nos valores padrão para que essas integrações sejam iniciadas.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados do ativo, incluindo etiquetas do ativo, do Tenable.io e processa-o em sua instância. • A partir da v3.0, se o Tenable.io A Integração de resultados de conformidade está ativada, você pode importar dados de avaliação de configuração segura junto com dados de ativos importados. Esses dados podem ajudar você a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativo. • A saída desta integração é Itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da v3.0, os dados de avaliação de configuração segura importados da Integração de resultados de conformidade junto com os dados importados da Integração de ativos podem ajudar você a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em seu ServiceNow AI Platform instância. Os dados importados incluem resultados de teste junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Os dados de avaliação de ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de teste for importado e seu ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) é listado em **ICs ignorados** . **Configuração** no registro de execução de integração para esta integração.
Tenable.io Integração de preenchimento de resultados de conformidade	• Quando ativada, esta integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com ativos ausentes listados na tabela [sn_vul_tenable_missing_asset]. • Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância depois que a importação de integração de ativos é concluída com sucesso. • Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos aos dados de avaliação de configuração correspondentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de credenciais de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API Credenciais. • A saída desta integração são credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas no ServiceNow AI Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante uma nova verificação. Esta integração recupera disponível Tenable.io credenciais a serem usadas para novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do Tenable.io produto. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por um Tenable.io execução de integração. • Essa importação garante que o Tenable.io Identificadores (dez IDs) são atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base nos filtros de gravidade do Tenable.io e processa-o em sua instância. Itens vulneráveis são criados para registros de detecção que estão no **Aberto** e. **Reaberto** porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **Corrigido** , mas itens vulneráveis não são criados para **Corrigido** Detecções por padrão, porque a Tenable considera **Corrigido** vulnerabilidades **Mitigado** . • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidades fixas** Está ativado no Assistente de configuração, novos VIS são criados no **Corrigido** estado para que você tenha visibilidade das

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	detecções que as criaram. Porque os VIS foram criados para **Corrigido** detecções que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para isso **Corrigido** as detecções atualizam somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. Esta execução de integração está programada. É uma integração encadeada, o que significa que, depois que uma execução é concluída com sucesso, a integração de vulnerabilidades em aberto descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações sobre as execuções de integração de vulnerabilidades: • **Total de blocos:** Número total de blocos gerados pela Tenable • **Blocos disponíveis:** Número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de vulnerabilidades em aberto	• Esta integração é acionada após a conclusão bem-sucedida do Tenable.io Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.io e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Novo/reaberto** Itens vulneráveis (VIS). Ele também cria itens de configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	e entradas de terceiros, se eles não existirem. A Tenable considera vulnerabilidades ativas **Cumulativo** (atual). • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações sobre as execuções de integração de vulnerabilidades: • **Total de blocos:** Número total de blocos gerados pela Tenable • **Blocos disponíveis:** Número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de metadados /scan	Esta integração recupera metadados do endpoint / vars. Extrai informações de verificação com base em last_schedule_id dos dados de ativos existentes em Tenable.io. A integração do endpoint /varns de Tenable.io envolve as seguintes etapas de implementação: • **Criação de tabela** : Uma nova tabela personalizada, **sn_vul_tenable_scan** , é criado para armazenar metadados de verificação recuperados do Tenable.io endpoint /verifica. Isso inclui detalhes como ID de verificação, nome, status, hora de início, hora de término, e tipo de verificação. • **Associação de dados** : Um campo de referência é estabelecido entre os itens descobertos (itens de configuração ou vulnerabilidades) e o registro de verificação mais recente correspondente no **sn_vul_tenable_scan** tabela. Este vínculo permite que você: ◦ Exiba as informações de verificação mais recentes associadas a cada item descoberto. ◦ Melhorar o contexto para triagem de vulnerabilidades e decisões de correção. ◦ Aprimore a auditabilidade e os recursos de emissão de relatórios mantendo um registro histórico das atividades de verificação.

Tenable.sc integrações com Resposta a vulnerabilidades aplicação

. Tenable.sc integrações no Integração de Resposta a vulnerabilidades com Tenable aplicação.

Começando com Resposta a vulnerabilidades V20.0, se um ativo for verificado por um agente, a coluna "Existe agente" na lista de itens descobertos exibirá o valor como "verdadeiro". Indica que a verificação é autêntica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de Tenable.sc integrações

O recurso de várias origens é compatível com todos os Tenable.io e. Tenable.sc integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também pode instalar e configurar o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

- Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Tenable.sc e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente.
- . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativos importados, a Integração de ativos do Tenable.sc o produto é composto por duas integrações. **. Tenable.sc Integração de ativos em aberto** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativo** (atual), ou **Aberto** . Os itens vulneráveis (VIS) que são criados em sua instância com estes dados de ativo importados são considerados abertos, ou seja, em **Aberto** estado. Esses itens vulneráveis exigem investigação e podem precisar de correção. **. Tenable.sc Integração de ativos fixos** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Mitigado** (não está mais vulnerável) ou **Corrigido** . Os itens vulneráveis para esses ativos fazem a transição do **Aberto** estado para **Encerrado/Corrigido** em sua instância, porque os resultados das verificações mostram que elas não estão mais vulneráveis. • Recupera todos os dados de ativos do Tenable.sc e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Ativos. • A saída desta integração é Itens descobertos. • O filtro de consulta do Tenable selecionado no Assistente de configuração também se aplica ao Tenable.sc

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Integração de ativos. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do Tenable.sc produto. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por um Tenable.sc execução de integração. • Essa importação garante que o Tenable.sc Identificadores (dez IDs) são atuais e somente vulnerabilidades ativas são importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base nos filtros de gravidade do Tenable.sc e processa-o em sua instância. Itens vulneráveis são criados para registros de detecção que estão no **Aberto** e. **Reaberto** porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **Corrigido** , mas itens vulneráveis não são criados para **Corrigido** Detecções por padrão, porque a Tenable considera **Corrigido** vulnerabilidades **Mitigado** . • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidades fixas** Está ativado no Assistente de configuração, ele cria VIS no **Corrigido** estado para que você tenha visibilidade das detecções que as criaram. Como os VIS são criados para **Corrigido** detecções que não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para isso **Corrigido** as detecções atualizam somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Esta execução de integração é uma execução programada. É uma integração encadeada, o que significa que depois que uma execução é concluída com sucesso, o. Tenable.sc A Integração de vulnerabilidades em aberto descrita a seguir é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de vulnerabilidades em aberto	• Esta integração é acionada após a conclusão bem-sucedida do Tenable.sc Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados no Tenable.sc e processa-o em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas. • Cria ICs exclusivos para ativos incompatíveis ou atualiza os ICs existentes com o atributo identificador de partição de rede para ativos em todo o ambiente que compartilham endereço IP. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. • A saída desta integração é **Atualizar/criar novo** Itens vulneráveis (VIS) se eles não existirem. Ele também cria itens de configuração e entradas de terceiros, se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de credenciais de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API Credenciais. • A saída desta integração são credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas no ServiceNow AI Platform. • Esta integração está programada para ser executada semanalmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de preenchimento importa todas as vulnerabilidades abertas e corrigidas que possam ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está inativa por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, você pode preferir programar as Integrações de vulnerabilidades fixas e vulnerabilidades abertas do Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é: ○ **Encerrado/Corrigido** Itens vulneráveis (VIS). Ele também cria ativos e entradas de terceiros se eles não existirem. ○ . **Atualizar/criar novo** Itens vulneráveis (VIS) se eles não existirem. Ele também cria itens de configuração e entradas de terceiros, se eles não existirem.

Autenticação de usuário e. Tenable.sc

A autenticação de usuário é compatível com ServiceNow AI Platform® e versão 5,13 do Tenable.sc produto. A autenticação do usuário será necessária se você estiver usando a versão 5,12 e anterior do Tenable.sc produto.

Quando você seleciona a autenticação de usuário para Tenable.sc tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Falha: A validação do token falhou . Nenhuma ação será necessária se esta mensagem for exibida. Tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Tenable.cs integrações com Resposta a vulnerabilidades e. Contêiner de Resposta a vulnerabilidades aplicação

. Tenable.cs integrações no Integração de Resposta a vulnerabilidades com Tenable Estão disponíveis no Vulnerability Response e Contêiner de Resposta a vulnerabilidades aplicações.

A partir da v20.0 Resposta a vulnerabilidades Se um ativo for verificado por um agente, a coluna "Existe agente" na lista Itens descobertos exibirá "Verdadeiro", indicando que a verificação é autêntica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de Tenable.cs integrações

O recurso de várias origens é compatível com todos os Tenable.io, Tenable.sc e Tenable.cs integrações. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Resposta a vulnerabilidades. Você também pode instalar e configurar o. Integração de Resposta a vulnerabilidades com Tenable Aplicação do Assistente de configuração.

Tenable.cs é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com Tenable.cs produto.

Integrações do Tenable.cs

Integração	Descrição
Tenable.cs Integração de ativos de contêiner em nuvem	• Recupera todos os dados de ativos de contêiner do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. Coordena as chamadas de mensagem REST para a API de ativo. A saída desta integração são imagens de contêiner descobertas, imagens do Docker e repositórios de contêiner.
Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta	Quando ativada, esta integração é executada automaticamente depois que a integração de ativos de contêiner é concluída com sucesso como parte de uma execução de integração encadeada. • Recupera dados de vulnerabilidade do contêiner com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Novos/ReopenedContainer Vulnerable Items (CVIS). Se eles não existirem, ele também criará imagens de contêiner descobertas, imagens do docker, repositórios de contêiner, descobertas de imagem, entradas de terceiros, e Vulnerabilidades e exposições comuns (CVE).
Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida	Esta integração é acionada após a conclusão bem-sucedida do Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta. • Recupera dados de vulnerabilidade do contêiner com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes • Coordena as chamadas de mensagem REST para a API Vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.cs

Integração	Descrição
	A saída desta integração é Novos/ReopenedContainer Vulnerable Items (CVIS). Se eles não existirem, ele também criará imagens de contêiner Discover, imagens do docker, repositórios de contêiner, descobertas de imagem, entradas de terceiros, e CVEs. As descobertas de imagem são criadas no estado Encerrado.
Tenable.cs Integração de vulnerabilidades de host na nuvem	• Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Itens vulneráveis novos/ reabertos (VIS). Se eles não existirem, ele também criará itens de configuração, entradas de terceiros e CVEs. Detecções de vulnerabilidades são criadas no estado Aberto.
Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida	Esta integração é acionada após a conclusão bem-sucedida do Tenable.cs Integração de vulnerabilidades de host na nuvem. • Recupera dados de vulnerabilidade com base nos filtros de severidade do Tenable.cs e processa-o em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes. • Coordena as chamadas de mensagem REST para a API Vulnerabilidades. A saída desta integração é Fechar Itens Vulneráveis (VIS). Se eles não existirem, ele também criará itens de configuração, entradas de terceiros e CVEs. Detecções de vulnerabilidades são criadas no estado Encerrado.

Autenticação de usuário e. Tenable.sc

A autenticação de usuário é compatível com ServiceNow AI Platform® e versão 5,13 do Tenable.sc produto. A autenticação do usuário será necessária se você estiver usando a versão 5,12 e anterior do Tenable.sc produto.

Quando você seleciona a autenticação de usuário para Tenable.sc tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Falha: A validação do token falhou . Se esta mensagem for exibida, nenhuma ação será necessária. Tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparando para a Integração de vulnerabilidades do Tenable

Prepare-se para ServiceNow® Integração do Tenable Vulnerability executando as tarefas de configuração a seguir.

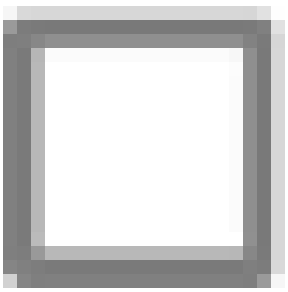
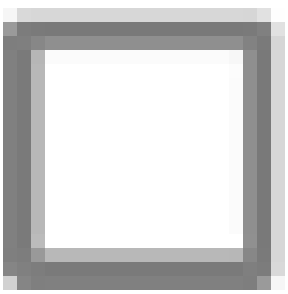
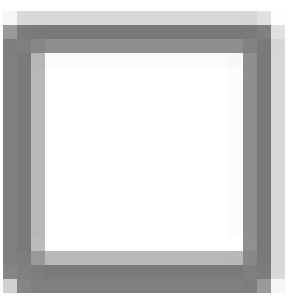
Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa de tarefas de pré-integração. Para uma instalação e configuração suaves do Integração de Resposta a vulnerabilidades com Tenable, você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para seu ServiceNow AI Platform® instância.

Nota: Se você estiver importando dados com a integração criada pelo Tenable e quiser começar a usar o. ServiceNow® Integração de Resposta a vulnerabilidades com a Tenable, consulte

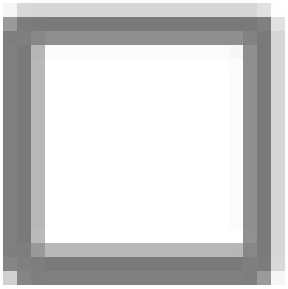
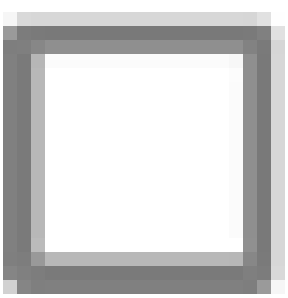
Para obter informações atuais de limpeza e migração de dados da integração criada pelo Tenable para a integração criada por ServiceNow, consulte Diretrizes para migrar da Integração do Tenable Vulnerability Response para a Integração do ServiceNow Vulnerability Response com o Tenable [KB0960106] artigo.

Função necessária: Administrador para baixar e instalar a aplicação.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, você pode preferir instalar o. Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar o. Resposta a vulnerabilidades aplicação, consulte, Instalar Resposta a vulnerabilidades. Esta integração requer a versão 12,1 de Resposta a vulnerabilidades ou posterior.
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe o. Integração de Resposta a vulnerabilidades com Tenable aplicação para seu ServiceNow AI Platform® instância. . Integração de Resposta a vulnerabilidades com Tenable a aplicação oferece suporte ao Tenable.sc produto a partir da versão 5,13 e. Tenable.cs produto a partir da versão 5,0.1. .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou, se precisar de assistência, entre em contato com ServiceNow® Suporte técnico.

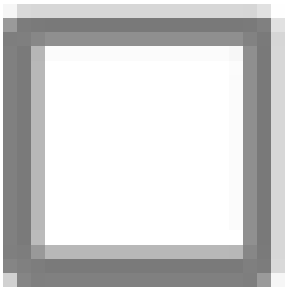
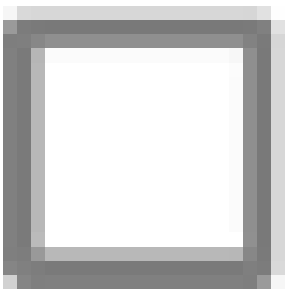
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **administrador** O administrador do sistema usa o Assistente de configuração para instalar o. Integração de Resposta a vulnerabilidades com Tenable aplicação. Se não for atribuído, o administrador atribuirá o administrador da vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Uma vez atribuída, o administrador de vulnerabilidades conclui a configuração das integrações do Tenable. Esta função tem acesso completo ao Resposta a vulnerabilidades(VR) e seus registros. Configura todos os aplicativos e regras de VR e configura integrações de terceiros. **sn_vul_tenable.configure_integration** Pode configurar a Integração de vulnerabilidades do Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration** Pode exibir (ler) registros da Integração de vulnerabilidades do Tenable. **Grupo de Resposta a vulnerabilidades** Por padrão, o grupo Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Crie um grupo de usuários . As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.
	Para promover um desempenho aprimorado para sua primeira importação, você pode preferir desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não usá-las. Essas calculadoras, além de todas as que você definiu, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	• Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, você pode preferir Desabilitar regras de negócios relacionadas a notificações, conforme descrito em Importar modificações para a Integração de vulnerabilidades do Tenable.
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.scÉ uma integração no local que oferece a opção de usar um MID Server se o Integração de Resposta a vulnerabilidades com Tenable e seu ServiceNow AI Platform as instâncias estão no mesmo ambiente. . Tenable.sc e seu ServiceNow AI Platform Não estão no mesmo ambiente, você deve usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . • Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ativa etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.
	Obtenha credenciais do Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos Tenable para que você tenha acesso a eles. Tenable.io Requer acesso de administrador com um atributo de permissão maior ou igual a 64. Tenable.sc Requer acesso de analista de segurança ou gerente. **Nota:** A partir da v3.8 de Integração de Resposta a vulnerabilidades com Tenable acessando Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instale o. Integração de Resposta a vulnerabilidades com Tenable Usando o Assistente de configuração.

Instale o. Integração de Resposta a vulnerabilidades com Tenable Usando o Assistente de configuração

Antes de executar o. ServiceNow® Integração de vulnerabilidades do Tenable, você precisa baixar o. Integração de Resposta a vulnerabilidades com Tenable aplicação do ServiceNow Store E instale e configure-o usando o Assistente de configuração no Resposta a vulnerabilidades aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens da check-list em Preparando para a Integração de vulnerabilidades do Tenable.

Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidades (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar a aplicação no Assistente de configuração depois que ela for instalada.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações que estão disponíveis para instalação em sua instância serão exibidas.

2. Localize **Tenable (plataforma Tenable)** lado a lado e clique **Instalar** .

   Esta ação instala o. Integração de Resposta a vulnerabilidades com Tenable aplicação que você baixou do ServiceNow Store.

3. Siga as instruções fornecidas no Assistente de configuração para continuar com a instalação.

4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades Aplicações de terceiros que usam o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** No Assistente de configuração para continuar com a configuração. Para obter mais informações para complementar os prompts fornecidos no Assistente de configuração, consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração.

Configurações de recuperação de dados para a Integração de vulnerabilidades do Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar do ServiceNow® Integração de vulnerabilidade do Tenable ao seu ServiceNow AI Platform® instância.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Instâncias de Integração** e selecione sua integração, Tenable.io, Tenable.sc ou Tenable.cs.

Na página Instância de integração exibida, selecione os Parâmetros de instância de integração para exibir uma lista de parâmetros ou as guias Integrações de vulnerabilidade para uma programação, Detalhes DO REST, Detalhes DE integração, Fontes de dados e informações de execução de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gravidade comum e configurações de recuperação e filtros para Tenable.io, Tenable.sc e. Tenable.cs em seu ServiceNow AI Platform instância

As configurações a seguir estão disponíveis para Tenable.io, Tenable.sc e Tenable.cs integrações em seu ServiceNow AI Platform instância. Essas e outras definições de configuração são exibidas na página Instância de integração do seu ServiceNow AI Platform instância. Você pode preferir deixar essas configurações em seus padrões nas primeiras execuções de integração.

Tenable.io

insert_fixed

Se você habilitar **insert_fixed** No Assistente de configuração para a integração Importação de vulnerabilidades, novos VIS são criados para detecções no **Corrigido** estado que não existe em sua instância.

severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_high

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de nível médio do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informações do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de baixo nível do Tenable.io Vulnerabilidades em aberto e. Tenable.io Integrações de vulnerabilidades corrigidas.

tamanho

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados do Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1 000. O tamanho máximo é 10 000.

num_assets

O número máximo de vulnerabilidades por bloco exportado do Tenable.io Vulnerabilidades corrigidas e. Tenable.io Integrações de vulnerabilidades em aberto. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pelo Tenable.io Integração de ativos. O padrão é 1 000.

Tenable.sc

async_request

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Uma vez habilitado, este parâmetro é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request ao existente Tenable.sc instâncias de integração. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

insert_fixed

Se você habilitar **insert_fixed** No Assistente de configuração para a integração Importação de vulnerabilidades, novos VIS são criados para detecções no **Corrigido** estado que não existe em sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Os filtros de consulta são configurados no console do Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração em seu ServiceNow AI Platform instância. Esses filtros são aplicados ao recuperar os dados do Tenable.sc integrações.

Tenable.cs

compute_severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_high

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de nível médio do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informações do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

compute_severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade de baixo nível do Tenable.cs Integração de vulnerabilidades de host na nuvem e Tenable.cs Integração de vulnerabilidades de host em nuvem corrigida.

container_severity_critical

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de contêiner de severidade crítica do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_high

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de contêiner de gravidade de alto nível do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_medium

Este filtro está inativo por padrão (falso). Habilite este filtro para receber Vulnerabilidades de contêiner de gravidade de nível médio do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber Vulnerabilidades de gravidade no nível de informações das Vulnerabilidades de contêiner do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

container_severity_low

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de contêiner de gravidade de baixo nível do Tenable.cs Integração de vulnerabilidades de contêiner na nuvem e Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida.

asset_page_limit

Esta configuração define o número de registros de ativos de contêiner a serem incluídos no conjunto de resultados do Tenable.cs Integração de ativos de contêiner em nuvem. O valor padrão é 1 000. O tamanho máximo é 1 000.

vuln_page_limit

Esta configuração define o número de registros de vulnerabilidades a serem incluídos no conjunto de resultados do Tenable.cs Integração de vulnerabilidades de host em nuvem aberta, Tenable.cs Integração de vulnerabilidades de host em nuvem fixa, Tenable.cs Integração de vulnerabilidades de contêiner em nuvem aberta, e. Tenable.cs Integração de vulnerabilidades de contêiner na nuvem corrigida. O valor padrão é 1 000. O tamanho máximo é 10 000.

Mensagens REST para a Integração de vulnerabilidades do Tenable

. ServiceNow® As mensagens REST da Integração de vulnerabilidades do Tenable são usadas para fazer chamadas para a API do Tenable.

Tenable.io Mensagem REST de ativos

. Tenable.io A mensagem REST DE ativos recupera informações de ativos para Tenable.io Integração de ativos. As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tenable.io Mensagem REST de plug-ins

. Tenable.io A mensagem REST DE plug-ins recupera informações de plug-in para Tenable.io Integração de plug-in. As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

. Tenable.io A mensagem REST DE vulnerabilidades recupera informações de vulnerabilidade para vulnerabilidades abertas e encerradas do Tenable.io Integração de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As mudanças no registro do método de mensagem REST afetam as solicitações feitas Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST DE consultas DO Tenable.sc

A mensagem REST Consultas do Tenable.sc recupera as informações do filtro de consulta da integração de ativos do Tenable.sc e da integração de vulnerabilidades do Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

. Tenable.sc A mensagem REST do plug-in recupera informações de plug-in para Tenable.sc Integração de plug-ins. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas Tenable.sc para recuperar informações de plug-ins.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado pelo código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore,TemporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, nome, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, família, riskfator, cpe, veeTambém, solução, exploitAvailable, exploitFrameworks, tipo, copyright, versão, sourceFile, dependências, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Indica a lista de campos importados da Tenable.

Tenable.sc Mensagem REST de vulnerabilidades

. Tenable.sc A mensagem REST DE vulnerabilidades recupera informações de vulnerabilidade do Tenable.sc Integração. Mudanças no método Buscar vulnerabilidades ou Buscar vulnerabilidades com patch da mensagem REST ou, começando com v14.0 Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable, o registro Buscar vulnerabilidades de preenchimento afetam as solicitações feitas Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Verificar mensagem REST de credenciais

Tenable.sc Mensagem REST da política

. Tenable.sc A mensagem REST POST DA política adiciona uma política para plug-ins solicitados. A política gerada é usada em Tenable.sc solicitações de verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.sc Verificar mensagem REST

A mensagem REST POST DA verificação do Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tenable.sc Mensagem REST do resultado da verificação

. Tenable.sc OBTER mensagem REST do resultado da verificação fornece detalhes da verificação gerada usando a mensagem REST DA verificação. Ele usa o scanResultId na resposta das mensagens REST da verificação e recupera os detalhes da verificação para a verificação acionada.

Tenable.sc Verificar credenciais

. Tenable.sc A mensagem REST DE credenciais de verificação recupera as informações de credenciais do Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	id,nome,descrição,tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis do Tenable.sc Mudanças em qualquer um dos parâmetros não são recomendadas.

Tenable.cs GraphQl mensagem REST: O. Tenable.cs A mensagem REST do GraphQl recupera informações de ativos do contêiner, host e informações de vulnerabilidade do contêiner para Tenable.cs Integração. As mudanças no registro Obter ativos do contêiner da mensagem REST, Buscar vulnerabilidades do contêiner, Buscar vulnerabilidades do método de computação afetam as solicitações feitas Tenable.cs para recuperar informações de ativos e vulnerabilidades.

Transformação de dados para a Integração de vulnerabilidades do Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de gravidade normalizados são instalados no módulo Mapeamento de gravidade normalizado. Esses mapas transformam os níveis de severidade importados do Tenable em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de gravidade, consulte Criar um mapa de gravidade de resposta a vulnerabilidades em Resposta a vulnerabilidades documentação.

Importação de ativos do Tenable.io

Os dados de ativos importados são carregados primeiro na tabela Importação de ativos do Tenable.io [sn_vul_Tenable_io_asset_import].

O mapa de transformação de integração de ativos do Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de Ativo do Tenable são processados. Para acessar este mapa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar `Transformação de ativo do Tenable.io` .

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos de mapa de transformação de ativo do Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e mapeia para o registro do item descoberto e é usada para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor ip para o campo ip_address no registro do item descoberto.
u_mac_addresses	mac_address	Mapeia o primeiro valor mac_address para o campo de endereço mac no registro do item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor de fqdn para o campo fqdn no registro do item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netbios para o campo netbios no registro do item descoberto.
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo SO no registro do item descoberto.
(Anterior à v14.0 Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable) u_last_scan_time	last_scan_date	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação de ativos do Tenable.io

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores no host e verifica se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados.Este script é para uso interno e não é recomendável modificá-los ou excluí-los.

Integração de plug-ins do Tenable.io

O mapa de transformação de plug-ins do Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins do Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE a transformação do plug-in Tenable.io.

A carga útil dos plug-ins do Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plug-in_import. O campo Atributos é analisado e mapeado para os registros da tabela de entrada de terceiros conforme listado na tabela a seguir.

Campo de origem	Campo de destino	Descrição
id	id	Mapeia o ID da origem e adiciona o prefixo DEZ a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será DEZ-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	A origem da entrada de terceiros importada (TPE) é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família de plug-in para a coluna de categoria
plug-in_modified_date	last_modified	Mapeia plug-in_modified_date para o último campo modificado.
plug-in_publication_date	date_published	Mapeia plug-in_publication_date para a data de publicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
has_patch	remediation_type	Mapeia o tipo de correção do valor has_patch.
sinopse	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__score	pontuação	Mapeia a pontuação base do CVSS (Common Vulnerability Score System, sistema de pontuação comum) para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
exploit_available	exploração	Mapeia exploit_available fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9–10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		para threat_intensity na tabela de entrada de terceiros.
vpr.drivers.ameaça_recency	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
cvss_temporal_score	cvss_temporal_score	Mapeia a pontuação temporal do CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mapeia a pontuação temporal do CVSS v3.
risk_factor	source_severity	Mapeia para a gravidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para nomear na tabela de entrada de terceiros.
stig_severity	stig_severity	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.

Tradução automática

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se as mesmas Vulnerabilidades e exposições comuns (CVE) na tabela de entrada de NVD (sn_vul_nvd_entry) forem encontradas, ele associará a vulnerabilidade atual à entrada NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
lance	A lista de bugs traqs é adicionada como referência.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
see_also	A lista de URLs é adicionada como referência.
refsCruzadas	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores na entrada de terceiros e verifica se a entrada de terceiros existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele pega a saída da integração de plug-ins do Tenable.io e a transforma em ServiceNow AI Platform entradas de vulnerabilidade de terceiros. Qualquer mudança nesta inclusão de script pode alterar a transformação dos dados de plug-ins do Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades do Tenable.io

O mapa de transformação de item vulnerável do Tenable.io é usado para transformar informações de vulnerabilidades abertas e corrigidas importadas do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades do Tenable são processados.

O mesmo mapa de transformação é usado para a Integração de vulnerabilidades fixas do Tenable.io e a Integração de vulnerabilidades abertas do Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE Mapa de transformação de item vulnerável do Tenable.io .

Campo de origem	Campo de destino	Descrição
u_asset.uuid	id	O UUID é mapeado para o campo ID do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo ipv4 é mapeado para o campo Endereço ip do registro cmdb_ci.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_asset.last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação de autenticação do registro cmdb_ci.
u_asset.mac_addess	mac_address	O endereço MAC é mapeado para o campo de endereço mac do host do registro cmdb_ci.
u_asset.netbios_name	netbios	NetBIOS é mapeado para o campo netbios do registro cmdb_ci.
u._plug-in.cvss3_base_score	v3_base_score	A pontuação de base do CVSS v3 é mapeada para a pontuação de base v3 do registro de entrada de terceiros.
u._plug-in.cvss3_temporal_score	v3_temporal_score	A pontuação temporal CVSS v3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u._plug-in.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.
u._plug-in.cvss_temporal_score	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_plug-in.family	categoria	Mapeia a família de plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plug-in.modified_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_plug-in.publication_date	date_published	A data de publicação é mapeada para o campo Data de publicação do registro de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plug-in.risk_factor	source_severity	O fator de risco é mapeado para o campo source_severity do registro de entrada de terceiros.
u_plug-in.solution	solução	A solução é mapeada para o campo de solução do registro de entrada de terceiros.
u_plug-in.synopsis	ameaça	A sinopse é mapeada para o campo Ameaça do registro de entrada de terceiros.
u_severity_id	prioridade	A prioridade é mapeada para o ID de gravidade da carga. O valor padrão é 5.
u_plug-in.exploit_available	exploração	Mapeia exploit_available fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9–10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_plug-in.vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_sources_last28	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_intensity_last28	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.threat_recency	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceiros.
u_plug-in.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plug-in.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plug-in.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.
u_plug-in.family_id	Family_id	Mapeia o ID da família de plug-in para a coluna family_id na tabela de entrada de terceiros.
porta	porta	A porta é mapeada para o campo de porta do registro do item vulnerável.
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro do item vulnerável.
u_first_found	first_found	Primeiro encontrado é mapeado para o primeiro campo encontrado do registro de item vulnerável.
u_last_found	last_found	Encontrado pela última vez é mapeado para o último campo encontrado do registro de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_state	estado	O estado é mapeado para o campo Estado no registro de item vulnerável
[script]	origem	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integration_instance	Integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para nomear na tabela de entrada de terceiros.
u_plug-in.stig_severity	stig_severity	Mapeia a severidade do stig do plug-in para a coluna Severidade do stig na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se o mesmo CVE na tabela de entrada de NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada de NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
lance	A lista de bugs traqs é adicionada como referência.
see_also	A lista de URLs é adicionada como referência.
refsCruzadas	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	TTriggers Tenable IO Vulnerabilities Processador que importa dados do Tenable.io usando o conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela Itens vulneráveis e na tabela de vulnerabilidades de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
Antes de um conjunto de importação concluir a transformação.	Verifica se a entrada e as detecções de terceiros existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Não é este script é para uso interno, e modificá-lo ou excluí-lo não é recomendado.
OnComplete (quando um conjunto de importação conclui a transformação).	Atualiza a contagem de ICs, Vits e detecções conforme importados do Tenable.io. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Importação de ativos do Tenable.sc

Os dados do ativo importados do Tenable.sc são carregados primeiro na tabela Importação de ativos do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos do Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de Ativo do Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. PESQUISE Transformação de ativo do Tenable.sc .

Campo de origem	Campo de destino	Descrição
u_uuid	id	O uuid não é preenchido a partir da API Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo uuid exclusivo para ativos e mapeá-lo para o registro cmdb_ci.
u_ip	ip_address	Mapeia o campo ip da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço mac da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.
u_netbiosname	netbios	Mapeia o campo netbios da API para o campo netbios no registro cmdb_ci.
u_oscpe	os	As informações do SO são extraídas do atributo oscpe na carga e as mapeiam para o campo SO no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.
u_lastauthrun e u_lastunauthrun	last_scan_date	O lastauthrun é extraído da API Tenable ou lastunauthrun. O campo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		last_scan_date no registro do item descoberto é preenchido com base no valor que aparece na carga.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Inicializa os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Atualiza os valores no host e verifica se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Define os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Importação de plug-ins do Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela Importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plug-in_import). O Mapa de transformação do plug-in Tenable.sc é usado para transformar as informações de plug-ins que foram importadas. As mudanças nesta transformação alteram como os dados da importação do plug-in Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar `Mapa de transformação do plug-in Tenable.sc` .

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será DEZ-12345.
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	O TPE importado desta integração tem o Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
u_family	categoria	Mapeia o campo de nome no objeto da família do plug-in para a coluna de categoria.
u_plug-in_modified_date	last_modified	Mapeia plug-in_modified_date para o último campo modificado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plug-in_publication_date	date_published	Mapeia plug-in_publication_date para a data de publicação.
u_has_patch	Remediation_type	Mapeia o tipo de correção do valor has_patch.
u_synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_base_score	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solution	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_temporal_score	cvss_temporal_score	Mapeia a pontuação temporal do CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mapeia a pontuação temporal do CVSS v3.
u_risk_factor	gravidade da origem	Mapeia para a gravidade de origem na tabela de entrada de terceiros.
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia o exploitAvailable fornecido pelo scanner para a coluna Exploit na tabela de entrada de terceiros.
u_vpr_score	source_risk_score	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9–10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_vpr_context	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_vpr_context	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id:"threat_sources_last_28"]	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
u_vpr_context[id:"threat_intensity_last_28"]	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_vpr_context	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceira parte.
u_vpr_context	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stig_severity	stig_severity	Mapeia o campo stig_severity no plug-in para stig_severity na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	family_id	Mapeia o plug-in family_id para family_id na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base em exploit_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como referência.
u_see_also	A lista de URLs é adicionada como referência.
u_exploit_frameworks	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele pega a saída da integração de plug-ins do Tenable.sc e a transforma em ServiceNow entradas de vulnerabilidade de terceiros. Qualquer mudança nesta inclusão de script pode alterar a transformação dos dados de plug-ins do Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades do Tenable.sc

O Mapa de transformação de vulnerabilidades abertas do Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades abertas do Tenable.sc, e o mapa de transformação de vulnerabilidades fixas do Tenable.sc é usado para transformar dados importados da Integração de vulnerabilidades fixas do Tenable.sc.

Nota: As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/abertas do Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e fixas do Tenable.sc, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Instâncias de Integração** > **Integração de vulnerabilidades fixas/abertas do Tenable.sc** > **Fontes de dados** > **Vulnerabilidades abertas/corrigidas do Tenable.sc** > **Transformações**.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada de terceiros.
u_riskfactor	source_severity	Este campo é mapeado para source_severity no registro de entrada de terceiros.
u_severity	prioridade	O campo Prioridade é mapeado com a severidade. O valor padrão é 5.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_hasbemitigado	estado	Foi mitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os VIS estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo ip do host da tabela cmdb_ci.
u_port	porta	A porta é mapeada para o campo de porta do registro do item vulnerável.
u_protocol	protocolo	O protocolo é mapeado para o campo de porta do registro do item vulnerável.
u_firstSeen	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro VI.
u_lastSeen	last_found	O último valor visto é mapeado para o último campo encontrado do registro VI.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo Exploit no registro de entrada de terceiros.
u_synopsis	ameaça	A sinopse é mapeada para o campo Ameaça no registro de entrada de terceiros.
u_description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_solution	solução	A solução é mapeada para o campo de solução no registro de entrada de terceiros.
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada de terceiros.
Pontuação u_temporal	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_cvssv3basecore	v3_base_score	Cvssv3basescocore é mapeado para a pontuação de base v3 no registro de entrada de terceiros.
pontuação u_cvsstemporalscore	v3_temporal_score	A pontuação temporal Cvssv3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u_pluginpublidata	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosName	netbios	NetbiosName é mapeado para o campo NETBIOS do registro cmdb_ci.
u_ip	ip	O IP é mapeado para o campo IP do registro cmdb_ci.
exclusividadeHost	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o uuid do host.
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugintext	prova	O texto do plug-in é mapeado para prova no registro tpe.
[script]	origem	A origem da integração é preenchida. Os itens vulneráveis criados a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		partir desta integração têm Tenable.sc como origem.
[script]	integration_instance	Integration_instance é o nome da instância da qual o item vulnerável é importado.
u_vpr_score	source_risk_score	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação VPR para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7–9 – Alto • 4–7 – Médio • 0–4 - Baixo
u_vpr_context	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id:"threat_sources_last_28]	threat_sources	Mapeia origens de ameaça nos últimos 28 dias do scanner para threat_sources na tabela de terceiros.
u_vpr_context[id:"threat_intensity_last_28]	threat_intensity	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para threat_intensity na tabela de entrada de terceiros.
u_vpr_context	threat_recency	Mapeia as informações de atualização da ameaça do scanner para threat_recency na tabela de entrada de terceira parte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_vpr_context	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stigseverity	stig_severity	Mapeia o campo stig_severity no plug-in para stig_severity na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	family_id	Mapeia o plug-in family.id para family_id na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela third_party_entry é preenchida com base em exploit_available e v3_attack_vector das colunas.

Campo de origem	Descrição
u_cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_ntd_entry). Se o mesmo CVE na tabela de entrada de NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada de NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.
u_bid	A lista de bugs traqs é adicionada como referência.
u_cpe	A lista de CPEs é adicionada como referência.
u_seealso	A lista de URLs é adicionada como referência.
u_xrefs	A lista de X-refs é adicionada como referência.
u_exploitframeworks	A lista de explorações desse plug-in e insere o mapeamento da estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Função usada para atualizar os valores na vulnerabilidade e verificar se ela existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de novos VIS criados e de VIS que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Importação de ativo de contêiner

Os dados de ativos importados são carregados primeiro no Tenable.cs Importação de ativos de contêiner [sn_vul_tenable_cs_container_asset_import].

. Tenable.cs O mapa de transformação de ativo de contêiner é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação do ativo do contêiner é processada. Para acessar este Mapa de transformação, navegue até Conjuntos para importação do sistema > Mapas de transformação. Pesquisar Tenable.cs Transformação de ativo de contêiner.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Tenable.cs Campos do mapa de transformação de ativo de contêiner

Campo de origem	Campo de destino	Descrição
u_digest	Image_id	A Tenable fornece um resumo exclusivo para os ativos do contêiner e mapeia para a imagem do contêiner descoberto e o registro de imagem do docker e é usado para pesquisa de IC.
u_digest	Image_digest	A Tenable fornece um resumo exclusivo para os ativos do contêiner e mapeia para a imagem do contêiner descoberto e o registro de imagem do docker e é usado para pesquisa de IC.
u_name	nome	Mapeia para o campo de nome do registro de imagem do docker.
u_positoryuri	nome	Mapeia para o registro do repositório de contêiner
u_positoryuri	reposição	Mapeia para o registro de imagem do contêiner descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos do mapa de transformação de ativo de contêiner

Campo de origem	Campo de destino	Descrição
u_virtualmachines	host_list	Mapeia para o registro de imagem do contêiner descoberto
u_labels	Image_labels	Mapeia o primeiro valor do SO para o campo SO do registro do item descoberto.
u_clusters	image_cluster	Mapeia para o registro de imagem do contêiner descoberto
u_imagetags	marcadores	Mapeia para o registro de imagem do contêiner descoberto
u_cloudprovider	cloud_providers	Mapeia para o registro de imagem do contêiner descoberto
u_accountid	cloud_account_ids	Mapeia para o registro de imagem do contêiner descoberto
u_region	cloud_regions	Mapeia para o registro de imagem do contêiner descoberto
u_operatingsystem	os	Mapeia para o registro de imagem do contêiner descoberto
u_scantime	last_scan_date	Mapeia para o registro de imagem do contêiner descoberto

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tenable.cs Tempo e finalidade do script do mapa de transformação de ativos do contêiner

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Uma função usada para atualizar valores no host e verificar se o host existe. Com base nos resultados, modifica os valores em um import_set. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Importação de vulnerabilidade do contêiner

Os dados de vulnerabilidade do contêiner importados são carregados primeiro no Tenable.cs Tabela de importação de vulnerabilidade de contêiner [sn_vul_tenable_cs_container_vuln_import].

. Tenable.cs O mapa de transformação de vuln do contêiner é usado para transformar as informações de vulnerabilidade do contêiner importado. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação de vulnerabilidade do contêiner é processada. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquisar Tenable.cs Transformação de vuln do contêiner.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
[script]	Image_id	O resumo é extraído do campo Resource.ID da API e mapeado para o campo image_id da imagem do contêiner descoberto e do registro de imagem do docker.
[script]	Image_digest	O Digest é extraído do campo Resource.ID da API e mapeado para o campo image_digest da imagem do contêiner descoberto e do registro de imagem do docker.
[script]	nome	As informações do repositório são extraídas do campo de nome e mapeadas para a imagem do docker e o registro do repositório de contêiner.
[script]	reposição	As informações do repositório são extraídas do campo de nome e mapeadas para o registro de imagem do contêiner Discover.
Rótulos.u_resource.Rótulos	Image_labels	Mapeia para o registro de imagem do contêiner descoberto
u_resource.CloudProvider	cloud_providers	Mapeia para o registro de imagem do contêiner descoberto
u_resource. AccountId	cloud_account_ids	Mapeia para o registro de imagem do contêiner descoberto
u_resource.Region	cloud_regions	Mapeia para o registro de imagem do contêiner descoberto
u_vulnerability. Id	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de entrada de terceiros será DEZ-12345.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_vulnerability. ID da descrição	sumaryid	Mapeia para o registro de entrada de terceiros. Ou registro CVE.
u_vulnerability.severity	v4_base_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprScore	source_risk_score	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprSeverity	source_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.AttackVector	v4_attack_vector	Mapeia para o registro de entrada de terceiros.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Mapeia para o registro de entrada de terceiros.
[script]	origem	A origem do TPE importado é Tenable.cs.
u_vulnerability.ID	nome	Mapeia para o registro de referências de vulnerabilidade
u_vulnerability. Links	URL	Mapeia para o registro de referências de vulnerabilidade
	vulnerabilidade	Referência de TPE ou CVE no registro de referências de vulnerabilidade
u_software.Name	nome	Mapeia para o registro do pacote de imagem do contêiner
u_software.Versão	versão	Mapeia para o registro do pacote de imagem do contêiner
u_software.Type	package_type	Mapeia para o registro do pacote de imagem do contêiner
u_softwarepaths	caminho	Mapeia para o registro do pacote de imagem do contêiner
u_resolvido	status	Mapeia para o registro de descoberta da imagem do contêiner
u_firstscantime	first_found	Mapeia para o registro de descoberta da imagem do contêiner
u_resource.ScanTime	last_found	Mapeia para o registro de descoberta da imagem do contêiner
u_vulnerability.Description	prova	Mapeia para o registro de descoberta da imagem do contêiner
u_resolvido	estado	Mapeia para o registro de item vulnerável do contêiner
u_firstscantime	first_found	Mapeia para o registro de item vulnerável do contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_resource.ScanTime	last_found	Mapeia para o registro de item vulnerável do contêiner
[script]	origem	A origem do registro de item vulnerável do contêiner é Tenable.cs.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tenable.cs Tempo e finalidade do script de mapa de transformação de vuln do contêiner

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Aciona o Processador de vulnerabilidades de contêiner TenableCS que importa dados do Tenable.cs O uso do conjunto de importação e carrega cada registro na tabela IC do CMDB, na tabela Item vulnerável, na tabela Entrada de vulnerabilidade de terceiros, na tabela de referência de vulnerabilidade, no pacote de imagens do contêiner, na descoberta de imagens do contêiner e no item vulnerável do contêiner. Não é recomendável modificar ou excluir.
Antes de um conjunto de importação concluir a transformação)	Verifica se a entrada de terceiros e as descobertas de imagem existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
OnComplete (quando um conjunto de importação conclui a transformação)	Atualiza a contagem de ICs, Vits e descobertas conforme importados de Tenable.cs. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Importação de Vulnerabilidade de Computação

Os dados de vulnerabilidade do host importados são carregados primeiro no Tenable.cs Tabela de importação de vulnerabilidade de computação [sn_vul_tenable_cs_compute_vuln_import].

. Tenable.cs O mapa de transformação de vuln de computação é usado para transformar as informações de vulnerabilidade do host importado. As mudanças nesta transformação alteram como os dados do Tenable.cs A importação de vulnerabilidade de computação é processada. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Conjuntos para importação do sistema**. Pesquisar Tenable.cs Transformação de vuln de computação.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_resource.ID	object_id	Mapeia para o registro de IC do CMDB.
u_resource.Name	nome	Mapeia para o registro de IC do CMDB.
	asset_category	A nuvem é mapeada como Categoria de ativo no registro de item descoberto.
U_resource.CloudProvider	cloud_service_provider	Mapeia para o registro do item descoberto
u_resource.Region	cloud_region	Mapeia para o registro do item descoberto
u_resource.AccountId	cloud_account	Mapeia para o registro do item descoberto
u_resource. CloudProvider	cloud_resource_type	Mapeia para o registro do item descoberto
u_resource.ID	resource_id	Mapeia para o registro do item descoberto
u_resource.Name	resource_name	Mapeia para o registro do item descoberto
u_vulnerability.ID	id	Mapeia o ID da origem e adiciona o prefixo DEZ. Por exemplo, se o ID recebido for 12345, o ID na tabela de entrada de terceiros será DEZ-12345. Mapeia o ID para CVEs também.
u_vulnerability. Descrição	resumo	Mapeia para o registro de entrada de terceiros.
u_vulnerability.severity	v4_base_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprScore	source_risk_score	Mapeia para o registro de entrada de terceiros.
u_vulnerability.VprSeverity	source_severity	Mapeia para o registro de entrada de terceiros.
u_vulnerability.AttackVector	v4_attack_vector	Mapeia para o registro de entrada de terceiros.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Mapeia para o registro de entrada de terceiros.
[script]	origem	A origem do TPE importado é Tenable.cs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_vulnerability.ID	nome	Mapeia para o registro de referências de vulnerabilidade
u_vulnerability.links	URL	Mapeia para o registro de referências de vulnerabilidade
	vulnerabilidade	Referência de TPE ou CVE no registro de referências de vulnerabilidade
u_resolvido	status	Mapeia para o registro de detecção de item vulnerável
u_firstscantime	first_found	Mapeia para o registro de detecção de item vulnerável
u_resource.ScanTime	last_found	Mapeia para o registro de detecção de item vulnerável
u_softwarepaths	prova	Mapeia para o registro de detecção de item vulnerável
u_softwareresoluçãoversões	solution_summary	Mapeia para o registro de detecção de item vulnerável
u_resolvido	estado	Mapeia para o registro de item vulnerável
u_firstscantime	first_found	Mapeia para o registro de item vulnerável
u_resource.ScanTime	last_found	Mapeia para o registro de item vulnerável
[script]	origem	A origem do registro de item vulnerável é Tenable.cs.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tenable.cs Calcular tempo e finalidade do script de mapa de transformação de vuln

Quando o script é executado	Finalidade
OnStart (quando um conjunto de importação inicia a transformação)	Aciona o processador de vulnerabilidades de computação do Tenable CS que importa dados do Tenable.cs O uso do conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de vulnerabilidades de terceiros. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.
Antes de um conjunto de importação concluir a transformação.	Verifica se a entrada e as detecções de terceiros existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.cs Calcular tempo e finalidade do script de mapa de transformação de vuln

Quando o script é executado	Finalidade
OnComplete (quando um conjunto de importação conclui a transformação).	Atualiza a contagem de ICs, Vits e detecções conforme importados de Tenable.cs. Este script é para uso interno e não é recomendável modificá-lo ou excluí-lo.

Tenable.cs Campos de mapa de transformação de vuln de contêiner

Campo de origem	Campo de destino	Descrição
u_digest	Image_id	Um resumo exclusivo fornecido pela Tenable para os ativos do contêiner. Mapeia para a imagem do contêiner descoberta e o registro de imagem do docker e é usado para pesquisa de IC.
u_name	nome	Mapeia para o campo de nome do registro de imagem do docker.

Defina parâmetros de filtro adicionais para Tenable.io importações

Personalize os parâmetros de filtragem para suas consultas programadas com Integrações de vulnerabilidade da Tenable para ajudar você a refinar ainda mais os dados de vulnerabilidade importados com Tenable.io produto.

Antes de Iniciar

Casos de uso: Como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você deseja exibir vulnerabilidades importadas que são filtradas por `cidr_range`, `num_assets`, `indexed_at`e `plugin_family`. Ou, digamos que você deseja executar um Tenable.io integração de forma que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudar você a coletar esses dados, você pode adicionar parâmetros compatíveis com o Tenable para ajudar a importar os detalhes de vulnerabilidade específicos necessários.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite personalizar as informações da solicitação HTTP com parâmetros do Tenable em seu ServiceNow AI Platform. A seguir Tenable.io As integrações oferecem suporte à filtragem fornecendo conteúdo JSON no corpo da solicitação:

- Integração de ativos
- Integração de Vulnerabilidade Corrigida
- Integração de vulnerabilidades em aberto

Você deve saber como usar JSON cadeias de caracteres para este recurso.

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Localize os parâmetros compatíveis com Tenable.io produto no site do desenvolvedor que você deseja usar para filtragem.

   Parâmetros e valores inseridos no Tenable.io os produtos são compatíveis somente no nível da instância de integração.

2. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
3. Na página de lista Integrações do Tenable, clique no registro do Tenable.io integração que você deseja abrir.
4. Com a guia Métodos REST do Tenable selecionada, clique no ícone de informações (I) do método REST seguido por **Registro em aberto** .
5. Selecione **Solicitação HTTP** guia.
6. Para editar o registro, na parte superior da página, clique no link em, para editar o registro, clique em **aqui** .
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON desejado como parte do corpo da solicitação.

   Como exemplo, você pode definir o parâmetro de severidade para vulnerabilidades importadas como, `{"filters": {"severity": ["critical"]}}`para Tenable.io Integração de ativos para importar somente vulnerabilidades críticas (pontuação CVSS de 10,0).

   Se você quiser inserir mais de um parâmetro, consulte Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Emissão de relatórios de Integração de vulnerabilidades do Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis no Resposta a vulnerabilidades painéis.

Visualizações de dados no Resposta a vulnerabilidades Espaços de trabalho

. Resposta a vulnerabilidades Os espaços incluem visualizações de dados que podem ajudar você a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizados conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços de trabalho, Explorar o. Espaço do gerente de vulnerabilidade e. Explorar o. Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos disponíveis.

Versões anteriores de Resposta a vulnerabilidades

O painel de visão geral da Resposta a vulnerabilidades (Gestão de vulnerabilidades) fornece uma visão executiva das vulnerabilidades e itens vulneráveis, ajudando o administrador de vulnerabilidades a identificar áreas de preocupação rapidamente. O painel Correção de resposta a vulnerabilidades (Correção de vulnerabilidades) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando o padrão Resposta a vulnerabilidades painéis.

Função necessária: Responsável pela correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

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

para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão Geral da Correção**.

Gráfico de status de execução de integração para a Integração de vulnerabilidade do Tenable

O módulo Status de execução de integração do Tenable fornece uma exibição gráfica do status das execuções de integração do Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer peça no gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: Administrador de vulnerabilidades.

As funções Persona e granular estão disponíveis para ajudar você a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração.

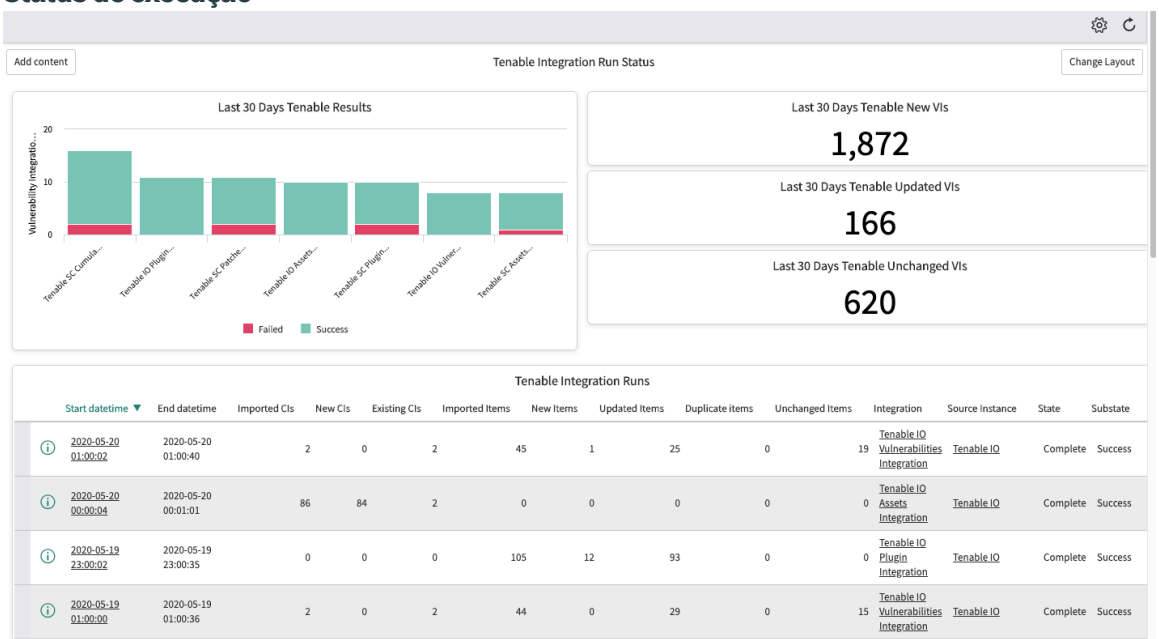
Para obter mais informações sobre como gerenciar funções granulares, consulte Gerencie funções granulares e de persona para Resposta a vulnerabilidades.

Para exibir os dados, navegue até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Status da Execução da Integração**.

A partir da versão 19,0 de Resposta a vulnerabilidades Este painel está disponível na IU da Nova experiência.

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

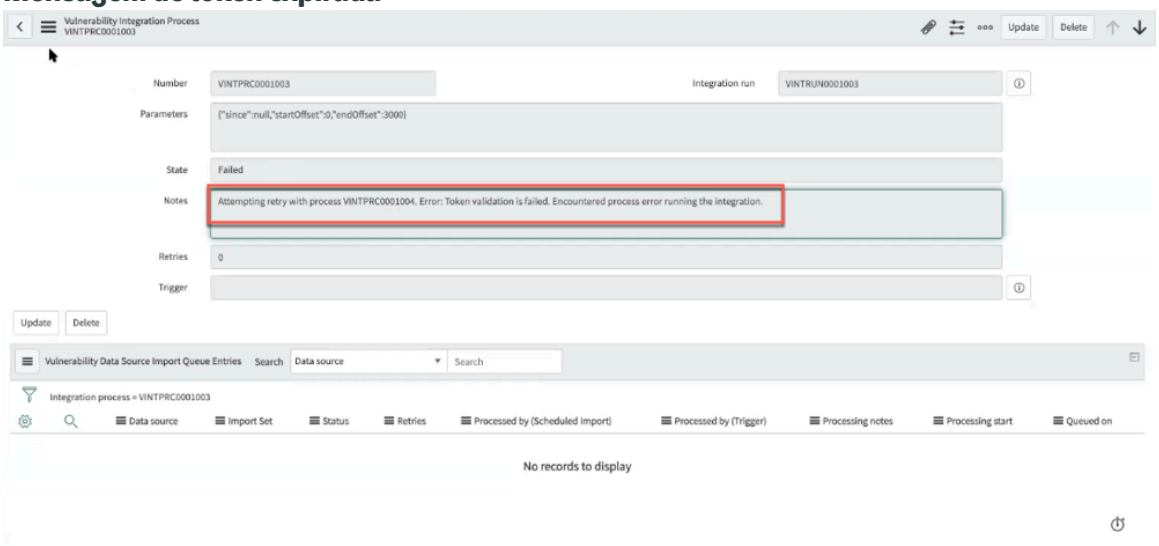
Relatórios de gráfico de status de execução da integração do Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução exibida como uma barra no gráfico.
VIs novos da Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs da Tenable atualizados nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções da integração com Tenable	Os registros de execução de integração em uma lista. **Nota: V16.1:** Para verificar detecções para esta integração, compare as detecções ou descobertas com ServiceNow dados de detecção no `sn_vul_detection`tabela. Enquanto a integração estiver em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Até contagem de datas" na instância, após a conclusão da execução da integração.

Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do Processo de integração de vulnerabilidades.

Mensagem de token expirada



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidades no registro Processo de integração de vulnerabilidades.

Iniciar uma nova verificação para Tenable.sc integração

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas varreduras na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Tenable.sc produto do seu ServiceNow AI Platform® instância.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota: Tenable.sc o não oferece suporte para iniciar uma nova verificação em máquinas baseadas em agente.

Antes de começar, verifique se o scanner está ativado. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

Para iniciar uma nova varredura nos espaços de trabalho, consulte Nova verificação Tenable.io e. Tenable.sc itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidades, ou os gerentes de vulnerabilidades podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas varreduras de itens vulneráveis (VI), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de itens descobertos do seu ServiceNow AI Platform instância.

Permitir novamente seu responsáveis pela correção e analistas de vulnerabilidades Para verificar se suas atividades de correção, patches e outras ações corrigiram com sucesso vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o seu ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Tenable.sc itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao solicitar uma nova verificação do seu ServiceNow AI Platform® instância, selecionando Integração de Resposta a vulnerabilidades com Tenable as credenciais são opcionais. . ServiceNow® Tenable.sc A integração de credenciais de verificação importa e atualiza as credenciais do scanner do Tenable.sc produto em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais do Tenable.

Observe que esses dados importados não incluem senhas do Tenable ou outras informações confidenciais da conta do Tenable. . ServiceNow® Tenable.sc A integração de credenciais de verificação está habilitada (Ativo Automaticamente de dentro do Assistente de configuração na sua instância quando você configura o. Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades em aberto e corrigido).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário no seu ServiceNow AI Platform instância:

- Credenciais criadas com Tenable.sc a função de usuário administrador está disponível para usuários em todas as suas organizações.
- Credenciais criadas com Tenable.sc a função usuários organizacionais só está disponível para usuários dessa organização. Essas credenciais não são importadas para ServiceNow AI Platform para usuários fora da organização do criador, a menos que eles sejam compartilhados com a conta do usuário que está sendo usada para se conectar à instância.

Consulte Tenable.sc site de documentação para obter mais informações.

Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração para obter mais informações sobre como configurar o. Tenable.sc aplicação. Para exibir mais informações sobre a Integração de credenciais de verificação, navegue até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Integrações** > **Integração de credenciais de verificação do Tenable.sc**.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas varreduras para VIS com Tenable.sc como a origem. Verificar Tenable.scé exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se a coluna Origem não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique em **Personalizar lista** (Ícone de engrenagem) e use o Slushbucket para mover **Origem** de **Disponível** . **Selecionado** .

3. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve ser do Tenable.sc produto e em qualquer estado diferente de **Encerrado** . Para vários registros de VI, todos os VIS devem ser do produto Tenable.sc e estar em qualquer estado diferente de **Encerrado** .
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ser do Tenable.sc produto.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do Tenable.sc produto em qualquer estado diferente de **Encerrado** .

4. No canto superior direito do registro, clique em **Nova verificação** .
   Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Estas são as credenciais importadas pelo Tenable.sc Integração de credenciais de verificação.
5. Na caixa de diálogo, selecione os filtros e os tipos de credencial desejados.
6. Clique em **Verificação de solicitação** .

   É exibida uma mensagem indicando que sua verificação está sendo processada. O status de todas as novas varreduras pode ser encontrado a qualquer momento nas listas relacionadas de Varredura nos registros VI, RT, TPE que você usou para iniciar as novas varreduras. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e exibir todas as outras novas verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida. Todos os VIS que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** São importados com a próxima importação programada da Integração de vulnerabilidades fixas do Tenable.sc.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar uma nova verificação para Tenable.io integração

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para Tenable.io produto do seu ServiceNow AI Platform® instância.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Antes de começar, verifique se o scanner está ativado. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade e. Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI Para iniciar uma nova verificação nos espaços de trabalho de Resposta a vulnerabilidades.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota: Tenable.io o não oferece suporte para iniciar uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, como responsável pela correção, especialista EM TI, analista de vulnerabilidades ou gerente de vulnerabilidades, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas varreduras de registros de item vulnerável (VI), tarefas de correção (VUL), entrada de terceiros (TPE) ou item descoberto (SDI) do seu ServiceNow AI Platform instância. Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao solicitar uma nova verificação do seu ServiceNow AI Platform® instância, selecionando Integração de Resposta a vulnerabilidades com Tenable as credenciais são opcionais. . ServiceNow® Tenable.io A integração de credenciais de verificação importa e atualiza as credenciais do scanner do Tenable.io produto em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais do Tenable.

Observe que esses dados importados não incluem senhas do Tenable ou outras informações confidenciais da conta do Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário no seu ServiceNow AI Platform instância:

- Credenciais criadas com Tenable.io a função de usuário administrador está disponível para usuários em todas as suas organizações.
- Credenciais criadas com Tenable.io a função usuários organizacionais só está disponível para usuários dessa organização. Essas credenciais não são importadas para ServiceNow AI Platform para usuários fora da organização do criador, a menos que eles sejam compartilhados com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte Tenable.io site de documentação para obter mais informações.

- . Tenable.io Integração de modelo e Tenable.io A integração de credenciais de verificação deve ser ativada antes de iniciar novas verificações. Para exibir mais informações sobre a Integração de credenciais de verificação, navegue até **Integração com a gestão de vulnerabilidades do Tenable** > **Integrações** > **Integração de credencial de verificação do Tenable.io**.

  Por padrão, as Integrações de credencial de modelo e verificação estão desativadas. Quando você insere suas credenciais para Tenable.io. todos Tenable.io as integrações são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize Tenable.io registros de integração desejados.
  3. Abra cada registro e selecione **Ativo** caixa de seleção para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com a configuração do Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

Consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração para obter mais informações sobre como configurar o. Tenable.io e. Tenable.sc produtos.

Todo o seu ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada do seu ServiceNow AI Platform para Tenable.io itens vulneráveis.

Você pode exibir resultados atualizados nos registros a partir dos quais você iniciou as verificações após a próxima importação programada da Integração de vulnerabilidades fixas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados nas páginas. Essas entradas devem processar os dados dentro do limite de tempo de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades carimbos de data/hora (heartbeats) são enviados periodicamente para indicar se a fila está ativa e processando dados. . **Último registro processado** O campo na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada de fila de importação exceda o limite de tempo de uma hora, o sistema verificará o. **Último registro processado** campo para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está presa e o tempo limite expirou para evitar atrasos adicionais no processamento.

Nota: . **Último registro processado** o campo é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: Define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: Define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Se você estiver usando Tenable.io Scanner, você só pode iniciar novas varreduras para VIS com Tenable.io como a origem. Verificar Tenable.ioé exibido em **Origem** Nas Exibições de lista de VI ou no **Origem** campos em registros individuais. Você pode usar o Construtor de condições para agrupar VIS por origem. Ou, se a coluna Origem não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique em **Personalizar lista** (Ícone de engrenagem) e use o Slushbucket para mover **Origem** de **Disponível** . **Selecionado** .

3. Como alternativa, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o **Nova verificação** o botão está disponível nos seguintes registros:

   - Em um único registro VI, o VI deve estar em qualquer estado diferente de **Encerrado** . Para vários registros de VI, todos os VIS devem ser de Tenable.io produto e em qualquer estado diferente de **Encerrado** .
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os VIS associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como a origem.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do Tenable.io produto em qualquer estado diferente de **Encerrado** .
   - Em registros de itens descobertos, o registro deve ter pelo menos um registro VI associado do Tenable.io produto em qualquer estado diferente de **Encerrado** .

Tradução automática

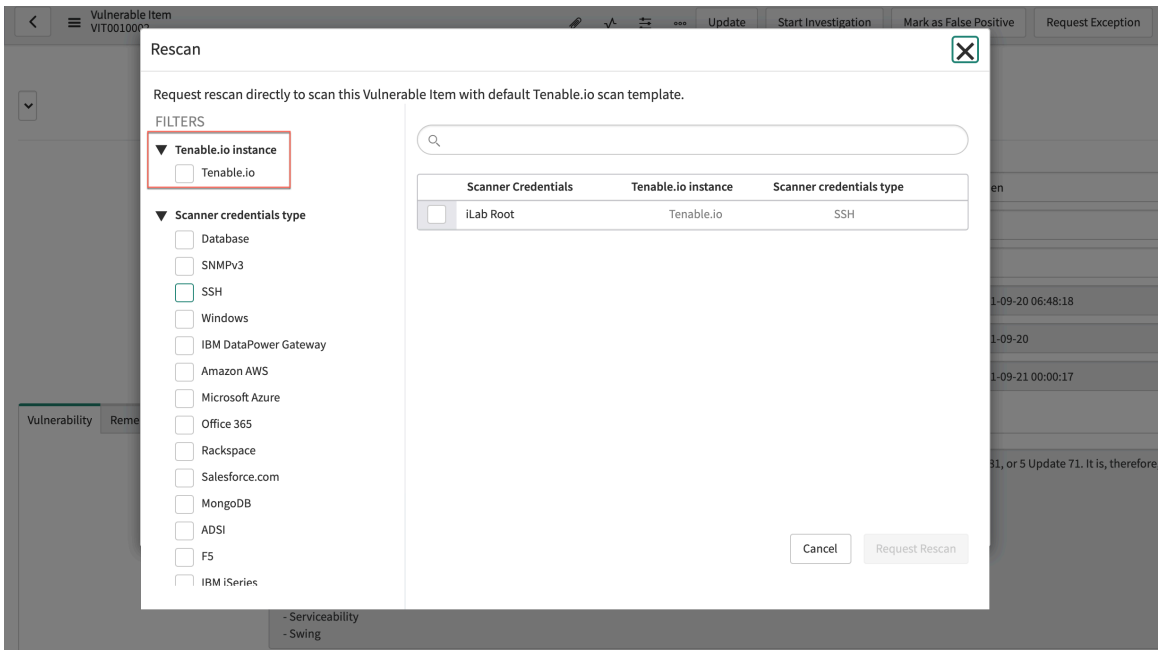
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Nova verificação** .
   Você será solicitado a escolher a instância ou instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pelo Tenable.io Integração de credenciais de verificação.

5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, Tenable.io é exibido. Se você tiver mais de um Tenable.io todos eles são exibidos em Tenable.io seção no formulário.



Campo	Descrição
Instância da Tenable.io	Escolha um Tenable.io instância de integração da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io são exibidos. Se existir uma VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar. **Nota:** Se você optar por verificar novamente o VIS de um registro de tarefa de correção para uma única instância de integração, somente os VIS ativos associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas, serão verificados.
Filtro de tipo de credenciais do scanner	Use este filtro para exibir credenciais por tipo.
Painel com credenciais do scanner, Tenable.io Tipo de credenciais do scanner	Estas são as credenciais do scanner disponíveis importadas do Tenable.io produtos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Escolha uma ou mais credenciais para usar na verificação.

6. Clique em **Solicitar nova verificação** .

   É exibida uma mensagem indicando que sua verificação está sendo processada e um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas à verificação nos registros VI, tarefa de correção, TPE e SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e exibir todas as outras novas verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode oferecer suporte é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida. Todos os VIS que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação programada do Tenable.io Integração de vulnerabilidades corrigidas.

   Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

   Você pode exibir resultados atualizados nos registros a partir dos quais você iniciou as verificações após a próxima importação programada da Integração de vulnerabilidades fixas.

Atualize itens de configuração com o identificador de partição de rede para Integrações de vulnerabilidade da Tenable

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão em Resposta a vulnerabilidades Uma maneira de identificar seus ativos é pelo endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (ICs) em seu ambiente podem compartilhar endereços IP, mas têm ids exclusivos de rede e repositório. No entanto, por padrão, esses ativos geralmente são identificados e armazenados como um único IC (IC 1) Durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para poder identificá-los como ativos distintos. A partir de uma importação de dados nova, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para Ativos e Integrações de vulnerabilidades fixas e abertas para Tenable.io e. Tenable.sc No Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o Identificador de partição de rede [network_partition_identifier] aos registros de IC existentes de dados importados. ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar seus dados existentes.

Quando você faz upgrade começando com v14.0 de Resposta a vulnerabilidades E v2.2 da Integração de vulnerabilidades do Tenable, os Modelos de classe de IC do CMDB (1,0.21.) é compatível. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de IRE (Identificação e reconciliação).

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados existentes do Tenable são criados ou atualizados para incluir a granularidade do identificador da partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são atualizados com os novos ICs.
Aguarde as importações de dados atualizados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo

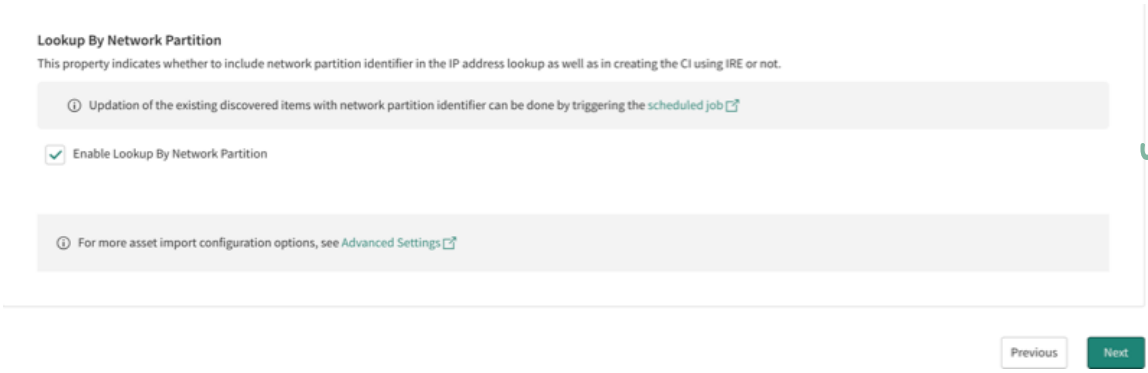
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	trabalho agendado. IC, item vulnerável e registros de detecção são atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Editar** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

Os identificadores de partição de rede NETWORK_ID e REPOSITÓRIO _ID são incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho agendado.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc Integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho agendado, as regras de pesquisa de identificação de endereço IP e de IC de endereço IP incompleto incluem o atributo identificador de partição de rede automaticamente para uma importação de dados das Integrações de ativos e vulnerabilidades fixas e abertas para Tenable.io e. Tenable.sc produtos.

Depois de habilitar a propriedade do sistema e salvar os registros, você também pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos agendados sob demanda.

Importar modificações para a Integração de vulnerabilidades do Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação do Tenable Vulnerabilities no ServiceNow® Integração de vulnerabilidades do Tenable.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação e conhecimento avançado sobre ServiceNow AI Platform.

Siga estas etapas para criar importações separadas por domínio para as Integrações do Tenable Vulnerabilities. O exemplo a seguir é para a integração Open Vulnerabilities do Tenable.io, mas este conteúdo é aplicável a outras integrações do Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio que você criar, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado run_as para o domínio no Tenable.io.

3. Integração de vulnerabilidades em aberto.
   O usuário é equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Considere este usuário como específico para esta função. O usuário não deve ter outra finalidade

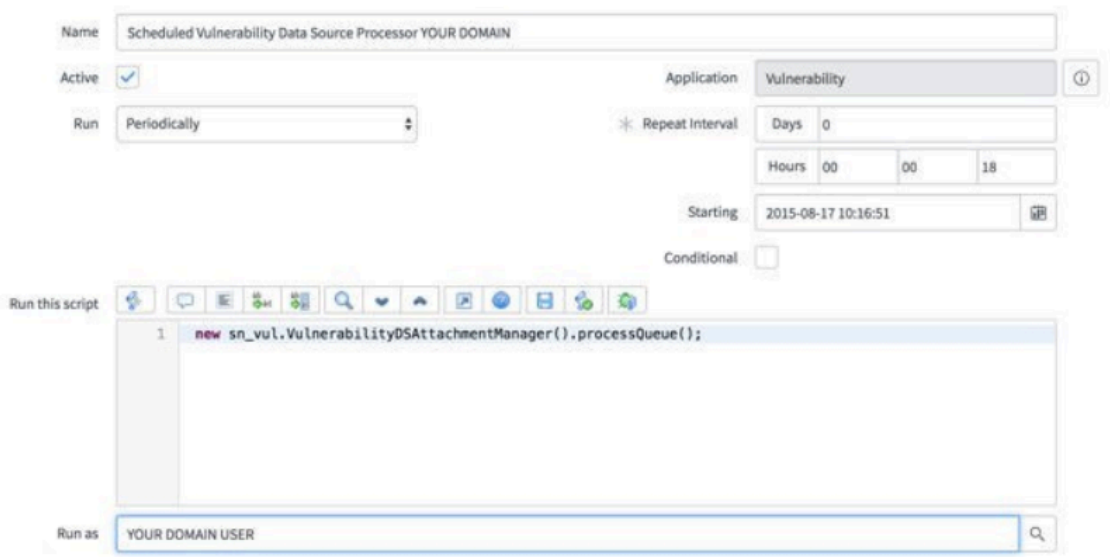
4. Em cada domínio, crie um trabalho agendado copiando o Processador da fonte de dados de vulnerabilidade programada encontrado em **Definição do Sistema** > **Trabalhos agendados**.
5. Anexe o domínio ao nome para identificar o trabalho agendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Mude o usuário run_as para o usuário que você criou na etapa anterior.

Nota: Edite a ação de IU a seguir para que a integração seja executada no domínio do usuário run_as.

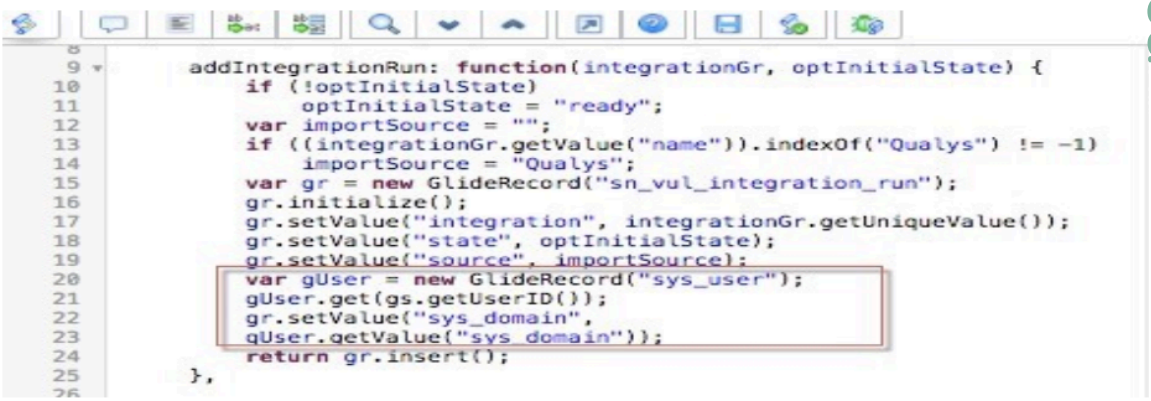


7. Edite a ação Executar IU do Now na Integração de vulnerabilidades abertas do Tenable.io para adicionar este bloco de código à parte superior do arquivo.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Nota: Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

8. Edite o script VulnerabilityIntegrationUtils include método addIntegrationRun para adicionar o código realçado.

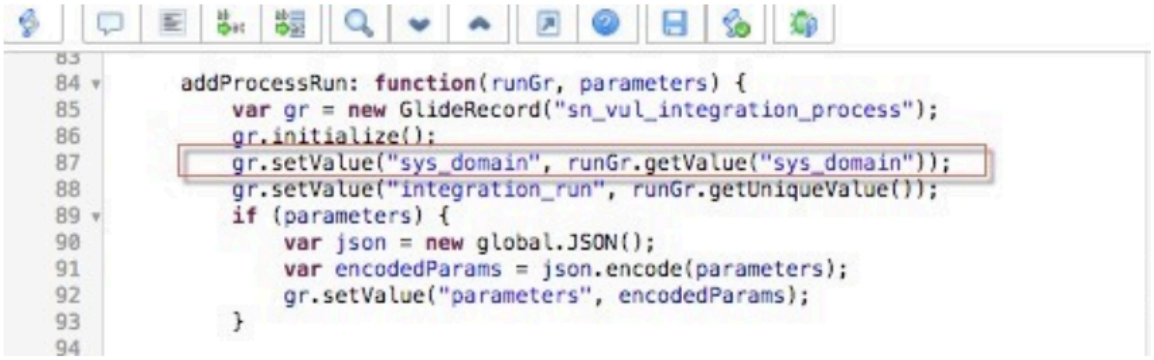


```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o script VulnerabilityIntegrationUtils include método addProcessRun para adicionar o código realçado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edite o método de inclusão de script DataSourceVulnReportRefresProcessor _processFromDataSourceGroups para mudar este código original: Código _processFromDataSourcesGroups original para o código _processFromDataSourcesGroups editado.
11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem para adicionar os blocos de código realçados a seguir queueItem, _getNext, _processQueueEntry.

    Você está pronto para importações de detecção de host separadas por domínio.

    Desabilite as calculadoras antes da importação

    Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de todas as outras que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e podem afetar o desempenho da instância.

    Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Tudo** > **Vulnerabilidade** > **Administração** > **Calculadoras de Vulnerabilidade**.
13. Abra o grupo Impacto da vulnerabilidade.
14. Abra a calculadora de Pontuação e Impacto baseado no serviço.
15. Desmarque o campo Ativo para desativar a calculadora.
16. Clique em Atualizar.

    Você desabilitou a calculadora padrão.

    Desabilite regras de negócios baseadas em notificação antes da importação inicial

    Siga estas etapas para desabilitar Desabilitar regras de negócios relacionadas a notificações antes da importação inicial de registro. Durante a importação inicial de registros, determinadas regras de negócios relacionadas a notificações podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desabilitá-las durante a importação.

    A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.
18. PESQUISE notificações de ic afetadas.
19. Abra a regra de negócio e insira a seguinte condição: `current.sys_class_name != “sn_vul_vulnerable_item"`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócios:
    - Notificações do centro de custos afetado
    - Notificações de grupo afetado
    - Notificações de local afetado

    Nota: Após a conclusão da importação de registro inicial, você tem a opção de reativar essas regras de negócios. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

    Modifique uma data de início inicial

    Siga estas etapas para Modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações do Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Tudo** > **Integração com a gestão de vulnerabilidades do Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde esse momento sejam detectadas.

    Se você configurou a Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente três meses antes da data de hoje e, posteriormente, até a data de hoje. Observação: Considere definir o valor como um máximo de um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da Tenable API, bem como acione tempos limite de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. **Opcional:** Clique em **Executar agora** para executar imediatamente.

Divida detecções do Tenable com base na instância de vulnerabilidade para dividir itens vulneráveis

ServiceNow® A Resposta a vulnerabilidades permite a divisão de detecções de scanners do Tenable, permitindo a criação de um item vulnerável exclusivo (VIT) para cada instância de vulnerabilidade detectada. Essa divisão permite a atribuição de Vits a várias equipes de correção, aprimorando o gerenciamento e o acompanhamento de vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A carga útil do scanner do Tenable contém dados de detecção, com cada caminho na prova usado para dividir as detecções. O marcador de saída na carga identifica o local da vulnerabilidade, facilitando a identificação e o gerenciamento precisos de vulnerabilidades de acordo com seus caminhos específicos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na tabela Integrações de terceiros [sn_sec_int_integration], defina **Incluir prova na chave vi** valor da coluna como verdadeiro para Tenable.io, Tenable.sc e Tenable.cs.
2. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.
3. Para Tenable.cs produto, navegue até **Configuração da chave de detecção** tabela [sn_vul_detection_key_config], selecione Tenable.cs registrar e atualizar,
4. No formulário Incluir porta, selecione **Incluir porta** e selecione **clique aqui** Link (aplica-se somente a Tenable.io e Tenable.sc).
5. Na lista Adicionar prova às chaves VI, selecione **Novo** .
6. No formulário Adicionar prova à chave VI - Novo registro, em **Vulnerabilidade** Adicione o ID da Tenable para o qual você deseja incluir a prova.

   Nota: Você pode dividir as detecções com base exclusivamente nas informações de caminho ou combinando detalhes de caminho e versão. Para obter detalhes adicionais, consulte a seção "Divisão de detecções de scanners Tenable" nesta página.

7. Em **Expressão regular para Dividir Vits do Tenable** campo:
   - Divida a detecção com base somente no caminho inserindo Caminho
   - Divida a detecção com base no caminho e nas versões instaladas e fixas inserindo Path:
8. Selecione **Enviar**.

Example: Dividindo detecções de scanners Tenable

A detecção a seguir de um scanner do Tenable mostra uma prova no marcador de saída que inclui informações de caminho e versão.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",

               "tracked": true
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
"output": "In C: 11 Program Files (x86) \ \Common Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed version
Path
"plugin":
"bid":
123456

"checks_for_default_account": false,
"checks_for malware": false,

"coe":
"cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"

"cvSs3_base_score": 7.8,
"cvss3 temporal score": 7.0,

"cvss3_temporal_vector": {
"exploitability": "Proof-of-Concept",
"remediation level": "Official Fix",
"report_confidence": "Confirmed",
"raw": "E: P/RL:0/RC: C"
```


Explorar o. Resultados de testes do Wiz e Integrações de problemas com Conformidade de configurações

Importe dados de configuração de nuvem com Resultados de testes do Wiz e Integrações de problemas com Conformidade de configurações incluídos com Wiz Resposta a vulnerabilidades Integração.

Wiz Integração de resultados de teste

Importar resultados de teste de configuração de Wiz para detectar configurações de nuvem fora de conformidade e ajudar você a impor políticas e padrões de segurança em todo o seu ambiente de nuvem.

As descobertas são mapeadas para resultados de teste de nuvem (CTRs) no Conformidade de configurações aplicação.

Nota: Configurações de host de Wiz não são importados.

Wiz Integração de problemas

Importar dados de problemas de Wiz ajudar gerentes de vulnerabilidades, analistas e equipes de segurança e risco na nuvem a identificar combinações de vulnerabilidades que podem revelar um caminho de ataque potencial em sua infraestrutura de nuvem.

Essas descobertas também são mapeadas para CTRs com Problemas do Wiz rotulado como a origem em Conformidade de configurações aplicação para ajudar você a rastrear e corrigir ativos que podem representar riscos multivetoriais complexos.

Para obter mais informações sobre as outras integrações incluídas com Wiz Resposta a vulnerabilidades Integração e instalação e etapas de configuração, consulte Noções básicas do Wiz Resposta a vulnerabilidades Integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações correção

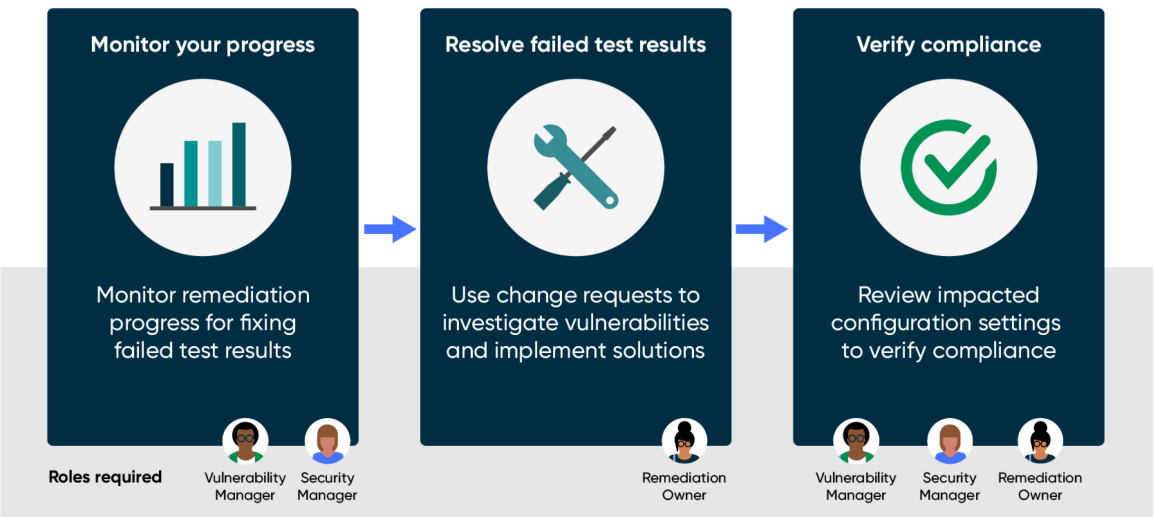
Conformidade de configurações a correção é principalmente um processo manual aumentado por trabalhos agendados (integrações), tarefas de correção, fluxos de trabalho e solicitações de mudança.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Remediation of test result groups



Plug-ins SCA de terceiros separados adquirem e transformam dados no Conformidade de configurações. Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

Use solicitações de mudança para corrigir falhas de teste individuais de tarefas de correção.

Os estados das tarefas de correção fazem a transição automaticamente conforme as solicitações de mudança associadas passam por seus ciclos de vida com Sincronização de estado entre solicitações de mudança e tarefas de correção. Usuários com a função itil podem criar e gerenciar solicitações de mudança diretamente de tarefas de correção.

Tópicos relacionados

- Criar manualmente um Conformidade de configurações tarefa de correção
- Criar manualmente um Conformidade de configurações Tarefa de correção da lista Resultados de teste
- Como criar uma solicitação de mudança no Conformidade de configurações
- Associe uma tarefa de correção a uma solicitação de mudança existente
- Remova atribuições de tarefas de correção para você ou seus grupos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechamento automático dos resultados de testes

Feche uma tarefa de correção

Configure regras de aprovação para Gestão de exceções em Conformidade de configurações

Criar manualmente um Conformidade de configurações tarefa de correção

Você pode criar manualmente uma tarefa de correção do **Tarefas de correção** e executar correção.

Importante: Você pode criar tarefas de correção em:

- Espaço do gerente de vulnerabilidade como um usuário com a função sn_vulc.admin.
- Espaço de correção de problemas de TI como um usuário com a função sn_vulc.remediation_owner.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O uso de regras de tarefa de correção preenche automaticamente o. **Resultados do teste** guia. A criação manual é útil para uma tarefa de correção que não precisa de uma regra ou de ser repetida.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

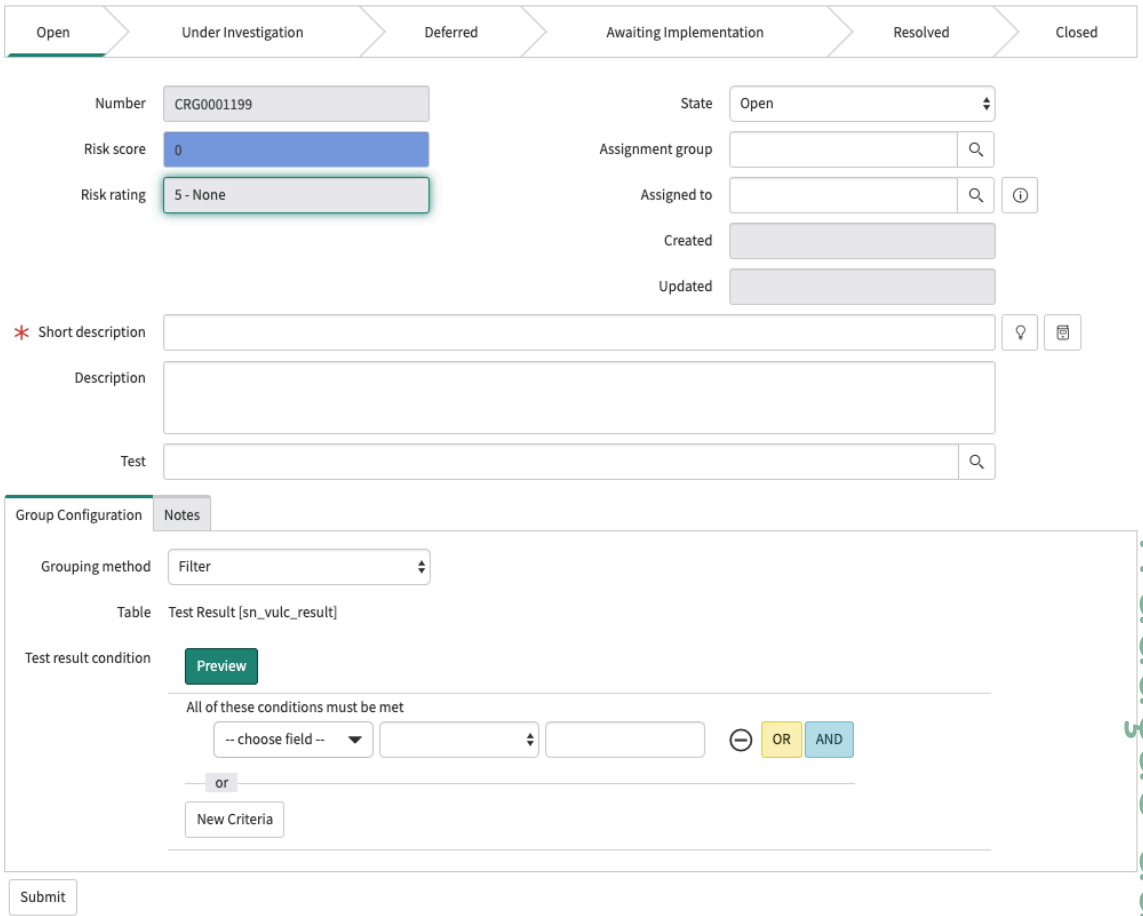
Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Tarefas de correção**.
2. No painel de navegação, clique em **Minhas tarefas em aberto** ou **Todas as tarefas em aberto** para exibir a lista.
3. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de tarefa de correção



4. Preencha os campos no formulário Tarefa de correção, conforme apropriado.

Formulário de tarefa de correção

Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os resultados de teste não "Encerrado" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido), e 15% da pontuação do número de resultados de testes que não estão "Encerrados".
Classificação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica o risco geral com base em um intervalo de pontuações de risco como 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade em versões anteriores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

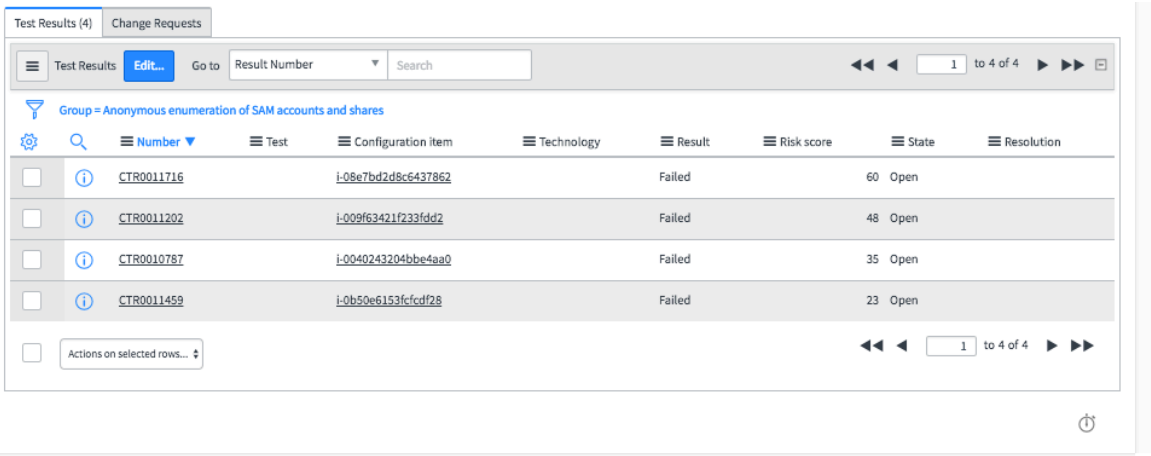
Campo	Descrição
Estado	Inicialmente **Aberto** é o estado de correção da tarefa de correção. Para obter mais informações, consulte Conformidade de configurações estados.
Grupo de atribuição	Atribua a tarefa de correção a um grupo de correção.
Atribuição a	Atribua uma equipe para corrigir a tarefa de correção.
Criação em	Data em que você criou esta tarefa de correção.
Atualização em	Data em que você atualizou esta tarefa de correção.
Descrição Resumida	Nome da tarefa de correção.
Descrição	Descrição desta tarefa de correção.
Testar	Selecione um Teste de configuração para esta tarefa de correção.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ◦ Manual (padrão): ◦ Regra de filtro ou grupo: Tabela: Pré-selecionado como resultado do teste [sn_vulc_result] Condição do resultado do teste: Escolha os filtros a serem usados. **Nota:** O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de teste que você escolheu em uma nova janela. Clique em **Visualização** para ver quantos resultados seus critérios de filtro retornam antes de salvar o novo grupo. A lista relacionada Resultados de teste deve ser criada manualmente clicando em **Editar** botão em **Resultados do teste** guia relacionada.
Anotações	Anotações de trabalho relacionadas a esta tarefa de correção.

5. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibe o. **Resultados do teste** e. **Solicitação de mudança** listas relacionadas.



Criar manualmente um Conformidade de configurações Tarefa de correção da lista Resultados de teste

Você pode criar manualmente uma tarefa de correção do **Resultado do teste** liste e execute a correção da tarefa de correção resultante.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Este método requer a seleção de resultados de teste para incluir e criar o grupo a partir de **Ações nas linhas selecionadas...** menu. Este método é bom para resultados que não são filtrados facilmente ou para situações em que você deseja especificar resultados de teste para correção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

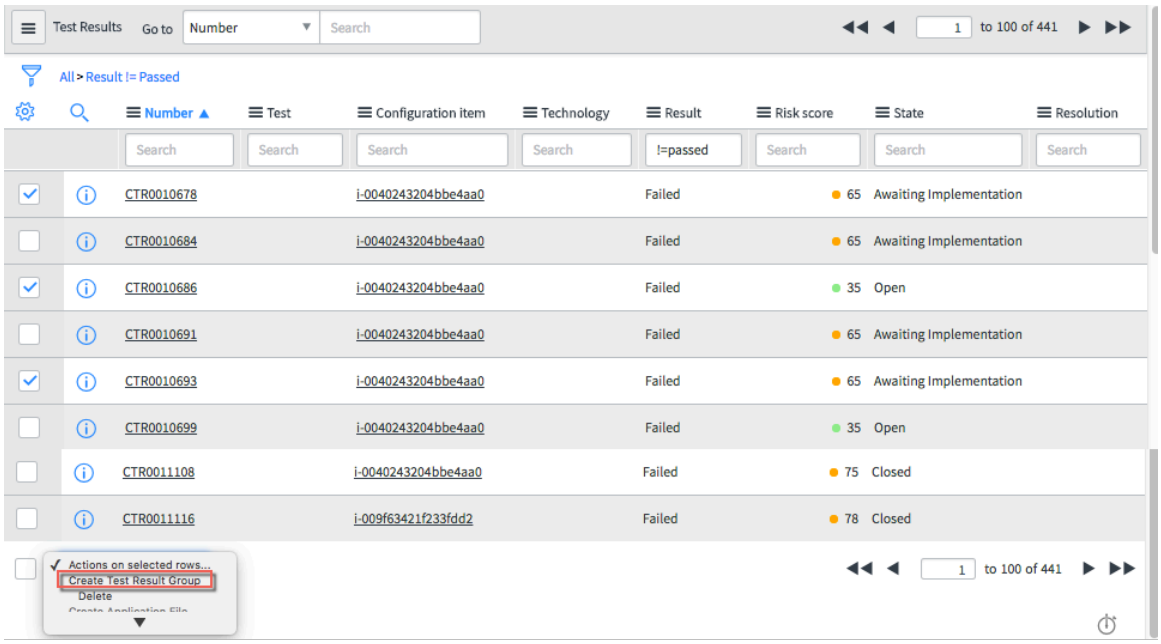
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

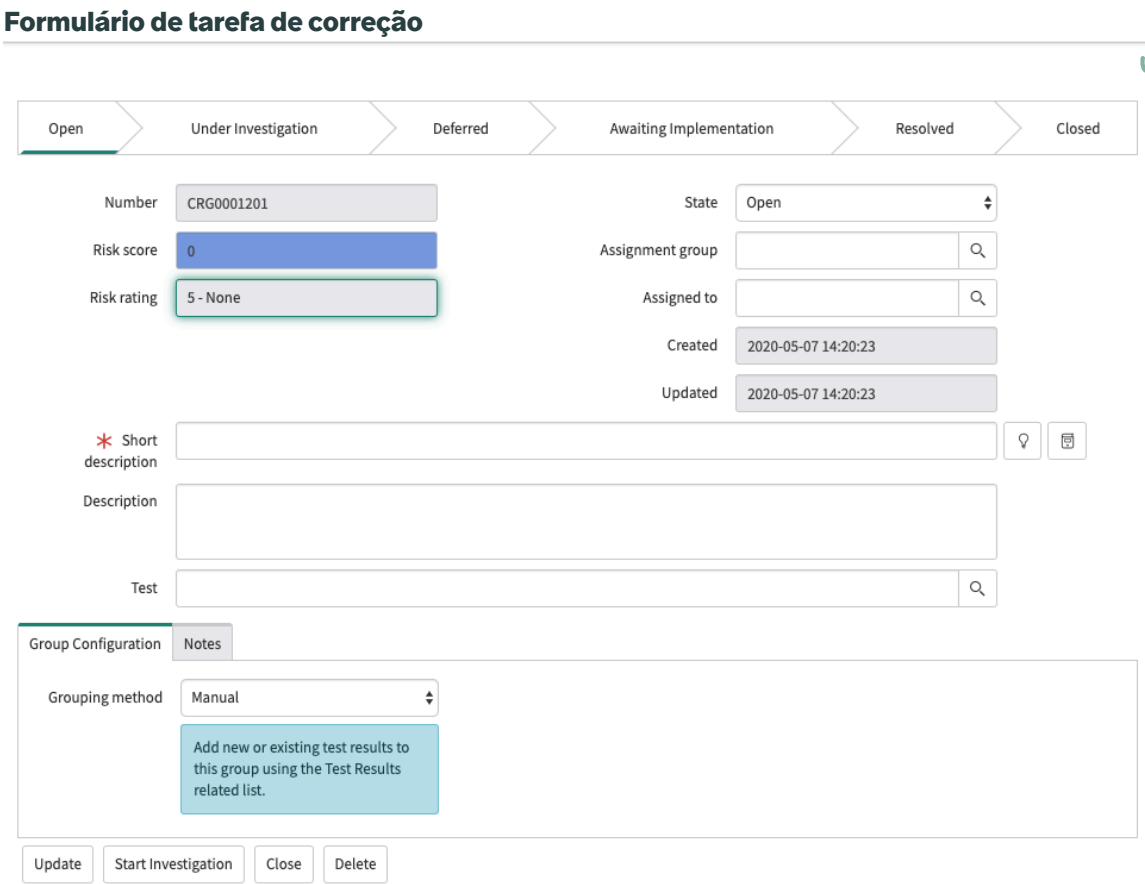
1. Navegar até **Tudo** > **Conformidade de configurações** > **Resultados de testes**.
2. No painel de navegação, selecione um módulo Resultado de teste para abrir uma lista.
3. Selecione os resultados de teste a serem incluídos na tarefa de correção marcando a caixa ao lado de cada um.
4. Abra o. **Ações nas linhas selecionadas...** menu na parte inferior da lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



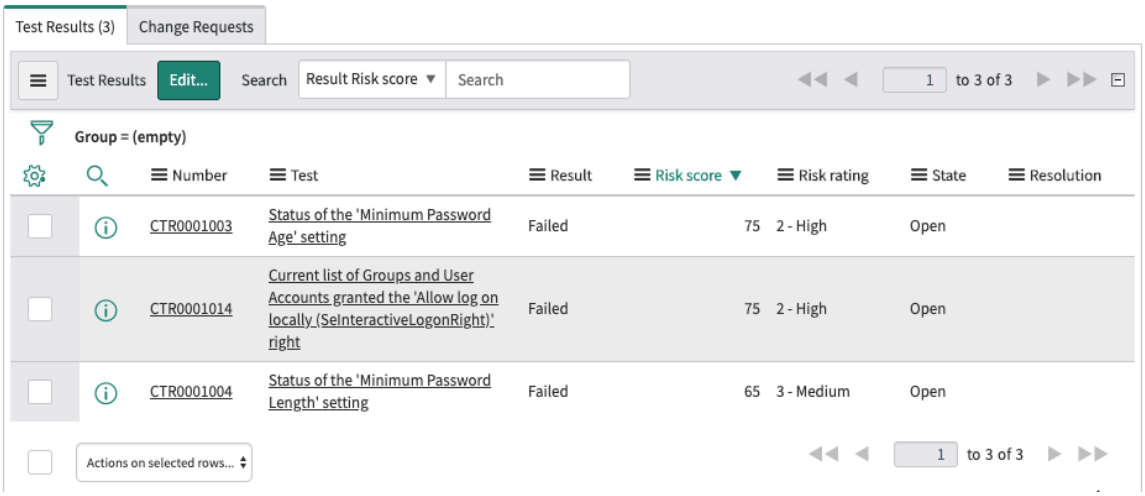
5. Escolha **Criar tarefa de correção** .
A tarefa de correção é criada e aberta.



Os resultados de teste selecionados para a tarefa de correção são exibidos na lista relacionada Resultados de teste junto com todas as solicitações de mudança associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os resultados de teste não "Encerrado" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido), e 15% da pontuação do número de resultados de testes que não estão "Encerrados".
Classificação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica o risco geral com base em um intervalo de pontuações de risco como 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade em versões anteriores.
Pontuação de risco histórico	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. A pontuação de risco inerente em todos os resultados de teste aprovados em uma tarefa de correção. Este campo exibe a quantidade de risco que foi corrigido por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.
Estado	Inicialmente **Aberto** é o estado de correção da tarefa de correção. Para obter mais informações, consulte Conformidade de configurações estados.
Grupo de atribuição	Atribua a tarefa de correção a um grupo de correção.
Atribuição a	Atribua uma equipe para corrigir a tarefa de correção.
Criação em	Data em que você criou esta tarefa de correção.
Atualização em	Data em que você atualizou esta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição Resumida	Nome da tarefa de correção.
Descrição	Descrição em texto desta tarefa de correção.
	Selecione um Teste de configuração para esta tarefa de correção.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ○ Manual (padrão) ○ Filtrar Tabela: Pré-selecionado como Resultado do teste Condição do resultado do teste: Escolha os filtros a serem usados. **Nota:** O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de teste que você escolheu em uma nova janela. Clique em **Visualização** para ver quantos resultados seus critérios de filtro retornam antes de salvar a nova tarefa de correção.
Anotações	Anotações de trabalho relacionadas a esta tarefa de correção.
Listas relacionadas	
Resultados de testes	Resultados de teste incluídos nesta tarefa de correção.
Solicitações de mudança	Solicitações de mudança associadas a esta tarefa de correção.

7. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de tarefas de correção.

Como criar uma solicitação de mudança no Conformidade de configurações

Você pode criar uma solicitação de mudança a partir de uma tarefa de correção no Conformidade de configurações aplicação.

Antes de Iniciar

Função necessária: Usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa

Ou especialista em TI ou correção, crie uma solicitação de mudança (CHG) diretamente de uma tarefa de correção para todos os resultados de teste nela. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de vulnerabilidades que exigem intervenção manual.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente das tarefas de correção atribuídas a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente a partir de uma tarefa de correção:

Padrão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento ou instrução de trabalho especificada.

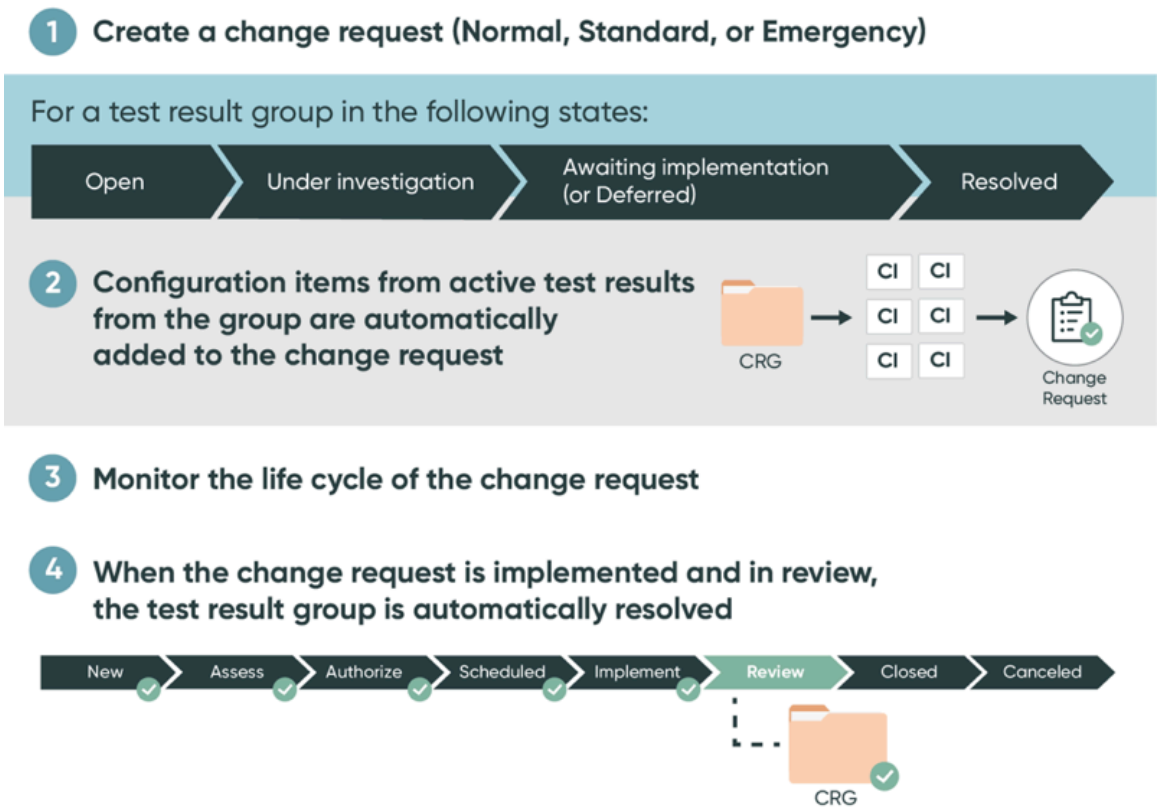
Normal

As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.

Emergência

Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de uma tarefa de correção. As etapas detalhadas deste fluxo seguem a imagem.



A partir da versão 19,0 de Resposta a vulnerabilidades, Você pode criar solicitações de mudança para tarefas de correção no Espaço de correção de TI. Para obter mais informações, consulte Crie uma solicitação de mudança no Espaço de correção de problemas de TI.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Tarefas de correção** > **Minhas tarefas em aberto**.
   A lista de tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção para a qual você deseja criar uma solicitação de mudança. Você pode criar solicitações de mudança a partir de tarefas de correção em qualquer estado diferente de **Encerrado** ou **Em revisão** .

   O registro da tarefa de correção é exibido.
3. No canto superior direito do registro, clique em **Criar mudança** .
   O formulário Solicitação de mudança é exibido.
4. Preencha os campos.
   a. Na lista de **Aplica-se a.** escolha um para continuar.

Opção	Descrição
Todos os resultados de testes ativos neste grupo	Se selecionado, todos os resultados de testes ativos desta tarefa de correção com um estado diferente de **Encerrado** são adicionados automaticamente à solicitação de mudança depois que você clica em **Criar mudança** .
Todos os resultados de testes ativos neste grupo que atendem a um conjunto de condições	Se selecionado, o Construtor de condições será exibido. Insira critérios de filtro para identificar os resultados de teste que você deseja para a nova solicitação de mudança. Um exemplo de filtro que você pode criar localizaria somente resultados de teste da tarefa de correção que correspondam a um estado específico e a uma pontuação de risco: O estado é **Aberto** E a Pontuação de risco é maior que **50** .

5. Para **Adicionar ICs ao CR** caixa de seleção, escolha uma para continuar.

Opção	Descrição
Caixa de seleção marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (ICs) que pertencem aos resultados de teste ativos desta tarefa de correção serão adicionados a esta solicitação de mudança. O resultado do teste faz a transição para **Aguardando implementação** .
Caixa de seleção desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos resultados de teste ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. A tarefa de correção permanece em seu estado atual.

6. Da lista para **Tipo de mudança** escolha um para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Emergência	Uma mudança para resolver um incidente grave.
Normal	Um tipo de mudança que é usado para implementar qualquer mudança em um serviço que não seja uma mudança padrão ou de emergência.
Padrão	Uma solicitação de mudança pré-autorizada e de baixo risco que é implementada com frequência. As solicitações de mudança padrão aprovadas podem ser predefinidas em um catálogo de modelos para tornar mais eficiente o acesso e a solicitação de uma mudança padrão. Se selecionado, dois campos serão exibidos. Selecione um de cada lista para preencher estes campos: ○ **Mudar categoria** : Selecione uma categoria para a mudança do seu catálogo existente, por exemplo, Hardware , Mudanças padrão do servidor , Software . ○ **Modelo de mudança** : Selecione um modelo disponível para solicitações de mudança com tarefas de suporte predefinidas do seu catálogo. Para obter mais informações sobre categorias de solicitação de mudança do ITSM, modelos e tipos de mudança, consulte Tipos de mudança .

O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Change Management. Por exemplo, se você mudar o nome das solicitações de Mudança padrão no ITSM de Padrão . Pré-aprovado Seu novo nome é exibido automaticamente na lista de tipo de mudança no formulário Criar solicitação de mudança.

7. Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações da tarefa de correção.
   Se necessário, edite esses campos.
8. Clique em **Criar mudança** .
   A solicitação de mudança é exibida. Na lista relacionada ICs afetados, os ICs dos resultados de teste que corresponderam aos seus critérios são exibidos. Se a solicitação de mudança exigir aprovação, o. **Aprovação da solicitação** o botão é exibido.

   Depois que a solicitação de mudança é criada, o grupo de resultados de teste é movido para **Aguardando implementação** estado. Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para **Resolvido** estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado ou você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente a tarefa de correção do Encerrado ou Adiado estados.

Associe uma tarefa de correção a uma solicitação de mudança existente

Associe uma tarefa de correção em Conformidade de configurações aplicação a uma solicitação de mudança existente.

Antes de Iniciar
Função necessária: Um usuário com a função itil

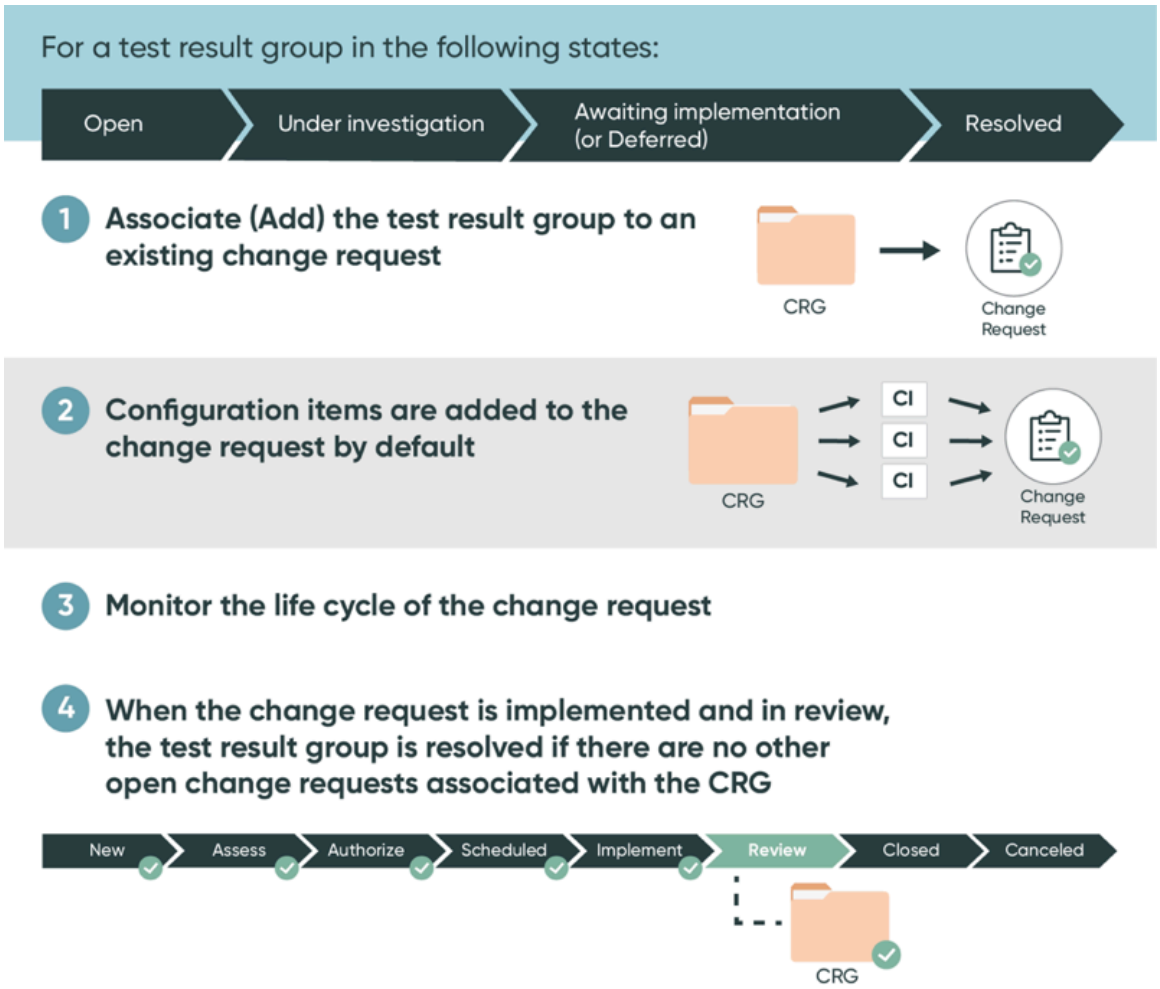
Por Que e Quando Desempenhar Esta Tarefa
Como especialista EM TI ou correção, evite criar solicitações de mudança duplicadas (CHG) ao trabalhar para resolver suas tarefas de correção associando uma tarefa de correção (RT) a uma solicitação de mudança que já esteja disponível em sua instância.

Você pode associar tarefas de correção atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros de tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança existente a uma tarefa de correção. As etapas detalhadas deste fluxo seguem a imagem.

Nota: Você pode associar uma solicitação de mudança existente a uma tarefa de correção em qualquer estado diferente de **Cancelado** (**Aberto** , **Em investigação** , **Aguardando implementação** , **Encerrado** e **Adiado**). As solicitações de mudança, incluindo as encerradas nos últimos 90 dias, estão disponíveis para associar no formulário. Quando você associa uma solicitação de mudança a uma tarefa de correção existente, somente os resultados de teste ativos e seus itens de configuração são adicionados à solicitação de mudança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Tarefas de correção** > **Minhas tarefas em aberto**.
   A lista de tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção para a qual você deseja criar uma solicitação de mudança.

   O registro da tarefa de correção é exibido.
3. No canto superior direito do registro, clique em **Criar mudança** .
   O formulário Solicitação de mudança é exibido.
4. Role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas à tarefa de correção são exibidas junto com **Adicionar** botão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Adicionar**.
   A caixa de diálogo Adicionar solicitação de mudança existente à tarefa de correção é exibida.
6. Clique no ícone de pesquisa e selecione um item na lista.
   Você pode filtrar a lista exibida para restringir sua pesquisa.
7. Clique em **Enviar**.
   O TRG é exibido junto com uma mensagem que indica que a solicitação de mudança foi associada com sucesso à tarefa de correção. Na lista relacionada Solicitações de mudança, a nova solicitação de mudança é exibida. Por padrão, os ICs da tarefa de correção são adicionados à solicitação de mudança e são exibidos na lista relacionada de ICs afetados. Você também pode adicionar ICs à solicitação de mudança a partir desta lista relacionada. Uma mensagem indica o número de resultados de teste que foram movidos para a nova tarefa de correção e o novo RT é exibido.

   Nota: Para menos de 200 resultados de teste, a operação de divisão é feita de forma síncrona e os resultados do teste são exibidos na nova tarefa de correção.

   Para mais de 200 resultados de teste, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados do teste apareçam na nova tarefa de correção. A seguinte mensagem também é exibida: n resultados de teste serão movidos de TRGxxxxxxx para a nova tarefa de correção GRCxxxxx em breve.

Você pode associar solicitações de mudança à tarefa de correção, com as seguintes exceções:

- Solicitações de mudança no **Cancelado** estado.
- Solicitações de mudança no **Encerrado** estado com mais de 90 dias.
- Solicitações de mudança já associadas ao RT. O sistema não permitirá que você associe uma solicitação de mudança que já esteja associada ao RT.

Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para **Resolvido** estado.

Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado ou você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente a tarefa de correção do Encerrado ou Adiado estados.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Divida uma tarefa de correção

De uma tarefa de correção existente no Conformidade de configurações Identifique um subconjunto de resultados de teste que você deseja mover para uma nova Tarefa de correção.

Importante: Como administrador e responsável pela correção, você pode dividir uma tarefa de correção do Vulnerability Manager Workspace e. Espaço de correção de TI respectivamente.

Antes de Iniciar

Função necessária: Um usuário com a função itil

Tradução automática

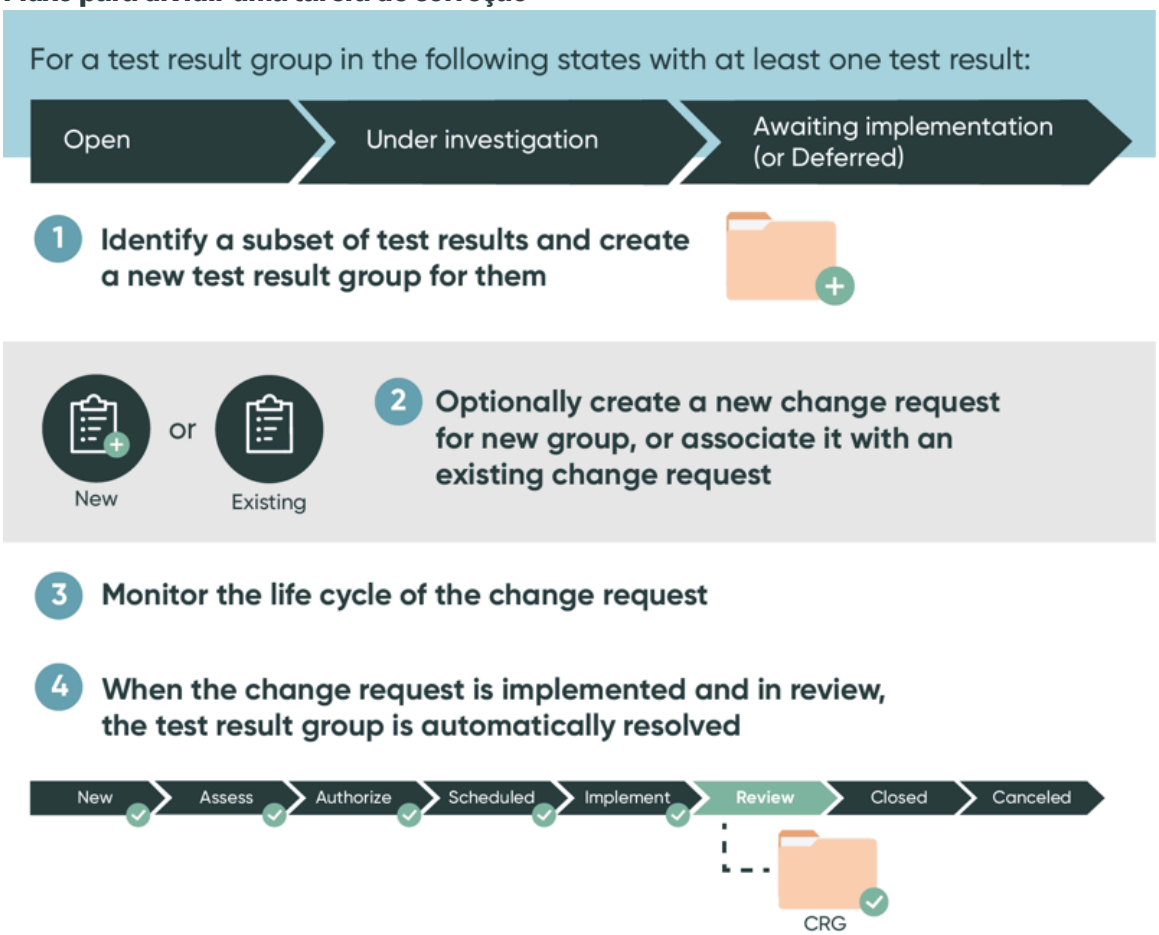
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Como especialista EM TI ou correção, você pode dividir tarefas de correção existentes no **Aberto** , **Em investigação** ou **Aguardando implementação** estados com mais de um resultado de teste. Ao criar uma nova tarefa de correção com resultados de teste que correspondem a critérios específicos, você pode trabalhar com um grupo específico de resultados de teste sem afetar a tarefa de correção original.

Quando você especifica as condições para os resultados de teste que deseja mover para uma nova tarefa de correção com o construtor de condições, somente os resultados de teste ativos que correspondem aos seus critérios são movidos para a nova tarefa. Você não precisa criar solicitações de mudança (CHGs) ao dividir uma tarefa de correção. Você tem a opção de dividir uma tarefa de correção ao criar uma solicitação de mudança ou dividir uma tarefa de correção sem criar uma solicitação de mudança.

A imagem a seguir ilustra o fluxo básico para dividir uma tarefa de correção. As etapas detalhadas deste fluxo seguem a imagem.

Fluxo para dividir uma tarefa de correção



Os casos de uso para dividir resultados de teste de tarefas de correção existentes em novas tarefas podem incluir os seguintes exemplos:

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para uma tarefa dividida.
- Quando você reatribui uma tarefa dividida para outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou exceção para uma tarefa dividida porque sabe que alguns resultados de teste em itens de configuração (IC) específicos não podem ser corrigidos em um determinado intervalo de tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Testes** > **Tarefas de correção** > **Minhas tarefas em aberto**.
   A lista de tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção que você deseja dividir.

   O registro da tarefa de correção é exibido.
3. Para criar um subconjunto de resultados de teste para uma nova tarefa que corresponda a critérios específicos, siga estas etapas.

   No canto superior direito do registro, clique em **Tarefa dividida** .

   Este método de criação de uma nova tarefa de correção pode ser preferencial se estiver trabalhando em um grupo grande com vários resultados de teste.

   O formulário Tarefa de correção dividida é exibido.
4. Com o Construtor de condições exibido, especifique as condições dos resultados de teste que você deseja mover para uma nova tarefa de correção.

   Por exemplo, você pode preferir filtrar somente resultados de teste que correspondam às seguintes condições:

   - Em **Aberto** estado.
   - Pontuações de risco maiores que 75.
   - O resultado é **Falha** .

   Se os resultados do teste corresponderem ao seu filtro depois que você inserir as condições, uma mensagem será exibida com o número de resultados de teste correspondentes.

   Se for exibida uma mensagem informando que nenhum resultado de teste corresponde ao seu filtro ou que todos os resultados de teste correspondem aos seus critérios, ajuste as condições para que pelo menos um resultado de teste corresponda aos critérios de filtro.
5. Clique em **Visualizar itens** para exibir os resultados de testes correspondentes.
   Uma nova janela, Tarefas de correção, exibe os itens.
6. Para visualizar detalhes sobre os resultados de teste que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Tarefa dividida** para criar o novo grupo.
   Esses detalhes incluem o grupo de atribuição e a quem o resultado do teste está atribuído. Exibir essas informações na visualização pode ajudar a garantir que a nova tarefa seja atribuída corretamente.

   a. Com a lista Correções exibida na visualização, clique em um item na coluna Resultado.
      O registro Resultado do teste é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Verifique **Grupo de atribuição** e. **Atribuído a.** os campos estão corretos.

c. Clique em **Atualizar**.

7. Quando você estiver pronto para criar a nova tarefa de correção, clique em **Tarefa dividida** .
Uma mensagem indica o número de resultados de teste que são movidos para a nova tarefa de correção e a nova tarefa de correção é exibida. Para ajudá-lo a identificar a nova tarefa, você pode preferir editar o texto no **Descrição resumida** E edite os campos Grupo de atribuição ou Atribuído a novamente, se necessário.

Nota: Para menos de 200 resultados de teste, a operação de divisão é feita de forma síncrona e os resultados do teste são exibidos na nova tarefa.

Para mais de 200 resultados de teste, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados do teste apareçam na nova tarefa. A seguinte mensagem também é exibida: n resultados de teste serão movidos de TRGxxxxxxx para a nova tarefa de correção GRCxxxxx em breve.

8. Como alternativa, você pode criar uma nova tarefa de correção selecionando resultados de teste diretamente na lista relacionada Resultados de teste em uma tarefa de correção.

Você pode preferir este método se tiver apenas alguns resultados de teste em uma tarefa de correção ou se souber exatamente quais testes deseja mover para uma nova tarefa de correção.

a. Com o registro da tarefa de correção exibido, role até a lista relacionada Resultados de teste.

b. Na coluna extrema esquerda, marque as caixas de seleção dos resultados de teste para os quais você deseja criar uma nova tarefa de correção.

c. Na lista Ações nas linhas selecionadas no canto inferior esquerdo do registro, clique em **Tarefa dividida** .

d. No formulário Tarefa de correção dividida que é exibido, para ajudar você a identificar o novo grupo, talvez você prefira editar o texto no **Descrição resumida** campo.

e. Clique em **Tarefa dividida** .
Uma mensagem indica o número de resultados de teste que foram movidos para a nova tarefa e a nova tarefa de correção é exibida.

Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para **Resolvido** estado.

Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado ou você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente a tarefa de correção do Encerrado ou Adiado estados.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você pode criar ou associar solicitações de mudança para suas novas tarefas de correção. Para obter mais informações, consulte Associe uma tarefa de correção a uma solicitação de mudança existente e Como criar uma solicitação de mudança no Conformidade de configurações.

Remova atribuições de tarefas de correção para você ou seus grupos

Reatribuir os registros de resultado de teste no Conformidade de configurações se os registros foram atribuídos incorretamente a você ou ao seu grupo.

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Se você determinar que as tarefas de correção (RTS) e os resultados de testes associados não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, poderá remover a si mesmo ou aos seus grupos dos campos Atribuído a e Grupo de atribuição nos registros de RT.

. **Cancelar atribuição** O botão é exibido nos registros de tarefa de correção em qualquer estado diferente dos estados Encerrado ou Resolvido.

Procedimento

1. Navegue até um registro de tarefa de correção atribuído a você que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar **Atribuído a.** e. **Grupo de atribuição** na parte superior do registro, selecione **Cancelar atribuição** .
3. Em **Cancelar atribuição** , forneça anotações de trabalho e selecione **Enviar** .
   - As anotações de trabalho fornecidas são exibidas na seção Anotações.
   - Em **Aprovação de mudança de estado** O registro de aprovação de mudança de estado (nº da CA) exibe o estado Em revisão, o que ajuda você a rastrear o fluxo de trabalho de aprovação.
   - Em **Aprovações solicitadas** Sua solicitação para remoção de você ou do seu grupo de atribuição é exibida como o estado Solicitado.
4. **Opcional:** Como alternativa, selecione **Cancelar atribuição** No menu Mais opções ( ) para limpar os campos de atribuição.

Resultado

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovar uma solicitação de cancelamento de atribuição em Conformidade de configuração .

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada farão a transição para **Aprovado** . Você e seus grupos serão removidos do **Atribuído a.** e. **Grupo de atribuição** campos. Não atribuído é exibido em **Tipo de atribuição** E a tarefa de correção é exibida na lista do módulo Não atribuído para Conformidade de configurações aplicação.

  As notificações de que registros não são atribuídos são enviadas automaticamente para gerentes ou analistas de vulnerabilidades no grupo de notificação Cancelar atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre as notificações e as propriedades desse recurso, consulte Removendo atribuições de grupos de resultados de teste de Conformidade de configuração .

- Se sua solicitação for rejeitada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada serão transferidos para Rejeitado.

Nota: Como administrador de vulnerabilidades, você pode definir *sn_vulc.unassign_test_result_group.approval_required*propriedade do sistema para **falso** para desabilitar o processo de aprovação.

O que Fazer Depois

Navegue até o módulo Não atribuído para Conformidade de configurações a aplicação monitora todos os registros não atribuídos para itens que podem se enquadrar no seu escopo e, em seguida, reatribua-os a você mesmo.

Aprovar uma solicitação de cancelamento de atribuição em Conformidade de configurações

Aprove solicitações para a remoção de tarefas de correção de um grupo de atribuição ou de um usuário individual no Conformidade de configurações aplicação.

Antes de Iniciar

Função necessária: sn_vulc.unassign_approver

Por Que e Quando Desempenhar Esta Tarefa

Uma configuração de aprovação é fornecida por padrão. Para aprovações de cancelamento de atribuição, um aprovador é necessário no grupo de aprovação Aprovador - Nível 1. Por padrão, o grupo de aprovação Cancelar atribuição (CC do aprovador - Nível 1) é criado e os usuários que fazem parte deste grupo podem aprovar a solicitação. Por padrão, este grupo contém a função de aprovador de cancelamento de atribuição, sn_vulc.unassign_approver. Você pode modificar ou criar um grupo e atualizar a configuração de aprovação navegando até **Tudo** > **Conformidade de configurações** > **Administração** > **Regras de aprovação** > **Solicitação de mudança do campo de tarefa de correção** > **Tarefa de correção não atribuída**.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação adicionando os comentários apropriados.

Fechamento automático dos resultados de testes

Você pode fechar automaticamente os resultados de teste (TRs) associados a itens de configuração (ICs) desativados.

Para configurar a opção de fechamento automático, navegue até a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** e defina como verdadeiro. Para fechar automaticamente TRs relacionados a ICs desativados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Trabalhar com itens de configuração desativados em Conformidade de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Trabalhar com itens de configuração desativados em Conformidade de configuração

Itens de configuração desativados (ICs) são movidos para o estado desativado, arquivado ou excluído em Configuration Management Database (CMDB). Conformidade de configurações Contém resultados de teste (TRs) compostos por ICs. Quando o estado de um IC é atualizado para desativado, os TRs associados são encerrados com o subestado "IC desativado".

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Se o CMDB mudar o status da fase do ciclo de vida de um IC para desativado, você poderá optar por fechar automaticamente os TRs associados. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O IC descontinuado é arquivado ou excluído permanentemente do CMDB.

Impacto de descontinuar os ICs:

- **Impacto nos itens descobertos:** Quando o IC é descontinuado, o DI relacionado é marcado como "IC desativado".
- **Impacto nos resultados do teste:** Quando o estado de um DI é atualizado para "IC desativado", o TR associado é encerrado e a seção Notas é atualizada automaticamente.

  Nota: O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando **sn_vulc.auto_close_test_results_linked_to_retired_CIs** a propriedade está definida como verdadeira. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O trabalho agendado *Close Test Results for decommissioned CIs* É executado diariamente para o DIS atualizado. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará o DI que contém um IC desativado e fechará o TR relacionado com o subestado "IC desativado". Se todos os TRs em uma tarefa de correção forem encerrados e seu subestado for IC desativado, a tarefa de correção também será encerrada com o subestado "Cancelado".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se um IC voltar para o estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os TRS são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente os resultados de testes relacionados a ICs desativados

. Configuration Management Database (CMDB) Muda o status da fase do ciclo de vida de um item de configuração (IC) para desativado. Você pode optar por fechar automaticamente os resultados de teste associados (TRs).

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Para fechar automaticamente os TRs associados, você deve habilitar propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** Para fechar automaticamente TRs associados a ICs descontinuados. Se esta opção estiver habilitada, TRs novos e existentes relatados para o mesmo IC serão criados ou atualizados automaticamente no estado "Encerrado". Eles são baseados no ID do ativo na carga do scanner e no status de entrada de itens descobertos. Para obter mais informações sobre o impacto de ICs descontinuados, consulte Trabalhar com itens de configuração desativados em Conformidade de configuração.

Nota: O estado de um DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando **sn_vulc.auto_close_test_results_linked_to_retired_CIs** a propriedade do sistema está habilitada.

Procedimento

1. Navegar até **Propriedades do sistema** > **Todas as propriedades** e filtrar por `sn_vulc.auto_close_test_results_linked_to_retired_CIs`Na coluna Nome.
2. Selecione a propriedade.
3. Para fechar automaticamente os resultados de teste associados aos ICs desativados, defina o valor da propriedade como verdadeiro.

Fechando automaticamente resultados de testes obsoletos em Conformidade de configurações

Você pode ativar o recurso Fechar automaticamente resultados de testes obsoletos para fechar automaticamente os resultados de testes mais antigos não encontrados recentemente por suas integrações de terceiros. Movendo estes resultados de teste para **Obsoleto** reduz o número de resultados de testes ativos e tarefas de correção em sua instância e ajuda a reconciliar ativos em Configuration Management Database (CMDB).

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

O módulo Encerramento automático de resultados de testes obsoletos ajuda a fechar automaticamente resultados de testes mais antigos e obsoletos que não foram encontrados recentemente por suas integrações de terceiros. Os resultados do teste são movidos para **Obsoleto** com base nas condições definidas no construtor de condições.

Termos principais

Resultado do teste

Os resultados dos testes são resultados importados de bibliotecas de testes de configuração que são mapeados para estruturas, políticas e fontes autorizadas que definem como uma classe de ativos de tecnologia deve ser governada. . Conformidade de configurações a aplicação não calcula os resultados do teste, mas os importa com integrações de terceiros.

Data da última verificação do ativo

Refere-se ao valor da coluna Data de verificação de conformidade da última configuração da tabela Item descoberto relacionado ao resultado do teste. Esta data se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Data da última falha

Refere-se à data da coluna Visto pela última vez da tabela Resultados de teste quando **Resultado** o valor do campo é [failed].

Resultados de testes obsoletos

Refere-se aos resultados de testes em sua instância que estão desatualizados e não foram encontrados, atualizados ou detectados por verificações de integração de terceiros por um período significativo.

Resultados de teste encontrados pela última vez

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data mais atual ou mais recente (dias atrás) em que os resultados do teste foram encontrados novamente pelo scanner. Este parâmetro pode ser configurado.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros. Quando isso acontece, os resultados do teste de configuração associados aos ativos não são atualizados no Conformidade de configurações por detecções importadas e elas se tornam inativas (obsoletas).

Para reduzir o número de resultados de testes (TRs) ativos e tarefas de correção (RTS) em sua instância, ative o recurso Encerrar automaticamente resultados de testes obsoletos. Este recurso fecha automaticamente os resultados de testes antigos que têm estados inalterados ou não foram importados recentemente por suas integrações.

Por exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado em detecções de um scanner de terceiros nos últimos 90 dias. Se você definir o construtor de condições no módulo Encerrar automaticamente resultados de testes obsoletos para fechar resultados de testes que não foram encontrados ou atualizados nos últimos 90 dias ou mais, esse recurso fechará automaticamente todos os resultados de teste que correspondam a esta filtragem.

Nota: Este recurso fecha detecções de resultado de teste somente com base nas condições de filtro que você define no Construtor de condições e são detectadas por integrações de scanner de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O campo Resolução

Para diferenciar as detecções que são encerradas por scanners de terceiros, como Qualys e. Tenable.io E o recurso Fechar automaticamente resultados de testes obsoletos em sua instância, um novo valor para **Resolução** O campo, [Encerrado-obsoleto], foi adicionado. **Obsoleto** Indica que um TR foi encerrado pelo recurso de fechamento automático. **Encerrado** ou **Fixo-Encerrado** Indica que um TR foi fechado por um scanner.

Acúmulo de estados de TR para TRGS com o recurso de fechamento automático

A progressão de estado e a precedência dos resultados de testes é: **Aberto** > **Encerrado** > **Fixo-Encerrado** > **Obsoleto**.

1. Se algum TRs em um TRG for **Aberto** , O estado de TRG não é alterado.
2. Se pelo menos um TR for **Encerrado - Corrigido** e o resto é **Encerrado - obsoleto** , O estado de TRG faz a transição para **Encerrado - Corrigido** .
3. Se todos os TRs em um TRG forem **Encerrado - obsoleto** , O estado de TRG faz a transição para **Cancelado - Cancelado** .

Integrações compatíveis

Para obter mais informações sobre as integrações de terceiros compatíveis com este recurso, consulte Noções básicas do Qualys Vulnerability Integration e. Tenable.io integrações com Resposta a vulnerabilidades e. Conformidade de configurações aplicações.

Fechar automaticamente resultados de testes obsoletos em Conformidade de configurações

Encerrar automaticamente resultados de testes obsoletos (TRs) para fechar automaticamente os resultados de testes mais antigos com base nas condições de filtro definidas.

Antes de Iniciar

Para obter mais informações sobre esse recurso, termos principais e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de resultado de teste, consulte Fechando automaticamente resultados de testes obsoletos em Conformidade de configurações.

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Administração** > **Fechar automaticamente os Resultados de testes obsoletos**.
2. Preencha os campos

Campo	Valor
Nome	Nome deste registro de configuração.
Ativo	Se selecionado, este registro estará ativo e fechará automaticamente todos os resultados de teste que correspondam aos critérios de filtro.
Ignorar TRs obsoletos para TRs adiados	Se selecionado, todos os TRs mapeados para **Em revisão** ou **Adiado** os estados são ignorados e não encerrados. Se você desmarcar esta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
	opção, todos os TRs que corresponderem aos seus critérios serão encerrados.
Ordem de execução	100 é o valor padrão. Este valor determina a ordem de execução em ordem crescente para cada registro de configuração usado para localizar e marcar resultados de teste obsoletos.
Descrição	Uma descrição deste registro. Este texto pode ajudá-lo a encontrá-lo facilmente novamente se você criar um número maior de registros.
Condição	As condições de filtragem usadas para encontrar TRs que você deseja encerrar. O filtro padrão é **Item descoberto** > **Última varredura**.

3. Clique em **Enviar**.

   O trabalho agendado, *`Auto-Close Stale Test Results`*, é executado diariamente. Este trabalho identifica os TRs com base nas condições que você forneceu e faz a transição das que correspondem ao estado: **Encerrado** .

   Depois que os TRs são marcados como Estado: **Obsoleto** Se o scanner encontrar esses TRs novamente, os resultados do teste serão reabertos e os estados voltarão para **Aberto** .

   Se um TR estiver marcado como Estado: **Obsoleto** E o scanner descobrir que foi corrigido (Resolução: **Corrigido** TR faz a transição para o estado: **Encerrado** Resolução: **Corrigido** . TRS que têm **Resultado** : **Aprovado** Permanecer como estado: **Encerrado** Resolução: **Corrigido** . Os estados também são acumulados em tarefas de correção, conforme descrito na lista a seguir:

   a. Se algum TRs em uma tarefa de correção for **Aberto** , o estado da tarefa de correção não é alterado.
   b. Se pelo menos um TR for Estado: **Encerrado** Resolução: **Corrigido** e o resto é **Obsoleto** , o estado da tarefa de correção faz a transição para **Encerrado** Resolução: **Corrigido** .
   c. Se todos os TRs em uma tarefa de correção forem **Encerrado** Resolução: **Corrigido** , O estado de TRG faz a transição para o Estado: **Encerrado** Resolução: **Cancelado** .

   Para obter mais informações sobre transições de estado, consulte Resultado de teste e transições de estado da tarefa de correção no Conformidade de configurações aplicação.

Feche uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção pode ser encerrado imediatamente sem análise adicional, poderá usar **Fechar** recurso.

Antes de Iniciar

Função necessária:

- sn_vulc.admin
- sn_vulc.remediation_owner

Nota: Com a função sn_vulc.remediation_owner, você pode reatribuir ou fechar tarefas de correção atribuídas a você ou aos seus grupos de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A partir da v15.0 de Conformidade de configurações. **Fechar** o botão foi removido para uma tarefa de correção.

Quando você resolve uma tarefa de correção, a resolução é anotada reflete nas anotações de trabalho de todos os resultados de testes.

Procedimento

1. Abra o registro da tarefa de correção.
2. Selecione **Fechar** botão.
3. Descreva por que o problema está sendo encerrado na janela pop-up.
4. Selecione **Fechar**.

Tópicos relacionados

Conformidade de configurações estados

Solicitação e aprovação de uma exceção para uma tarefa de correção

Você pode solicitar o adiamento da correção de uma tarefa de correção por um período especificado. Os usuários que fazem parte do grupo de aprovadores podem aprovar solicitações de exceção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Para solicitar ou aprovar solicitações de exceção, consulte:

- Solicite uma exceção para uma tarefa de correção em Conformidade de configurações
- Aprovar uma solicitação de exceção em Conformidade de configurações

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v14.11 de Conformidade de configurações, você pode configurar os intervalos de tempo para aprovar exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o resultado do teste muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o resultado do teste será revertido para o status Aberto. O estado anterior é armazenado em **backup_state** campo. Para obter mais informações, consulte Configure regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma exceção para uma tarefa de correção em Conformidade de configurações

Solicite uma exceção para adiar a correção de uma tarefa de correção por um período especificado se ela não puder ser corrigida imediatamente.

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Importante: Você pode solicitar uma exceção para:

- tarefas de correção no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI. Para obter mais informações, consulte Solicite uma exceção no Espaço de correção de problemas de TI.
- vários resultados de testes simultaneamente do Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Tarefas de correção** > **Todas as tarefas**.
2. Selecione a tarefa de correção para a qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Em investigação ou Aguardando implementação.
3. No formulário Tarefa de correção, clique em **Exceção de solicitação** .

   Nota: Dependendo de Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade está selecionado em **Conformidade de configurações** > **Gestão de exceção** , o formulário Solicitar exceção muda. Veja Configure a Gestão de exceções para Conformidade de configurações

4. Se Resposta a vulnerabilidades Estiver selecionado na tela Gestão de exceções e faça o seguinte:

   a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Tudo** > **Conformidade de configurações** > **Administração** > **Gestão de exceção** tela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando a solicitação de exceção expira, a tarefa de correção é revertida para o estado Aberto. **Nota:** A partir da versão 14,7 de Conformidade de configurações(CC), se uma tarefa de correção adiada for reaberta por um scanner antes que a janela de exceção expire, o estado da tarefa de correção mudará de Aberto para Adiado. Esta funcionalidade está desabilitada por padrão. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema `sn_vulc.auto_defer_test_result_in_active_exc` verdadeiro. Além disso, a data Adiado até persiste mesmo depois que a tarefa de correção é reaberta após a data de expiração.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Defina mapeamentos de motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Aprovação da solicitação** .

Resultado

O estado da tarefa de correção muda para Em revisão. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicite uma extensão para uma regra de exceção em Conformidade de configurações

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do Resposta a vulnerabilidades Espaços de trabalho. Para obter mais informações, consulte Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Extensão da solicitação** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até a qual a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Aprovação da solicitação** .
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas. Um e-mail também é acionado no envio da solicitação e na ação subsequente pelo aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicite uma exceção para tarefas de correção usando GRC: Gestão de políticas e conformidade

Solicitar exceções de política usando GRC capacidade de gestão de exceções de política no Gestão de políticas e conformidade aplicação a partir de Conformidade de configurações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de usar a Integração de exceção de política para solicitar exceções de política, você deve baixar o. GRC: Gestão de políticas e conformidade aplicação do ServiceNow Store.

Função necessária: sn_vulc.remediation_owner

Você também pode solicitar exceções na IU clássica.

Por Que e Quando Desempenhar Esta Tarefa

Importante: Como administrador e responsável pela correção, você pode solicitar uma exceção de política para uma tarefa de correção (RT) no Vulnerability Manager Workspace e. Espaço de correção de TI respectivamente.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** (ou **Tarefas de correção**)> **Todos** e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Exceção de solicitação** .
3. Se GRC: Gestão de políticas e conformidade Selecionado na tela Gestão de exceções, faça o seguinte.

   a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começará. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e quando o estado do item vulnerável ou grupo muda de Adiado para Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** Que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Aprovação da solicitação** .
O estado da tarefa de correção muda para Em revisão e uma exceção de política é criada. Use **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

c. Exiba a exceção de política clicando na lista relacionada Exceções de política.

d. Clique no número da exceção de política.

e. Em **Aprovador** , selecione o nome do aprovador.

f. Clique na guia Origem e selecione um objetivo de controle no **Objetivo de controle** campo.

g. Clique na guia Avaliação de risco e selecione a classificação de risco em **Classificação de risco** campo.

h. Salve o formulário.

i. Clique em **Controles afetados** guia.

j. Adicione os controles clicando em **Adicionar** .

k. Salve o formulário.

Nota: Você pode criar uma revisão de conformidade clicando em **Solicitar revisão de conformidade** .

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicite aprovação adicional clicando em **Solicitar aprovação adicional** .

O estado do registro muda para Adiado. O motivo informado é aquele que você selecionou ao gerar a solicitação de exceção. . **Adiamento** fornece anotações adicionais sobre o registro.

Nota: Se a solicitação for rejeitada, o registro será movido para o estado anterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.
   Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Aprovar uma solicitação de exceção em Conformidade de configurações

Aprove solicitações de exceção para tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações de risco e aprová-las para adiamento até que possam ser corrigidas.

Importante: Como administrador ou analista, você pode aprovar ou rejeitar uma solicitação de exceção do Vulnerability Manager Worksapce.

Antes de Iniciar
Função necessária: sn_vulc.exception_approver

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprovar ou rejeitar a solicitação com comentários apropriados.

Nota: No caso de um fluxo de trabalho de aprovação de dois níveis, após a aprovação de primeiro nível, a solicitação é enviada para o segundo nível para aprovação posterior. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.

Depois que a solicitação é aprovada, a tarefa de correção passa para um estado Adiado. Em caso de rejeição, a tarefa de correção será revertida para o estado anterior.

Defina mapeamentos de motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar
Função necessária: sn_vul.compliance.manager e sn_vulc.admin

Procedimento

1. Navegar até **Tudo** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

2. Clique no registro de integração Resposta a vulnerabilidades do contêiner - CVIT.
3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista Opções de motivo, clique em **Novo** .
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Opções de motivo, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na lista Opções de motivo, clique em **Novo** .

b. Clique no ícone de lupa.

c. Clique em **Nova**.

d. No formulário, preencha os campos.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos do motivo da exceção de política para as respectivas aplicações. Para navegar até esta tabela, insira sn_sec_cmn_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Pedido para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham **Padrão** o campo selecionado estará disponível.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Análise e emissão de relatórios para Conformidade de configurações

Os relatórios a seguir são fornecidos para monitoramento.

Exiba políticas, ICs, testes e resultados de testes no Conformidade de configurações Relatórios de visão geral.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Conformidade de configurações emissão de relatórios

. Conformidade de configurações A página inicial fornece uma visão executiva de políticas, ICs, testes e resultados de testes, ajudando a equipe de segurança a identificar áreas de preocupação rapidamente. Conformidade de configurações gráficos de significância podem ser

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adicionados, conforme necessário. Você também pode retornar Conformidade de configurações- informações relacionadas usando o recurso de pesquisa global.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

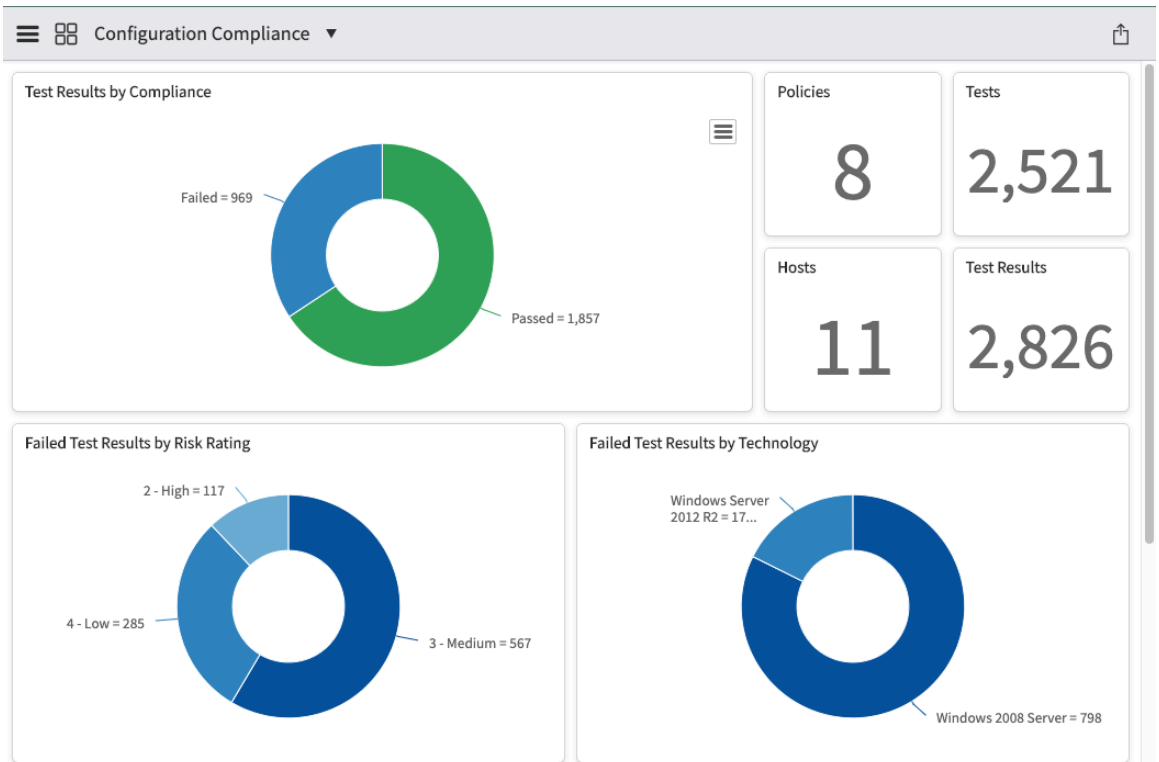
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados) para exibir dados gerais específicos dessa parte do gráfico. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota:

- Painéis no Conformidade de configurações A página inicial está disponível somente quando a aplicação Performance Analytics para Conformidade de configuração está ativada. Para obter as etapas para ativar esta aplicação, consulte Ativar Performance Analytics para Conformidade de configurações.
- Qualquer pessoa com a função sn_vulc.read pode exibir o painel. Qualquer pessoa na função sn_vulc.write ou sn_vulc.admin pode criar e editar um painel. Somente sn_vulc.admin pode excluir um painel.

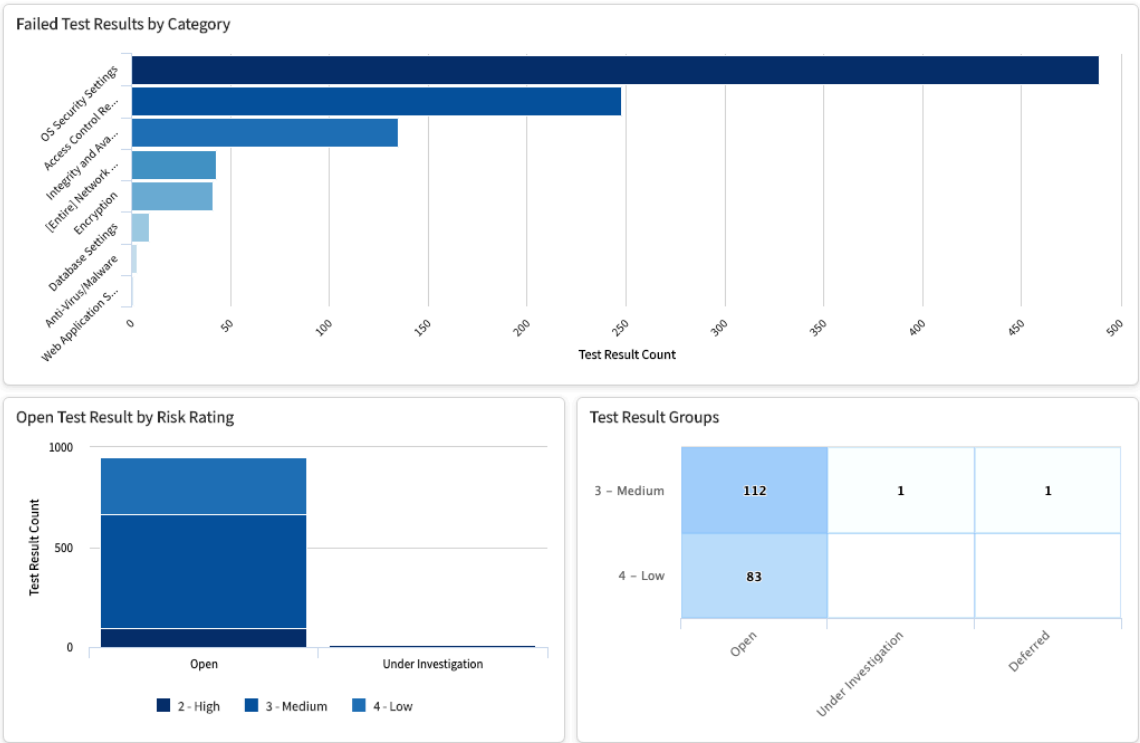
Relatórios de Visão geral da vulnerabilidade



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatório de conformidade de configuração



Relatórios de Visão geral da vulnerabilidade

Nome	Visual	Descrição
Resultados de testes por conformidade	Donut	Exibe o número de testes em aberto aprovados ou reprovados.
Políticas	Número	Número de políticas com resultados de teste com falha.
Testes	Número	Número de testes com resultados de teste reprovados.
Hosts	Número	Número de hosts com resultados de teste com falha.
Resultados de testes	Número	Exibe o número de resultados de testes.
Resultados de testes com falha por classificação de risco	Donut	Exibe o número de testes com falha por classificação de risco.
Resultados de testes com falha por tecnologia	Donut	Exibe modelos com testes com falha.
Resultados de testes com falha por categoria	Barra	Exibe categorias com os resultados de teste mais reprovados.
Resultado de teste em aberto por classificação de risco	Barra	Exibe o número de resultados de testes em aberto por classificação de risco.
Tarefas de correção	Gráfico	Exibe tarefas de correção por estado e classificação de risco.

Conformidade de configurações painel

Isso Solução para Performance Analytics e relatórios pré-empacotado Performance Analytics e. Emissão de relatórios conteúdo para uso com outros ServiceNow AI Platform produtos. Isso Solução para Performance Analytics e relatórios fornece visibilidade sobre configurações de nível de host fora de conformidade e do plano de controle de nuvem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta Solução de análise de plataforma contém conteúdo de Performance Analytics e relatório pré-empacotado para uso com outros ServiceNow AI Platform produtos. Esta Solução de análise de plataforma fornece visibilidade sobre configurações de nível de host não compatíveis e do plano de controle de nuvem.

O painel Performance Analytics para Conformidade de configuração contém vários widgets que apresentam dados para diferentes dimensões. Ele fornece uma exibição abrangente das tendências de conformidade, problemas de configuração, tendências de correção e gestão de exceções.

Nota: . Performance Analytics para Conformidade de configurações o plug-in deve ser instalado para exibir o. Conformidade de configurações Painel [PA] no Next Experience estrutura. Se não estiver instalado, você poderá exibir o painel existente, que é criado usando a estrutura de emissão de relatórios.

Ativar Performance Analytics para Conformidade de configurações

Ative o pacote de conteúdo ServiceNow Store aplicação para Solução para Performance Analytics e relatórios.

Antes de Iniciar

Ative a versão de assinatura completa de Performance Analytics na instância em que você está ativando isso Solução para Performance Analytics e relatórios. Você pode ativar Performance Analytics em uma instância de não produção sem comprar uma assinatura. Para obter mais informações, consulte Ativar assinatura da Análise de desempenho .

Você precisa de um Now Support conta e permissão para solicitar aplicações para as instâncias em consideração. . Now Support a conta e a instância devem fazer parte da mesma empresa. Para obter mais informações, consulte Instale um produto da ServiceNow em ServiceNow Store.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Usar Performance Analytics para Conformidade de configurações painel para gerar relatórios sobre as tarefas de correção, o status de conformidade, as ações de correção e as solicitações de exceção.

Procedimento

1. Navegar até **Tudo** > **Aplicações do sistema** > **Todas as aplicações** > **ServiceNow Store**.
2. Procure Performance Analytics para Conformidade de configurações e verifique se você tem os direitos válidos.
3. Pesquisar Performance Analytics para Conformidade de configuração .
4. Instale a aplicação .

   Ao instalar este aplicativo, você também ativa o. Conformidade de configurações aplicação.

Exibindo o. Performance Analytics para Conformidade de configurações painel

Você pode gerenciar seus problemas de configuração mais importantes e corrigi-los rapidamente exibindo os relatórios no Conformidade de configurações Performance Analytics Painel (PA).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Funções necessárias de ServiceNow AI Platform

As funções a seguir são necessárias para Conformidade de configurações Performance Analytics painel:

- administrador: Um administrador pode instalar e ativar o. Performance Analytics para Conformidade de configuraçõese fazer mudanças nas propriedades do sistema.
- pa_admin: Um administrador de análise de desempenho pode criar e revisar trabalhos em segundo plano, indicadores, detalhamentos, widgets e painéis. Este administrador também pode configurar e iniciar a coleta de dados.
- sn_vulc.read: Um usuário com a função de leitura pode revisar os dados do painel.

Acesse Conformidade de configurações painel

Para abrir o painel, navegue até **Tudo** > **Conformidade de configurações** > **Visão geral**.

Importante:

A partir da versão 14,9 de Conformidade de configurações Este painel também pode ser exibido na IU do Next Experience. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique em **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e. Painéis no Espaço de correção de TI .

Nota: Se você estiver em Tokyo, Você pode exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações Guias do painel [PA]

Guia "Visão geral"

. **Visão geral** fornece cinco filtros. Esses filtros são Categoria Ativo, Tipo de recurso de nuvem, Provedor de serviço de nuvem, Conta de nuvem e Região de nuvem, que você pode aplicar para visualizar os relatórios dos filtros aplicados. Se você selecionar uma categoria e aplicar as mudanças, todos os widgets compatíveis com a categoria serão atualizados. Cada widget exibe o filtro aplicado na parte inferior e o número de filtros aplicados no ícone de filtro do widget. Clique no relatório em um widget para exibir as informações adicionais no **Detalhes do KPI** guia. Em **Detalhes do KPI** , você pode:

- Mostre os registros.
- Compare os registros.
- Altere o tipo de gráfico.
- Selecione o intervalo de datas.
- Exiba as tendências baseadas na duração.
- Aplique os filtros adicionais, incluindo os filtros que não estão disponíveis no **Visão geral** guia. Um exemplo é o marcador Host.

O exemplo a seguir mostra como você pode aplicar os filtros no **Visão geral** e execute as ações no **Detalhes do KPI** guia.

Guia Visão geral no painel Conformidade de configuração

Guia Conformidade

. **Conformidade** Exibe a porcentagem de conformidade das várias fontes autorizadas, como HIPAA (Health Insurance Portability and Accountability Act) e DISA (Data Interchange Standards Association). Você pode refinar esta lista usando os filtros de cabeçalho da coluna e selecionando uma categoria.

O exemplo a seguir mostra como você pode filtrar os dados no **Conformidade** guia.

Guia Conformidade no painel Configuração Conformidade

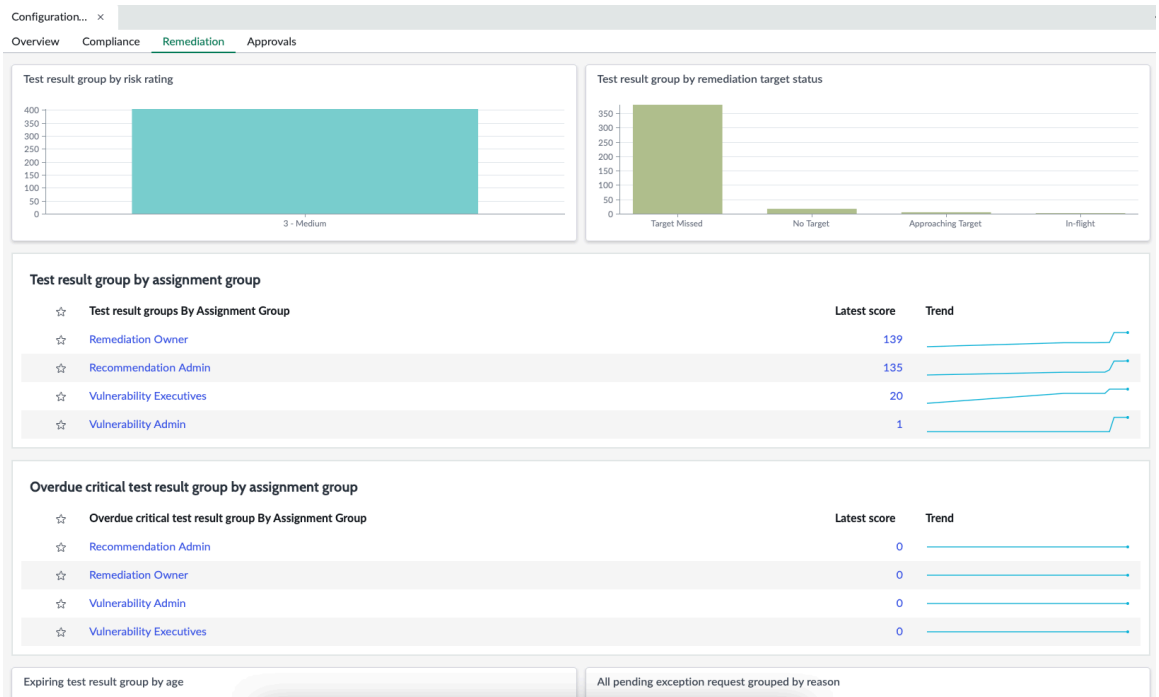
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Correção

. **Correção** exibe as informações sobre o andamento da correção. Você pode usar esta guia para ver a higiene da correção de configuração incorreta.

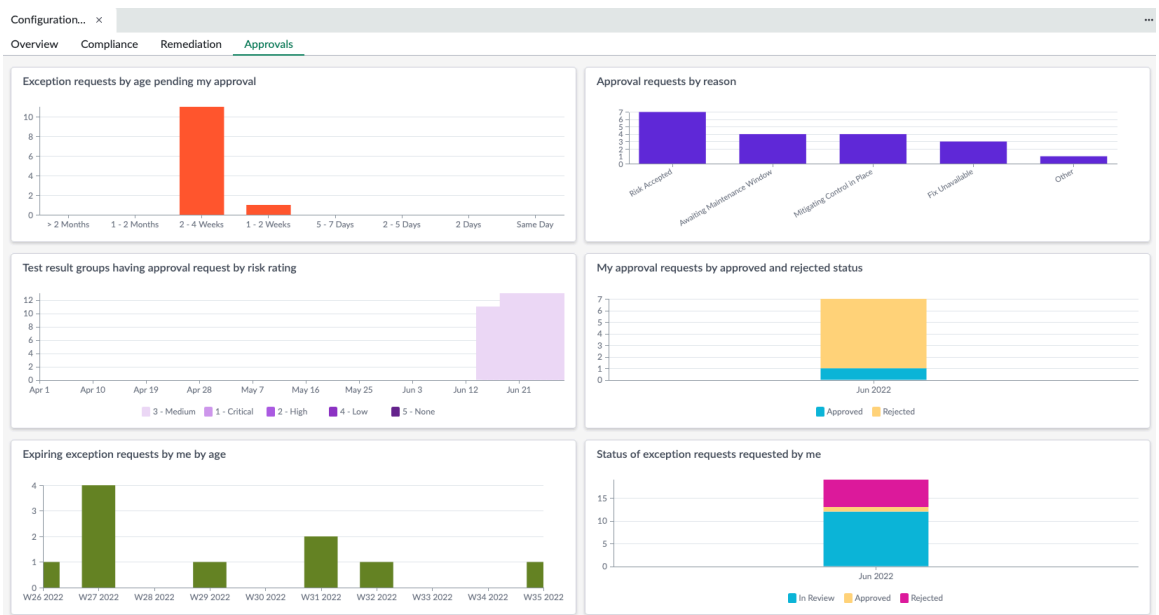
O exemplo a seguir mostra o. **Correção** guia.



Guia Aprovações

Os relatórios no **Aprovações** exibe as informações sobre as solicitações de exceção e seu status de aprovação.

O exemplo a seguir mostra o. **Aprovações** guia.



Detalhamentos

Os detalhamentos usados pelos indicadores são os seguintes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Motivo adiado
- Idade
- Grupo de atribuição
- Status da correção
- Resultado
- Classificação de risco
- Categoria do ativo
- Marcador de host
- Teste de configuração
- Provedor de serviços em nuvem
- Região da nuvem
- Conta de nuvem
- Tipo de recurso de nuvem

Nota: Personalizar o cálculo Idade e Idade de encerramento para resultados de testes pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para resultados de testes, consulte KB1703270 artigo da base de conhecimento.

Filtros

Em **Visão geral** , você pode aplicar os seguintes filtros aos widgets para visualizar os dados filtrados.

Nome	Tipo	Descrição
Categoria do ativo	Escolha	Tipo de ativo. As quatro opções são: • Nuvem • Contêiner • Infraestrutura • OT
Tipo de recurso de nuvem	Escolha	Tipo de recurso. Um exemplo é uma máquina virtual. Os dados no filtro são preenchidos quando você executa a integração.
Provedor de serviços em nuvem	Escolha	Provedor de serviço para a nuvem. As três opções são:

Tradução automática

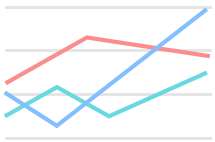
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		• Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Conta de nuvem	Escolha	ID da conta que é criado quando uma conta é criada em um serviço de nuvem. Por exemplo, AWS. Os dados do ID da conta são preenchidos no filtro quando você executa a integração.
Região da nuvem	Escolha	Local onde o recurso está hospedado.

Nota: Você pode selecionar várias opções nos filtros e selecionar **Aplicar** . Cada widget mostra os filtros que são aplicados e os filtros que não são aplicados. Dependendo dos dados disponíveis, o relatório é gerado. O widget também mostra a contagem do filtro compatível.

Visualizações de dados

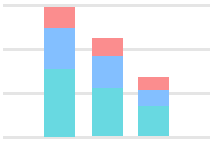
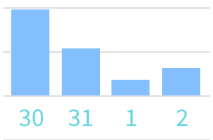
Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Tendência de conformidade	Gráfico de linhas 	Resultados de testes	Informações sobre a tendência de conformidade: • Recursos: Número total de recursos disponíveis no sistema. • Número de recursos com pelo menos um resultado de teste com falha. • Aprovado: Número de recursos com todos os resultados de teste no estado Aprovado.
Tarefa de correção	Pontuação única 	Resultados de testes	Número de tarefas de correção presentes no sistema e em um estado ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

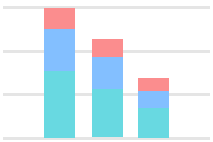
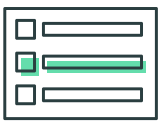
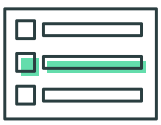
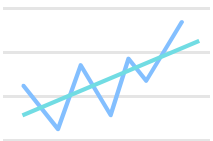
Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Tarefas de correção críticas próximas ao vencimento	Pontuação única 	Resultados de testes	Número de tarefas de correção em que a classificação de risco é "crítica" e o status de correção é "aproximando o destino".
Resultados de testes por classificação de risco	Barra 	Resultados de testes	Resultados de teste no estado com falha, que são agrupados de acordo com a classificação de risco.
Resultados de testes por idade	Barra 	Resultados de testes	Resultados de teste no estado com falha, que são agrupados de acordo com quando os resultados do teste foram criados. **Nota:** Personalizar o cálculo Idade e Idade de encerramento para resultados de testes pode levar a um aumento ou queda brusca nos relatórios de Análise de desempenho (PA) que incluem essas métricas. Para obter mais informações sobre como personalizar o cálculo de Idade e Idade de encerramento para resultados de testes, consulte KB1703270 artigo da base de conhecimento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Resultados de testes encerrados por adesão à meta de correção	Barra 	Resultados de testes	Os resultados do teste estão no estado Aprovado, o que indica que este teste está encerrado.
Resultados de testes críticos atrasado por grupo de atribuição	Lista e Pontuação 	Resultados de testes	Número de resultados de testes em que a classificação de risco é "crítica" e o status de correção é "meta perdida". O relatório indica que os resultados do teste estão em um estado Aberto. Se os resultados do teste ultrapassarem a data de destino de correção, isso será considerado atrasado.
Resultados de testes atrasados- serviços	Lista, Pontuação e Tendência  	Exibição do banco de dados dos painéis do PA para Serviços	Número de resultados de teste para serviços em que o status de correção é "destino perdido". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de teste mais altos.
Resultados de testes atrasados- responsáveis pelo serviço	Lista, Pontuação e Tendência	Exibição do banco de dados dos painéis do PA para Serviços	Número de resultados de testes para responsáveis pelo serviço cujo status de correção é "destino perdido". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de teste mais altos.

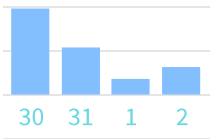
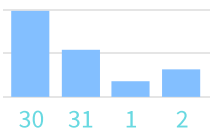
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
			

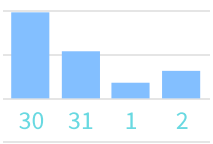
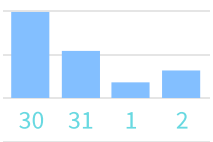
Visualizações da guia Correção

Título	Tipo	Tabela de origem	Descrição
Tarefa de correção por classificação de risco	Barra 	Tarefa de correção	Detalhamento das classificações de risco de todos os grupos de resultados de teste que estão no estado ativo.
Tarefa de correção por status da meta de correção	Barra 	Tarefa de correção	Detalhamento das metas de correção de todos os grupos de resultados de teste que não atingiram a meta, não têm meta e estão se aproximando da meta.
Tarefa de correção por grupo de atribuição	Lista, Pontuação e Tendência	Tarefa de correção	Detalhamento das tarefas de correção baseadas em um grupo de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

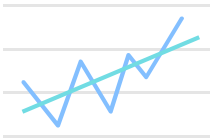
Visualizações da guia Correção

Título	Tipo	Tabela de origem	Descrição
			
Tarefa de correção crítica em atraso por grupo de atribuição	Lista, Pontuação e Tendência 	Tarefa de correção	Detalhamento das tarefas de correção baseadas em um grupo de atribuição. Essas tarefas de correção têm uma classificação de risco como "crítica" e sua meta de correção não foi atingida.
Tarefa de correção expirando por idade	Barra 	Tarefa de correção	Tarefas de correção que expirarão em uma determinada duração. Máximo de 10 buckets de duração podem ser criados.
Todas as solicitações de exceção pendentes agrupadas por motivo	Barra 	Aprovação de mudança de estado	Solicitações de aprovação de mudança de estado que são agrupadas pelo motivo da exceção.
Exceções críticas nos resultados de testes por grupo de atribuição	Lista, Pontuação e Tendência	Resultados de testes	Resultados de teste que estão em um estado adiado e crítico e são

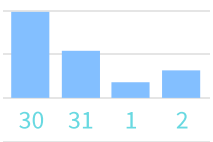
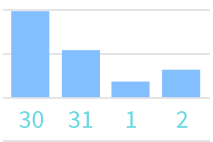
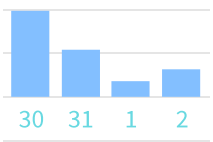
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Correção

Título	Tipo	Tabela de origem	Descrição
	 		agrupados com base no grupo de atribuição.

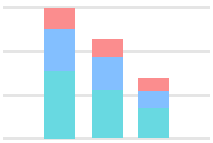
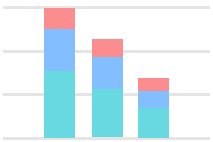
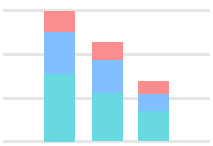
Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
Solicitações de exceção por idade com minha aprovação pendente	Barra 	Aprovação	Solicitações de exceção criadas por você e que estão com aprovação pendente. As solicitações são agrupadas de acordo com a duração da solicitação.
Solicitações de aprovação por motivo	Barra 	Aprovação de mudança de estado	Solicitações de aprovação de mudança de estado para criar uma exceção e incluir o motivo da exceção.
Tarefas de correção com solicitação de aprovação por avaliação de risco	Barra 	Tarefa de correção	Tarefas de correção que têm uma solicitação de aprovação baseada na criticidade.
Minhas solicitações de aprovação por status aprovado e rejeitado	Barra	Aprovação de mudança de estado	Solicitações de exceção agrupadas pelos status Aprovado e Rejeitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
			
Expiração das solicitações de exceção por mim por idade	Barra 	Aprovação de mudança de estado	Solicitações de exceção que expirarão nas próximas semanas. As solicitações de exceção são agrupadas com base em semanas. Sempre que uma solicitação de exceção é criada, uma data é selecionada para a validade da solicitação de exceção. O cálculo da idade da solicitação é baseado nesta data.
Status das solicitações de exceção solicitadas por mim	Barra 	Aprovação de mudança de estado	Solicitações de exceção criadas por você e agrupadas de acordo com os seguintes status: • Em revisão • Aprovada • Rejeitado

Estrutura de relatórios agregados para Conformidade de configurações

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas dinâmicas complexas e de longa execução para melhorar o desempenho.

A estrutura de relatórios agregados melhora o desempenho ao:

- usando menos recursos e renderizando relatórios mais rapidamente,
- Agregação de dados e reutilização de agregações e detalhamentos (Agrupar por) e.
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de resultados de teste de configuração, use a estrutura de relatórios agregados junto com os relatórios padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- ServiceNow AI Platform Administrador (admin): Instale e ative isso Solução para Performance Analytics e relatórios e fazer as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): Revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Sn_vul_cmn.admin): Criar agregações.
- VR write(sn_vul_cmn.write): Edite os dados nas agregações e nos resultados agregados.
- VR read (sn_vul_cmn.read): Revise os dados nas agregações e nos resultados agregados.
- Analista de vulnerabilidades (sn_vul.vulnerability_analyst): Revise os resultados agregados.

Tópicos relacionados

Configure uma agregação para dados de origem

Execute várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Crie um relatório usando uma agregação

Conformidade de configurações informações de referência

Vários tipos de componentes são instalados com a ativação do Conformidade de configurações aplicação, incluindo tabelas, trabalhos agendados e funções de usuário.

Os tópicos a seguir fornecem informações de referência, solução de problemas, além de dados de campo nos formulários e registros encontrados em Conformidade de configurações.

- Componentes instalados com Conformidade de configurações
- Campos do formulário Resultado do teste
- Resolvendo Conformidade de configurações importar problemas
- Modifique a data de início dos resultados do PC da Qualys

Componentes instalados com Conformidade de configurações

Vários tipos de componentes são instalados com a ativação do plug-in Conformidade de configurações, incluindo tabelas e funções do usuário.

A partir da v15.1.5 de Conformidade de configurações, as propriedades do sistema usadas com mais frequência agora estão acessíveis em Conformidade de configurações aplicação. Para exibir essas propriedades do sistema, navegue até **Tudo**Conformidade de configurações**Propriedades**.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, trabalhos agendados e tabelas instaladas com uma aplicação sejam exibidas. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o Construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **E.** e, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função** , **Trabalho agendado** ou **Tabela** .
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de conformidade de configuração [sn_vulc.admin]	Capaz de modificar propriedade da aplicação, configuração, regras de atualização e integrações de Conformidade de configurações aplicação. A partir da v15.0, um usuário administrador não pode excluir registros de origem, como Expanots, CVEs etc.	sn_vulc.write **Nota:** Herda as funções necessárias para a administração dos registros da aplicação Conformidade de configuração.
lido [sn_vulc.read]	Leia listas e registros em Conformidade de configuração.	• sn_sec_cmn.calc_read • sn_vul.view_manager_workspace

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	Importante: A partir da v24.0 de Resposta a vulnerabilidades, a função sn_vulc.read tem o privilégio de acessar o. Espaço do gerente de vulnerabilidade.	
gravar [sn_vulc.write]	Grave listas e registros em Conformidade de configuração.	• sn_vulc.read • sn_vulc.remediation_owner
gravar atribuição [sn_vulc.write_assignment	Gravar nos campos de atribuição de resultado de teste.	Contido na função sn_vulc.remediation_owner.
responsável pela correção sn_vulc.remediation_owner	Exiba e atualize a permissão para resultados de testes atribuídos a você ou ao seu grupo.	Contido na função itil. Contém: • sn_sec_cmn.read • sn_vulc.write_assignment • sn_vul.view_rem_workspace
CC.System sn_vulc.import_admin	Executa todos os trabalhos agendados na aplicação de conformidade de configuração. **Nota:** Este usuário é o usuário de execução padrão para cada trabalho agendado em conformidade de configuração.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration
VRCommon.System sn_vul_cmn.admin	Executar como usuário padrão para todos os trabalhos agendados na aplicação comum Resposta a vulnerabilidades.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
SecCommon.System sn_sec_cmn.admin	Executar como usuário padrão para todos os trabalhos agendados que são usados para o recurso Trabalhos em segundo plano na aplicação comum Suporte de segurança	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7: sn_vulc.edit_watch_topic	Edite tópicos de observação para Conformidade de configuração.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Leia os tópicos de observação para Conformidade de configuração.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Crie tópicos de observação para Conformidade de configuração.	sn_vulc.read_watch_topic
sn_vulc.auditor	Permitir leitura para todos os módulos de conformidade de configuração	sn_vulc.read sn_vulc.advanced_read
sn_vulc.advanced_read	Permitir leitura para todos os módulos de administração de conformidade de configuração	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
		sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	Permitir leitura para mapeamento de criticalidade de teste	
sn_vulc.read_task_rules	Permitir leitura para regras de tarefa de correção	
sn_vulc.read_assignment_rules	Permitir leitura para regras de atribuição	
sn_vulc.read_risk_score_configuration	Permitir leitura para configuração de pontuação de risco	
sn_vulc.read_auto_close_rules	Permitir leitura para configuração de fechamento automático	
sn_vulc.false_positive_approver	Permite aprovar/ rejeitar tarefas de correção de fechamento como falso positivo	sn_vul.view_manager_workspace
sn_vulc.exception_approver	Solicitações de exceção aprovadas ou rejeitadas.	sn_vul.view_manager_workspace
sn_vulc.delete	Exclui registros de origem.	

Trabalhos agendados instalados

Trabalho agendado	Descrição
V15.0: Atualizar grupo de testes em testes de configuração	Atualiza o grupo de testes em testes para a origem do Tenable e do Microsoft Defender. Este é um trabalho único.
V15.0: Preencha os campos de resultado de teste existentes	Atualiza valores em colunas recém-adicionadas (como Idade, Idade fechada, Ativo etc.) na tabela de resultados de teste, filtros salvos e módulos. Este é um trabalho único.
V15.0: Preencher a tabela ICs vulneráveis - Excluir e preencher novamente para Resultados de teste	Preenche o total de registros na tabela ICs vulneráveis. Este é um trabalho único.
Versão 12,0 Calcule métricas de correção para todos os grupos de resultados de teste	Calcula e atualiza valores para métricas de status em registros de tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Versão 12,0: Calcule métricas de correção para todos os resultados de testes	Calcula e atualiza valores para métricas de status em registros de resultados de teste.
Versão 12,0: Sincronização do estado da solicitação de mudança	Trabalho sob demanda que sincroniza os estados de todas as tarefas de correção (RTS) existentes com as solicitações de mudança (CHGs). À medida que uma solicitação de mudança avança pelo ciclo de vida, ela também move os estados de todas as tarefas de correção relacionadas automaticamente. Habilita a sincronização de estado daqui para frente.
Versão 11,1: Verificar Adiamento de grupos de resultados de teste Vencimento	Envia notificações se as tarefas de correção expirarem (e se expirarem em uma semana).
Contagem de IC de conformidade da configuração	Preenche a contagem de itens de configuração (IC) distintos e a média contínua de 90 dias na tabela Contagem de itens de configuração [sn_vulc_cc_configuration_item_count].
Versão 11,1: Avaliar e notificar destinos de correção	Define ou atualiza datas de destino de correção em todos os resultados de teste. Determina o status das datas de destino de correção em relação às regras. Envia notificações
V14.7: Insira grupos de resultados de teste na tarefa de correção unificada	Trabalho agendado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).
Versão 12,0: Preencher CR-TRG m2m para CR e CR-primário	Preenche solicitações de mudança em tarefas de correção.
Removido na v11.1: Reabrir grupos de resultados de teste adiados **Nota:** Obsoleto para versões anteriores a 11,1. Não use.	Reabre grupos adiados quando a data de vencimento tiver passado.
Reaplique todas as regras de atribuição	Reaplica todas as regras de atribuição.
Versão 14,3: Contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de resultados de teste e tarefas de correção que não estão atribuídas por este recurso para uma regra de atribuição específica.
Reavalie o estado dos grupos de resultados de teste	Reavalia o estado das tarefas de correção das entradas em que **assess_state** falso. Executado a cada 15 minutos.
Pontuação de risco do resultado de teste de acúmulo para o grupo de	É executado por hora e calcula as pontuações de acúmulo para os testes de configuração alterados e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
resultados de teste e a configuração teste	• Calcula a pontuação de risco de acúmulo para todos os testes em sn_vulc_test_manifest e exclui o registro do manifesto após a conclusão. • Calcula a pontuação de risco de acúmulo de todos os testes em sn_vulc_result_group_manifest e exclui o manifesto após a conclusão.
Versão 12,0: Atualizar métricas de correção de política	A partir da v15.0 de Conformidade de configurações Este trabalho agendado foi renomeado para Atualizar métricas de correção. • Calcula e atualiza valores para métricas de status em registros de política. • Calcula % de conformidade do resultado de teste de um IC no item descoberto.
Versão 14,3: Definir contagens de adiamentos	Coleta o número de vezes que um resultado de teste ou uma tarefa de correção é adiada.
Atualizar classificação de risco para resultados de teste	Atualiza a classificação de risco para resultados de teste.
Atualizar pontuação de risco de acúmulo para todos os grupos de resultados não encerrados e testes de configuração.	Atualiza a pontuação de risco de acúmulo para todos os grupos de resultados não encerrados e Conformidade de configurações testes.

Tabelas instaladas

Tabela	Descrição
Regra de atribuição [sn_vulc_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição nos resultados do teste.
Fonte Autorizada [sn_vulc_auth_src]	Armazene fontes autorizadas importadas.
Calculadora [sn_vulc_calculator_risk_score]	Contém a calculadora que define determinados campos de resultado de teste quando determinadas condições são atendidas.
Contagem de Itens de Configuração do CC [sn_vulc_cc_configuration_item_count]	Contém o número total de itens de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Versão 12,0: Associação de solicitação de mudança [sn_vulc_action_associate_cr]	Tabela de preparação usada para associar solicitações de mudança a tarefas de correção.
Versão 12,0: Criação de solicitação de mudança [sn_vulc_action_create_cr]	Tabela de preparação usada para criar formulários de solicitação de mudança.
Versão 12,0: Formulário de solicitação de mudança [sn_vulc_cr_form]	Tabela base para gestão de solicitações de mudança.
Citação [sn_vulc_citation]	Contém citações importadas
Teste de configuração [sn_vulc_test]	Contém dados de teste de configuração importados.
Manifesto de teste de configuração [sn_vulc_test_manifest]	Contém os testes de configuração para os quais a pontuação de risco de acúmulo precisa ser calculada.
Tabela de ativos ausente da versão 12,2 [sn_vul_missing_asset]	Contém registros de ativos temporários para dados de avaliação de conformidade de configuração importados com ativos incompatíveis.
Tecnologia de Teste de Configuração [sn_vulc_test_technology]	Contém tecnologias de teste de configuração importadas.
Regra de tarefa de correção [sn_vulc_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de resultados de teste.
Grupos de teste [sn_vulc_policy]	Contém políticas importadas.
Teste de Configuração de Política [sn_vulc_policy_test]	Contém dados de teste de configuração de política importados.
Regra de meta de correção [sn_vulc_ttr_rule]	Define o intervalo de tempo esperado para corrigir um resultado de teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Calculadoras de risco [sn_vulc_calculator_group]	Contém o agrupamento de Conformidade de configurações calculadoras. A ordem do grupo de calculadoras determina qual grupo é avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Calculadora de acúmulo de pontuação de risco [sn_vulc_risk_score_rollup]	Contém configurações da calculadora de acúmulo.
Dividir tarefas de correção [sn_vulc_action_split_trg]	Tabela de preparação usada para dividir tarefas de correção.
Aprovação de mudança de estado [sn_vulc_state_change_approval]	Contém dados do processo do estado de aprovação.
Tecnologia [sn_vulc_technology]	Contém tecnologias importadas.
Mapa de Criticidade de Teste [sn_vulc_test_criticality_map]	Contém dados do mapa de criticalidade.
Resultado do Teste [sn_vulc_result]	Contém resultados de testes importados.
Tarefas de correção [sn_vulc_result_group]	Contém tarefas de correção importadas.
Versão 12,0: Solicitações de Mudança de tarefa de correção	Contém solicitações de mudança para tarefas de correção.
Manifesto da tarefa de correção [sn_vulc_result_group_manifest]	Contém as tarefas de correção para as quais a pontuação de risco de acúmulo precisa ser calculada.
Tarefas de correção [sn_vulc_m2m_result_result_group]	Contém dados da tarefa de correção.
Histórico de Resultado de testes	Contém histórico de resultados de teste importado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vulc_result_history]	
Status de correção do resultado de testes	Status do resultado do teste em relação à regra de destino de correção aplicada mais próxima.
V14.7: Contagens de testes do tópico de observação [sn_vulc_wt_test_counts]	Tabela de cache para a guia Testes de configuração distintos no espaço do Gerenciador de vulnerabilidades.

Exibir Conformidade de configurações grupos de teste

Depois de importar os resultados de uma verificação de terceiros para sua instância, você poderá ver sua conformidade de teste no nível do grupo de testes. Use esta exibição antes de uma auditoria desse grupo de testes e de todos os registros de teste associados.

Antes de Iniciar

Função necessária: sn_vulc.read e sn_vulc.remediation_owner para exibição

Por Que e Quando Desempenhar Esta Tarefa

Grupos de teste são registros importados e você não pode editá-los no Conformidade de configurações aplicação.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Grupos de teste**.
   A lista de Resultados de teste é exibida. A partir da v15.0 de Conformidade de configurações. **% De conformidade do resultado do teste** a coluna exibe a porcentagem de resultados de teste que estão em conformidade com os testes em um grupo de testes.

   % De conformidade do resultado de teste: (Nº de resultados de teste encerrados em um grupo de teste/número total de resultados de testes associados a um grupo de testes) * 100

2. Clique em **Descrição resumida** Do Grupo de testes que você deseja exibir.

Conformidade de configurações Campos de formulário Grupo de teste

Campo	Descrição
Origem	Nome do sistema do scanner de terceiros ou o nome inserido em ServiceNow Plug-in para a API que é usada para se comunicar com Conformidade de configurações.
Tecnologias	Lista de tecnologias associadas ao grupo de teste na aplicação de scanner de terceiros.
ID da origem	Identificador atribuído a este grupo de teste pelo scanner de terceiros.
Origem de criação	Data e hora em que o grupo de testes foi definido na aplicação de scanner de terceiros.
Origem atualizada	Data e hora em que o grupo de testes foi modificado pela última vez na aplicação de verificação de terceira política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Descrição resumida ou título atribuído ao grupo de teste na aplicação de scanner de terceiros.
Descrição	Descrição detalhada do grupo de teste conforme definido na aplicação de scanner de terceiros.
Testes	Lista de testes que fazem referência a este grupo de testes. Importado do scanner de terceiros. Você pode navegar na lista para obter informações detalhadas sobre um teste específico, se necessário.
Status de correção (versão 12,0)	
Exclui os adiados	Esses valores não incluem ICs de resultados de testes adiados. ○ **ICs restantes** Número (contagem) de itens de configuração (ICs) com resultados de teste ativos (qualquer estado diferente de **Encerrado**) para esta política. ○ **% De ICs corrigidos** Percentual de ICs compatíveis para este grupo de testes. Este número exclui ICs com resultados de teste adiados. ○ **Total de ICs** Número total de ICs afetados por este grupo de testes. Esta contagem exclui resultados de testes adiados.
Inclui os adiados	Os valores representam ICs de todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**). ○ **ICs restantes** Número de ICs exclusivos associados a um ou mais resultados de teste não encerrados aos quais este grupo de testes foi aplicado. ○ **% De ICs corrigidos** Percentual de ICs compatíveis para este grupo de testes. ○ **Total de ICs** Número total de ICs afetados por este grupo de testes.

A partir da versão 12,0, para atualizar esses valores sob demanda, abaixo da guia Status de correção, clique em **Atualizar status** link relacionado. É exibida uma mensagem indicando que os dados estão sendo atualizados. Clique em **Exibir status** link para exibir o andamento da atualização. Após alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho agendado são atualizados no registro. Os valores de campo atualizados são atualizados.

3. **Opcional:** Desabilite a importação de resultados de teste para um grupo de testes selecionando **Desabilitar importação** botão.

   (Optional) O valor em **Importação desabilitada** a coluna muda para *verdadeiro* . Os resultados do teste do grupo de testes não são importados da próxima ingestão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Desabilitar importação** o botão está disponível para os resultados de teste obtidos do Qualys scanner somente.

A partir da v23.0 de Resposta a vulnerabilidades:

- Você pode habilitar ou desabilitar a importação de resultados de teste para um Qualys grupo de testes no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Habilitar ou desabilitar a importação de resultados de teste para um Qualys grupo de teste.
- . **Descontinuado** o botão foi renomeado para **Desabilitar importação** .
- . **Descontinuado** a coluna foi renomeada para **Importação desabilitada** .

Exibir Conformidade de configurações fontes autorizadas

Use este módulo para exibir informações resumidas sobre cada fonte autorizada e para pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin a ser atualizado
- sn_vulc.remediation_owner a ser exibido

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Dados de suporte** > **Fontes Autorizadas**.
2. Clique em **Descrição resumida** da fonte autorizada que você deseja exibir.

Conformidade de configurações campos do formulário fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à fonte autorizada pela sua instância durante o processo de importação.
Origem	Nome do sistema da aplicação do scanner de terceiros ou o nome inserido no plug-in do scanner para a API que se comunica com Conformidade de configurações.
ID da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.
Descrição resumida	Nome fornecido a esta fonte autorizada no scanner de terceiros.
Fornecedor	Nome da organização ou publicação que foi a fonte original de informações desta fonte autorizada.
Citações	Lista de informações citadas sobre os resultados do teste. Importado do scanner de terceiros. Você pode navegar nesta lista para obter informações detalhadas sobre um teste específico, se necessário.

3. **Opcional:** Adicione um **Fornecedor** .
4. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Você pode excluir este registro clicando em **Excluir** .
   Remove o registro da sua instância. Se ele ainda estiver em uso em sua integração de terceiros, ele retornará na próxima importação

Exibir Conformidade de configurações.

Use este módulo para exibir informações resumidas sobre cada fonte autorizada e citação (também conhecidas, na Qualys, como uma estrutura). Você pode pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin a ser atualizado
- sn_vulc.remediation_owner a ser exibido

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Dados de suporte** > **Tecnologias**.
2. Clique em **Descrição resumida** da fonte autorizada que você deseja exibir.

Conformidade de configurações campos do formulário fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à fonte autorizada pela sua instância durante o processo de importação.
Origem	Nome do sistema do scanner de terceiros ou o nome inserido no plug-in do scanner de terceiros para a API que se comunica com Conformidade de configurações.
ID da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.

3. Você pode excluir este registro clicando em **Excluir** .
   Remove o registro da sua instância. Se ele ainda estiver em uso em sua integração de terceiros, ele retornará na próxima importação

Exibir Conformidade de configurações testes

Use este módulo para pesquisar informações detalhadas sobre esses testes. Estão incluídas as citações de origem de especialistas que foram usadas ao criá-las, as políticas de configuração de terceiros nas quais elas são usadas e os resultados obtidos da verificação.

Antes de Iniciar

Função necessária:

- sn_vulc.admin a ser atualizado
- sn_vulc.remediation_owner a ser exibido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Controles**.
2. Navegar até **Tudo** > **Conformidade de configurações** > **Testes**
3. Na lista, abra o controle (teste de conformidade) que você deseja exibir.

A partir da versão 12,0, para atualizar esses valores sob demanda, abaixo da guia Status de correção, clique em **Atualizar status** Link relacionado. É exibida uma mensagem indicando que os dados estão sendo atualizados. Clique em **Exibir status** link para exibir o andamento da atualização. Após alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho agendado são atualizados no registro. Valores de campo, como **Pontuação de risco** , **Classificação de risco** , **Data de destino de correção** , **Estado** e os campos no **Status de correção** são atualizadas.

Conformidade de configurações campos de formulário de teste

Campo	Descrição
Número	Número atribuído ao controle durante o processo de importação.
Resultado	Status da verificação. Aprovado ou reprovado. Se este teste pertencer a várias tarefas de correção, seu estado será determinado após um ordem de precedência .
Origem	Nome do sistema da aplicação de integração de terceiros ou o nome inserido no plug-in para a API que é usada para se comunicar com Conformidade de configurações.
Criticidade	A gravidade do problema de configuração ou problemas associados ao controle, conforme definido na integração de terceiros. O nível de criticidade é ajustado para corresponder à granularidade de indicadores de vulnerabilidade semelhantes disponíveis em Resposta a vulnerabilidades. Os níveis possíveis são: **Crítico** O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. **Alto(a)**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos críticos da rede. **Moderado** O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. **Baixo(a)** O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor de ICs que estão em maior risco. **Secundário** O problema de configuração associado ao controle é um risco secundário e pode ser ignorado, se necessário.
ID da origem	Identificador atribuído ao controle pela integração de terceiros.
Categoria	Categoria de classificação principal fornecida a este tipo de controle pelo fornecedor terceirizado.
Pontuação de risco	Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os resultados de teste não "Encerrado" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido), e 15% da pontuação do número de resultados de testes que não estão "Encerrados".Valor calculado pelas calculadoras de pontuação de risco que é baseado nos valores de criticidade comercial e de criticidade de teste dos resultados de testes.
Subcategoria	Subcategoria atribuída a esta classe de teste pelo fornecedor terceirizado.
Classificação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica o risco geral com base em um intervalo de pontuações de risco como 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade em versões anteriores.
Tecnologias	Lista de tecnologias cobertas por este teste.
Origem de criação	Data em que o teste foi definido pela primeira vez na integração de terceiros.
Origem atualizada	Data em que o teste foi atualizado pela última vez na integração de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Descrição resumida ou título inserido ou atribuído ao teste na integração de terceiros.
Status de correção (v 12,0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ○ **Resultados de teste em aberto** : O número (contagem) de ativos (qualquer estado diferente de **Encerrado** resultados de teste para este teste de configuração. ○ **% De resultados de testes corrigidos** Percentual de resultados de testes corrigidos para esta tarefa de correção. ○ **Total de resultados de testes** Número total de resultados de teste para esta tarefa de correção.
Inclui os adiados	Esses valores incluem resultados de testes adiados. ○ **Resultados de teste em aberto** : O número (contagem) de todos os ativos (qualquer estado diferente de **Encerrado** resultados de teste para esta tarefa de correção. ○ **% De resultados de testes corrigidos** Percentual de resultados de testes corrigidos para esta tarefa de correção. ○ **Total de resultados de testes** Número total de resultados de teste para esta tarefa de correção.
Descrição	Descrição longa do teste. Para a Integração de vulnerabilidades da Qualys, este campo usa o conteúdo do Qualys Cloud Platform folha de rosto.
Correção	Instruções de etapas que descrevem como corrigir a não conformidade.
Guias relacionadas	
Citações	Lista de citações inseridas para cada fonte autorizada associada ao teste.
Grupos de teste	Lista de Conformidade de configurações grupos de teste que usam este teste.
Resultados de testes	Lista de ICs afetados pelo problema de configuração ou problemas associados a este teste. Você pode acessar testes individuais, ServiceNow itens de configuração ou a lista de tecnologias afetadas, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Declarações de políticas de GRC	. GRC Gestão de políticas e conformidade o plug-in está instalado, esta guia contém o relacionado GRC política. Você pode editar esta lista para adicionar ou remover declarações de política.

Exibir Conformidade de configurações resultados do teste

Exibir Conformidade de configurações resultados de testes para auditoria e correção. Os resultados do teste são criados automaticamente durante as importações de integração de vulnerabilidades de terceiros.

Importante: Você pode exibir os resultados de teste criados durante as importações de integração de vulnerabilidades de terceiros no Espaço do Gerenciador de vulnerabilidades. Para obter mais informações, consulte Página de lista no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vulc.read para exibir
- sn_vulc.remediation_owner para exibir e atualizar
- sn_vulc.delete a ser excluído

Por Que e Quando Desempenhar Esta Tarefa

Conformidade de configurações não cria ou atualiza os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando eles estiverem visíveis em Conformidade de configurações, eles são corrigidos usando **Grupos de resultados de teste** .

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Resultados de testes**.
   A partir da v15.0 de Conformidade de configurações, As colunas a seguir aparecem na lista Resultados do teste.

Lista de resultados do teste

Coluna	Descrição
Ativo	Indica se um resultado de teste está ativo. Um resultado de teste é marcado: ○ Verdadeiro: Se o Estado não for Encerrado. ○ Falso: Se o Estado for Encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Idade	Período em que um resultado de teste está ativo desde que foi aberto pela última vez. Este campo está vazio para um resultado de teste encerrado. Formato: Dias HH:MM: SS Para obter mais informações sobre como personalizar o cálculo de Idade, consulte KB1703270 artigo.
Idade do encerramento	Período de tempo em que um resultado de teste estava ativo antes da transição para "Encerrado". Quando o resultado do teste muda para "Encerrado", o valor da coluna Idade é exibido no campo Encerrado envelhecido. Este campo está vazio para um resultado de teste ativo. Formato: Dias HH:MM: SS Para obter mais informações sobre como personalizar o cálculo de Idade de encerramento, consulte KB1703270 artigo.
Encerrado	Carimbo de data/hora em que um resultado de teste é encerrado. FORMATO: AAAA-MM-DD HH:MM: SS
Aberto pela última vez	Carimbo de data/hora em que um resultado de teste é aberto, ou seja, quando **Ativo** o valor do campo muda para *verdadeiro* .

2. Abra o controle que você deseja exibir.

Conformidade de configurações campos do formulário resultado do teste

Campo	Descrição
Número	O número atribuído ao teste durante o processo de importação.
Origem	O nome do sistema da aplicação SCA de terceiros ou o nome inserido no plug-in da aplicação para a API que é usada para se comunicar com Conformidade de configurações.
ID da origem	O identificador atribuído ao controle pela aplicação SCA.
Resultado	Aprovado, Falha, Erro ou Desconhecido. Importado da Qualys.
Pontuação de risco	Resultado da calculadora para este teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	V15.0 de Conformidade de configurações, a pontuação de risco de um resultado de teste aprovado é definida como "0". A partir da v15.0 de Conformidade de configurações, a pontuação de risco do resultado do teste aprovado não é alterada para "0" para que você possa estimar o risco mitigado. A pontuação de risco do resultado de teste aprovado não está incluída no cálculo da pontuação de risco de uma tarefa de correção.
Classificação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica o risco geral com base em um intervalo de pontuações de risco como 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade em versões anteriores.
Estado	Calculado a partir das tarefas de correção às quais o resultado do teste pertence. Se o resultado do teste pertencer a vários grupos, um ordem de precedência é aplicado para determinar o estado.
Resolução	Calculado a partir das tarefas de correção às quais o resultado do teste pertence. Se o resultado do teste pertencer a vários grupos, um ordem de precedência é aplicado para determinar a resolução.
Visto pela primeira vez	Data da primeira importação em Conformidade de configurações. A partir da v13.1.1, o. **Visto pela primeira vez** o campo exibe a data fornecida pelo scanner. Caso contrário, ele exibirá a data importada pela primeira vez em Conformidade de configurações.
Visto pela última vez	Data da última importação em Conformidade de configurações. A partir da v13.1.1, o. **Visto pela última vez** o campo exibe a data fornecida pelo scanner. Caso contrário, ele exibirá a data da última importação em Conformidade de configurações.
Última aprovação	Data mais recente em que o resultado do teste foi aprovado.
Testar	Nome do teste.
Item de configuração	Nome do IC anexado ao teste.
Tecnologia	Versão do software em execução no IC.
Descrição	Descrição do teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Valores Esperados	Valores esperados configurados na Qualys e importados por Conformidade de configurações. Este valor é uma expressão booliana que, quando avaliada como verdadeira, faz o resultado do teste **Aprovado** . A expressão pode ser uma combinação de operadores de expressão lógicos, definidos ou regulares.
Valores reais	Valores retornados pelo teste. Esses valores são conectados à expressão booliana Valores esperados para determinar se o resultado deve ser aprovado ou reprovado. Eles são importados da Qualys. A partir da versão 14,9 de Conformidade de configurações, Os valores Evidência estendida e Causa da falha são adicionados à coluna Valores reais.
Correção	Instruções de correção.
Guias relacionadas	
Tarefas de correção	Tarefas de correção associadas a este resultado de teste.
Histórico de Resultado de testes	Lista relacionada de resultados de teste que mostram o histórico de resultados de aprovação/reprovação para o mesmo IC/tecnologia/teste.

Exiba uma tarefa de correção

Ou, como alternativa, você pode exibir uma tarefa de correção e executar a correção.

Importante: Você pode exibir as tarefas de correção no Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Página de lista no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar ou criar
- sn_vulc.remediation_owner a ser exibido

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Conformidade de configurações** > **Tarefas de correção**.
2. Na lista, clique no registro que você deseja exibir.
3. Como alternativa, clique em **Novo** para criar uma nova tarefa de correção e preencher os campos.

Campos do formulário Tarefa de correção de conformidade de configuração

Campo	Descrição
Número	O número gerado automaticamente para este registro.
Estado	Status do andamento da tarefa de correção. ○ Aberto ○ Sob investigação ○ Aguardando Implementação ○ Adiado ○ Resolvido ○ Encerrado
Pontuação de risco	Esta pontuação é o valor acumulado das pontuações de risco de todos os resultados de teste ativos em uma tarefa de correção. Essa pontuação muda conforme os resultados do teste são corrigidos na tarefa de correção.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Classificação de risco	A quantidade de risco que um resultado de teste com falha representa para o seu sistema. É baseado em um intervalo de pontuações de risco em uma escala numérica de 1-5 que classifica os riscos como Crítico (1) a Nenhum (5).
Atribuição a	Indivíduo do grupo de atribuição selecionado que trabalha neste conjunto de tarefas.
Meta da correção	Data em que os resultados do teste devem ser corrigidos, desde que identificados pela primeira vez.
Criação em	A data e a hora em que esta tarefa de correção foi criada.
Status da correção	Status da correção do grupo. É determinado pelo resultado do teste com a data de vencimento mais próxima. Para grupos em aberto, os estados incluem Em trânsito, Destino aproximado e Destino perdido. Para os estados de Grupos encerrados, incluem Sem destino, Destino atingido e Destino perdido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para datas de destino de correção calculadas, se a tarefa de correção for Encerrada, o status geral de correção de todos os resultados de testes encerrados será mostrado na tarefa de correção. Esses determinam se o grupo atendeu à data ou não. Um status de correção de tarefa de correção encerrada é **Nenhum destino** se nenhum dos resultados encerrados tiver uma data de destino de correção. É **Meta perdida** se algum dos resultados encerrados não tiver atingido a data de destino. É **Meta atingida** se pelo menos um resultado encerrado atingiu sua meta e nenhum dos outros falhou.
Atualização em	A data e a hora em que este registro foi modificado pela última vez.
Descrição resumida	Breve descrição desta tarefa de correção.
Descrição	Descrição longa da tarefa de correção que inclui a lista de softwares associados a esta tarefa de correção.
Testar	O teste de configuração associado a esta tarefa de correção.
Status de correção (versão 12,0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ○ **Resultados de teste em aberto** : O número (contagem) de ativos (qualquer estado diferente de **Encerrado** resultados de teste para esta tarefa de correção. ○ **% De resultados de testes corrigidos** Percentual de resultados de testes corrigidos (encerrados) para esta tarefa de correção. ○ **Total de resultados de testes** Número total de resultados de teste para esta tarefa de correção.
Inclui os adiados	Os valores representam todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Resultados de teste em aberto** : O número (contagem) de ativos (qualquer estado diferente de **Encerrado** resultados de teste para esta tarefa de correção. ○ **% De resultados de testes corrigidos** Percentual de resultados de testes corrigidos (encerrados) para esta tarefa de correção. ○ **Total de resultados de testes** Número total de resultados de teste para esta tarefa de correção.
Configuração de Grupo	O tipo de filtragem usado para selecionar os resultados de teste para a tarefa de correção.
Método de agrupamento	Nome do método usado.
Regra de grupo	Nome da regra de grupo usada.
Anotações	Anotações do sistema associadas ao registro.
Links relacionados	**Versão 12,0: Atualizar link de status** . Atualize os valores no registro de resultado de teste sob demanda. Exiba todos os dados que foram alterados ou atualizados desde o último trabalho agendado.
Resultados de testes	Os resultados do teste nesta tarefa de correção.
Solicitações de mudança (v 12,0)	A lista de solicitações de mudança associadas a esta tarefa de correção.
Aprovações de mudança de estado (v 12,0)	Status e estados das aprovações de solicitação de mudança associados a esta tarefa de correção.

Resultado de teste e transições de estado da tarefa de correção no Conformidade de configurações aplicação

Os estados dos registros de teste de configuração e suas tarefas de correção (RTS) associadas serão afetados se os registros de resultado de teste forem adiados, resolvidos, reabertos e transferidos para outros esforços de correção (RES).

Cenários de transição de estado entre resultados de teste e tarefas de correção

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

A tabela a seguir detalha como os estados e subestados fazem a transição entre os resultados do teste de configuração e as tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um estado de tarefa de correção fizer a transição de...	... para estado/ subestados	os estados de resultados de testes associados fazem a transição de...	... para estado/ subestados	Descrição
Aberto	Sob Investigação	Aberto	Sob Investigação	Transição de estados bidirecionalmente.
Aberto	Em revisão	Aberto	Em revisão	Transição de estados bidirecionalmente.
Aberto	Adiado/com qualquer motivo selecionado para Resolução	Aberto	Adiado	Os resultados do teste mantêm o mesmo Motivo para Resolução que a tarefa de correção.
Adiado/com qualquer Motivo para Resolução	Aberto	Os resultados do teste permanecem adiados		Os resultados do teste mantêm a mesma resolução da tarefa de correção.
Aberto	Resolvido/Corrigido	Aberto	Resolvido	Transição de estados/subestados bidirecional.
Aberto	Resolvido e Resolvido como Encerrado/Corrigido	Aberto	Resolvido	Se uma tarefa de correção fizer a transição para Encerrada/ Corrigida, ela poderá fazer a transição de volta para aberta. Se a tarefa fizer a transição para Abrir, os resultados de teste associados serão transferidos de Resolvido novamente para Aberto.
Aberto	Resolvido	Abertos	Resolvido	Transição de estados/subestados bidirecional.
Aberto	Resolvido/ Cancelado	Aberto	Resolvido	Transição de estados/subestados bidirecional.
Aberto	Resolvido e Resolvido como Encerrado	Aberto	Resolvido	Se uma tarefa de correção fizer a transição para Encerrada automaticamente, os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um estado de tarefa de correção fizer a transição de...	... para estado/ subestados	os estados de resultados de testes associados fazem a transição de...	... para estado/ subestados	Descrição
				resultados de teste associados poderão fazer a transição de volta para Aberto.
Aberto	Resolvido e Resolvido para Encerrado/ Resultado inválido	Aberto	Resolvido e Resolvido para Encerrado/ Resultado inválido	Se uma tarefa de correção fizer a transição para Resolvido, ela poderá fazer a transição de volta para Aberto. Se uma tarefa de correção fizer a transição para Encerrado/ Resultado inválido, ela e seus resultados de teste associados não poderão ser reabertos.
Aberto	Encerrado/Corrigido	Os resultados do teste permanecem em aberto		

Nota:

- A partir da v14.12 de Conformidade de configurações. **Resultado inválido** a opção é removida em **Resolução** Campo no modal Fechar.
- A partir da v14.12 de Conformidade de configurações. **Aprovação do estado da tarefa de correção** O fluxo de trabalho foi descontinuado e substituído pela Aprovação do estado da tarefa de correção de fluxo no designer de fluxo.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos Estado das tarefas de correção e os campos Estado das solicitações de mudança (CHGs) no Conformidade de configurações aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

À medida que uma solicitação de mudança avança pelo ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente. A sincronização de estado é habilitada por uma propriedade do sistema (sn_vulc.cr_state_sync) por padrão em sua instância quando você baixa o. Conformidade de configurações aplicação do ServiceNow Store a partir da v12.0.

Quando a sincronização de estado está habilitada, o campo Estado de CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

- Quando uma nova solicitação de mudança é criada para uma tarefa de correção, se ela não estiver em **Aguardando implementação** , o estado da tarefa de correção avança para **Aguardando implementação** .
- Quando uma solicitação de mudança existente é associada a uma tarefa de correção, se não estiver em **Aguardando implementação** , o estado da tarefa de correção avança para **Aguardando implementação** .
- Depois que as tarefas em uma solicitação de mudança são concluídas (Implementado E o CHG é movido para **Revisão** estado, para o qual a tarefa de correção avança **Resolvido** .

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

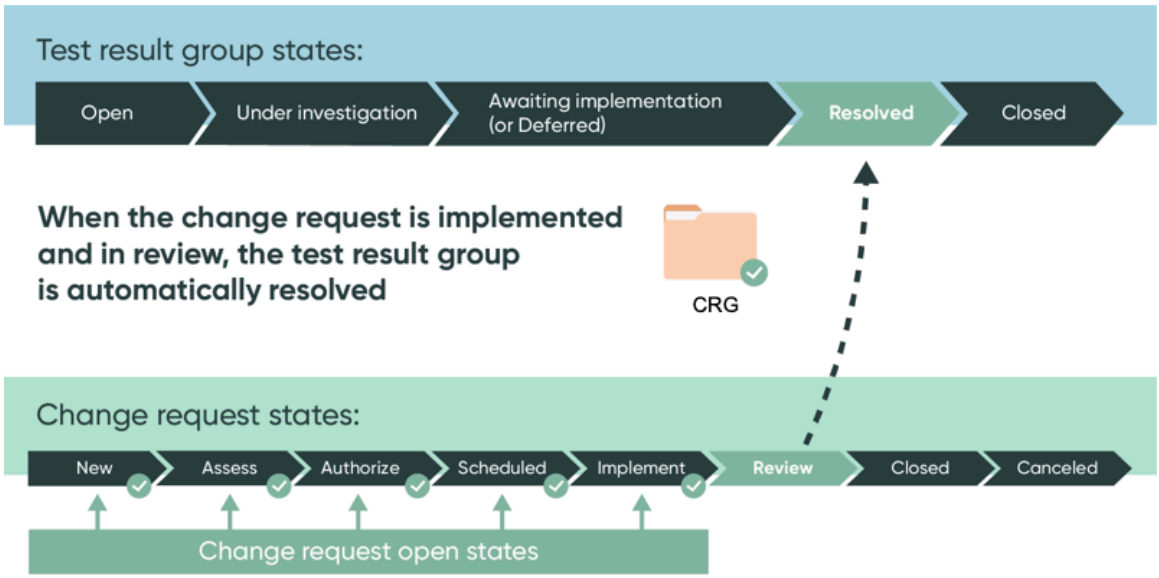
Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado ou você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente a tarefa de correção do **Encerrado** .

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados de CHG movem automaticamente os estados da tarefa de correção em um ciclo de vida avançado, ou seja, do **Aberto** . **Resolvido** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de **Resolvido** ou **Encerrado** . A sincronização de estado move automaticamente o TRG bidirecional por meio do **Aberto** , **Em investigação** , **Aguardando implementação** e **Resolvido** estados. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (**Adicionar ICs ao CR**) é exibido em um formulário e você escolhe desmarcar a caixa de seleção.

A tarefa de correção não avança para **Resolvido** Quando um CHG está em seus estados abertos. Qualquer CHG nos estados anteriores a. **Revisão** em seu ciclo de vida, como, **Novo** , **Avaliar** , **Autorizar** , **Programado** ou **Implementar** , Conforme mostrado na figura anterior, são considerados estados abertos para o CHG. os estados em aberto não movem o campo de estado na tarefa de correção, porque as investigações ou tarefas no CHG não foram concluídas. A sincronização de estado é invocada quando um CHG é criado ou associado à tarefa de correção ou quando o estado de um relacionamento existente muda no CHG. Os estados CHG concluídos são **Revisão** e com sucesso **Encerrado** . Quando um CHG é encerrado com sucesso, seus códigos encerrados são: **Bem-sucedido** ou **Problemas bem-sucedidos** caso em que a tarefa de correção avança para **Resolvido** .

Sincronização de estado reverso

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Se o CHG for **Cancelado** ou **Encerrado** (com um código de fechamento de **Malsucedido**), a tarefa de correção retorna automaticamente para **Em investigação** . A tarefa de correção retorna para **Em investigação** porque não há plano ativo para corrigir a vulnerabilidade.

Se uma tarefa de correção estiver em um **Resolvido** E você cria um novo CHG ou o associa a um CHG existente em um dos estados abertos iniciais, a tarefa de correção retorna automaticamente para **Aguardando implementação** . A tarefa de correção retorna para este estado, porque agora mais trabalho está atribuído ao CHG.

Tarefas de correção com mais de um CHG

Se for uma tarefa de correção em **Aguardando implementação** Tem mais de um CHG associado a ele, a sincronização de estado é baseada no status do CHG no estado mais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

antigo de seu ciclo de vida. Por exemplo, digamos que uma tarefa de correção tenha quatro CHGs associados a ela, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número de CHG	Estado de CHG
1	**Implementar**
2	**Cancelado**
3	Encerrado (código de fechamento de **Malsucedido**)
4	Encerrado (código de fechamento **Malsucedido**)

A sincronização de estado entre o CHG e a tarefa de correção, nesse caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (**Implementar**). Nesse caso, a tarefa de correção permanece em **Aguardando implementação** .

Em outro exemplo, se uma tarefa de correção estiver em **Resolvido** E tem um CHG existente que foi implementado e está em **Revisão** E um novo CHG é criado, a tarefa de correção é movida para trás **Resolvido** . **Aguardando implementação** . A sincronização de estado é baseada no CHG no **Novo** estado, que é o CHG no estado mais antigo.

Número de CHG	Estado de CHG
1	Revisão
2	Novo(a)

Além disso, quando as tarefas de correção têm mais de um CHG, o estado da tarefa de correção muda automaticamente nos seguintes casos:

- Quando um CHG avança para **Revisão** Se todos os outros CHGs associados à tarefa de correção estiverem em **Revisão** ou **Encerrado** (com um código de fechamento bem-sucedido),a tarefa de correção faz a transição automática para **Resolvido** . Quaisquer outros CHGs relacionados que forem cancelados ou encerrados sem sucesso serão ignorados.
- Quando um CHG se move para **Cancelado** ou **Encerrado** (código de fechamento de **Malsucedido** Se todos os outros CHGs associados à tarefa de correção estiverem no mesmo estado, a tarefa de correção retornará automaticamente para **Em investigação** .

Para obter mais informações sobre estados de tarefa de correção e o que você pode fazer em cada estado, consulte Conformidade de configurações estados.

Domain Separation e Conformidade de configurações

Domain Separation é compatível com Conformidade de configurações. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Nível de suporte: Padrão

- Inclui todos os aspectos de **Básico** suporte de nível.
- As propriedades da aplicação reconhecem domínio conforme necessário.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Conformidade de configurações

Com o Domain Separation, você pode padronizar (Conformidade de configurações), em toda a base de clientes que você atende, com custos operacionais reduzidos e maior qualidade de serviço.

Separar espaços de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte ao Domain Separation em Conformidade de configurações por versões

Versão	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Roma	Padrão	
San Diego	Padrão	
Tóquio	Padrão	
Utah	Padrão	
Vancouver	Padrão	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Separação de domínio para Conformidade de configurações a aplicação abrange as seguintes funcionalidades do produto:

- Ingere os resultados do teste de scanners de terceiros (Qualys) no domínio correto.

  Os dados ingeridos no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.

- Verifica novamente hosts específicos de Conformidade de configurações no domínio do qual foi solicitado.
- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula pontuações de risco no nível de resultado de teste de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- As regras de tarefa de correção podem ser definidas, atribuídas e permanecer no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de tarefa de correção de documento permanecem no mesmo domínio em que as regras de tarefa de correção são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados do resultado do teste, como idade dos resultados do teste, resultados do teste em aberto por IC, resultados do teste por impacto no domínio ao qual ele pertence.
- Conhecimento de scanners de terceiros (Qualys) podem ser ingeridos no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota: Em todos os casos acima, os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform se aplicam.

Casos de uso

. Conformidade de configurações a aplicação gerencia o ciclo de vida de um resultado de teste de ponta a ponta Os seguintes casos de uso reconhecem a separação de domínios:

- **Ingerir** resultados do teste de Qualys
  - Ingerir dados de várias instâncias
  - Desduplique os resultados do teste
  - Corresponder ao IC do CMDB
- **Aprimoramento** de resultados de testes com pontuações de risco
  - Aprimoramento de ativos (CMDB)
  - Pontuação de risco
- **Grupo** teste os resultados e atribua a tarefa de correção
  - Agrupar automaticamente os resultados do teste
  - Atribua automaticamente a tarefa de correção
- **Corrigir**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Tarefa de correção atribuída como tarefa de correção
  - Ciclo de vida de correção abrangente
  - Fluxo de trabalho de adiamento
- **Medida** a postura de segurança da organização e do programa de gestão de conformidade
  - Tendência de resultados, por conformidade, categoria, criticidade e tecnologia
  - Status e distribuição em políticas, testes, hosts, resultados de testes e pontuação de risco

Configuração

Configuração do Domain Separation para Conformidade de configurações não requer etapas adicionais. Todos Conformidade de configurações As tabelas adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar dados de importação de integração de resultado de teste para domínios específicos. Para obter mais informações, consulte Crie importações separadas por domínio para uma integração. Para obter mais informações sobre precauções e configurações adicionais, consulte Configurações adicionais para Domain Separation.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os resultados de teste ingeridos de scanners de terceiros permanecem no mesmo domínio que o domínio do usuário de integração e não podem ser acessados de nenhum outro domínio.
- Os resultados de testes ou hosts em um domínio não podem ser exibidos de outros domínios.
- O algoritmo de pontuação de risco e as regras do grupo de resultados de teste não podem ser exibidos por ninguém fora do domínio.
- Os fluxos de trabalho de adiamento criados em um domínio não estão visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Como os analistas de conformidade gerenciam seus próprios dados de aplicações

- Os analistas criam sua própria instalação de aplicações, gestão de aplicações de várias origens e regras de pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de gestão de adiamento e mudanças.
- Os analistas podem criar suas próprias regras de tarefa de correção, lógica de pontuação de risco para priorizar resultados com precisão, atribuir tarefas de correção automaticamente e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam uma tarefa de correção manual e a encerram.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Conformidade de configurações usuários e grupos
- Conformidade de configurações Integrações (a partir da versão Madrid)
- Configuração de configuração completa (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de tarefa de correção, calculadoras de risco etc.)
- Ciclo de vida de correção completo, incluindo adiamento

Tópicos relacionados

Domain Separation para provedores de serviço

Conformidade de configurações mapas de criticalidade

Conformidade de configurações o mapeamento de criticalidade transforma os campos de criticalidade da origem em campos em Conformidade de configurações.

. Conformidade de configurações o sistema de base é fornecido com um padrão Qualys Cloud Platform padrão ServiceNow mapeamento. Criar ou editar um mapa de criticalidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Conformidade de configurações estados

Com Conformidade de configurações, você pode ver um modelo de estado para saber qual é o status da tarefa de correção a qualquer momento. Os estados da tarefa de correção controlam os estados do resultado do teste por precedência.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Estados da tarefa de correção

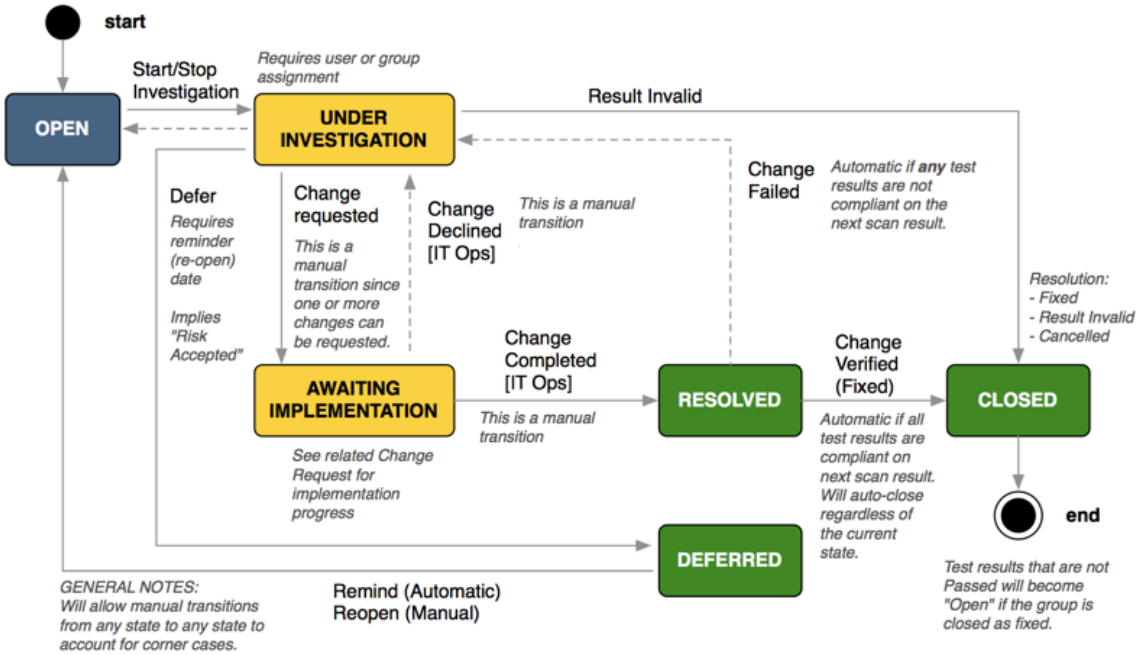
As tarefas de correção (RTS) têm muitos estados possíveis. A transição automática está disponível no estado Resolvido com base nos próximos resultados da verificação. Se todos os resultados de teste forem aprovados na próxima verificação, a tarefa de correção será encerrada. Caso contrário, ele fará a transição para o estado Em investigação. O sistema verifica esse estado encerrado, mas reavalia o estado da tarefa de correção se um resultado de teste for adicionado ou excluído da tarefa de correção. As anotações de trabalho são atualizadas para refletir a transição.

A figura a seguir mostra como o estado de uma tarefa de correção faz a transição do estado aberto para o estado encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo do estado de conformidade da configuração (anterior à v15.0)



Nota:

- Cada formulário de tarefa de correção contém **Seguir** e. **Atualização** botões, que são padrão para ServiceNow tarefas.
- A partir da v15.0 de Conformidade de configurações, os seguintes itens foram removidos:
  - **Fechar** botão
  - . **Resolução** Campo no modal Resolver.

A tabela a seguir lista o. Conformidade de configurações estados.

estados de conformidade da configuração

Estado	Descrição
Aberto	Estado após a criação.
Sob Investigação	Acionado por **Iniciar investigação** botão. Neste estado, você pode: **Crie uma solicitação de mudança** Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações. **Solicitar exceção** Forneça um motivo e selecione uma data de reabertura. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. **Marcar como falso positivo** Forneça um motivo e anotações. Marca a tarefa de correção como falso positivo.
Em revisão	Acionado quando a tarefa de correção está sendo avaliada para a próxima ação. Normalmente usado para validar resultados de investigação ou aprovar mudanças/

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados de conformidade da configuração

Estado	Descrição
	exceções propostas antes da implementação. A partir deste estado, você pode fazer a transição para qualquer um dos seguintes com base em sua aprovação ou rejeições: **Aguardando Implementação** Transição para Aguardando implementação, se aprovado **Sob Investigação** Faça a transição de volta para Em investigação se for necessária uma análise mais detalhada. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.
Adiado	Acionado por **Adiar** botão. A partir deste estado, você pode: **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove o grupo. As informações de adiamento aparecem em **Adiar/Encerrar** guia relacionada. Na data de adiamento, o grupo é reaberto para correção.
Aguardando Implementação	Acionado por **Aguardando implementação** botão. A partir deste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Crie uma solicitação de mudança** Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações. **Resolver** Em **Anotações de resolução** , Adicione o motivo pelo qual você está resolvendo a Tarefa de Correção. O estado se torna Resolvido. As anotações aparecem em **Resolução** guia relacionada. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.
Resolvido	Acionado a partir de **Resolver** botão. A partir deste estado, você pode: **Criar um Incidente de Segurança** Para obter mais informações, consulte Crie um incidente de segurança . **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados de conformidade da configuração

Estado	Descrição
	As anotações aparecem em **Anotações** guia relacionada. As informações de resolução aparecem em **Resolução** guia relacionada. As anotações são refletidas no **Anotações de trabalho** De todos os resultados de teste associados à tarefa de correção.
Encerrado	Acionado a partir de **Fechar** ou **Marcar como falso positivo** botão. A partir da v14.12 de Conformidade de configurações, você pode fechar uma tarefa de correção marcando-a como falso positivo. A partir deste estado, você pode: **Reabrir** Faça a transição de volta para um estado aberto. **Excluir** Confirmar a exclusão. Remove o grupo. As informações de fechamento aparecem em **Adiar/Encerrar** guia relacionada. As anotações são refletidas no **Anotações de trabalho** De todos os resultados de teste associados à tarefa de correção.

- Se a Tarefa de Correção estiver marcada como Encerrada ou Fixa e se o resultado do teste adicionado não for Encerrado ou Fixo, o estado do resultado do teste não mudará e o estado da tarefa de correção será alterado para Aberto.
- Ao criar uma nova tarefa de correção ou dividir uma tarefa de correção, o **Motivo** e **Até** os campos são reavaliados para tarefas de correção novas e antigas. Quando o estado de todos os resultados de teste é Adiado, o valor no **Motivo** e. **Até** os campos são acumulados para a tarefa de correção.
  - Se todos os resultados de teste em uma tarefa de correção forem adiados e tiverem o mesmo **Motivo** , em seguida, a tarefa de correção será atribuída à mesma **Motivo** . Caso contrário, o **Motivo** o campo foi alterado para **Nenhum** .
  - A data em **Até** o campo é atualizado com a data até mais próxima de todas as tarefas de correção às quais os resultados de teste pertencem.

> **Nota:** Esta avaliação é feita pelo `Rollup test result values to test result RT1nd configuration test` trabalho agendado, que é executado a cada uma hora.

- . **Visto pela última vez** é maior que **Data de resolução** para um resultado de teste resolvido, o resultado do teste é reaberto. Em uma tarefa de correção resolvida, se pelo menos um resultado de teste for reaberto durante a ingestão, a tarefa de correção será movida para o estado Em investigação.

Estados do resultado do teste

O estado de uma tarefa de correção também muda o estado dos resultados de teste associados. Este mecanismo tem dois casos:

Resultados de teste que pertencem a apenas uma tarefa de correção

Os resultados correspondem ao estado da tarefa de correção com três exceções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se a tarefa de correção Muda seu estado para Encerrado e sua resolução (subestado) para Fixo, o item ignora essa mudança e retorna para o estado Aberto.
- Se a tarefa de correção Muda seu estado para Encerrado e sua resolução (subestado) para Cancelado, o item ignora essa mudança e retorna para o estado Aberto.
- Se o status da origem do resultado do teste for Corrigido (atualizado por uma verificação ou importação), quando a tarefa de correção Muda seu estado, o resultado do teste muda seu estado para Encerrado (fixo), independentemente do estado da tarefa de correção em.

Resultados de teste que pertencem a várias tarefas de correção

Os resultados do teste não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele pesquisa entre todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicado. Este é o estado de precedência:

Encerrado > **Encerrado (subestado: Falso positivo)** > **Adiado** > **Resolvido** > **Em revisão** > **Aguardando Implementação** > **Sob Investigação** > **Aberto** > **Encerrado (subestado: Cancelado)** > **Encerrado (subestado: Fixo)**

Nota: **Encerrado (subestado: Fixo)** e. **Encerrado (subestado: Cancelado)** dois casos especiais.

Nota: A partir da v15.0 de Conformidade de configurações. **Resultado inválido** o subestado foi descontinuado.

Exemplos de estado da tarefa de correção

Por exemplo:

Estado das tarefas de correção	Estado do resultado do teste
RT1: **Aberto** > **Sob Investigação** RT2: **Aberto**	**Sob Investigação** Quando RT1 está sob investigação e RT2 está aberto, o resultado do teste muda para Em investigação, já que, após a pesquisa, entre RT1 e RT2, RT1 tem o estado com a precedência mais alta.
RT1: **Em investigação** RT2: **Aberto** > **Sob Investigação**	**Em investigação** Quando o RT2 está sob investigação e RT1 está sob investigação, o resultado do teste permanece como Sob investigação, já que, após a pesquisa, entre RT1 e RT2, ele tem o estado com a mesma precedência.
RT1: **Em investigação** RT2: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o RT2 está aguardando implementação e o RT1 está em investigação, o resultado do teste muda para Aguardando implementação, já

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado das tarefas de correção	Estado do resultado do teste
	que, após a pesquisa, entre RT1 e RT2, o RT2 tem o estado com a precedência mais alta.
RT1: **Sob Investigação** > **Adiado** RT2: **Aguardando Implementação**	**Adiado** Quando RT1 é adiado e RT2 está aguardando implementação, o resultado do teste muda para Adiado, já que, após a pesquisa, o item 1 descobriu que, entre RT1 e RT2, RT1 tem o estado com a precedência mais alta
RT1: **Adiado** RT2: **Aguardando Implementação** > **Encerrado (resultado inválido)**	**Encerrado (resultado inválido)** > **Adiado** Quando RT2 é fechado e a resolução (subestado) é Resultado inválido e RT1 é adiado, o resultado do teste muda para Encerrado (resultado inválido), já que, após a pesquisa, entre RT1 e RT2, RT2 tem o estado com a precedência mais alta.
RT1: **Adiado** RT2: **Encerrado (resultado inválido)** > **Aberto (via reabertura)**	**Adiado** Quando o RT2 é reaberto e seu estado muda para Aberto e RT1 é Adiado, o resultado do teste muda para Adiado, já que, após a pesquisa, entre RT1 e RT2, RT1 tem o estado com a precedência mais alta.
RT1: **Adiado** RT2: **Aguardando Implementação** > **Encerrado (falso-positivo)**	**Encerrado (falso-positivo)** Quando RT2 é fechado e a resolução (subestado) é falso positivo e RT1 é adiado, o resultado do teste muda para Encerrado (falso-positivo), já que, após a pesquisa, entre RT1 e RT2, o RT2 tem o estado com a precedência mais alta.

Tradução automática

Casos especiais do estado do resultado do teste

Estado da tarefa de correção	Estado do resultado do teste
RT1: **Sob Investigação** RT2: **Aguardando Implementação** > **Encerrado (fixo ou cancelado)**	**Sob Investigação** Quando o RT2 é encerrado (subestado fixo ou subestado cancelado) e o RT1 está em investigação, o resultado do teste muda de Aguardando implementação (anteriormente, a precedência mais alta) para Em investigação (atualmente, a precedência mais alta).
RT1: Qualquer estado RT2: Qualquer estado	Se o status da origem do resultado do teste for Corrigido (atualizado por uma verificação ou importação), quando a tarefa de correção Muda seu estado, o resultado do teste muda seu estado para Encerrado (fixo), independentemente de quais estados as outras tarefas de correção associadas

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos especiais do estado do resultado do teste

Estado da tarefa de correção	Estado do resultado do teste
	em. A pesquisa de resultado de teste para a tarefa de correção o estado não ocorre.

Cenários de roll-up e roll-down de estado

Os cenários de roll-up e roll-down de estado sincronizam automaticamente o status das tarefas de correção (RTS) e o resultado do teste de configuração (CTR), garantindo atualizações em tempo real em ambos. Essa interação dinâmica reduz o acompanhamento manual, aumenta a precisão e fornece aos usuários uma exibição atualizada do andamento, tornando a conformidade da configuração mais eficiente e ajudando os usuários a tomar decisões informadas rapidamente.

Comportamento de acúmulo

Quando o estado do resultado do teste de configuração (CTR) muda, essas mudanças podem se propagar até o nível da tarefa de correção (RT).

A tabela a seguir resume os principais cenários de acúmulo em que as mudanças no estado de resultado de teste de configuração (CTR) podem influenciar o estado da tarefa de correção (RT) associada, com base nas condições de fechamento, reatribuições e adiamentos.

Cenários de acúmulo

Estado de CTR	Estado de RT
Aberto > Encerrado-fixo	Aberto > Encerrado-fixo
Aberto > Encerrado-obsoleto	Aberto > Encerrado-Cancelado

Comportamento de rolagem

Quando o estado de uma tarefa de correção muda, o estado geralmente é propagado para os CTRs associados, a menos que seja substituído por atualizações manuais ou exceções.

A tabela a seguir resume os principais cenários de acúmulo em que as mudanças no estado da tarefa de correção (RT) podem afetar o estado de resultado de teste de configuração (CTR) associado, com base em regras de precedência e condições especiais.

Cenários de acúmulo

Estado de RT	Estado de CTR
Aberto > Em investigação	Aberto > Em investigação
Abrir > Em Revisão	Abrir > Em Revisão
Aberto > Adiado	Aberto > Adiado
Adiado > Aberto	Permanece adiado
Aberto > Resolvido-Corrigido	Aberto > Resolvido-Corrigido
Aberto > Resolvido-fixo > Encerrado-fixo	Aberto > Resolvido-fixo > Encerrado-fixo
Resolved-Result inválido	Resolved-Result inválido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cenários de acúmulo

Estado de RT	Estado de CTR
Aberto > Resolvido-Cancelado	Aberto > Resolvido-Cancelado
Aberto > Resolvido-Cancelado > Encerrado	Aberto > Resolvido-Cancelado > Encerrado
Resolved-Result Inválido > Encerrado-Resultado Inválido	Resolved-Result Inválido > Encerrado-Resultado Inválido
Aberto > Encerrado-fixo	Aberto > Encerrado-fixo

Resolvendo Conformidade de configurações importar problemas

Resolva problemas com importação de integração de terceiros.

Importar resolução de problemas

Ocorrência	Resolução
Resultados de teste ausentes	Verifique *`Start Time`*em **Resultados de PC da Qualys** integração. Ele pode não ser definido para trás o suficiente. Consulte Modifique a data de início dos resultados do PC da Qualys.
A integração está falhando	Verifique **Execução de integração de vulnerabilidades** status. Entradas de processo de integração individuais contêm o XML importado, que pode ser examinado em busca de informações inesperadas. Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados do QualysPC** > **Execuções de integrações de vulnerabilidade** guia relacionada. Escolha a execução mais recente. Examine o status e as anotações das entradas na lista relacionada **Processo de integração de vulnerabilidades** para anomalias. .

Modifique a data de início dos resultados do PC da Qualys

Se os dados estiverem ausentes para a data de início na importação de resultados do PC da Qualys, eles poderão ser modificados.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Tudo** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique em **Resultados de PC da Qualys** integração.
3. Clique em **Detalhes da integração** .
4. Defina **Hora de início** para um valor no passado, para que todos os resultados de testes verificados e detectados, desde esse momento, sejam detectados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se a data for deixada em branco, nenhum dado será retornado na primeira execução. Defina o valor como um máximo de um mês no passado. Esta configuração impede que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como acione tempos limite de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. **Opcional:** Clique em **Executar agora** para executar imediatamente.

Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Operações de segurança e. Palo Alto Prisma Cloud

Você pode usar as regras de pesquisa de item de configuração (IC) para Microsoft Defender for Cloud Integration e. Palo Alto Prisma Cloud integrações para encontrar uma correspondência correta com os tipos de recursos mais usados no Configuration Management Database (CMDB).

Visão geral

O módulo Regras de pesquisa de IC contém as regras que ajudam você a definir os campos que têm os dados correspondentes no Configuration Management Database (CMDB). Você pode usar essas regras para identificar as aplicações e as versões da aplicação. Todos Microsoft Defender for Cloud Integration e. Palo Alto Prisma Cloud Os ativos são identificados exclusivamente pela combinação de ID de objeto, conta de nuvem e datacenter lógico no ServiceNow plataforma . ServiceNow a descoberta preenche o ID do recurso no Object_id coluna do CMDB em diferentes formatos para os diferentes tipos de recursos. A tabela a seguir mostra os formatos de ID de objeto dos tipos de recursos comumente usados que o serviço de descoberta usa para preencher no Object_id Coluna do IC. Qualquer scanner que queira pesquisar um ativo de um tipo de recurso específico deve pesquisar usando o formato de ID de objeto correto. Você Pode obter o formato de ID de objeto correto analisando a coluna de ID de objeto correspondente CMDB Classe de IC e tente construir o ID do objeto usando os valores recebidos do scanner.

Formato de ID de objeto para vários tipos de recursos

Tipo de recurso	Formato
AWS::EC2::Instance	ID do objeto
AWS::ElasticLoadBalancing::LoadBalancer	Nome do balanceador de carga
AWS::S3::Bucket	aws:s3:::<Bucket Name>

A correspondência de IC para um resultado de teste pode não ser encontrada com precisão em Configuration Management Database (CMDB) a menos que seja o mesmo formato do object_id é usado na regra de pesquisa. Na maioria das vezes, as regras de pesquisa de IC OOB encontram uma correspondência para os tipos de recursos mais usados para Microsoft Defender for Cloud Integration e. Palo Alto Prisma Cloud.Se as regras de pesquisa de IC a seguir não estiverem encontrando os ICs no CMDB Para os resultados do teste, você pode criar uma regra de pesquisa de IC para um tipo de recurso. Para obter mais informações sobre como criar uma regra de pesquisa de IC, consulte Crie uma regra de pesquisa de IC .

Regras de pesquisa de IC

As regras de pesquisa de IC a seguir são específicas do Microsoft Defender for Cloud Integration e. Palo Alto Prisma Cloud.

Bucket S3

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo valor obtido concatenando o. aws:s3:::: e nome do recurso. O valor obtido é pesquisado em `object_id` coluna do `cmdb_ci_cloud_object_storage` tabela. Esta regra de pesquisa se aplica somente quando o tipo de recurso é `AWS::S3::Bucket` .

Nome

Esta regra de pesquisa tenta encontrar o IC no CMDB por nome. O nome, que é pesquisado em `Object_id` A coluna da classe de IC corresponde a um tipo de recurso no `sn_capi_resource_type` tabela.

Nota: Para a aplicação Palo Alto Prisma Cloud, esta regra de pesquisa de IC é executada somente para `AWS::RDS::DBInstance` , `AWS::ElasticLoadBalancing::LoadBalancer` e `AWS::CloudTrail::Trail` tipos de recursos. Você pode adicionar os tipos de recursos para os quais você deseja executar esta regra de pesquisa de IC.

ID do recurso

Esta regra de pesquisa tenta encontrar o IC no CMDB Pelo ID do recurso. O ID do recurso, que é pesquisado em `Object_id` A coluna da classe de IC corresponde a um tipo de recurso no `sn_capi_resource_type` tabela.

Nota: Você pode definir a prioridade para uma regra de pesquisa de IC no **Pedido** campo. A regra de pesquisa de IC com o menor valor de ordem é executada primeiro.

Resposta a vulnerabilidades Espaços de trabalho

Os espaços de resposta a vulnerabilidades oferecem uma exibição consolidada dos recursos isso permite que você execute várias tarefas no mesmo painel, aumentando a produtividade e economizando tempo.

Resposta a vulnerabilidades Espaços de trabalho

Espaço para gerentes de vulnerabilidades	Espaço de correção de TI	Espaço de avaliação de vulnerabilidade
		
Saiba mais sobre o Espaço do gerenciador de vulnerabilidades	Saiba mais sobre o Espaço de correção de TI	Saiba mais sobre o Espaço de avaliação de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de começar

Antes de usar os espaços:

- Você precisa executar algumas tarefas de configuração. Para obter mais informações, consulte Configure o. Resposta a vulnerabilidades Espaços de trabalho.
- Revise informações importantes sobre atualizações de tarefas de correção, regras de tarefa de correção e os principais termos e conceitos sobre os espaços, em Resposta a vulnerabilidades Espaços de trabalho e atualizações para tarefas de correção e tarefa de correção regras.

Solucionar problemas e obter ajuda

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

Resposta a vulnerabilidades visão geral dos espaços

O Gerenciador de vulnerabilidades e os espaços de correção de TI são compatíveis Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações.

Os espaços de trabalho Gerenciador de vulnerabilidades, Correção de TI e Avaliação de vulnerabilidades

Espaço do gerente de vulnerabilidade

Como gerente de vulnerabilidades, proteja os ativos da sua empresa contra malware e ataques mal-intencionados. De uma única área de trabalho em seu ServiceNow AI Platform®. com Resposta a vulnerabilidades A aplicação, junto com os dados de vulnerabilidade atuais importados para sua instância de bibliotecas de vulnerabilidades e aplicações de dados de scanner de terceiros, identifica vulnerabilidades críticas e configurações incorretas, priorize-as e envia listas de tarefas de correção para que seus especialistas ajam.

Espaço de correção de problemas de TI

Como especialista DE TI, use listas ou tarefas de correção (RT) enviadas por gerentes de vulnerabilidades para monitorar e resolver vulnerabilidades críticas atribuídas a você ou a seus grupos. Corrigir grupos de itens vulneráveis com patches, soluções, novas verificações de vulnerabilidade, solicitações de mudança, exceções, e outras ferramentas para corrigir itens vulneráveis e resultados de testes, tudo em um único local.

Espaço de avaliação de vulnerabilidade

Como gerente de eventos de vulnerabilidade, execute a avaliação de exposição e gerencie proativamente eventos de vulnerabilidade crítica, especialmente durante os eventos de vulnerabilidade crítica, como um evento de dia zero.

Principais recursos

. Resposta a vulnerabilidades os espaços de trabalho incluem os seguintes recursos e melhorias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Use o recurso Edição em massa no Espaço do gerente de vulnerabilidade para atualizar vários registros simultaneamente. Para obter mais informações, consulte Usando a edição em massa no Espaço do gerente de vulnerabilidade.
- Exiba a Gestão de vulnerabilidades (PA), Aprovações de vulnerabilidades, CISO, Visão geral da Gestão de vulnerabilidades de contêiner, Painel da Gestão de vulnerabilidades da aplicação, Resposta unificada de vulnerabilidades e Painéis de integridade na IU do Next Experience na página Painéis do Espaço do Gerenciador de vulnerabilidades. Para obter mais informações, consulte Página Painéis em Espaço do gerente de vulnerabilidade.
- Exiba o painel Correção de vulnerabilidades na IU do Next Experience na página Painéis do Espaço de correção de TI. Para obter mais informações, consulte Página Painéis em Espaço de correção de problemas de TI.
- Crie as tarefas de correção (VUL, avul, CVUL ou CRG) manualmente no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI. Para obter mais informações, consulte Crie uma tarefa de correção manualmente no Espaço do gerente de vulnerabilidade e Crie uma tarefa de correção manualmente no Espaço de correção de problemas de TI.
- Divida as tarefas de correção (VUL, avul, CVUL e CRG) no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade e. Divida uma tarefa de correção no Espaço de correção de problemas de TI respectivamente.
- Solicite as exceções de política para itens vulneráveis (Vits, AVITs e CVITs) e tarefas de correção (VUL, AVUL, CVUL e CRG) no Gerenciador de vulnerabilidades e nos espaços de correção de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade e. Solicite uma exceção usando GRC: Gestão de políticas e conformidade em Espaço de correção de problemas de TI respectivamente.
- Crie e rastreie eventos de vulnerabilidade crítica por meio do Gestão de crises de vulnerabilidade (VCM). Para obter mais informações, consulte Explorar o Espaço de avaliação de vulnerabilidade.
- Adicione controles de compensação à biblioteca de controles de compensação no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Adicione um controle de compensação à biblioteca.
- Solicitar redução de risco para um item vulnerável do host e tarefa de correção no espaço de correção DE TI. Para obter mais informações, consulte Solicitar redução de risco para um item vulnerável ou tarefa de correção.
- Crie um problema ágil e um problema Jira para itens vulneráveis à aplicação e contêiner do Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte Crie um problema ágil manualmente usando a ação de formulário e Crie um problema ágil manualmente usando a ação de lista.

Para obter mais informações sobre compatibilidade de versões com as versões da família, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão artigo na Base de conhecimento HI.

Orquestração de patches com Resposta a vulnerabilidades Espaços de trabalho

Você pode gerenciar patches e implantações de patches para vulnerabilidades críticas para grandes grupos de seus ativos com a Orquestração de patches com Resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração de patches nos espaços

Orquestração de patches com Resposta a vulnerabilidades a aplicação usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e verificadores de vulnerabilidades.

Orquestração de patches com Resposta a vulnerabilidades a aplicação é compatível com o ambiente clássico e o. Resposta a vulnerabilidades espaços de trabalho. Os dados correlacionados são acumulados e exibidos nos espaços de trabalho e no ambiente clássico. Para obter uma visão geral sobre os recursos, requisitos e informações sobre orquestração de patches no ambiente clássico, consulte Orquestração de patches com Resposta a vulnerabilidades.

- Para obter mais informações sobre as integrações compatíveis com fornecedores de patch, consulte Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades e. Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.
- Para obter informações sobre como programar registros de formulário de patches nos espaços de trabalho, consulte Programar patches com Microsoft Integração do SCCM com Resposta a vulnerabilidades e. Programar patches com Resposta a vulnerabilidades Integração de orquestração de patches HCL BigFix.

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

Para exibir dados de Orquestração de patch e atualizações disponíveis (patches) nos espaços de trabalho em Resposta a vulnerabilidades as seguintes aplicações são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas. Consulte Orquestração de patches com Resposta a vulnerabilidades.

Funções necessárias

Além das funções sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin necessárias para Resposta a vulnerabilidades, os usuários precisam de funções específicas para as integrações de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as integrações compatíveis a seguir para obter mais informações sobre essas funções.

Consulte Noções básicas sobre a integração da Orquestração de patches do BigFix do HCL com Resposta a vulnerabilidades e Noções básicas do Resposta a vulnerabilidades integração da orquestração de patches com Microsoft SCCM.

Dados de patch no Resposta a vulnerabilidades Espaços de trabalho

Em Espaço de correção de TI , você pode exibir dados de patch nos espaços de trabalho:

- Na exibição inicial, clique em cartões de pontuação para exibir registros de soluções preferenciais em VIS, ICs vulneráveis e patches preferenciais em VIS.
- Na exibição de lista, exiba todos os registros de atualização de patch (VPUs) e os itens vulneráveis atribuídos a você que têm patches dos links disponíveis.

Você pode programar patches a partir dos seguintes registros:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

Em Espaço para gerentes de vulnerabilidades, você pode exibir patches:

- Na exibição Página inicial dos tópicos de exibição na guia Itens vulneráveis, você pode exibir patches preferenciais e potenciais, datas programadas de patch e outras informações.
- Na exibição de lista em registros de esforço de correção, você pode exibir dados de patch em registros de VIT na guia Itens vulneráveis.

Resposta a vulnerabilidades Espaços de trabalho e atualizações para tarefas de correção e tarefa de correção regras

Registros de pacote de tarefas de correção (Vits, AVITs, CVITs ou CTRs) no Resposta a vulnerabilidades Espaços de trabalho.

Termos-chave para Resposta a vulnerabilidades Espaços de trabalho

Espaços de resposta a vulnerabilidades ou espaços de trabalho

Resposta a vulnerabilidades o oferece suporte ao Resposta a vulnerabilidades Espaços de trabalho. Você pode usar o clássico IU principal ou os espaços de trabalho.

IU clássica (legada)

Refere-se ao IU principal experiência. Você ainda executa algumas ações e exibe algumas listas no ambiente clássico.

Espaço para gerentes de vulnerabilidades

Neste espaço, os gerentes monitoram as vulnerabilidades direcionadas e selecionam os resultados de VIS e de teste que mais se importam para atribuir a ELE.

Espaço de correção de TI

Neste espaço, as equipes DE TI podem se concentrar nas vulnerabilidades mais importantes atribuídas a elas pela segurança. Informações centradas EM TI que incluem itens de configuração (ICs) distintos afetados, soluções e andamento da correção estão facilmente disponíveis para os responsáveis pela correção neste espaço.

Espaço de avaliação de vulnerabilidade

Neste espaço, os analistas de vulnerabilidade podem executar avaliação de vulnerabilidade durante a análise de vulnerabilidade de dia zero. Depois que uma vulnerabilidade de dia zero é identificada, eles podem avaliar o possível impacto e o risco associados à vulnerabilidade. Os analistas podem analisar o sistema, as aplicações ou os componentes de rede afetados para entender a gravidade e os possíveis vetores de ataque na organização.

Tópico de observação

Os tópicos de observação definem um segmento dos itens vulneráveis que os gerentes e analistas de vulnerabilidades desejam monitorar no Espaço do gerenciador de vulnerabilidades. Os tópicos de observação mostram um conjunto de visão geral focado de relatórios que pertencem a um segmento de VIS e resultados de testes Com tendências, IC e estatísticas relacionadas a vulnerabilidades. Os painéis sobre esses tópicos podem ser usados para monitorar tendências. Os painéis também podem ajudar os gerentes a:

- Exiba o andamento da correção em itens críticos
- Determine a existência de vulnerabilidades em sistemas críticos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Veja quando um novo exploit é lançado
- Gere uma resposta rápida para resolver um conjunto específico de vulnerabilidades

Esforço de correção (ER)

Os esforços de correção são criados por gerentes de vulnerabilidades quando determinam que é hora de A TI corrigir as vulnerabilidades listadas em um tópico de observação. Gerentes e analistas de vulnerabilidades podem escolher como desejam criar tarefas de correção, por grupo de atribuição e vulnerabilidade, por exemplo. As tarefas de correção estão contidas no esforço de correção.

Tarefa de correção (VUL)

As equipes DE TI usam tarefas de correção para corrigir as vulnerabilidades atribuídas a elas pela segurança. Tarefas de correção são listas de ações necessárias para corrigir vulnerabilidades. As tarefas de correção são criadas automaticamente quando os gerentes de segurança criam esforços de correção.

Desenvolvimento dos espaços

Em versões anteriores de Resposta a vulnerabilidades, Você tinha duas opções para monitorar um conjunto de registros (Vits, AVITs, CVITs ou CTRs) como analista de segurança e vulnerabilidade:

- O painel Visão geral, que resume todos os VIS
- Tarefas de correção

Itens vulneráveis foram classificados em tarefas de correção automaticamente de acordo com suas regras de tarefa de correção predefinidas. Tarefas de correção Foram projetados para oferecer suporte às equipes DE TI na correção de blocos gerenciáveis de itens vulneráveis.

Essa automação tornou possível agrupar números muito grandes de registros automaticamente para atribuição e correção em massa. No entanto, os analistas e gerentes de vulnerabilidades consideraram desafiador o monitoramento de todo o conjunto de registros das tarefas de correção. Além de problemas de desempenho com grupos grandes, criando funcional tarefa de correção regras que filtraram somente as vulnerabilidades que você considerou mais críticas podem ser difíceis.

. Resposta a vulnerabilidades Espaços:

- Ajude os gerentes de segurança a filtrar, monitorar os VIS ativos e. resultados do teste e direcionam a correção das vulnerabilidades que determinam como as mais importantes.
- Forneça às equipes DE TI informações centradas em TI em um local que elas possam usar para corrigir as vulnerabilidades atribuídas a elas pela segurança.

Atualizações das tarefas de correção nos espaços de trabalho

No espaço do Gerenciador de vulnerabilidades, os analistas de vulnerabilidades e gerentes usam *Tópicos de observação* e. *Esforços de correção* Dois novos métodos para monitorar e atribuir VIS para correção.

Grupos de vulnerabilidades são renomeados, *Tarefas de correção* . Esta mudança se aplica a rótulos em listas, registros e regras na IU legada e nos espaços de trabalho. As tarefas de correção são configuradas para que as equipes DE TI possam trabalhar com elas no Espaço de correção de TI. A lista a seguir ilustra como, como gerente de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ou analista de vulnerabilidades, você pode monitorar vulnerabilidades e resultados de testes, filtre-os e atribua-os:

1. No Espaço do gerenciador de vulnerabilidades, os gerentes monitoram vulnerabilidades importadas e configurações incorretas nos tópicos de observação. Gerentes e analistas usam tópicos de observação para monitorar um conjunto dinâmico de registros filtrados ao longo do tempo que eles acham que são os mais críticos.
2. Com os tópicos de observação, os gerentes de segurança podem determinar quando e que tipo de VIS entregar para as equipes DE TI nos esforços de correção (RES). Essas RES são listas estáticas dos VIS que as equipes de TI desejam corrigir.

   Dos esforços de correção, os gerentes têm quatro opções para agrupar registros em tarefas de correção (VULs, AVULs, CVULs ou CRGs). As tarefas de correção são atribuídas automaticamente às equipes DE TI com base nos grupos de atribuição que são originalmente associados aos registros.
3. As equipes DE TI trabalham em tarefas de correção no Espaço de correção de TI sem precisar classificar todos os registros.

   Uma tarefa de correção passa pelos mesmos estados que a tarefa de correção faz nas versões anteriores do Resposta a vulnerabilidades. Quando todos os registros em uma tarefa de correção são encerrados, a tarefa de correção é encerrada e definida como **Inativo** .

   O andamento da correção é atualizado nas visualizações de dados nos tópicos de exibição e na página inicial de correção DE TI.

Atualizações das regras de tarefa de correção nos espaços de trabalho

As regras de grupo de vulnerabilidades são chamadas *Regras da tarefa de correção* . Esta mudança se aplica aos rótulos em listas, registros e regras na IU legada e nos espaços de trabalho.

Nomes de tabelas, por exemplo, [sn_vul_m2m_vul_group_item], não são alterados.

Se você criou regras de grupos de vulnerabilidade em versões anteriores do Resposta a vulnerabilidades eles ainda estão disponíveis para você rotulados como regras de tarefa de correção.

No entanto, nos espaços, as regras de tarefa de correção não são mais usadas como o método primário de organizar um grande volume de registros em tarefas de correção. Você pode preferir deixar suas regras de tarefa de correção inativas conforme se acostuma com os espaços.

Em vez disso, você pode preferir começar a usar gradualmente o. Resposta a vulnerabilidades Espaços de trabalho.

1. Se você estiver atualizando de uma versão anterior de Resposta a vulnerabilidades suas regras de tarefa de correção existentes são preservadas. Eles ainda estão disponíveis para você nos espaços de trabalho. A regra de grupo padrão, Vulnerabilidade, está inativa por padrão.
2. Configure regras de atribuição e, talvez se quiser, regras de risco e execute uma importação.
3. Como gerente ou analista de vulnerabilidades, você pode escolher segmentos para monitorar nos tópicos de observação no Espaço do gerenciador de vulnerabilidades. Você pode usar tópicos de observação como recursos autônomos. Escolha qualquer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

subconjunto de registros e use o painel neles para monitorar tendências. Com eles, você pode decidir onde e quando concentrar os esforços de correção.

4. Como gerente ou analista de vulnerabilidades, você cria esforços de correção a partir de tópicos de observação quando decide que é hora de corrigir um subconjunto de registros. Uma tarefa de correção também é criada automaticamente para entregar a ELA quando você cria um esforço de correção.
5. Ao longo do tempo, como gerente ou analista de vulnerabilidades, você pode descobrir alguns padrões de rotina que pode lidar com regras de tarefas de correção automaticamente.

Para exibir suas regras de tarefa de correção, navegue até respectivo **Regras da tarefa de correção** módulos em Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações em **Todos** menu.

Mais informações sobre regras de atribuição, regras de tarefa de correção, esforços de correção e itens vulneráveis em Resposta a vulnerabilidades Espaços de trabalho

- Os registros da tarefa de correção são exibidos em listas e registros no ambiente clássico e nos espaços de trabalho.
- Uma tarefa de correção passa pelos mesmos estados de um grupo de vulnerabilidades. Quando todos os registros em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado inativo.
- Para ajudar suas equipes com a correção, um item vulnerável só pode estar em um esforço de correção. Quando ele estiver em um esforço de correção, um item vulnerável não será adicionado a nenhum outro esforço de correção que você criar.
- Se você excluir um esforço de correção, o esforço de correção se tornará inativo e todos os VIS ativos estarão disponíveis para novos esforços de correção.
- Um registro (VIT, AVIT, CVIT ou CTR) pode estar em várias tarefas de correção.
- As tarefas de correção são atribuídas automaticamente às equipes DE TI com base no grupo de atribuição associado a um item vulnerável em um esforço de correção. Se você criar uma tarefa de correção sob demanda, selecione o grupo de atribuição.
- Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades Suas regras de atribuição foram preservadas na IU legada.
- Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades seus usuários e grupos atuais são herdados e acessíveis para você nos espaços de trabalho.

Para obter mais informações sobre os ciclos de vida dos esforços de correção, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Configuração e configuração do Resposta a vulnerabilidades Espaços de trabalho

Para obter mais informações sobre regras de atribuição e regras de tarefa de correção, consulte Configure o. Resposta a vulnerabilidades Espaços de trabalho e. Resposta a vulnerabilidades visão geral das regras de atribuição.

Se você for um novo cliente e ainda não o tiver adicionado, configure usuários e grupos para que itens vulneráveis e tarefas de correção sejam atribuídos aos grupos de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

desejados. Regras de atribuição de Resposta a vulnerabilidades são usados para atribuir trabalho a grupos.

Configure o. Resposta a vulnerabilidades Espaços de trabalho

Antes de usar os espaços, confirme se você concluiu as tarefas de configuração a seguir.

Antes de Iniciar
Função necessária: administrador para atribuir funções a usuários e grupos e usuários a grupos.

sn_vul.vulnerability_admin para editar, criar regras e configurar o. Resposta a vulnerabilidades aplicação.

Confirme que você concluiu as tarefas de configuração a seguir. Consulte as etapas após a lista para obter mais informações sobre como executar essas tarefas.

Tarefa	Descrição
☐	Se ainda não estiver atribuído, atribua usuários e grupos com as funções apropriadas para que eles tenham acesso aos espaços de trabalho. Função necessária: administrador Consulte as etapas abaixo para obter mais informações.
☐	Configure regras de atribuição para que os itens vulneráveis sejam atribuídos aos grupos apropriados para correção. Função necessária: sn_vul.vulnerability_admin. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.
☐	(Opcional): Edite ou crie suas regras de tarefa de correção. Função necessária: sn_vul.vulnerability_admin. **Nota:** Funcionalmente, as regras de tarefa de correção funcionam exatamente como as regras de tarefa de correção faziam nas versões anteriores de Resposta a vulnerabilidades. No entanto, ao contrário dos grupos de vulnerabilidades que foram criados automaticamente a partir de suas regras de tarefa de correção, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção: • Por grupo de atribuição • Por grupo de atribuição e item de configuração • Por grupo de atribuição e vulnerabilidade • Nenhum - Use esta opção se quiser adicionar o VIS manualmente a uma tarefa de correção. Para obter mais informações, consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade.

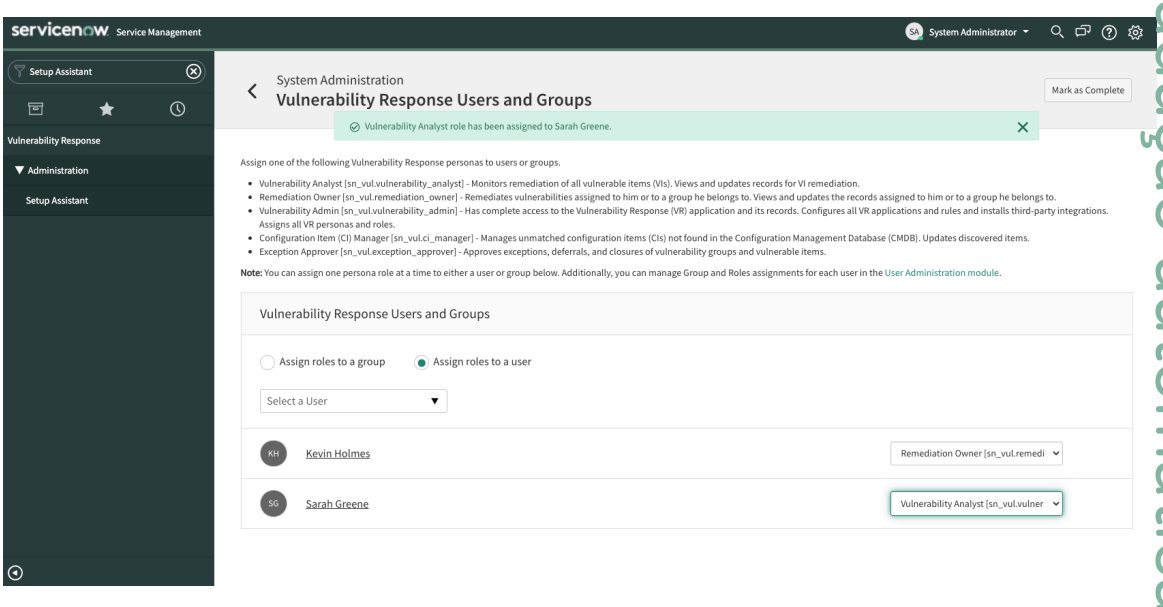
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Para obter mais informações sobre como os VIS são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção.
☐	Edite regras de destino de correção. Função necessária: sn_vul.vulnerability_admin. Adicione regras de destino de correção no ambiente clássico. Para obter mais informações sobre regras de destino de correção, consulte Criar ou editar Resposta a vulnerabilidades regras de destino de correção.

Procedimento

1. Depois de instalar e ativar o. Resposta a vulnerabilidades no ambiente clássico como um usuário com a função de administrador, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.



2. No Assistente de configuração, atribua usuários aos seguintes grupos.

> **Nota:** 1000 é o limite do número de grupos de usuários aos quais um usuário pode ser atribuído nos Espaços de resposta a vulnerabilidades.

Os grupos a seguir são fornecidos com Resposta a vulnerabilidades e são usados nos espaços de trabalho. Você pode atribuir usuários a eles no Assistente de configuração:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Responsável pela correção - Este grupo é destinado aos responsáveis pela correção de TI no Espaço de correção de TI. Usuários com esta função corrigem vulnerabilidades atribuídas a eles em tarefas de correção.

  Nota:

  Se você quiser que os responsáveis pela correção criem e exibam solicitações de mudança E exibir dados de item de configuração (IC) vulnerável no Espaço de correção de TI e no ambiente clássico atribua a eles a função itil. Você pode preferir atribuir a função itil a usuários individuais em vez de a todos os membros de um grupo. A função cmdb_read também é uma opção para os usuários exibirem dados de IC nos espaços de trabalho.

- A partir da v16.1, você pode configurar lembretes por e-mail para os responsáveis pela correção de TI. Para configurar notificações por e-mail para os espaços de trabalho, consulte Configurar notificações por e-mail no Resposta a vulnerabilidades Espaços de trabalho.
- Administrador de vulnerabilidades - Este grupo é para gerentes de vulnerabilidades. . Esta função configura o. Resposta a vulnerabilidades No Assistente de configuração. Esta função também tem permissão para processar solicitações de exceção e falso positivo.
- Analista de vulnerabilidades - Este grupo é para gerentes de segurança, gerentes de vulnerabilidades e analistas no Espaço do gerenciador de vulnerabilidades. Esta função monitora vulnerabilidades, cria tópicos de observação e esforços de correção e monitora o andamento da correção.
- Aprovador de falso positivo - Os usuários neste grupo processam solicitações de falso positivo para itens vulneráveis ou tarefas de correção. Uma solicitação falso-positivo requer um processo de aprovação de nível único. Você pode gerenciar a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários** .
- Aprovador de exceção - Uma solicitação de exceção para um item vulnerável ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Adicione usuários a ambos os grupos de aprovação: Aprovador de exceção - Nível 1 e Aprovador de exceção - 2. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível. Você gerencia a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários** .

  Nota: Adicione usuários aos grupos de aprovação antes de enviar solicitações de falso positivo e exceção. Se você criar solicitações antes de atribuir usuários com permissão de aprovação, as solicitações poderão não estar visíveis para eles.

Como alternativa, clique em **Administração de usuários** link para gerenciar e atribuir as seguintes funções granulares aos usuários e grupos existentes. Essas funções permitem que os usuários executem ações específicas no Resposta a vulnerabilidades e os espaços de trabalho.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Para criar e exibir solicitações de mudança No Espaço de correção de TI e no ambiente clássico, atribua a eles a função itil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Resposta a vulnerabilidades personas e funções granulares e. Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

3. As tarefas de correção são entregues automaticamente aos grupos de atribuição de correção de TI para processamento quando são criadas.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum - Use esta opção se quiser adicionar o VIS manualmente a uma tarefa de correção.

   Nota: Para a versão 18,0 de Resposta a vulnerabilidades. **Nenhum** a opção não está disponível.

   Se você estiver atualizando de uma versão anterior de Resposta a vulnerabilidades seus grupos de atribuição são preservados. No entanto, você pode preferir editar esses grupos para que os itens vulneráveis sejam associados a grupos de atribuição específicos até se acostumar a como os tópicos de observação e os esforços de correção funcionam. Por exemplo, você pode criar grupos de atribuição por produto ou região, mas pode usar qualquer critério que melhor se adapte à sua organização.

   Você também pode usar regras de atribuição para atribuir tarefas de correção a grupos. Você pode preferir executar somente regras de alta prioridade para os seguintes itens:
   - Itens que precisam de tratamento especial
   - Itens em que o risco é crítico ou um VI requer manipulação pela conformidade regulatória

   As seguintes regras de atribuição fornecidas com a aplicação estão ativas por padrão:
   - Regra de atribuição de IC descontinuada
   - Atribuir ao grupo de suporte de IC
   - Regra de atribuição de estação de trabalho
   - Regra de atribuição de banco de dados
   - Regra de atribuição de aplicações da Web
   - Regra de atribuição do Windows Server
   - Regra de atribuição de servidor que não seja Windows
   - Regra de atribuição Captar tudo

   Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.

4. **Opcional:** Edite ou crie suas regras de tarefa de correção.

   (Optional) Nos espaços de trabalho, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção:
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Por grupo de atribuição e vulnerabilidade
- Nenhum - Use esta opção se quiser adicionar o VIS manualmente a uma tarefa de correção. Para obter mais informações, consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade.

Nota: Em t versão 18,0 de Resposta a vulnerabilidades. **Nenhum** a opção não está disponível.

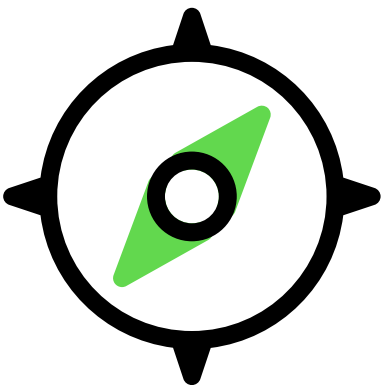
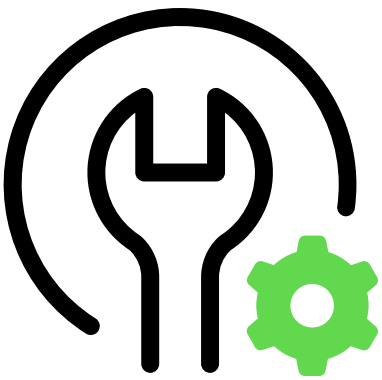
Para obter mais informações sobre como os VIS são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Resposta a vulnerabilidades tarefas de correção e visão geral das regras de tarefa de correção.

Espaço do gerente de vulnerabilidade

. Espaço do gerente de vulnerabilidade Permite que gerentes e analistas de vulnerabilidades monitorem as vulnerabilidades e as configurações incorretas com as quais eles mais se importam e decidam estrategicamente quais vulnerabilidades eles enviam para as equipes DE TI corrigirem.

Demonstração do Espaço do gerenciador de vulnerabilidades V18.0

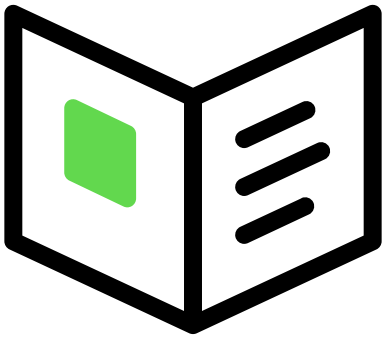
Iniciar

Explorar	Monitorar e gerenciar	Corrigir
		
Saiba mais sobre os recursos do Espaço do gerente de vulnerabilidade	Saiba como monitorar e gerenciar itens vulneráveis (Vits, AVITs e CVITs) e resultados de testes no Espaço do gerente de vulnerabilidade	Saiba como corrigir itens vulneráveis (Vits, AVITs e CVITs) e testar resultados no Espaço do gerente de vulnerabilidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referência



Saiba mais sobre as informações adicionais necessárias para usar o. Espaço do gerente de vulnerabilidade

Solucionar problemas e obter ajuda

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

Explorar o. Espaço do gerente de vulnerabilidade

Como gerente de vulnerabilidades e analista, obtenha um exibição unificada de todos os tipos de vulnerabilidade no Espaço do gerente de vulnerabilidade. Você pode ver vulnerabilidades de host, aplicação e contêiner e problemas de configuração, criar tópicos de observação nessas vulnerabilidades e configurações incorretas, criar esforços de correção e tarefas de correção.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Você pode exibir Espaço do gerente de vulnerabilidade navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades**.

. Espaço do gerente de vulnerabilidade consiste nas seguintes páginas:

Página inicial

Consiste em filtros predefinidos que são usados para visualizar o resumo de vulnerabilidades do host, vulnerabilidades da aplicação, vulnerabilidades do contêiner e resultados do teste de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre a página inicial, consulte Página inicial do Espaço do gerente de vulnerabilidade.

Nota: A partir de v21.0 de Resposta a vulnerabilidades, Os tópicos de observação aparecem na página Tópicos de observação.

Página Tópicos de observação

Consiste em uma lista de tópicos de observação, que são categorizados em quatro módulos: Vulnerabilidades do host, vulnerabilidades da aplicação, vulnerabilidades do contêiner e resultados do teste de configuração.

Para obter mais informações sobre tópicos de observação, consulte Página Tópicos de observação no Espaço do gerente de vulnerabilidade.

Página Painéis

Consiste nos painéis Gestão de vulnerabilidades, Gestão de vulnerabilidades (PA), Aprovações de vulnerabilidades, CISO, Visão geral da Gestão de vulnerabilidades de contêiner, Gestão de vulnerabilidades de aplicações, Resposta unificada de vulnerabilidades e Integridade.

Para obter mais informações, consulte Página Painéis em Espaço do gerente de vulnerabilidade.

Nota: A página Painéis é exibida a partir da versão 19,0 de Resposta a vulnerabilidades.

Página da lista

Consiste nas páginas de lista padrão e personalizadas para esforços de correção, tarefas de correção, itens vulneráveis do host, itens vulneráveis da aplicação, itens vulneráveis do contêiner, resultados de testes de configuração, exceções, aprovações e bibliotecas.

Para obter mais informações, consulte Página de lista no Espaço do gerente de vulnerabilidade.

Página inicial do Espaço do gerente de vulnerabilidade

A página inicial do Espaço do gerente de vulnerabilidade fornece um resumo dos registros ativos, mostrando visualizações de classificação de risco, andamento de correção, atribuições a grupos de atribuição, registros em tarefas de correção e vulnerabilidades de recursos de nuvem.

Na página inicial, você pode exibir as visualizações dos itens vulneráveis do host pré-filtrados, itens vulneráveis do contêiner, itens vulneráveis à aplicação e resultados de teste de configuração. Você também pode exibir visualizações de um conjunto de registros desejados criando e aplicando filtros. Para obter mais informações sobre como criar, atualizar, aplicar e excluir filtros, consulte Criar e aplicar filtros O resumo de registros ativos (Vits, AVITs, CVITs e CTR).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dica:

. *sn_vul_cmn_ws.navigate_to_workspace*a propriedade do sistema está definida como verdadeiro Pelo administrador, ao selecionar os links de filtro predefinidos nos módulos Itens vulneráveis, Itens vulneráveis à aplicação, Itens vulneráveis ao contêiner e Resultados de teste do **Todos** , esses links são abertos no Espaço do gerente de vulnerabilidade Página inicial de com seleção automática do filtro salvo correspondente.

Por exemplo, se você selecionar **Alto risco** navegando até **Tudo** > **Resposta a vulnerabilidades** > **Itens vulneráveis**Este link é redirecionado para a página inicial do Espaço do gerente de vulnerabilidade com seleção automática de **Alto risco** Filtre na guia Vulnerabilidades do host.

Na página inicial, você pode executar o seguinte:

- Detalhar os dados e exibir a lista de registros clicando nas visualizações.
- Navegue até a lista de registros ativos na IU clássica selecionando **Exibir lista clássica** link.
- Abra a lista de registros ativos no Espaço do gerente de vulnerabilidade selecionando a contagem de registros ativos ao lado de **Exibir por** menu suspenso.
- Atualize as visualizações selecionando **Atualizar filtro salvo selecionado** ícone.
- Para exibir as informações mais recentes, selecione **Atualizar** opção no menu de três pontos em um widget.

Vulnerabilidades dos servidores (host)

. **Vulnerabilidades do host** contém visualizações que fornecem um resumo geral das vulnerabilidades do host ativo.

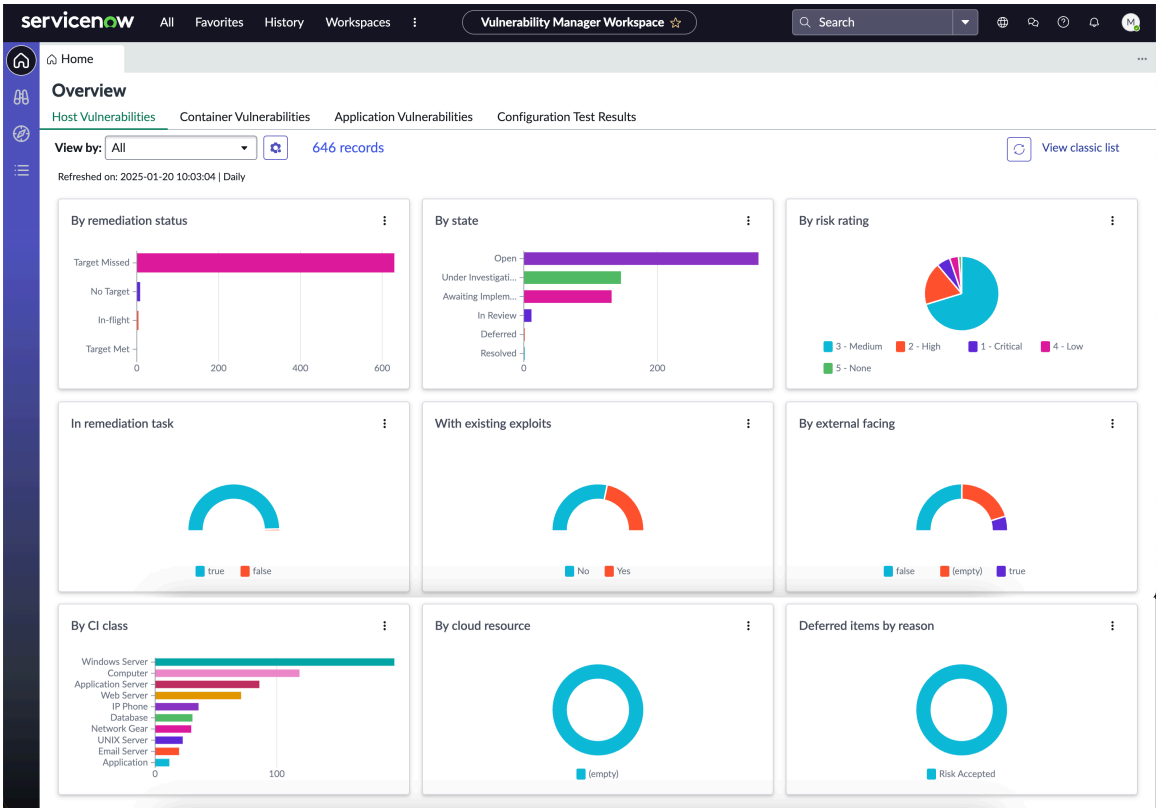
Funções necessárias:

- sn_vul.vulnerability_analyst e sn_vul.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- função granular sn_vul.read_all para exibir as visualizações aplicando filtros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Vulnerabilidades do host



A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Vulnerabilidades do host na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Em investigação, Aguardando implementação, Em revisão, Resolvido, e adiado).
Por classificação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Em tarefa de correção	Rosca semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com exploits existentes	Rosca semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca semicírculo	Registros ativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do host na página inicial

Visualização	Tipo	Descrição
Por recurso de nuvem	Gráfico de rosca	Registros ativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de rosca	Registros adiados ativos agrupados por motivo.

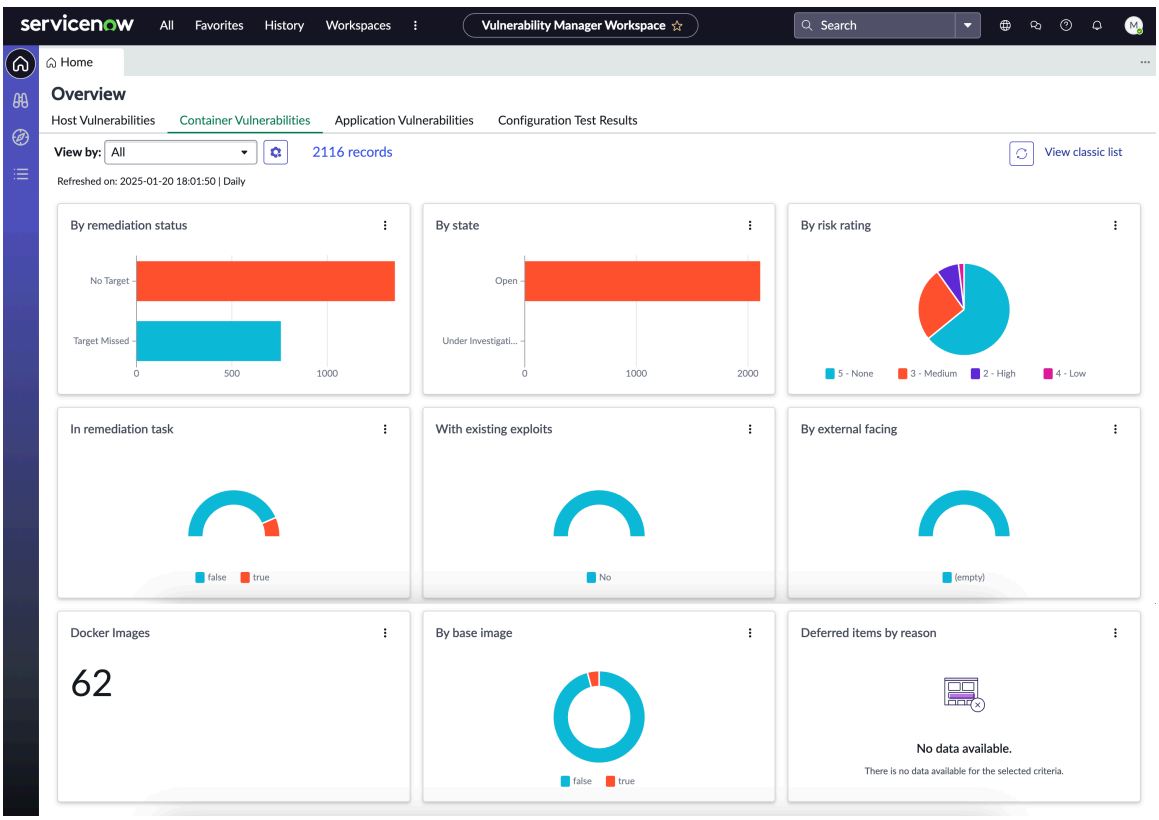
Vulnerabilidades do contêiner

. **Vulnerabilidades de contêiner** contém visualizações que fornecem um resumo geral dos itens vulneráveis do contêiner ativo.

Funções necessárias:

- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- função granular sn_vul_container.read_all para exibir as visualizações aplicando filtros.

Guia Vulnerabilidades do contêiner



A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial. Selecione essas visualizações para obter a lista de registros correspondentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do contêiner na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Em investigação, Aguardando implementação, Em revisão, Resolvido, e adiado).
Por classificação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Em tarefa de correção	Rosca semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com exploits existentes	Rosca semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca semicírculo	Registros ativos categorizados pela exposição do ativo à internet.
Imagens do Docker	Contagem	Número de imagens exclusivas do docker.
Por imagem base	Gráfico de rosca	Registros ativos categorizados pelo tipo de imagem.
Itens adiados por motivo	Gráfico de rosca	Registros adiados ativos agrupados por motivo.

Vulnerabilidades de aplicações

. **Vulnerabilidades da aplicação** contém visualizações que fornecem um resumo geral das vulnerabilidades da aplicação.

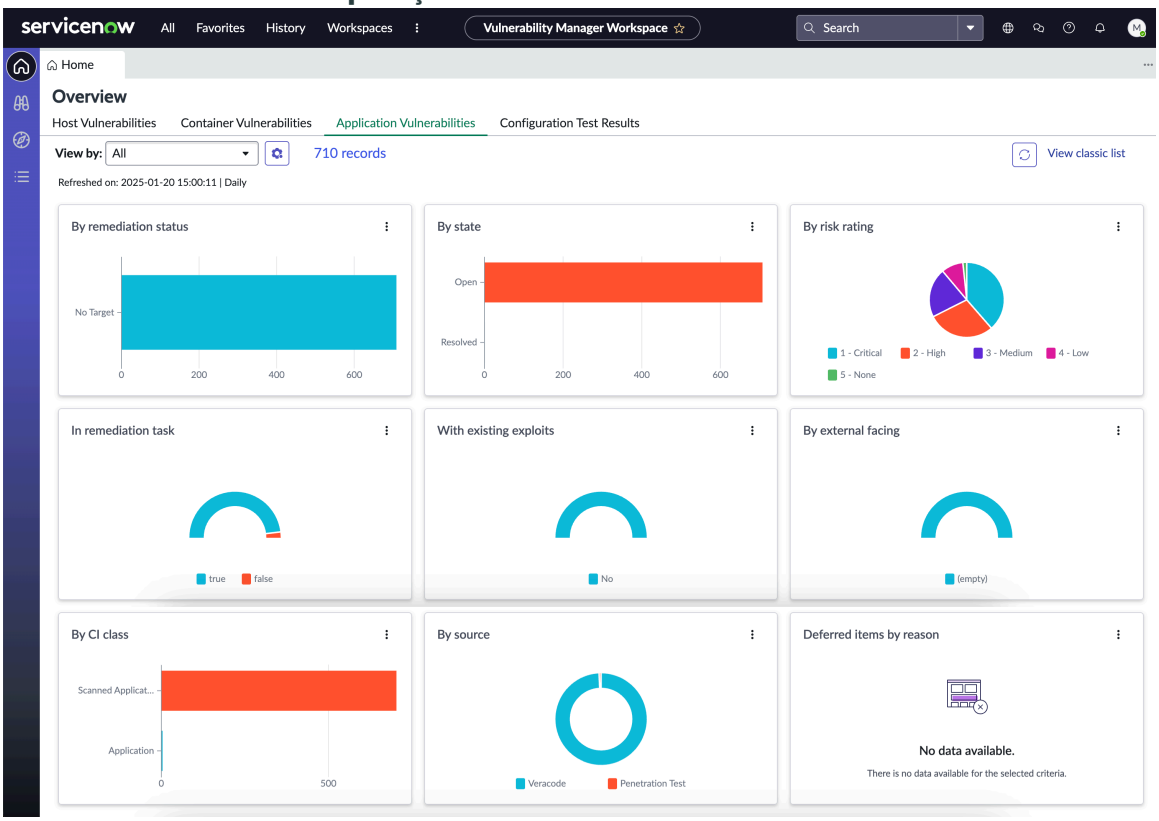
Funções necessárias:

- sn_vul.app_sec_manager para exibir as visualizações aplicando filtros e criar filtros.
- função granular sn_vul.app_read_all para exibir as visualizações aplicando filtros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Vulnerabilidades da aplicação



A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Vulnerabilidades da aplicação na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Em investigação, Aguardando implementação, Em revisão, Resolvido, e adiado).
Por classificação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Em tarefa de correção	Rosca semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com exploits existentes	Rosca semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca semicírculo	Registros ativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades da aplicação na página inicial

Visualização	Tipo	Descrição
Por recurso de nuvem	Gráfico de rosca	Registros ativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de rosca	Registros adiados ativos agrupados por motivo.

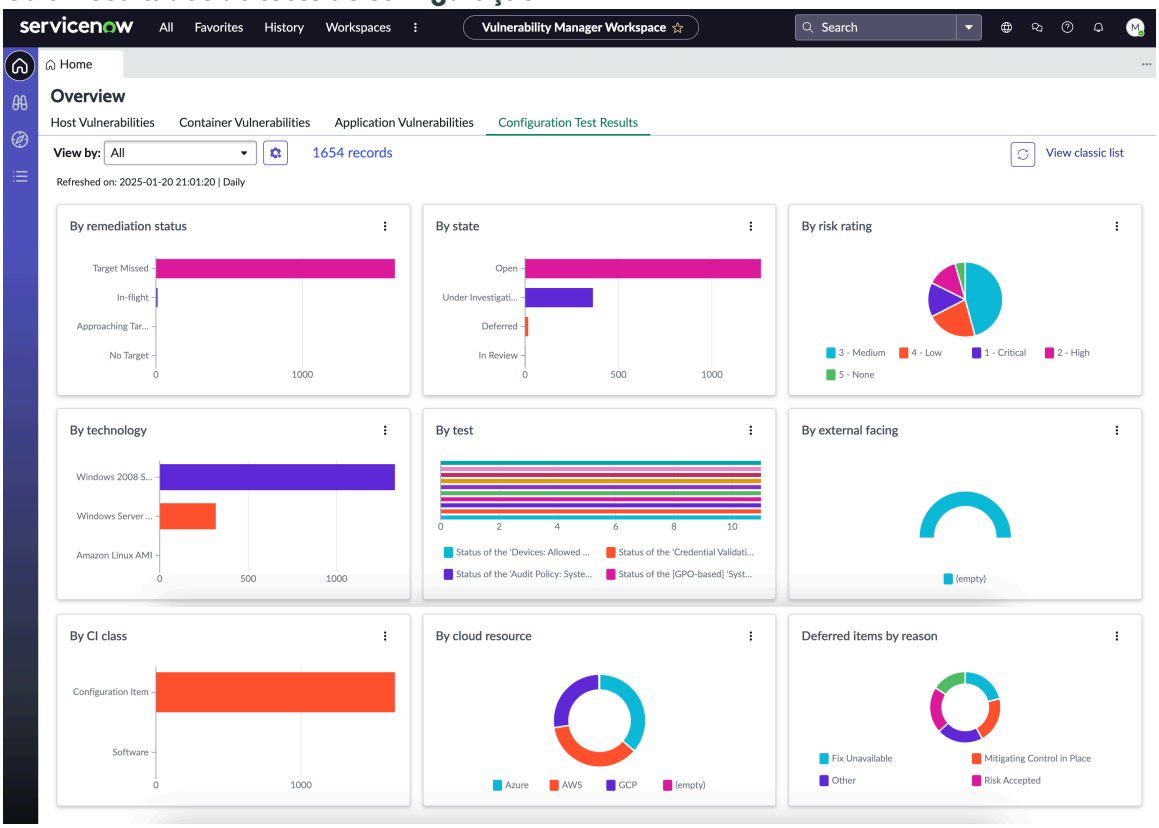
Resultados de testes de configuração

. **Resultados do teste de configuração** contém visualizações que fornecem um resumo geral das configurações incorretas ativas dos ativos em sua organização.

Funções necessárias:

- sn_vulc.admin para exibir as visualizações aplicando filtros e criar filtros.
- função granular sn_vulc.read para exibir as visualizações aplicando filtros.

Guia Resultados do teste de configuração



A tabela a seguir descreve as visualizações na guia Resultados do teste de configuração na página inicial. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Resultados do teste de configuração na página inicial

Visualização		Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Resultados do teste de configuração na página inicial

Visualização		Descrição
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Em investigação, Aguardando implementação, Em revisão, Resolvido, e adiado).
Por classificação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Por tecnologia	Barra	Registros ativos categorizados por tecnologia.
Por teste	Barra	Registros ativos categorizados por testes.
Por face externa	Rosca semicírculo	Registros ativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Gráfico de rosca	Registros ativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de rosca	Registros adiados ativos agrupados por motivo.

Página Tópicos de observação no Espaço do gerente de vulnerabilidade

A página Tópicos de observação no Espaço do gerente de vulnerabilidade permite que você crie e edite um tópico de observação. . *Tópico de observação* É um conjunto de visualizações de dados que permite monitorar um conjunto filtrado de registros (Vits, AVITs, CVITs e CTRs) ao longo do tempo em um painel que pode ser de um interesse ou prioridade específico para sua organização.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Os dados exibidos nas visualizações de dados nos tópicos de observação são atualizados dinamicamente conforme os dados de vulnerabilidade mudam na importação. Use os painéis para monitorar as tendências, o escopo e os tipos de vulnerabilidades e os itens de configuração do tópico de exibição selecionado. Essas informações ajudam a determinar como as vulnerabilidades em cada tópico de observação afetam seu ambiente. A página Tópicos de observação consiste em quatro módulos - Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação, Resultados do teste de configuração e Inativo. Para obter mais informações sobre as guias Itens relacionados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e suas visualizações em um tópico de observação, consulte Lista de itens relacionados e visualizações em um tópico de observação.

Os tópicos de observação a seguir são fornecidos com o sistema de base no módulo Vulnerabilidades do host na página Tópicos de observação:

- Vulnerabilidades em ativos externos
- Vulnerabilidades com explorações disponíveis
- Vulnerabilidades em servidores Windows
- Vulnerabilidades em servidores LINUX
- Vulnerabilidades críticas atrasadas
- Vulnerabilidades críticas que não estão em tarefas de correção

Nota: Se uma visualização de dados mostrar que não há registros para essa categoria, mas você puder ver uma lista de registros ao clicar no ícone de gráfico, verifique a coluna com o nome do tópico de observação na lista exibida. Verifique se o valor de todos os registros listados na coluna do tópico de observação, por exemplo, voltados para a Internet, é falso . Este valor neste exemplo indica que não há registros voltados para a internet para este tópico de observação.

Para iniciar a correção ou quando surgir uma necessidade crítica para os registros que estão em um tópico de observação, você pode criar um *Esforço de correção* de um tópico de observação. Para obter mais informações, consulte Crie um esforço de correção no Espaço do gerente de vulnerabilidade.

Tópicos relacionados

Lista de itens relacionados e visualizações em um tópico de observação

Usar tópicos de observação no Espaço do gerente de vulnerabilidade

Crie um tópico de observação no Espaço do gerente de vulnerabilidade

Edite ou exclua um tópico de observação no Espaço do gerente de vulnerabilidade

Desative ou ative um tópico de observação

Lista de itens relacionados e visualizações em um tópico de observação

Na página Tópicos de observação de Espaço do gerente de vulnerabilidade, Você pode criar tópicos de observação categorizados em quatro módulos: Vulnerabilidades de host, Vulnerabilidades de contêiner, Vulnerabilidades de aplicações e Resultados de testes de configuração. As guias Itens relacionados em um tópico de observação diferem para cada módulo.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

O painel de navegação na página Tópicos de observação contém os seguintes módulos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidades do host: Exibe os tópicos de observação que incluem os itens vulneráveis do host.
- Vulnerabilidades de contêiner: Exibe os tópicos de observação que incluem os itens vulneráveis do contêiner.
- Vulnerabilidades da aplicação: Exibe os tópicos de observação que incluem os itens vulneráveis da aplicação.
- Resultados do teste de configuração: Exibe os tópicos de observação que incluem os itens de configuração.
- Inativo: Exibe os tópicos de observação inativos de todos os quatro módulos.

A tabela a seguir mostra as guias Itens relacionados que estão disponíveis para diferentes módulos de tópico de observação:

Tópico de observação e seus itens relacionados

Tópico de observação	Guias Itens relacionados
Vulnerabilidades dos servidores (host)	Visão geral, ICs afetados, vulnerabilidades distintas e Itens vulneráveis
Vulnerabilidades do contêiner	Visão geral, ICs afetados, vulnerabilidades distintas e Itens vulneráveis
Vulnerabilidades de aplicações	Visão geral e itens vulneráveis
Resultados de testes de configuração	Visão geral, ICs afetados, Testes de configuração distintos e Resultados de teste de configuração

A tabela a seguir fornece uma descrição das guias Itens relacionados e das visualizações em um tópico de observação.

Guias de Itens relacionados e visualização em um tópico de observação

Guia Itens relacionados e visualização	Descrição
Visão geral	
Itens vulneráveis ativos ao longo do tempo	Número de itens vulneráveis (VIS) ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias. Você também pode filtrar os dados usando Categoria do ativo filtros.
IVs em esforços de correção	Número de VIS ativos do número total de VIS que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista de esforços de correção ativos.
Afetado ICs	
ICs distintos	Número de itens de configuração (ICs) (ativos) afetado por essas vulnerabilidades.
IVs por classe de IC	Número de itens vulneráveis (VIS) para cada um Configuration Management Database (CMDB) Classe de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de Itens relacionados e visualização em um tópico de observação

Guia Itens relacionados e visualização	Descrição
	Nota: Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração por classe de IC	Número de ICs para cada um Configuration Management Database (CMDB) Classe de IC. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
IVs voltados para a Internet	Número de VIS ativos do número total de VIS de seus ativos que estão expostos à internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração voltados para a Internet	Número de ICs ativos do número total de ICs para seus ativos expostos à Internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
Vulnerabilidades distintas	
IVs com explorações existentes	VIS ativo com explorações conhecidas.
Vulnerabilidades distintas	Número de vulnerabilidades individuais e distintas associadas aos seus ativos. As vulnerabilidades distintas podem ser filtradas com base no tipo de problema.
IVs com vulnerabilidades de PCI	Número de ativos individuais distintos que têm VIS ativos com vulnerabilidades do setor de cartão de pagamento (PCI).
Itens vulneráveis	
Itens vulneráveis de host	Lista de todos os itens vulneráveis do host. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do host.
Itens vulneráveis da aplicação	Lista de todos os itens vulneráveis à aplicação. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de Itens relacionados e visualização em um tópico de observação

Guia Itens relacionados e visualização	Descrição
	Nota: Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades da aplicação.
Itens vulneráveis de contêiner	Lista de todos os itens vulneráveis do contêiner. Você pode filtrar esta lista para exibir para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do contêiner.
Visão geral Em um tópico de observação no módulo Resultados de teste de configuração	
Resultados de testes de configuração ativos ao longo do tempo	Número de resultados de testes de configuração ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias.
Resultados de testes de configuração em esforços de correção	Número de resultados de testes de configuração ativos do número total de registros que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista de esforços de correção ativos.
Testes de configuração distintos Em um tópico de observação no módulo Resultados de teste de configuração	
Resultados do teste de configuração via Criticalidade do teste	Resultados de testes de configuração baseados na criticidade dos problemas.
Testes de configuração distinta	Número de testes de configuração distintos.
Resultados do teste de configuração Em um tópico de observação no módulo Resultados de teste de configuração	Lista de resultados de testes de configuração.

Você pode adquirir os detalhes mais recentes de um tópico de observação selecionando **Atualizar** botão. O status de atualização e o carimbo de data/hora mais recentes são exibidos sob o nome do tópico de observação. Quando você atualiza um tópico de observação, todos os detalhes do tópico de observação, incluindo os gráficos e os esforços de correção, são atualizados. Um tópico de observação é atualizado automaticamente quando é criado ou atualizado.

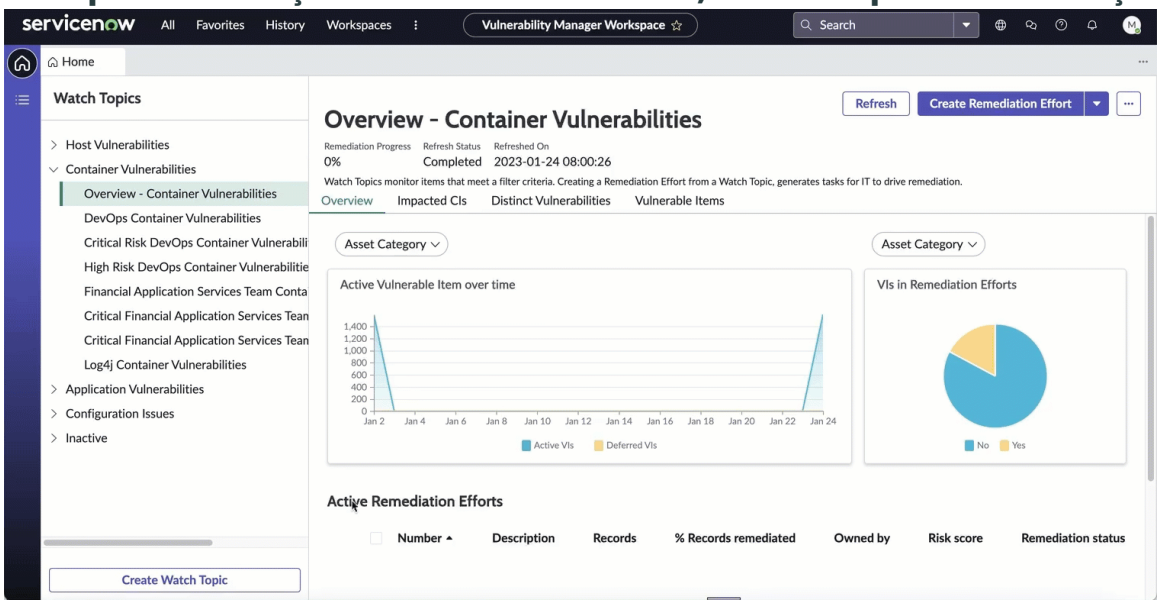
Nota: Como você não pode atualizar um tópico de observação inativo, o. **Atualizar** o botão está inativo para um tópico de observação inativo.

Clique em um gráfico de dados em qualquer um dos widgets para exibir informações adicionais sobre os registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Visualizações de dados da versão 18,0 em um tópico de observação



Esforços de correção no Espaço do gerente de vulnerabilidade

Um esforço de correção é um conjunto de registros associados a um tópico de observação. Os registros listados em um esforço de correção são estáticos. Eles não são atualizados por novos dados de importação ou mudanças que você faz nos tópicos de observação.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Com **Ativo** selecionado em **Esforços de correção** Lista Na página Lista, clique em um link de esforço de correção para abri-lo. Para categorizar os esforços de correção em itens vulneráveis do host (Vits), itens vulneráveis à aplicação (AVITs), itens vulneráveis do contêiner (CVITs) e resultados de teste de configuração (CTRs), selecione o menu de três pontos no **Tipo de registro** e selecione **Agrupar por tipo de registro** .

Os itens da lista relacionada no registro de esforço de correção permitem exibir o andamento geral da correção e o status nos registros associados a ele.

- Em **Visão geral** monitore os registros associados a este esforço de correção que foram encerrados ao longo do tempo. À direita do registro, clique no ícone de filtro no gráfico para ver os filtros aplicados à visualização de dados.
- Em **Detalhes** Exiba detalhes sobre o esforço de correção, incluindo o tópico de observação associado e o status (Ativo ou Inativo). Você pode desativar um esforço de correção nesta página. Se você desativar o esforço de correção antes que todos os registros sejam encerrados, todos os registros ativos ficarão disponíveis para adicionar a novos esforços de correção.
- Em **Tarefas de correção** Exiba as tarefas de correção associadas a este esforço de correção. Veja a porcentagem dos registros associados a esta tarefa que foram corrigidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em **Itens vulneráveis** exiba os registros associados a este esforço de correção. Quando todos os registros em uma tarefa de correção são concluídos e encerrados, o esforço de correção muda para inativo. Quando um esforço de correção está inativo, todos os registros encerrados associados ao esforço de correção não estão disponíveis para adicionar aos novos esforços de correção.

  Nota: . **Itens vulneráveis** Aparece para os esforços de correção associados aos tópicos de observação nos módulos Vulnerabilidades do host, Vulnerabilidades da aplicação e Vulnerabilidades do contêiner.

- Em **Resultados do teste de configuração** Exiba os Resultados do teste de configuração associados ao esforço de correção. Quando todos os registros em uma tarefa de correção são concluídos e encerrados, o esforço de correção muda para inativo. Quando um esforço de correção está inativo, todos os registros encerrados associados ao esforço de correção não estão disponíveis para adicionar aos novos esforços de correção.

  Nota: . **Resultados do teste de configuração** Aparece para os esforços de correção associados aos tópicos de observação no módulo Resultados do teste de configuração.

Para obter mais detalhes e ações de IU que você pode executar a partir de um esforço de correção, consulte Usar registros de esforço de correção.

Tópicos relacionados

Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades

Crie um esforço de correção no Espaço do gerente de vulnerabilidade

Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade

Crie um esforço de correção recorrente no Espaço do gerente de vulnerabilidade

Transfira registros para esforços de correção no Espaço do gerente de vulnerabilidade

Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades

Os estados dos registros e suas tarefas de correção associadas (RTS) serão afetados se os registros forem adiados, resolvidos, reabertos e transferidos para outros esforços de correção (RES).

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Criando esforços de correção

Como os estados e os ciclos de vida dos esforços de correção, tarefas de correção e registros são afetados depende de como um esforço de correção é criado, quando é criado e se foi desativado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na lista no canto superior direito de um tópico de observação, você pode criar um esforço de correção clicando em **Crie um esforço de correção** ou **Criar esforço recorrente** . Você pode criar um esforço de correção recorrente por tópico de exibição. Se você criar um esforço de correção recorrente, os esforços de correção subsequentes para o tópico de observação associado serão criados automaticamente com base nos critérios definidos. Em ambos os casos:

- Para facilitar a correção, somente registros ativos são adicionados aos esforços de correção.
- Todos os registros em novos esforços de correção são colocados em novas tarefas de correção. Registros podem existir em várias tarefas de correção, mas somente um registro pode ser associado a um esforço de correção.

Nota: Um esforço de correção é desativado automaticamente quando não há registros ativos.

Transferindo registros ou transferência de registro

Você pode transferir registros de um esforço de correção para outro ao criar um esforço de correção selecionando **Transfira registros correspondentes de outros esforços de correção ativos** caixa de seleção. Para obter mais informações sobre como transferir os registros, consulte Transfira registros para esforços de correção no Espaço do gerente de vulnerabilidade. Se os registros forem transferidos de um esforço de correção ou transferidos para esforços de correção recorrentes:

Para um novo esforço de correção no mesmo tópico de observação

- Todas as tarefas de correção do esforço de correção antigo são movidas para o novo esforço de correção.
- Novas tarefas de correção são criadas com base nos critérios de agrupamento escolhidos para os registros que anteriormente não faziam parte de nenhuma tarefa de correção.
- O esforço de correção antigo está desativado.

Para um novo esforço de correção em um tópico de observação diferente

Todos os registros do esforço de correção antigo são movidos para o novo esforço de correção e as tarefas de correção são criadas com base nos critérios de agrupamento escolhidos.

- Se todos os registros nas tarefas de correção associadas ao esforço de correção antigo forem transferidos, essas tarefas de correção serão encerradas e canceladas.
- Se somente um subconjunto de registros for transferido, as tarefas de correção associadas ao esforço de correção antigo serão divididas e permanecerão ativas.

As tarefas de correção encerradas associadas ao esforço de correção antigo não são afetadas.

Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção existentes e não recorrentes para novos esforços de correção. Consulte Transfira registros para esforços de correção no Espaço do gerente de vulnerabilidade para obter mais informações sobre como transferir registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página Painéis em Espaço do gerente de vulnerabilidade

Na página Painéis do Espaço do gerente de vulnerabilidade, você pode exibir os painéis no Next Experience E use esses painéis para rastrear e analisar as vulnerabilidades.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Acesse os painéis no Espaço do gerente de vulnerabilidade navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades** e selecionando **Painéis** ícone. O painel padrão é exibido com base em sua função.

A tabela a seguir mostra o painel padrão exibido para uma função específica.

Painel padrão

Painel padrão	Função
Painel unificado	sn_vul_cmn_vulnerability_admin ou sn_vul_cmn_vulnerability_analyst
Painel de PA de vulnerabilidades	sn_vul_vulnerability_admin ou sn_vul_vulnerability_analyst
Visão geral das candidaturas	sn_vul_app_sec_manager
Visão geral do contêiner	sn_vul_container_vulnerability_admin ou sn_vul_container_analyst

Você pode exibir os seguintes painéis para as tarefas que deseja executar selecionando-os no menu suspenso na página Painéis.

Painéis no Espaço do gerente de vulnerabilidade

Painel	Descrição
Gestão de vulnerabilidade (PA)	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do host, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Gestão de vulnerabilidade(PA) painel.
Aprovações de vulnerabilidade	Exiba o número de solicitações de aprovação aprovadas, rejeitadas e pendentes para você. Para obter mais informações, consulte Usando o padrão Resposta a vulnerabilidades painéis.
Painel do CISO	Revela a postura de segurança geral da sua organização, incluindo a vulnerabilidade de segurança e os incidentes. Para obter mais informações, consulte Gestão de vulnerabilidade CISO painel.

Tradução automática

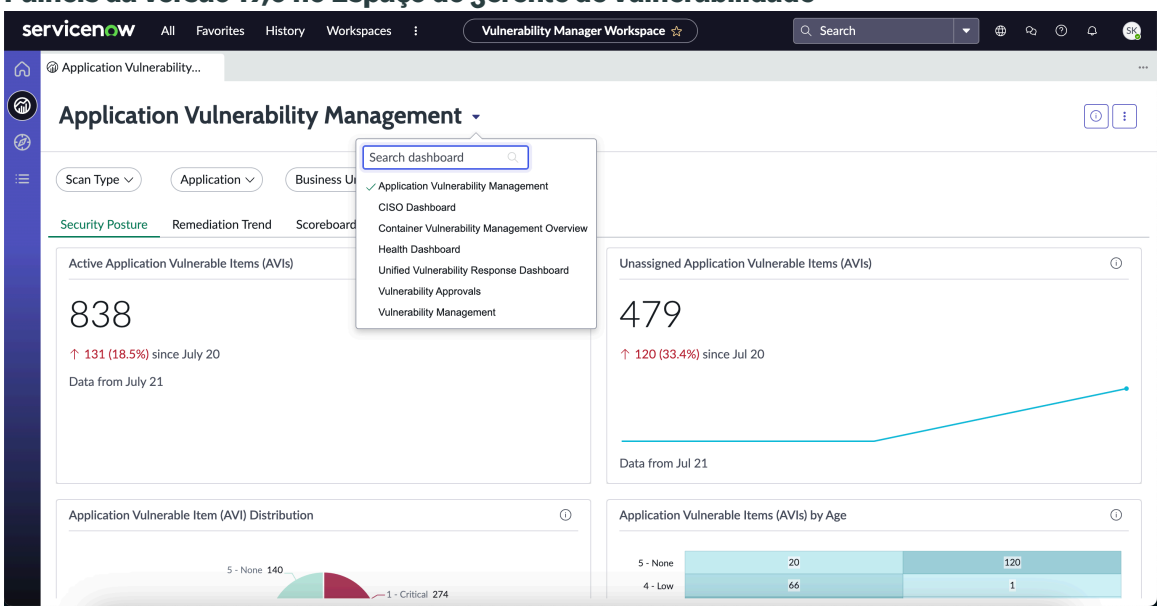
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis no Espaço do gerente de vulnerabilidade

Painel	Descrição
Visão geral da gestão de vulnerabilidade do contêiner	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do contêiner, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Painel do Contêiner de Resposta a vulnerabilidades.
Painel da Gestão de vulnerabilidades da aplicação	Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Gestão de vulnerabilidades de aplicações Painel (PA).
Painel da Resposta a vulnerabilidades unificado	Fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma visão abrangente das vulnerabilidades e riscos de uma organização. Para obter mais informações, consulte Soluções de análise e emissão de relatórios para o Painel de resposta unificada a vulnerabilidades.
Painel de Integridade de Resposta a vulnerabilidades	Exibe a pontuação de integridade geral da aplicação Resposta a vulnerabilidades. Para obter mais informações, consulte Painel Integridade de resposta a vulnerabilidades SecOps.

A imagem a seguir mostra a página Painéis no Espaço do gerente de vulnerabilidade.

Painéis da versão 19,0 no Espaço do gerente de vulnerabilidade



Você também pode criar um painel personalizado selecionando o ícone Mais opções ⋮ e selecionando **Criar novo painel** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página de lista no Espaço do gerente de vulnerabilidade

A página Lista no Espaço do gerente de vulnerabilidade permite que gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção em registros, detalhem registros e exibam o status de suas solicitações de aprovação e exceções.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Essas listas e links fornecem acesso fácil a registros e tarefas. Ele contém duas guias:

- **Listas** Guia: Exibe as listas padrão para esforços de correção, tarefas de correção, itens vulneráveis, resultados de testes de configuração, soluções, e bibliotecas.
- **Minhas listas** Guia: Exibe todas as listas renomeadas na guia Listas e todas as listas que você criar.

  Você também pode criar sua própria lista para monitorar o andamento da correção. Para obter mais informações, consulte Crie uma lista personalizada de registros.

Guia Listas

A tabela a seguir mostra as listas disponíveis na guia Listas da página Lista:

Dica:

. *sn_vul_cmn_ws.navigate_to_workspace*a propriedade do sistema está definida como verdadeiro Por um administrador, ao selecionar os links de filtro predefinidos nos módulos Resposta a vulnerabilidades, Resposta a vulnerabilidades da aplicação, Resposta a vulnerabilidades do contêiner e Conformidade de configuração do **Todos** , esses links são abertos na página Lista do Espaço do gerente de vulnerabilidade com base em sua função.

Por exemplo, se você selecionar **Atribuído a Meus grupos** navegando até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**este link é redirecionado para Espaço do gerente de vulnerabilidade. . **Atribuído a Meus grupos** lista no **Tarefas de correção** O módulo será aberto na página Lista do Espaço do gerenciador de vulnerabilidades se você tiver a função de administrador ou analista de vulnerabilidades. Para exibir as tarefas de correção do host, agrupe as tarefas por tipo de registro.

Você pode ocultar a contagem de registros nas listas usando *glide.ui.list.seismic.omit.count*propriedade do sistema. Para obter mais informações sobre como ativar/desativar a contagem de registros em uma lista, consulte KBB0010402 artigo da base de conhecimento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
Esforços de correção (RES)	Lista de RES ativos e todos os RES atribuídos aos seus grupos de atribuição. Agrupe os esforços de correção por **Tipo de registro** categorizá-los por itens vulneráveis do host, itens vulneráveis à aplicação, itens vulneráveis ao contêiner e resultados de teste de configuração.	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs) • sn_vulc.admin para resultados de teste de configuração (CTRs)
Tarefas de correção	Contém as seguintes listas: • Ativo: Lista de todas as tarefas ativas de correção de host, aplicação, contêiner e resultado de teste. • Todos: Lista de tarefas de correção de host, aplicação, contêiner e resultado de teste ativas e inativas. • Atribuído a mim: Lista de tarefas de correção atribuídas a você para correção. • Atribuído ao meu grupo: Tarefas de correção atribuídas aos seus grupos de atribuição para correção.	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs) • sn_vulc.admin para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	Agrupe as tarefas de correção por **Tipo de registro** categorizá-los por itens vulneráveis do host, itens vulneráveis à aplicação, itens vulneráveis ao contêiner e resultados de teste de configuração. **Nota:** A lista Tarefas de correção inclui tarefas geradas durante a criação do esforço de correção no Espaço do gerente de vulnerabilidade, Bem como aqueles criados manualmente e por regras de tarefa de correção e outros processos na IU clássica. A coluna Esforço de correção ficará vazia para todas as tarefas de correção que não foram criadas como parte do esforço de correção.		
Itens vulneráveis de host	Contém as listas a seguir • Ativo: Lista de todos os itens vulneráveis do host ativo. • Todos: Lista de itens vulneráveis do host ativos e inativos. • Atribuído a mim: Lista de itens vulneráveis do host atribuídos a você para correção.	Resposta a vulnerabilidades	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	• Atribuído ao meu grupo: Lista de itens vulneráveis do host atribuídos aos seus grupos de atribuição para correção.		
Itens vulneráveis da aplicação	Contém as seguintes listas: • Ativo: Lista de todos os itens vulneráveis da aplicação ativos. • Todos: Lista de itens vulneráveis à aplicação ativos e inativos. • Atribuído a mim: Lista de itens vulneráveis à aplicação atribuídos a você para correção. • Atribuído ao meu grupo: Lista de itens vulneráveis à aplicação atribuídos aos seus grupos de atribuição para correção. Você pode criar um novo item vulnerável à aplicação selecionando **Novo** botão.	Resposta a vulnerabilidades de aplicações	sn_vul.app_sec_manager
Itens vulneráveis de contêiner	Contém as seguintes listas: • Ativo: Lista de todos os itens vulneráveis do contêiner ativo. • Todos: Lista de itens vulneráveis de contêiner ativos e inativos.	Contêiner de Resposta a vulnerabilidades	sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	• Atribuído a mim: Lista de itens vulneráveis de contêiner atribuídos a você para correção. • Atribuído ao meu grupo: Lista de itens vulneráveis ao contêiner atribuídos aos seus grupos de atribuição para correção.		
Resultados de testes de configuração	Contém as seguintes listas: • Ativo: Lista de todos os resultados de testes ativos. • Todos: Lista de resultados de testes ativos e inativos. • Atribuído a mim: Lista de resultados de testes atribuídos a você para correção. • Atribuído ao meu grupo: Lista de resultados de testes atribuídos aos seus grupos de atribuição para correção.	Conformidade de configurações	sn_vulc.admin
Soluções	Contém as seguintes listas: • Todos - Mostra todas as soluções disponíveis que você pode usar para corrigir os itens vulneráveis do host.	Resposta a vulnerabilidades	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	• Maior substituição - Mostra todas as soluções usadas para preencher as Soluções preferenciais. • Com itens vulneráveis - Mostra as soluções que estão sendo usadas como Solução preferencial em itens vulneráveis.		
Exceções	Mostra os estados de aprovação de todas as solicitações de exceção e falso-positivo associadas aos seus grupos de atribuição. • Todos: Lista de solicitações de aprovação de exceção, falso-positivo e cancelamento de atribuição relacionadas a Vits, AVITs e CVITs e suas tarefas de correção (VUL, AVUL e CVUL). • Tudo (Conformidade de configuração): Lista de exceções, falso-positivo e tarefas de correção relacionadas a solicitações de aprovação de cancelamento de atribuição (número de CTR). Agrupe as exceções por **Tipo de registro** categorizá-	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs) • sn_vulc.admin para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	los por itens vulneráveis do host, itens vulneráveis à aplicação, itens vulneráveis ao contêiner e resultados de teste de configuração.		
Aprovações	Atribuído a mim: Mostra as solicitações de aprovação atribuídas a você para processamento. Para processar suas aprovações no espaço, consulte Aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade.	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs) • sn_vulc.admin para resultados de teste de configuração (CTRs)
Bibliotecas	Consiste nas seguintes listas: • CVEs (NVD) - Lista de todas as vulnerabilidades e exposições comuns (CVEs) de Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações e Contêiner de Resposta a vulnerabilidades. • TPEs - Lista de vulnerabilidades de terceiros importadas em sua instância.	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs. • CWEs - Lista de todas as enumerações de pontos fracos comuns (CWEs) de Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações e Contêiner de Resposta a vulnerabilidades. • Vulnerabilidades da aplicação - Lista de todas as entradas de vulnerabilidade da aplicação de terceiros. • Grupos de teste - Lista de todos os Conformidade de configurações grupos de teste. Você pode exibir a porcentagem de conformidade de IC e a conformidade dos resultados de testes de um Grupo de testes na exibição de registro. • Testes - Lista de todos os testes de Conformidade de configurações. Você pode exibir a porcentagem de conformidade dos resultados de teste para um teste na exibição de registro.		• sn_vulc.admin para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	• Controles de compensação - Lista de todos os controles de compensação que podem ser usados para solicitações de redução de risco. Você pode adicionar um controle de compensação clicando em **Novo** . Para obter mais informações sobre como adicionar um controle de compensação, consulte Adicione um controle de compensação à biblioteca.		
CMDB	Contém as listas a seguir • **Itens descobertos** : Lista de todos os itens descobertos. • **Imagens de contêiner descobertas** : Lista de imagens de contêiner. Essas imagens de contêiner fornecem informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens junto com as informações da camada. • **Tabela Aplicações descobertas** Adicionado à exibição do Espaço do gerenciador de vulnerabilidades. Reaplicar itens descobertos	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits) • sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi para Itens vulneráveis ao contêiner (CVITs) • sn_vulc.admin para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	selecionados ou filtrados ou aplicações no espaço.		
Solicitações de avaliação de teste de invasão	Contém as seguintes listas: • **Ativo** : Lista de solicitações de avaliação de teste de invasão ativas. • **Todos** : Lista de solicitações de avaliação de teste de invasão ativas e inativas • **Atribuído a mim** : Lista de solicitações de avaliação de teste de invasão feitas por você. • **Atribuído ao meu grupo** : Lista de solicitações de avaliação de teste de invasão geradas pelos usuários em seus grupos de atribuição. Para obter informações sobre como criar uma solicitação de avaliação de teste de invasão, consulte Criar uma nova solicitação de avaliação de teste de invasão.	Resposta a vulnerabilidades de aplicações	sn_vul.app_sec_manager
Descobertas do teste de invasão	Contém as seguintes listas: • Ativo: Lista de todas as descobertas ativas do teste de invasão.	Resposta a vulnerabilidades de aplicações	sn_vul.app_sec_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	• Todos: Lista de descobertas ativas e inativas do teste de invasão. • Atribuído a mim: Lista de descobertas do teste de invasão atribuídas a você para correção. • Atribuído ao meu grupo: Lista de descobertas do teste de invasão atribuídas aos seus grupos de atribuição para correção. Para obter informações sobre como criar descobertas de teste de invasão, consulte Crie descobertas de teste de invasão com base em um questionário de avaliação.		
Patches	Todos: Lista de todos os patches disponíveis que podem ser usados para corrigir itens vulneráveis do host.	Resposta a vulnerabilidades	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin
Dados de suporte	Contém as seguintes listas: • **Fontes autorizadas** : Lista de fontes autorizadas que fornecem informações resumidas que são úteis para pesquisar as publicações de origem. • . : Lista de tecnologias que fornecem as	Conformidade de configurações	sn_vulc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Módulos	Funções Obrigatórias
	informações resumidas sobre cada fonte autorizada e citação (também conhecidas, na Qualys, como uma estrutura).		

Tópicos relacionados

Use a Exibição de lista no Espaço do gerente de vulnerabilidade

Edição em massa no Espaço do gerente de vulnerabilidade

Em Espaço do gerente de vulnerabilidade, O recurso de edição em massa permite que você atualize vários itens vulneráveis (Vits, AVITs ou CVITs) ou resultados de teste de configuração (TRs) simultaneamente, simplificando o processo de gestão e correção.

Com a edição em massa, você pode selecionar várias vulnerabilidades e aplicar mudanças consistentes, como atribuir responsáveis pela correção, atualizar status, adicionar anotações de trabalho, solicitar exceções e solicitar falso positivo. Isso economiza tempo e esforço, eliminando a necessidade de editar itens vulneráveis individualmente, promovendo o gerenciamento eficiente e consistente de vulnerabilidades.

O recurso de edição em massa está disponível para:

- Itens vulneráveis do host (Vits) a partir de v21.0 de Resposta a vulnerabilidades.
- Itens vulneráveis à aplicação (AVITs) e Itens vulneráveis ao contêiner (CVITs) a partir da v22.0 de Resposta a vulnerabilidades.
- Resultados de testes (TRs) a partir da v23.0 de Resposta a vulnerabilidades.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Você pode executar as seguintes tarefas usando o recurso de edição em massa no Espaço do gerente de vulnerabilidade:

- Atribua registros a um grupo de atribuição em massa
- Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades
- Remova atribuições de itens vulneráveis do host em massa
- Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades
- Feche registros em massa no Espaço do gerente de vulnerabilidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre controles de compensação para redução de risco

Controles de compensação são as medidas tomadas para reduzir o risco representado por vulnerabilidades que não podem ser corrigidas imediatamente. Eles podem ser usados para mitigar a probabilidade ou o impacto de uma exploração bem-sucedida.

Nota: O recurso Controles de compensação está disponível somente para vulnerabilidades de host.

Aplicar controles de compensação pode ajudar a reduzir o risco de uma vulnerabilidade.

A tabela a seguir mostra os casos de uso para controles de compensação:

Casos de uso para controles de compensação

Caso de uso	Controle de compensação
Uma vulnerabilidade em um servidor web que permite que invasores executem código arbitrário.	Implemente um Web Application Firewall (WAF) para bloquear solicitações mal-intencionadas para o servidor web.
Uma vulnerabilidade em um sistema operacional que permite que os invasores escalem privilégios para raiz.	Implemente um controle de aplicações para restringir a execução de aplicações no sistema host.
Uma vulnerabilidade em um servidor de banco de dados que permite que invasores acessem dados confidenciais.	Implemente segmentação de rede para isolar o servidor de banco de dados de outros hosts e sistemas críticos.

Para obter mais informações sobre o impacto dos controles de compensação na pontuação de risco de um item vulnerável e na tarefa de correção, consulte Impacto dos controles de compensação na pontuação de risco e na data de vencimento.

Tópicos relacionados

- Adicione um controle de compensação à biblioteca
- Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco
- Desabilite ou habilite a redução de risco para um CVE ou TPE

Soluções de análise e emissão de relatórios para o Painel de resposta unificada a vulnerabilidades

O Painel unificado de resposta a vulnerabilidades é um painel agregado centralizado que fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma visão abrangente das vulnerabilidades e riscos de uma organização.

Funções necessárias

As funções e tarefas a seguir estão associadas a esta Solução. Eles são necessários para exibir e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Painel da Resposta a vulnerabilidades unificado

O painel de Resposta unificada a vulnerabilidades fornece uma exibição abrangente das vulnerabilidades e riscos de uma organização. As vulnerabilidades relacionadas à infraestrutura, nuvem, aplicações e contêineres podem ser exibidas em um painel centralizado para melhor visibilidade e correção.

Assista a este vídeo de quatro minutos para saber mais sobre o Painel de resposta unificada a vulnerabilidades.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

Funções necessárias de ServiceNow AI Platform

As funções a seguir estão associadas a esta solução. Eles são necessários para exibir, editar e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

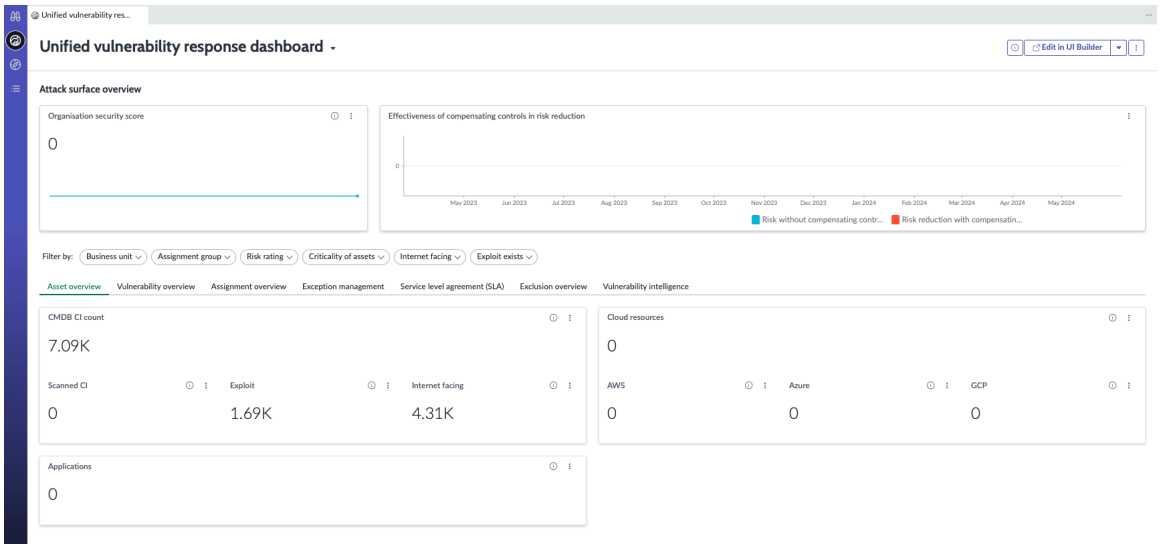
Acesse Painel unificado de resposta a vulnerabilidades

Para abrir o painel, navegue até:

- **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades** e selecione **Painéis** ícone. Dependendo da sua função, o painel padrão será exibido. Para exibir o Painel de resposta unificada a vulnerabilidades, selecione o menu suspenso ao lado do nome do painel.
- **Espaços** > **Espaço de análise da plataforma** > **Painéis** > **Painel da Resposta a vulnerabilidades unificado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuários	Uso do painel
• Vulnerability Managers • Analistas de vulnerabilidades	• Fornece visibilidade em tempo real dos riscos presentes na infraestrutura, aplicações, configurações e contêineres. Permite que os gerentes de vulnerabilidades e os analistas de vulnerabilidades priorizem e corrijam as vulnerabilidades em tempo hábil. • Fornece uma Visão geral da superfície de ataque de ativos críticos, que pode ser usada para rastrear o andamento e os esforços de correção. • Fornece uma visão geral dos riscos nas unidades de negócios (BUs). Você pode usar filtros para selecionar o barramento e comparar o andamento para realocar recursos, conforme necessário. O acesso no nível da função deve ser fornecido ao chefe da BU. • Fornece visibilidade do possível impacto por barramento. Você pode usar o filtro CVE (Common Vulnerability and Exposure, vulnerabilidade e exposição comum) para identificar exposições em toda a organização. • Fornece visibilidade das pontuações EPSS obtidas por entradas vulneráveis

Tradução automática

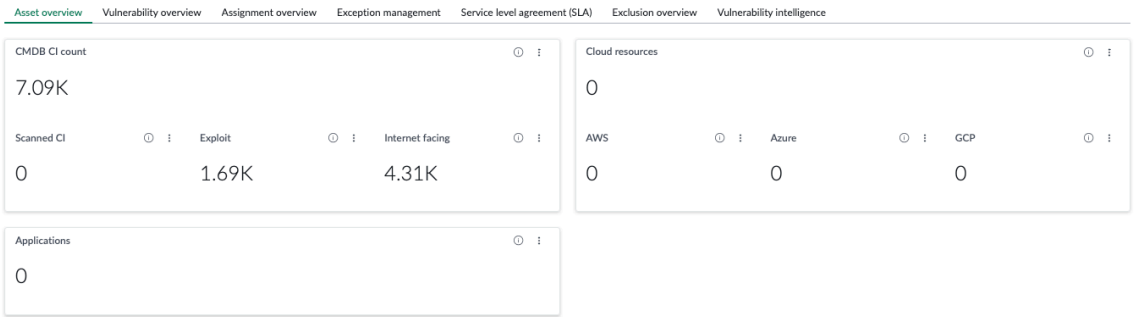
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuários	Uso do painel
	que existem no catálogo do CISA KEV para itens vulneráveis à aplicação, host e contêiner.

Guias do Painel de resposta unificada a vulnerabilidades

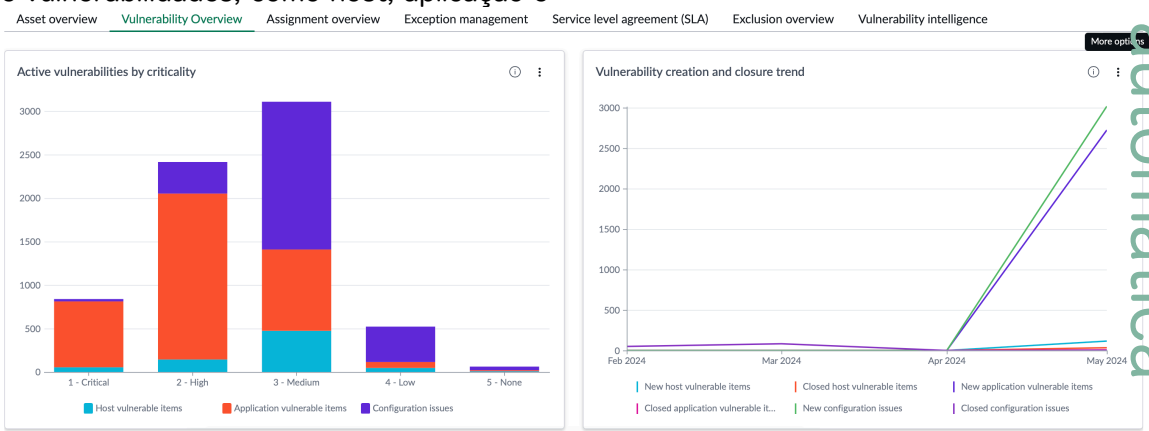
Este painel permite que você veja as vulnerabilidades ou problemas presentes em hosts, nuvem, configurações, aplicações e contêineres. Você pode exibir as vulnerabilidades com base na unidade de negócios, grupo de atribuição, classificação de risco, criticidade e se existe uma exploração para as vulnerabilidades.

. **Visão geral do ativo**Fornece o status geral dos itens de configuração (ICs) no



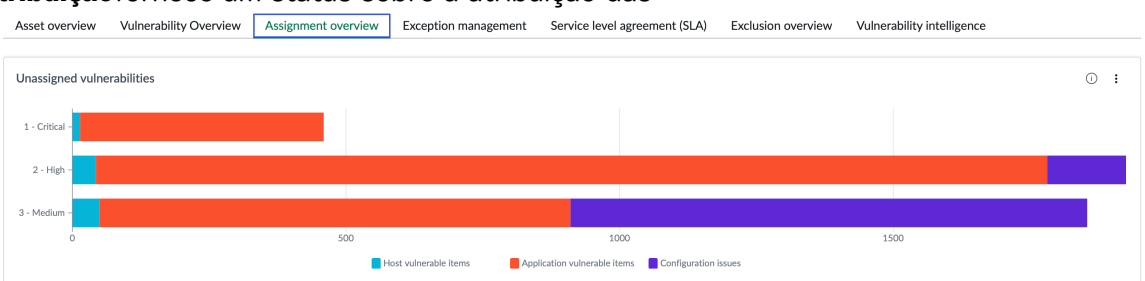
sistema.

. **Visão geral da vulnerabilidade**fornece um status sobre os tipos de vulnerabilidades, como host, aplicação e



contêiner.

. **Visão geral da atribuição**fornece um status sobre a atribuição das

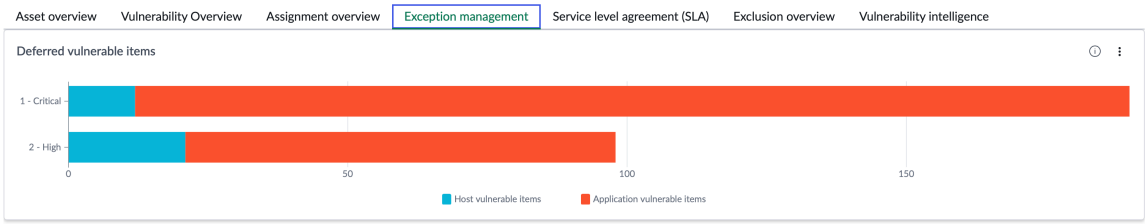


vulnerabilidades.

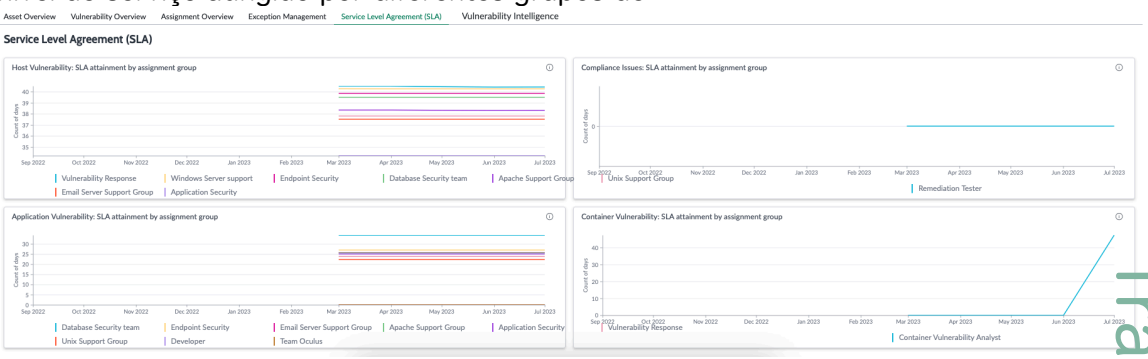
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

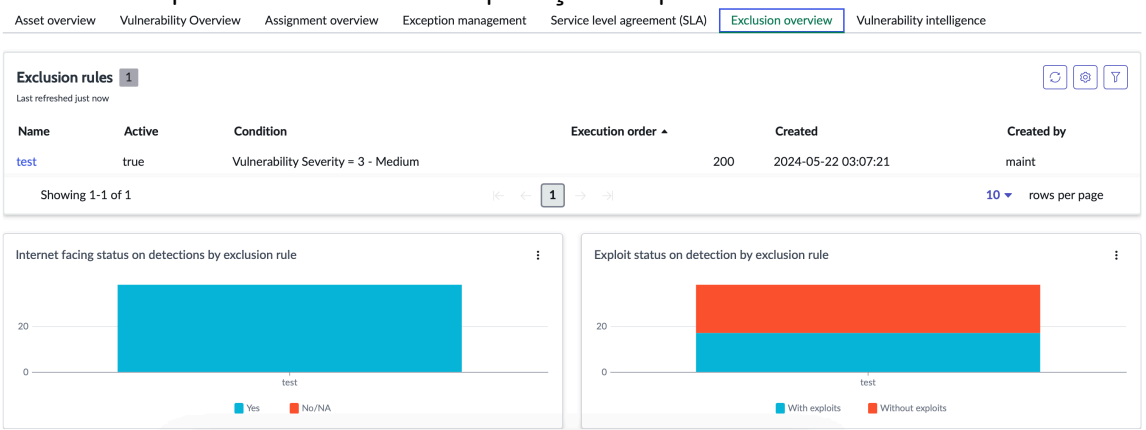
. **Gestão de exceções**fornece um status sobre as vulnerabilidades adiadas.



. **Acordo de nível de serviço (ANS)**fornece um status no acordo de nível de serviço atingido por diferentes grupos de atribuição.



. **Visão geral da exclusão**fornece um status das regras de exclusão que você criou, bem como as que afetam as detecções que são voltadas para a internet e têm explorações disponíveis.

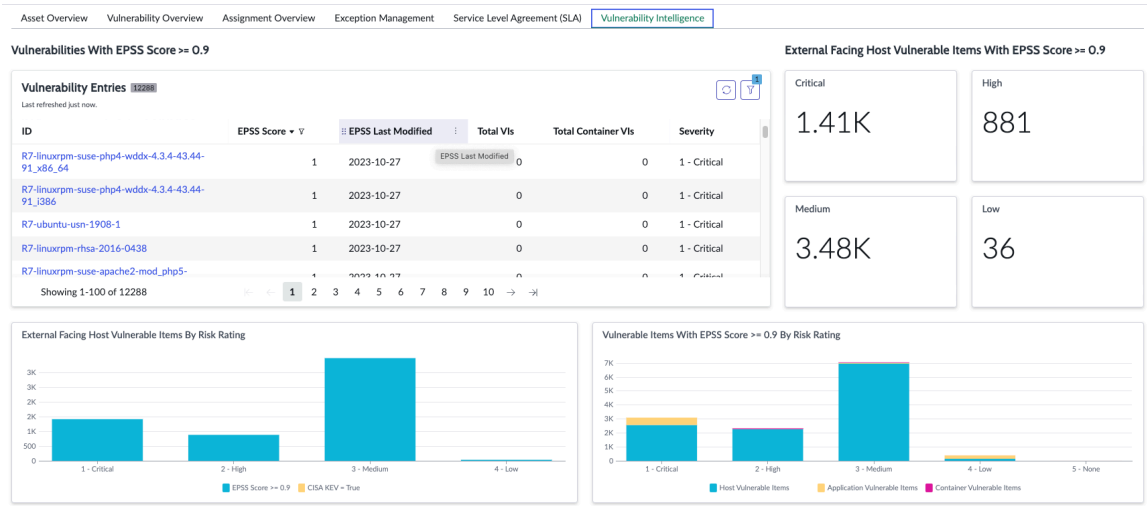


. **Inteligência de vulnerabilidades**Fornece um status nas pontuações de EPSS obtidas por vulnerabilidades com o sinalizador CISA KEV verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e pontuação de EPSS > 0,9 para itens vulneráveis de aplicação, host e contêiner.



Filtros

Você pode filtrar os widgets com base no seguinte:

- Unidade de negócios
- Grupo de atribuição
- Classificação de risco
- Criticidade de ativos
- Acessível pela internet
- Exploração presente

Quando um filtro é selecionado, os dados em todos os widgets são atualizados. No entanto, se um filtro não for aplicável a um widget, um símbolo de cruz será mostrado ao lado do nome do filtro.

Nota: Os filtros Unidade de negócios e Grupo de atribuição estão disponíveis em Tokyo. Todos os filtros estão disponíveis em Utah em diante.

Indicadores

Ativos verificados

Indicador de fórmula para ativos verificados nos últimos 60 dias. Contém ativos de item descoberto verificados, ativos de versão da aplicação verificados, ativos de imagem de contêiner descobertos verificados como indicadores contribuintes.

Ativos - Existe exploração

Indicador de fórmula para ativos em que existe exploração nas vulnerabilidades. Contém ativos de host - Existe exploração, Ativos de aplicação - Existe exploração, Ativos de contêiner - Existe exploração como indicadores contribuintes.

Ativo de infraestrutura – Voltado para a internet

Indicador para buscar a contagem de ativos, que estão voltados para a Internet.

Itens descobertos com base no tipo de recurso de nuvem

Indicador para buscar a contagem de ativos com uma categoria de ativo, como nuvem.

Imagens base

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador para buscar a contagem de imagens de base.

Tipo de ativo de KEVs de CISA

Indicador de fórmula, que fornece a contagem de itens vulneráveis do contêiner e do host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro. CISA Existe CVR e CISA Existe itens Vul como indicadores contribuintes.

CISA Existem itens vulneráveis - não atribuídos

Indicador de fórmula, que fornece a contagem de itens vulneráveis do contêiner e do host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não estão atribuídos. Contém itens de Vul de contêiner não atribuídos, item de Vul de host não atribuído como indicadores de contribuição.

Existem Itens Vulneráveis CISA – Meta não Atingida

Indicador de fórmula, que fornece a contagem de itens vulneráveis do contêiner e do host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não atingiram o destino. Contém itens de Vul existentes do CISA, CISA existe CVR como indicadores contribuintes.

VITs de host ativo

Contagem de itens vulneráveis do host (Vits) ativos.

VITs da aplicação ativos

Contagem de itens vulneráveis à aplicação (AVITs) ativos.

VITs de contêiner ativo

Contagem de itens vulneráveis ao contêiner (CVITs) ativos.

Novos VITs

Contagem de Vits que abriram em um dia.

Novos AVITs

Contagem de AVITs que foram abertos em um dia.

Novos CVITs

Contagem de CVITs que foram abertos em um dia.

Novos Resultados de testes

Contagem de resultados de testes (TRs) que foram criados em um dia.

AVITs encerrados

Contagem de Vits encerrados em um dia.

VITs encerrados

Contagem de AVITs encerrados em um dia.

CVITs encerrados

Contagem de CVITs encerrados em um dia.

Resultados de testes fechados

Contagem de TRs encerrados em um dia.

Problemas de configuração em aberto – Resultados de testes

Contagem de todos os resultados de testes em aberto, que estão no estado com falha.

Pontuação de risco da organização

Pontuação de risco de uma organização da tabela Pontuação de risco da aplicação de acúmulo.

Itens vulneráveis de aplicação não atribuídos

AVITs sem grupo de atribuição ou atribuídos a.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item Vulnerável de Host Não Atribuído

Vits sem grupo de atribuição ou atribuído a.

Itens vulneráveis de contêiner não atribuídos

CVITs sem grupo de atribuição ou atribuídos a.

Problemas de configuração não atribuídos

TRS sem grupo de atribuição ou atribuído a.

VITs adiados

Vits no estado Adiado.

AVITs adiados

AVITs no estado Adiado.

CVITs adiados

CVITs no estado Adiado.

ANS de host – Encerrado

Idade média de encerramento dos Vits encerrados.

ANS de aplicação – Encerrado

Idade média de encerramento de AVITs encerrados.

ANS de contêiner – Encerrado

Idade média de encerramento de CVITs encerrados.

ANS de Resultado de testes – Aprovado

Idade média de encerramento dos TRs aprovados.

ANS de host – Encerrado (crítico e alto)

Idade média de encerramento de Vits críticos encerrados e altos encerrados.

ANS de aplicação – Encerrado (crítico e alto)

Idade média de encerramento de AVITs críticos e altos.

ANS de contêiner – Encerrado (crítico e alto)

Idade média de encerramento de CVITs críticos e altos encerrados.

ANS do resultado de testes – Aprovado (crítico e alto)

Idade média de encerramento de TRs críticos e altos aprovados.

MTTR agregado

Idade média de encerramento de Vits, AVITs, CVITs e TRs encerrados.

ANS não Atingido

Idade média de encerramento de VITs, AVITs, CVITs e TRs encerrados e de destino perdidos.

Vulnerabilidades com pontuações EPSS > 0,9

Contagem de entradas de vulnerabilidade com pontuações EPSS maiores ou iguais a 0,9.

Detalhamentos

- Tipo de VIT (unificado)
- Voltado para a internet (unificado)
- Classificação de risco (unificada)
- Existe exploração (unificada)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tipo de recurso de nuvem do item descoberto (unificado)
- CISA existe (unificada)
- Classe do CMDB (unificada)
- Unidade de negócios (unificada)
- Essencial para os negócios (unificado)
- Motivo adiado (unificado)
- Grupo de atribuição (unificado)
- Status de correção (unificado)

Visualizações de dados

Guia Visão geral do ativo

Título	Tipo	Descrição
Visão geral da superfície de ataque	Pontuação  única	Número que representa a pontuação agregada da segurança de uma organização.
Contagem de IC do CMDB	Pontuação  única	Número de ICs na organização registrados e rastreados no Configuration Management Database (CMDB). Fornece um detalhamento dos seguintes ICs: • ICs verificados: Número de ICs verificados • Exploração: Número de explorações disponíveis • Voltado para a Internet: Número de ICs voltados para a Internet
Recurso de nuvem	Pontuação  única	Número de ICs com categoria de ativo, como nuvem. Fornece um detalhamento dos seguintes ativos de nuvem: • AWS • Azure • GCP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral do ativo

Título	Tipo	Descrição
Imagem do Docker	Pontuação  única	Número de imagens do docker, incluindo o número de imagens de base.
Aplicações	Pontuação  única	Número de aplicações na organização.

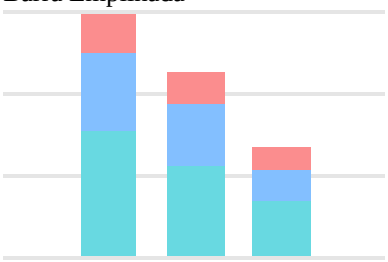
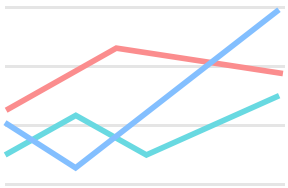
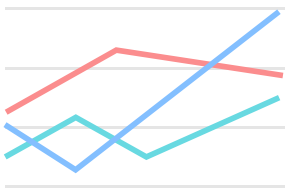
Guia Visão geral da vulnerabilidade

Título	Tipo	Descrição
KEVs de CISA	Gráfico de pizza	Número de vulnerabilidades associadas ao CISA Sinalizador de catálogo e CISA como verdadeiro. Fornece um detalhamento com base no seguinte: • Vulnerabilidade da CISA: Tipos de vulnerabilidades com sinalizador CISA como verdadeiro • ICs do host - voltados para a Internet: ICs voltados para a Internet • Vits não atribuídos: Vits não atribuídos com sinalizador CISA como verdadeiro • Vits meta perdida: Vits que não atingiu o destino com sinalizador CISA como verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da vulnerabilidade

Título	Tipo	Descrição
Vulnerabilidades ativas por criticidade	Barra Empilhada 	Número de Vits, AVITs e CVITs ativos com base na criticidade.
Tendência de criação e fechamento de vulnerabilidade	Linha múltipla 	Número de vulnerabilidades novas e encerradas para todas as aplicações. Fornece uma tendência para os últimos três meses.
Configuração incorreta por plataforma de nuvem	Linha múltipla 	Número de problemas de configuração com base na classificação de risco para cada ativo de nuvem.
Conformidade de nuvem	Tabela	Lista de recursos com a categoria de ativo como nuvem junto com os seguintes detalhes: • Nome do recurso • Classe • Problemas de vulnerabilidade: Número de problemas presentes no recurso que são agregados com base na classificação de risco. • Problemas de configuração: Número de recursos com problemas de configuração junto com a classificação de risco. • Conta de nuvem: ID da conta de nuvem.

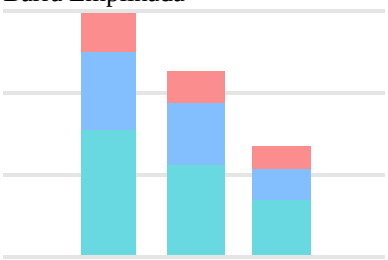
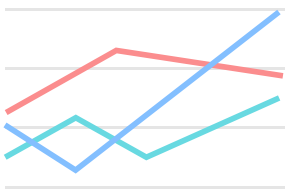
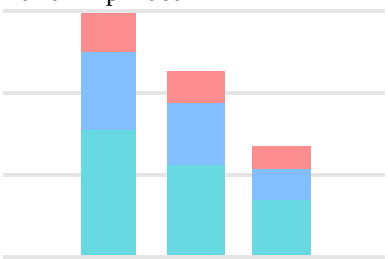
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da vulnerabilidade

Título	Tipo	Descrição
		• Região da nuvem: Localização dos recursos de nuvem. • Provedor de nuvem: Nome do provedor de nuvem.

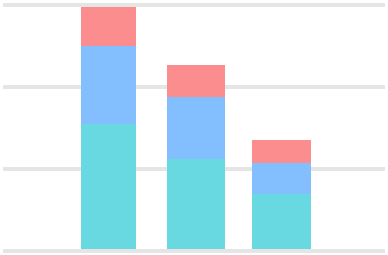
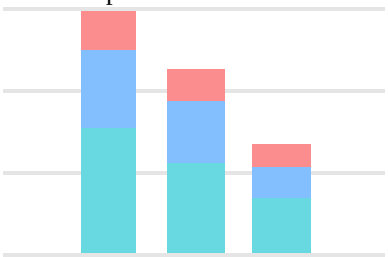
Guia Visão geral da atribuição

Título	Tipo	Descrição
VITs não atribuídos	Barra Empilhada 	Número de vulnerabilidades que não são atribuídas a nenhum grupo ou indivíduo junto com a classificação de risco.
MTTR por grupo de atribuição – 10 principais	Linha múltipla 	Tempo médio gasto por um grupo de atribuição para identificar e corrigir as vulnerabilidades ou problemas de segurança. São exibidos os 10 principais grupos de atribuição que têm o maior tempo médio de correção.
10 principais grupos de atribuição sem ANS (vulnerabilidade crítica e alta)	Barra Empilhada 	10 principais grupos de atribuição que perderam a data de destino de correção de vulnerabilidades críticas e altas.

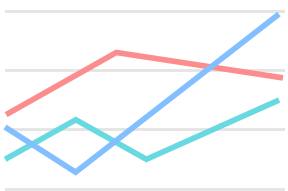
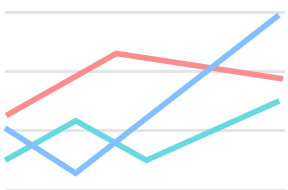
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Gestão de exceções

Título	Tipo	Descrição
VITs adiados	Barra Empilhada 	Número de vulnerabilidades no estado adiado com base na classificação de risco.
VITs críticos e altos adiados por grupo de atribuição	Barra Empilhada 	Número de vulnerabilidades com classificações críticas e de alto risco no estado Adiado categorizado com base nos grupos de atribuição.

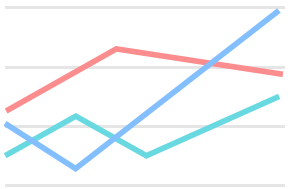
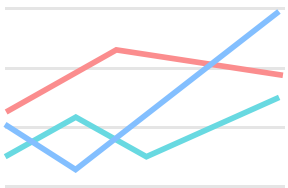
Guia Acordo de nível de serviço (ANS)

Título	Tipo	Descrição
Vulnerabilidade do host: obtenção de ANS por grupo de atribuição	Linha múltipla 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades de host. Fornece uma tendência para os últimos 10 meses.
Problemas de conformidade: obtenção de ANS por grupo de atribuição	Linha múltipla 	Tempo gasto por um grupo de atribuição para corrigir problemas de conformidade. Fornece uma tendência para os últimos 10 meses.

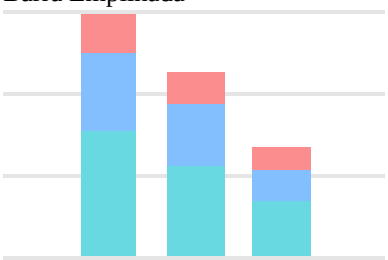
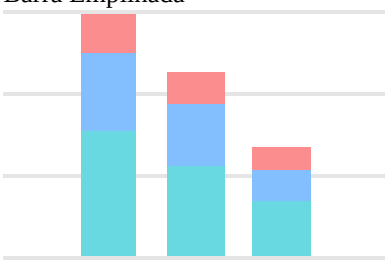
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Acordo de nível de serviço (ANS)

Título	Tipo	Descrição
Vulnerabilidade da aplicação: obtenção de ANS por grupo de atribuição	Linha múltipla 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades da aplicação. Fornece uma tendência para os últimos 10 meses.
Vulnerabilidade da contêiner: obtenção de ANS por grupo de atribuição	Linha múltipla 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades de contêiner. Fornece uma tendência para os últimos 10 meses.

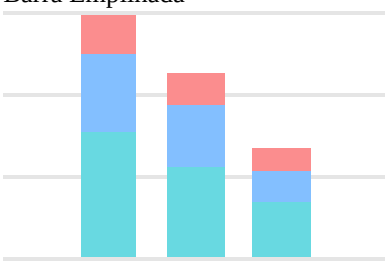
Guia Visão geral da exclusão

Título	Tipo	Descrição
Regras de exclusão	Tabela	Lista de todas as regras de exclusão que você criou.
Regras de exclusão v/s Internet Facing	Barra Empilhada 	Regras de exclusão que afetam detecções que pertencem a ativos voltados para a Internet.
Existem regras de exclusão v/s de exploração	Barra Empilhada 	Regras de exclusão que afetam detecções vulneráveis a explorações existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

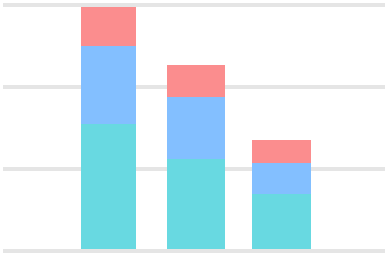
Guia Inteligência de vulnerabilidades

Título	Tipo	Descrição
Vulnerabilidades com pontuação EPSS> 0,9	Tabela	Exibição de lista completa de todas as entradas vulneráveis (CVEs ou TPEs) que têm uma pontuação EPSS maior ou igual a 0,9, junto com os detalhes a seguir. • ID: ID CVE da vulnerabilidade • Pontuação de EPSS • Última modificação de EPSS • CISA KEV BOD 22-01: Indica se a entrada existe no CISA KEV BOD (diretiva operacional vinculativa 22-01) • Total de VIS: Contagem total de VIS existentes para esta entrada de vulnerabilidade. • Total de VIS do contêiner: Contagem total de VIS do contêiner que existem para esta entrada de vulnerabilidade. • Gravidade
Itens vulneráveis do host externo com pontuação EPSS >= 0,9	Pontuação  única	Número que indica a contagem agregada de itens vulneráveis ao host externos com uma pontuação EPSS maior ou igual a 0,9. Fornece pontuações únicas classificadas por gravidade da classificação de risco.
Itens vulneráveis de host voltados externamente por avaliação de risco	Barra Empilhada 	Número de itens vulneráveis ao host externos por classificação de risco. As barras de pilha são categorizadas por Pontuação EPSS > 0,9 e CISA KEV verdadeiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Inteligência de vulnerabilidades

Título	Tipo	Descrição
Itens vulneráveis com pontuação de EPSS >= 0,9 por avaliação de risco	Barra Empilhada 	Número de vulnerabilidades com pontuação EPSS maior ou igual a 0,9 classificadas por classificação de risco. Fornece um detalhamento por itens vulneráveis do host, itens vulneráveis à aplicação e itens vulneráveis ao contêiner.

Trabalhos agendados para coleta de dados

Os trabalhos de coleta de dados coletam pontuações automaticamente para detalhamentos e indicadores automatizados. Os trabalhos agendados a seguir são executados para coletar pontuações em novos dados automaticamente.

Aviso: Por padrão, os seguintes trabalhos de coleta de dados são desativados no sistema de base:

- Coleta diária de dados do painel unificado
- Coleta de dados semanais do painel unificado
- Coleta de dados históricos do painel unificado

Antes de habilitar os trabalhos, consulte BASE DE CONHECIMENTO .

Trabalho programado	Frequência	Descrição
Coleta de dados históricos do painel unificado	Uma vez	Coleta pontuações e snapshots para registros existentes.
Coleta de dados semanais do painel unificado	Semanalmente	Coleta dados semanalmente.
Coleta diária de dados do painel unificado	Diariamente	Coleta dados todos os dias.
Acúmulo de pontuações de risco para a organização	Diariamente	Coleta a pontuação de risco agregada de uma organização.
Preencha as contagens diárias de conformidade na nuvem	Diariamente	Coleta dados para conformidade na nuvem.
Trabalho diário do EPSS	Diariamente	Coleta dados EPSS de First.org.

Uma nova tabela Pontuação de risco da aplicação de acúmulo [sn_vul_cmn_rollup_app_risk_score] é criada no Escopo Comum de Vulnerabilidade. Esta tabela é preenchida usando as seguintes calculadoras de acúmulo por meio dos trabalhos agendados todos os dias.

Nome da calculadora de acúmulo	Descrição
Acúmulo de pontuação de risco da organização	Acumula as pontuações de risco para todos os itens vulneráveis e problemas de configuração em uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da calculadora de acúmulo	Descrição
	organização. Ele fornece uma pontuação de risco geral para uma organização.
Acúmulo do item vulnerável	Acumula as pontuações de risco de todos os itens vulneráveis em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo de item vulnerável da aplicação	Acumula as pontuações de risco de todos os itens vulneráveis à aplicação em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do item vulnerável de contêiner	Acumula as pontuações de risco de todos os itens vulneráveis ao contêiner em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do resultado de testes	Acumula as pontuações de risco de todos os resultados de testes em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acumular pontuações de EPSS de NVDs para TPEs	Acumula pontuações de EPSS de NVDs para TPEs para contribuir com a pontuação de risco geral de uma organização.

Monitoramento e gerenciamento de itens vulneráveis e resultados de testes no Espaço do gerente de vulnerabilidade

. Espaço do gerente de vulnerabilidade O permite monitorar itens vulneráveis (Vits, AVITs e CVITs) e Resultados de teste (TRs) usando tópicos de observação e rastrear e gerenciar o andamento da correção criando esforços de correção.

Abrir resultados da pesquisa em Espaço do gerente de vulnerabilidade

Abrir resultados da pesquisa em Espaço do gerente de vulnerabilidade Em vez da IU clássica, alterando o escopo da aplicação.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.read_all para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager ou sn_vul.app_read_all para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin ou sn_vul_container.read_all para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin ou sn_vulc.read para resultados de teste de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Exemplo: Se você pesquisar um item vulnerável do host com seu número no **Pesquisa** definindo o escopo da aplicação como Espaço do gerente de vulnerabilidade, O VIT é aberto em sua exibição de registro no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na barra de navegação unificada, selecione o ícone Globo .
2. Selecione **Escopo da aplicação** .
3. Defina o escopo como **Vulnerability Manager Workspace** .

O que Fazer Depois

Quando você pesquisa registros como Vits, tarefas de correção, aprovações de mudança de estado e assim por diante, no **Pesquisa** na barra de navegação unificada, os registros são abertos no Espaço do gerente de vulnerabilidade.

Quando o escopo não é Global, o ícone de globo é exibido com um anel vermelho . Selecione-o novamente para mudar o escopo.

Criar e aplicar filtros O resumo de registros ativos (Vits, AVITs, CVITs e CTR)

Como gerente e analista de vulnerabilidades, você pode filtrar os registros desejados para visualizar seu resumo na página inicial do Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Página inicial**.
2. Selecione o ícone de engrenagem e selecione **Criar filtro** Nas guias Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação ou Resultados do teste de configuração.
3. Na janela pop-up Criar filtro, preencha os campos.

Criar Janela pop-up Filtros

Campo	Descrição
Nome do Filtro	Nome do filtro.
Condições	Condição para mostrar somente os registros cujos visualizações você deseja ver.
Atualizar diariamente	Atualize as informações de visualização todos os dias.

4. Selecione **Save** (Salvar).
5. Exiba as visualizações dos registros filtrados selecionando o novo filtro em **Exibir por** campo. Para obter mais informações sobre os widgets, consulte Página inicial do Espaço do gerente de vulnerabilidade.
6. Para atualizar ou excluir um filtro:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione o ícone de engrenagem e selecione **Editar filtro** .

b. Na janela pop-up Filtros salvos, selecione o filtro que você deseja atualizar ou excluir.

c. Atualize ou exclua o filtro.

Ação	Etapas
Exclua o filtro.	Selecione **Excluir**.
Modifique o nome do filtro	Edite o nome do filtro e selecione **Atualização** .
Mude as condições do filtro	Edite a condição para exibir informações somente para determinados registros e selecione **Atualização** .
Atualizar diariamente	Determine se as informações de visualização devem ser atualizadas todos os dias e selecione **Atualização** .

Tópicos relacionados

Página inicial do Espaço do gerente de vulnerabilidade

Usar tópicos de observação no Espaço do gerente de vulnerabilidade

Use tópicos de observação no Espaço do gerente de vulnerabilidade para exibir vulnerabilidades e configurações incorretas que são filtradas de seus dados importados a partir dos critérios definidos. Use essas informações para determinar como as vulnerabilidades e as configurações incorretas em cada tópico de observação podem afetar seu ambiente.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Na página Tópicos de observação, você pode executar as seguintes tarefas:

- Monitore o número de esforços de correção e registros (Vits, AVITs, CVITs e TRs) para ver o andamento da correção de vulnerabilidade.
- Edite ou exclua os tópicos de observação existentes e crie tópicos de observação.
- Crie os esforços de correção e entregue automaticamente as tarefas de correção para suas equipes DE TI somente para as vulnerabilidades que você deseja corrigir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

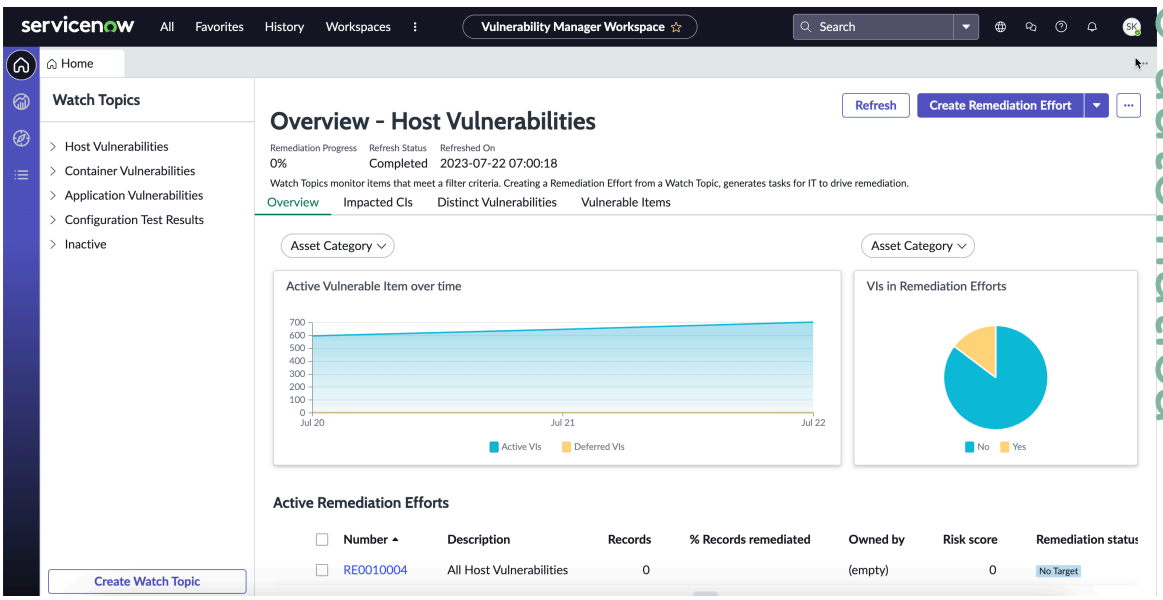
Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Ícone Tópicos de observação.
3. Selecione um tópico de observação nas guias Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação ou Resultados do teste de configuração na página Tópicos de observação.

   Ao selecionar um tópico de observação, o **Visão geral** a guia é exibida por padrão.

   Para obter mais informações sobre os tópicos de observação, consulte Página Tópicos de observação no Espaço do gerente de vulnerabilidade.

   Guia Visão geral da versão 19,0 no Página inicial do Espaço do gerenciador de vulnerabilidades



   Os painéis são dinâmicos e novas atualizações de dados de vulnerabilidade na importação.

4. Selecione um **Guia Itens relacionados** para exibir mais dados.

   Para obter mais informações sobre a lista de itens relacionados e as visualizações em um tópico de observação, consulte Lista de itens relacionados e visualizações em um tópico de observação.

5. Execute as ações de IU na página Tópicos de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
Crie um tópico de observação	Crie seu próprio tópico de observação usando seu próprio conjunto de condições para as vulnerabilidades e configurações incorretas que você considera importantes. Para obter mais informações sobre como criar um tópico de observação, consulte Crie um tópico de observação no Espaço do gerente de vulnerabilidade.
Edite ou exclua um Tópico de Observação existente	Para obter mais informações sobre como editar ou excluir um tópico de observação, consulte Edite ou exclua um tópico de observação no Espaço do gerente de vulnerabilidade.
Desative ou ative um tópico de observação	Você pode desativar ou ativar um tópico de observação. Para obter mais informações sobre como desativar ou ativar um tópico de observação, consulte Desative ou ative um tópico de observação.
Atualizar um tópico de observação	Você pode adquirir os detalhes mais recentes de um tópico de observação selecionando **Atualizar** botão. O status de atualização e o carimbo de data/hora mais recentes são exibidos sob o nome do tópico de observação. ◦ Um tópico de observação é atualizado automaticamente quando é criado ou atualizado. ◦ Quando você atualiza um tópico de observação, todos os detalhes do tópico de observação, incluindo os gráficos e os esforços de correção, são atualizados. **Nota:** Como você não pode atualizar um tópico de observação inativo, o. **Atualizar** o botão está inativo para um tópico de observação inativo.
Crie um esforço de correção	◦ Crie um esforço de correção. Um esforço de correção contém as tarefas de correção atribuídas às suas equipes DE TI. Você pode usar esta ferramenta para orientar e rastrear o andamento da correção da atribuição até a resolução. ◦ Quando você cria um esforço de correção, todos os itens vulneráveis ativos são extraídos automaticamente se ainda não fizerem parte de um esforço de correção existente para esse tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	◦ As tarefas de correção são atribuídas às equipes DE TI automaticamente com base no grupo de atribuição de VI. ◦ Um exemplo de um esforço de correção do *Vulnerabilidades em servidores Windows* o tópico de observação pode ser, *Vulnerabilidades nos servidores Windows no segundo trimestre de 2021* . As tarefas de correção nesse esforço são atribuídas aos grupos de atribuição listados nos registros associados.
Crie um esforço recorrente	Crie esforços de correção recorrentes em uma programação que ajude você a rastrear as vulnerabilidades que podem exigir sua atenção imediata e contínua. Para obter mais informações sobre a criação de esforço recorrente, consulte Crie um esforço de correção recorrente no Espaço do gerente de vulnerabilidade. **Nota:** Você não pode criar um esforço recorrente para um tópico de exibição inativo.
Refinar filtros para uma coluna em uma lista	Passe o mouse sobre o título de uma coluna e clique no menu de três pontos verticais para definir os filtros para essa coluna. Por exemplo, digamos que você queira fazer mais filtragem nos itens de configuração associados aos registros. Você pode selecionar a coluna Item de configuração para exibir as condições de filtro disponíveis. Você pode definir condições para filtrar seus ativos para que você veja somente os ativos que contêm os dados PCI.
Filtre itens ou corresponda itens de uma linha em uma coluna	Filtre itens ou corresponda itens de uma linha em uma coluna. Por exemplo, digamos que você queira exibir somente os registros que têm uma vulnerabilidade específica. Com a guia Lista de itens relacionados a Itens vulneráveis selecionada, na lista de registros, selecione a linha de um registro na coluna Resumo. Selecione o menu de três pontos verticais exibido e selecione uma das seguintes opções: ◦ **Mostrar correspondência** : Mostra todos os outros registros que têm esta vulnerabilidade. ◦ **Descartar** : Mostra todos os registros que não têm esta vulnerabilidade.

6. Opcional: Selecione um registro para exibir mais detalhes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um tópico de observação no Espaço do gerente de vulnerabilidade

Gerentes e analistas de vulnerabilidades podem criar tópicos de observação usando um conjunto de condições para filtrar subconjuntos de registros (Vits, AVITs, CVITs ou CTRs) que desejam monitorar.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Na guia Visão geral dos tópicos de observação, um relatório de tendências atualizado todas as noites, junto com outros relatórios, mostra o status atual dos registros desse tópico de observação.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades** > **Tópicos de observação**.
2. **Opcional:** Como alternativa, à direita do botão Criar esforço de correção, clique nos três pontos ..., seguido por editar para modificar um tópico de observação existente.

   Nota: Você pode notar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

3. No canto inferior esquerdo da página, selecione **Criar Tópico de Observação** .
4. No modal exibido, preencha os campos.
   Para obter mais informações sobre os campos do modal Criar tópico de observação, consulte Campos de formulário Criar tópico de observação.
5. Defina condições para a categoria de registro selecionada.

Opção no menu suspenso Categoria	Etapas
Vulnerabilidades dos servidores (host)	Em **Condição de item vulnerável** defina condições para identificar as vulnerabilida–des do host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção no menu suspenso Categoria	Etapas
	As vulnerabilidades do host são detectadas com base nas condições definidas.
Vulnerabilidades de aplicações	Em **Condição de item vulnerável da aplicação** defina condições para identificar as vulnerabilidades do host. As vulnerabilidades da aplicação (ou AVITs) são detectadas com base nas condições definidas.
Vulnerabilidades do contêiner	Em **Condição de item vulnerável do contêiner** defina condições para identificar as vulnerabilidades do host. As vulnerabilidades de contêiner (CVITs) são detectadas com base nas condições definidas.
Resultados de testes de configuração	Em **Condição de resultados do teste de configuração** defina condições para identificar os problemas de configuração. Os resultados do teste de configuração são detectados com base nas condições definidas.

Nota: Se você não definir nenhuma condição no tópico de exibição, nenhum dado será extraído para o painel.

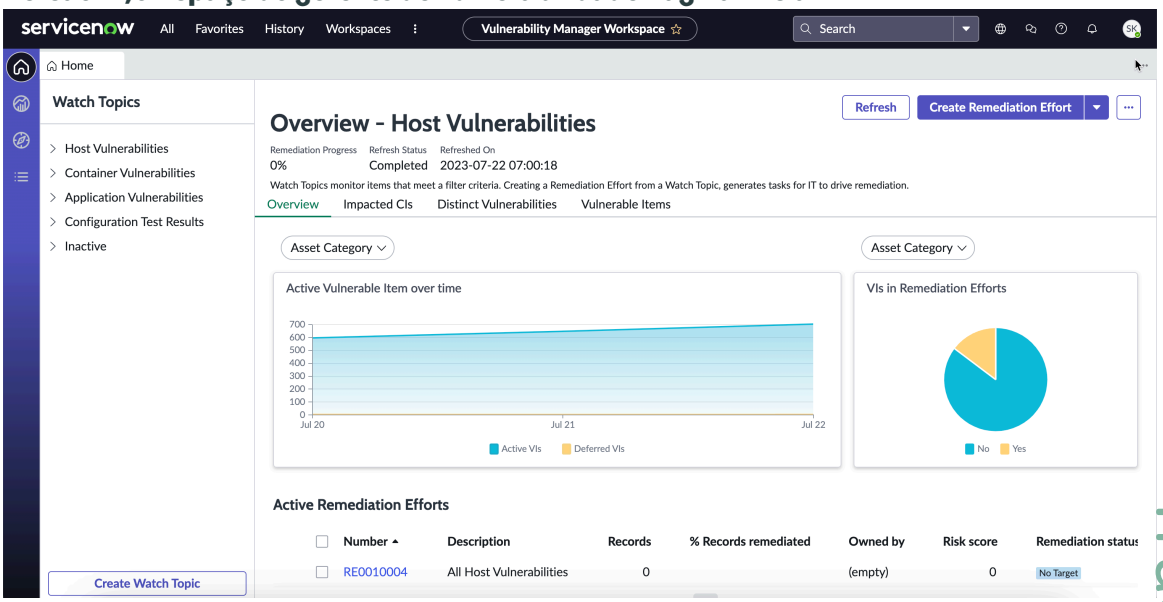
6. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seu novo tópico de exibição é exibido na página principal da Página inicial. T os tópicos de observação são categorizados por tipo de registro no painel de navegação.

Versão 19,0 Espaço do gerente de vulnerabilidade Página inicial



O que Fazer Depois

Crie um esforço de correção.

Edite ou exclua um tópico de observação no Espaço do gerente de vulnerabilidade

Você pode editar ou excluir um tópico de observação existente no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Se você editar um tópico de observação existente:

- Os dados no painel são atualizados para refletir suas mudanças.
- Os registros que estão atualmente nos esforços de correção existentes permanecem inalterados.
- Os registros que não estão em esforços de correção no momento são exibidos com base nos critérios inseridos no construtor de condições.

Se você excluir um tópico de observação antes que todos os registros associados sejam corrigidos, os registros exibidos com esse tópico de observação não serão afetados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Tópicos de observação**.
2. Abra o tópico de observação que você deseja editar.
3. Clique nos três pontos e clique em **Editar** .

   Nota: Você não pode editar um tópico de observação inativo.

4. No modal Editar tópico de observação, modifique os campos.
5. Clique em **Enviar**.

   Nota: Você pode notar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

   Você também pode editar os esforços de correção recorrentes existentes. Se houver um esforço de correção recorrente existente para um tópico de observação, **Editar esforço recorrente** está disponível no menu. Selecione esta opção para editar o esforço recorrente.

   As mudanças feitas e salvas no registro de esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

6. **Opcional:** Para excluir um tópico de observação, selecione o menu de três pontos no tópico de exibição e selecione **Excluir** .

Desative ou ative um tópico de observação

Você pode desativar ou ativar um tópico de observação no Espaço do Gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

- Todos os tópicos de observação inativos são exibidos no **Inativo** no painel de navegação.
- Você não pode criar um esforço de correção ou um esforço de correção recorrente para um tópico de observação inativo.
- Você não pode atualizar um tópico de observação inativo.
- Os detalhes de um tópico de observação inativo e seus esforços de correção associados não são atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Tópicos de observação**.
2. Abra o tópico de observação que você deseja desativar.
3. Clique nos três pontos e clique em **Desativar** .
   O tópico de observação aparece no módulo inativo.
4. Para ativar um tópico de observação, selecione um tópico de observação no módulo inativo, selecione o menu de três pontos e selecione **Ativar** .
   O tópico de observação ativado é movido para o módulo apropriado no painel de navegação.

Usar registros de esforço de correção

Quando gerentes e analistas de vulnerabilidades criam esforços de correção (RES), as tarefas de correção (VUL, avul, CVUL e CRG) são atribuídas automaticamente às equipes DE TI para correção.

Antes de Iniciar

Você precisa criar um esforço de correção antes de usá-lo para monitorar o andamento da correção nas tarefas de correção.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Se não estiver selecionado, no canto superior esquerdo, clique no ícone Lista.

   A exibição de lista com registros de esforço de correção ativos é exibida.
2. Na coluna Tipo de registro, selecione o menu de três pontos e selecione **Agrupar por tipo de registro** .
   Os esforços de correção categorizam em itens vulneráveis ao host, itens vulneráveis à aplicação, itens vulneráveis ao contêiner e resultados de teste de configuração.
3. Na página principal Exibição de lista, com os esforços de correção ativos selecionados nas listas filtradas, clique em um registro para abri-lo.
   O registro é exibido. Você pode exibir as tarefas de correção e. registros associados ao esforço de correção selecionado.
4. Consulte a tabela a seguir para obter as ações que você pode executar no registro de esforço de correção.

   Depois de criar um registro, pode levar alguns minutos para que as tarefas de correção e um grande número de registros sejam exibidos.

Ação de IU	Descrição
Adicione um marcador	À direita do cabeçalho, clique no ícone de marcador pequeno. Você pode querer adicionar texto que ajude a identificar ainda mais este registro. Por exemplo, você pode adicionar um marcador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	informando que este registro tem PCI ou outros dados críticos.
Adicione uma anotação de trabalho ao registro	Na extrema direita da tela, clique em **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel.
Atualizar o registro	Em **Detalhes** para todos os campos editáveis, clique em um campo para selecioná-lo, fazer suas mudanças e clique em **Salvar** para atualizar o registro.
Quando exibido, clique no ícone de filtro para refinar os dados na página exibida	Com qualquer uma das tarefas de correção, itens vulneráveis, o r Resultados do teste de configuração guias selecionadas, na extrema direita, clique no ícone de filtro para mostrar os filtros que se aplicam à guia. No painel exibido, clique em **Exibição avançada** para adicionar ou mudar condições de filtro para os itens na página. Clique em **Atualizar** para salvar suas mudanças. Por exemplo, em **Itens vulneráveis** , você pode preferir adicionar o campo Idade e inserir um intervalo para exibir somente registros de um período de tempo específico. Registros que correspondem às condições definidas são exibidos na lista.
Refinar filtros para itens em uma coluna	Selecione uma coluna e clique no menu de três pontos verticais Expanda-a e insira condições para refinar e agrupar os dados na coluna.
Filtre itens ou corresponda itens de uma linha em uma coluna	Digamos, por exemplo, que você deseja exibir somente registros que têm uma vulnerabilidade específica. Na lista de registros, selecione a linha do registro em **Resumo** coluna. Clique no menu de ponto vertical exibido e escolha um: ○ **Mostrar correspondência** - mostrar todos os outros registros que têm esta vulnerabilidade. ○ **Descartar** - mostrar todos os registros que não têm esta vulnerabilidade.

5. Nas guias Tarefas de correção, Itens vulneráveis e Resultados de teste de configuração, você pode detalhar uma Tarefa de correção individual (VUL, avul, CVUL ou CRG), um item vulnerável (VIT, AVIT, ou CVIT) E Resultado do teste (CTR) respectivamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Se você quiser criar uma tarefa de correção sob demanda a partir de um esforço de correção, consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade. Você também pode Crie uma lista personalizada de registros para ajudar você a monitorar o andamento da correção.

Crie um esforço de correção no Espaço do gerente de vulnerabilidade

Um registro de esforço de correção é uma lista estática de registros que você cria a partir de um tópico de observação no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Você usa esforços de correção para entregar as tarefas que as equipes DE TI usam para corrigir vulnerabilidades e configurações incorretas.

- Você pode editar os esforços de correção existentes.
- Crie esforços de correção criados automaticamente nas datas e horas definidas.
- Transfira registros de esforços de correção existentes para um novo esforço de correção.

A partir da versão 18,0, porque você não pode criar um esforço de correção para um tópico de observação inativo, o. **Criar esforço de correção** o botão está inativo.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades** > **Tópicos de observação**.
2. Na página Tópicos de observação, selecione um tópico de observação para o qual você deseja criar um esforço de correção.
3. Para exibir os registros associados ao tópico de observação selecionado, no cabeçalho do registro, clique em **Itens vulneráveis** , **Itens vulneráveis à aplicação** , **Itens vulneráveis do contêiner** ou **Resultados do teste de configuração** em seus respectivos tópicos de observação.

   Os registros são exibidos.

   Por exemplo, no cabeçalho na guia Itens vulneráveis, você pode exibir o número total de registros que este tópico de observação tem.

   As seguintes colunas e dados são exibidos:

Colunas na guia Itens vulneráveis

Coluna	Descrição
Número	O número do registro.
Resumo	Descrição da vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Item de configuração	O ativo associado à vulnerabilidade.
Classificação de risco	Pontuação de risco quantificada que separa registros em Crítico, Alto, Médio, Baixo e Nenhum.
Estado	Status do registro.
Status da correção	Status da correção de um registro.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.
Esforço de correção	Se for atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois que ele for adicionado a um esforço de correção, um registro não será adicionado a nenhum outro esforço de correção que você criar.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.
Esforço de correção	Se for atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois que ele for adicionado a um esforço de correção, um registro não será adicionado a nenhum outro esforço de correção que você criar.
Em tarefa de correção	Se verdadeiro este valor indica que um registro já está em uma tarefa de correção. Os registros podem estar em várias tarefas de correção, mas um registro pode ser adicionado apenas a um esforço de correção.
Exploração presente	Indica se existe uma exploração conhecida para um registro.
Aberto pela última vez	Data em que o registro foi aberto pela última vez em seu ServiceNow AI Platform. Se o registro foi fechado e reaberto, esta será a última vez que o registro foi reaberto.

4. Para criar um esforço de correção, clique em **Criar esforço de correção** .

   Quando você cria um esforço de correção, os registros que já estão em esforços de correção existentes não são adicionados a nenhum novo esforço de correção criado a partir deste tópico de observação.

   Conforme os registros são atualizados ou novos registros são criados nos tópicos de observação, você pode criar esforços de correção.

5. Como alternativa, você pode Crie um esforço de correção recorrente no Espaço do gerente de vulnerabilidade.

   . **Editar** o botão está disponível no menu para esforços de correção existentes. Você tem a opção de modificar os campos e condições de um modal exibido. As mudanças feitas e salvas no registro de esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Na etapa 1 do modal Criar esforço de correção, preencha os campos.

   No campo Descrição resumida, insira um texto que descreva o esforço de correção recorrente e ajude a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção.

7. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os registros nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.

Opção	Descrição
Por grupo de atribuição	Registros com o mesmo grupo de atribuição são agrupados em uma tarefa de correção.
Por grupo de atribuição e item de configuração	Registros com o mesmo grupo de atribuição e Item de configuração são agrupados em uma Tarefa de correção.
Por grupo de atribuição e (vulnerabilidade ou teste de configuração)	Registros com o mesmo grupo de atribuição e Item de configuração são agrupados em uma Tarefa de correção.
Nenhuma (nenhuma tarefa de correção foi criada).	Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade.

8. Para atualizar automaticamente os itens vulneráveis do host duplicados, você deve selecionar **Atualizar automaticamente itens vulneráveis duplicados para as tarefas de correção criadas** caixa de seleção.

   Nota: Esta caixa de seleção está disponível somente para vulnerabilidades de host.

9. Na etapa 3, Transferir, verifique quantos registros você deseja adicionar ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.

   Se não houver registros novos e ativos para adicionar, o seguinte texto será exibido:

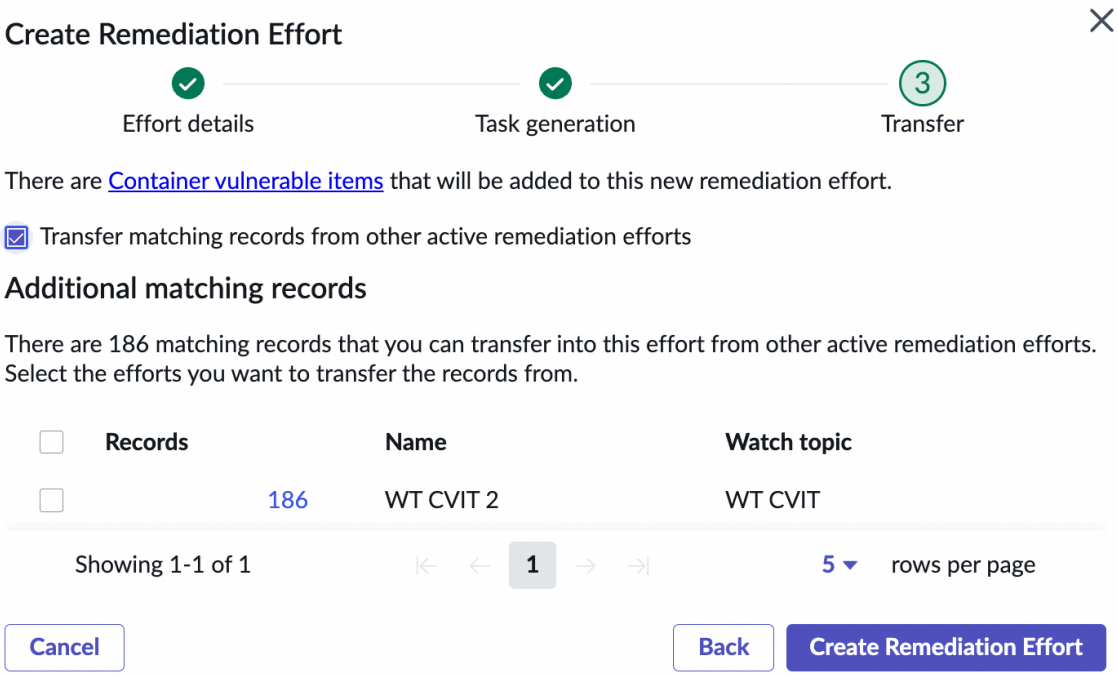
   Não há registros ativos disponíveis que você possa adicionar a este novo esforço de correção.

   Todos os registros adicionais que estão disponíveis para transferência para este esforço estão listados em Registros correspondentes adicionais .

   Selecione **Transfira registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esforço de correção de criação da versão 18,0



Depois de clicar em **Criar esforço de correção** em alguns momentos, o novo esforço de correção é exibido. Dependendo do número de registros, pode levar algum tempo para preencher o novo registro. Uma mensagem indica se o registro ainda está sendo preenchido.

O novo esforço de correção é criado com todos os registros disponíveis no tópico de observação usado para criá-lo, além de todos os registros selecionados para transferência de esforços existentes.

Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado. Para obter mais informações sobre como as tarefas de correção associadas aos esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Nota: Se não houver registros disponíveis no tópico de observação ou registros selecionados para transferência, o. **Criar esforço de correção** o botão está desativado.

. *Populate Efforts*o trabalho agendado é executado a cada 10 minutos para preencher os dados nos widgets com base na condição selecionada.

Clique na guia Andamento da correção para exibir o andamento da correção. Clique em qualquer item para exibir detalhes, incluindo tipo de registro, pontuação de risco, classificação de risco, percentual de registros corrigidos, registros em estado adiado e não adiado e número total de registros, condições usadas no tópico de exibição e status de correção. As informações de Status de correção, como destino de correção e status de correção, são acumuladas da tabela Itens vulneráveis. A pontuação de risco de registro mais alta é acumulada na tabela Calculadoras de vulnerabilidades, enquanto a pontuação de risco é acumulada na **Calculadoras de acúmulo de vulnerabilidades** > **Agregar esforço de correção**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia Tarefas de correção exibe as tarefas para todos os tipos de problemas. Os campos são preenchidos quando os seguintes trabalhos agendados são executados. Eles são executados automaticamente a cada 15 minutos:

- Acumule valores de item vulnerável da aplicação para vulnerabilidade e grupo.
- Acumular valores de item vulnerável do contêiner para vulnerabilidade e grupo.
- Valores de resultado de teste de acúmulo para grupo de resultados de teste e teste de configuração.
- Acumule valores de item vulnerável para vulnerabilidade e grupo.

Na exibição de listas, você pode exibir os esforços de correção, tarefas de correção, itens vulneráveis, resultados de teste de configurações e assim por diante. Você pode abrir uma tarefa de correção ou um item vulnerável e exibir a página Detalhes. Clique nas reticências Mais ações e clique em **Iniciar investigação** para resolver uma tarefa de correção.

10. **Opcional:** Você também pode editar os esforços de correção recorrentes existentes.

(Optional) Se houver um esforço de correção recorrente existente para um tópico de observação, **Editar esforço recorrente** está disponível no menu no canto superior direito de um tópico de observação. Escolha esta opção para editar o esforço recorrente.

As mudanças feitas e salvas no registro de esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade

Crie uma tarefa de correção sob demanda a partir de um esforço de correção. Se você criar uma tarefa de correção sob demanda, escolherá os registros que deseja adicionar manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Para a versão 18,0 de Resposta a vulnerabilidades, Você não pode criar uma Tarefa de Correção a partir da exibição de registro de um esforço de correção.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na parte superior esquerda do espaço com a página inicial exibida, clique em **Lista** Ícone Exibir, para exibir a página principal da Lista.
3. Em Esforços de correção, clique em qualquer um **Ativo** ou **Todos** .
4. Na lista exibida, clique em um registro para abri-lo.
   A guia Visão geral do registro é exibida.
5. Clique em **Itens vulneráveis** guia.
   A lista de registros é exibida.
6. Para criar uma nova tarefa de correção, na coluna Número, selecione os registros que você deseja adicionar.
7. Clique em **Criar tarefa de correção** .
8. No modal exibido, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Insira um texto que possa ajudar você a identificar essas tarefas de correção facilmente a partir de suas tarefas de correção existentes.
Grupo de atribuição	Escolha um grupo de atribuição para as tarefas. Use o filtro para ajudá-lo a localizar o grupo desejado.

9. Clique em **Criar**.
10. A nova tarefa de correção é exibida com os registros ativos selecionados.

Crie um esforço de correção recorrente no Espaço do gerente de vulnerabilidade

Você pode criar e programar esforços de correção recorrentes que são gerados automaticamente nas datas e horas definidas.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar automaticamente esforços de correção recorrentes em uma programação que ajuda a rastrear vulnerabilidades que podem surgir e exigir atenção imediata e contínua.

A partir da versão 18,0, porque você não pode criar um esforço de correção recorrente para um tópico de exibição inativo, o. **Criar esforço recorrente** a opção está inativa. Se você desativar um tópico de observação que tenha um esforço recorrente já programado, um novo esforço de correção não será criado até que o tópico de observação seja ativado. . **Recorrência de esforço** e. **Próxima data de recorrência** os detalhes desaparecem no canto superior direito. Depois que você ativa o tópico de observação, um esforço de correção é criado na próxima programação.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades** > **Tópicos de observação**.
2. Na página Tópicos de observação, selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.

   Você pode criar um esforço de correção recorrente por tópico de exibição.

   Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção existentes e não recorrentes para novos esforços de correção. Consulte Transfira registros para esforços de correção no Espaço do gerente de vulnerabilidade para obter mais informações sobre como transferir registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em um tópico de observação, no canto superior direito da lista Criar esforço de correção, selecione **Criar esforço recorrente** .

   O modal Criar esforço recorrente é exibido.

4. Na etapa 1, Detalhes do esforço, preencha os campos obrigatórios.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, `Vulnerabilidades em ativos externos` .

5. Clique em **Avançar**.
   Os detalhes da geração da tarefa são exibidos.

6. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os itens vulneráveis nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhuma (nenhuma tarefa de correção foi criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade.

7. Para atualizar automaticamente os itens vulneráveis do host duplicados, você deve selecionar **Atualizar automaticamente itens vulneráveis duplicados para as tarefas de correção criadas** opção.

   Nota: Esta caixa de seleção está disponível somente para vulnerabilidades de host.

8. Clique em **Próximo** para continuar.

9. Na etapa 3, Recorrência, selecione a frequência.

Opção	Descrição
Trimestralmente (a cada 3 meses)	Programa o esforço de correção uma vez a cada três meses. **Nota:** Se o mês selecionado tiver apenas 30 dias, o esforço de correção será cria–do na última data do mês.
Mensalmente	Programa o esforço de correção uma vez por mês.
Semanalmente	Programa o esforço de correção uma vez por semana. **Nota:** Esta opção está disponível a partir da versão 19,0 de Resposta a vulnerabilidades.
Diariamente	Programa esforços de correção todos os dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Esta opção está disponível a partir da versão 19,0 de Resposta a vulnerabilidades.

a. Defina a programação de recorrência.

Use as listas para selecionar o mês/dia/hora/minuto em que você deseja que o esforço de correção seja criado. Por padrão, o fuso horário para programação é o seu fuso horário.

Nota: Se você tiver muitas vulnerabilidades, talvez prefira definir a criação como fora do horário comercial.

Se você quiser que o trabalho seja criado no último dia do mês, o trabalho agendado criará o esforço de correção recorrente no último dia do mês. Uma mensagem será exibida se o mês não tiver 31 dias.

b. Opcional: Selecione **Transferir vulnerabilidades** para vulnerabilidades ativas neste esforço de correção para prosseguir para cada esforço de correção subsequente criado.

10. Clique em **Recorrência de programação** .
É exibida uma mensagem informando que o registro de correção recorrente foi criado. O novo esforço de correção não é exibido imediatamente, ele é criado quando você o programou. Ele é exibido em suas listas depois que é criado pelo trabalho agendado.

A data em que o esforço de correção será criado é mostrada no tópico de observação correspondente. Para obter mais informações sobre como as tarefas de correção associadas aos esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Transfira registros para esforços de correção no Espaço do gerente de vulnerabilidade

Você pode transferir registros de esforços de correção existentes para novos esforços de correção no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Se for confrontado por uma ameaça de dia zero ou uma vulnerabilidade muito crítica que você deseja resolver rapidamente, convém consolidar todos os registros ativos que você já tem para esta vulnerabilidade em um esforço de correção. No entanto, cada registro só pode estar em um esforço, e os registros podem se sobrepor entre os tópicos de observação. Portanto, para reunir todos eles, você precisa transferir esses registros de vários esforços existentes para um único esforço de correção.

Digamos, por exemplo, que você criou um esforço de correção que tem uma vulnerabilidade de alta prioridade. Como essa vulnerabilidade é generalizada e potencialmente afeta outras áreas do seu ambiente, você pode ter registros associados a essa vulnerabilidade já em esforços de correção existentes. Para combinar esses registros para que eles estejam todos em um esforço de correção, você pode transferir todos os registros dos esforços de correção existentes para um novo esforço de correção.

Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. Para obter mais informações, consulte Crie um esforço de correção recorrente no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Ícone Tópicos de observação.
3. Na página Tópicos de observação, selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.
4. Clique em **Criar esforço de correção** .
   O modal Criar esforço de correção é exibido.
5. Na etapa um, Detalhes do esforço, preencha os campos obrigatórios.

   No campo Descrição resumida, insira o texto que descreva o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, `Vulnerabilidades ativas do Log4J` .

   a. No campo Nome, insira um nome para o novo esforço de correção.
   Por padrão, o nome do tópico de observação é exibido.

   b. No campo Descrição, insira o texto que ajudará você a localizar esse esforço de correção facilmente na lista de esforços de correção.

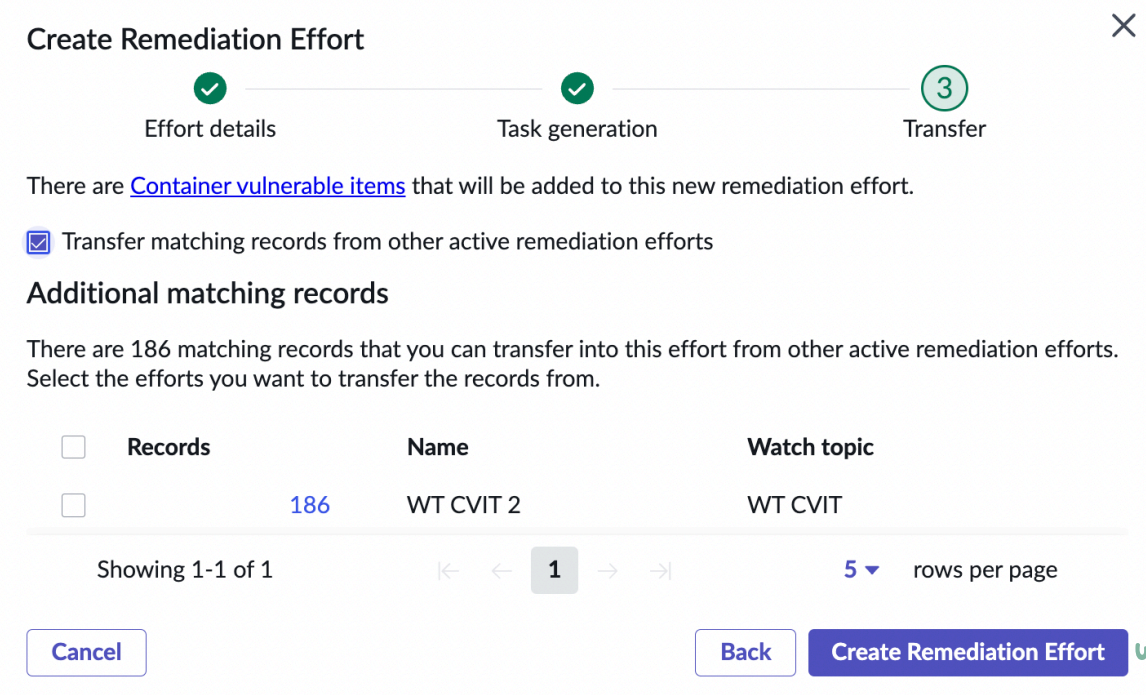
6. Clique em **Avançar**.
   Os detalhes da geração da tarefa são exibidos.
7. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os registros nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhuma (nenhuma tarefa de correção foi criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Crie uma tarefa de correção sob demanda a partir do esforço de correção no Espaço do gerente de vulnerabilidade.
8. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar **Atualizar automaticamente itens vulneráveis duplicados para as tarefas de correção criadas** opção.
9. Clique em **Avançar**.
10. Na etapa 3, Transferir, verifique quantos registros serão adicionados ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.
11. Para transferir registros de outros esforços, na lista, marque as caixas de seleção dos registros desejados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione **Transfira registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

Esforço de correção de criação da versão 18,0



12. Clique em **Criar esforço de correção** .

Após alguns momentos, o novo esforço de correção é exibido. Dependendo do número de registros, pode levar algum tempo. Uma mensagem indica que o registro está sendo preenchido.

O novo esforço de correção é criado com todos os registros disponíveis no tópico de observação usado para criá-lo, além de todos os registros selecionados para transferência de esforços existentes.

Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado.

Nota: Se não houver registros disponíveis no tópico de observação nem registros selecionados para transferência, o. **Criar esforço de correção** o botão está desativado.

Para obter mais informações sobre como as tarefas de correção associadas aos esforços de correção são afetadas pela transferência de registros, consulte Transferindo registros ou transferência de registro .

Adicione um controle de compensação à biblioteca

Como gerente ou analista de vulnerabilidades, adicione uma lista de controles compensatórios à biblioteca de controles de compensação no Espaço do gerente de vulnerabilidade, que pode ser aplicado para a redução de risco de itens vulneráveis do host e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Alguns controles de compensação comumente usados são enviados com o sistema de base. Você pode exibir esses controles de compensação navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas** > **Bibliotecas** > **Controles de remuneração**. Você pode ativar ou desativar esses controles de compensação de acordo com sua necessidade.

Nota: O recurso Controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento
1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista em Bibliotecas, selecione **Controles de compensação** .
3. Clique em **Nova**.
4. No formulário Criar controles de compensação, preencha os campos.

Campos de formulário Criar controles de compensação

Campo	Descrição
Nome	Nome do controle de compensação, que aparece como uma opção no **Controles de compensação** Menu suspenso do modal de exceção de solicitação.
Descrição	Breves informações que fornecem detalhes sobre o Controle de compensação.
Ativo	Status do controle de compensação. Somente controles ativos aparecem em **Controles de compensação** Menu suspenso do modal de exceção de solicitação.

5. Selecione **Save** (Salvar).
6. Na lista Controles de compensação em Bibliotecas, selecione o controle de compensação desejado e selecione **Editar** ative ou desative um controle de compensação e clique em **Salvar** para modificar os controles de compensação.
   Todos os controles de compensação ativos aparecem como uma opção no **Controles de compensação** Menu suspenso do modal de exceção de solicitação para solicitações de redução de risco.

O que Fazer Depois
A partir de v21.0 de Resposta a vulnerabilidades, Você pode associar controles de compensação a CVEs ou TPEs depois de adicionar controles de compensação à biblioteca. Para obter mais informações sobre como associar controles de compensação, consulte Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Desabilite ou habilite a redução de risco para um CVE ou TPE

Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco

Impacto dos controles de compensação na pontuação de risco e na data de vencimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco

Como gerente ou analista de vulnerabilidades, você pode associar controles de compensação relevantes a uma CVE (Common Vulnerability Entry, entrada de vulnerabilidade comum) ou entrada de terceiros (TPE) no Espaço do gerente de vulnerabilidade, que pode ser usado para reduzir o risco representado por uma vulnerabilidade.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

- Se você não associar controles de compensação a um CVE ou TPE, todos os controles ativos serão exibidos em Selecione Controles de compensação Campo do formulário Exceção de solicitação.
- Se você associar um controle de compensação a um CVE, esse controle de compensação será associado automaticamente ao TPE, que é mapeado para o CVE.

Nota: O recurso Controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Listas, em Bibliotecas, abra uma das seguintes opções para as quais você deseja associar os controles:
   - **CVE** Na lista CVEs.
   - **TPE** Da lista TPEs.
3. Selecione **Controles de associação** .

   Nota: . **Controles de associação** O botão aparece somente quando a redução de risco está habilitada para um CVE ou TPE. Em outras palavras, você pode associar controles de compensação somente quando a redução de risco está habilitada para um CVE ou TPE. . **Controles de associação** o botão não está visível, selecione **Habilitar redução de risco** .

4. No modal Associar controles, selecione os controles de compensação que podem ser aplicados a vulnerabilidades associadas ao CVE ou ao TPE para redução de risco.
5. Selecione **Enviar**.
   - Os controles de compensação associados aparecem na guia Controles de compensação aplicáveis na exibição de registro do CVE e do TPE.
   - Enquanto um responsável pela correção solicita redução de risco, esses controles de compensação associados aparecem no Selecione Controles de compensação Campo no modal de exceção de solicitação.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Desabilite ou habilite a redução de risco para um CVE ou TPE

Adicione um controle de compensação à biblioteca

Impacto dos controles de compensação na pontuação de risco e na data de vencimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desabilite ou habilite a redução de risco para um CVE ou TPE

Como gerente e analista de vulnerabilidades, você pode desabilitar ou habilitar as solicitações de redução de risco para as vulnerabilidades do host associadas a uma CVE (Common Vulnerability Entry, entrada de vulnerabilidade comum) ou Entrada de terceiros (TPE) no Espaço do gerente de vulnerabilidade.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A redução de risco para CVE e TPE é habilitada por padrão.

Nota: O recurso Controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   Na página Listas, em Bibliotecas, abra uma das seguintes opções para as quais você deseja desabilitar as solicitações de redução de risco:
   - **CVE** Na lista CVEs.
   - **TPEs** Da lista TPEs.
2. Selecione **Desabilitar redução de risco** .
   O responsável pela correção não pode solicitar redução de risco para os itens vulneráveis do host relacionados a este CVE ou TPE. Em outras palavras, o. Solicitação de redução de risco a caixa de seleção não aparece quando **Motivo** selecionado como Mitigação do controle em vigor No modal de exceção de solicitação.
3. Para habilitar as solicitações de redução de risco para itens vulneráveis do host, selecione **Habilitar redução de risco** .

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Adicione um controle de compensação à biblioteca

Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco

Impacto dos controles de compensação na pontuação de risco e na data de vencimento

Novos registros e tarefas de correção no Espaço do gerente de vulnerabilidade

Para verificar se suas tarefas de correção e registros foram resolvidos entre os ciclos de verificação programados, inicie novas varreduras do seu ServiceNow AI Platform sob demanda.

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.

Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

. Rapid7 e. Qualys os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto do scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem nos registros de item vulnerável e tarefa de correção após a próxima importação, e. **Nova verificação** Está disponível como uma ação de IU.

A nova verificação é compatível com registros e tarefas de correção com as seguintes integrações no Espaço do gerente de vulnerabilidade. Para obter mais informações, consulte os tópicos a seguir:

- Nova verificação Rapid7 itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho
- Nova verificação Qualys itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho
- Nova verificação Tenable.io e. Tenable.sc itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho

Para iniciar novas varreduras no Espaço do gerente de vulnerabilidade de itens vulneráveis e registros de tarefa de correção, os registros exigem um scanner compatível como origem.

Você pode preferir criar uma lista filtrada que exiba registros por origem. Consulte Crie uma lista personalizada de registros para obter um exemplo de como criar uma lista.

Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade

Avalie as atribuições, a data de destino de correção, as tarefas de correção, as exceções e a pontuação de risco de um conjunto de registros (Vits, AVITs, CVITs ou TRs) no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Antes da versão 23,0 do Vulnerability Response, era necessário aplicar as regras a todos os registros para obter as atribuições, datas de destino de correção, pontuações de risco e tarefas de correção mais recentes, o que era um processo demorado. A partir da versão 23,0, você pode avaliar e atualizar seletivamente essas propriedades para registros específicos, reduzindo assim o tempo de processamento. Além disso, você pode refinar o processo de correção com base nessas propriedades atualizadas. A partir da v24.0.6 do Vulnerability Response, você pode avaliar as regras de exceção para registros selecionados no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis da aplicação
   - Itens vulneráveis de contêiner
   - Resultados de testes de configuração
3. **Opcional:** Marque a caixa de seleção dos registros desejados para atualizar somente os registros selecionados selecionando a opção Itens selecionados no modal.
4. Selecione **Reavaliar** botão.
5. No modal Reavaliar e atualizar propriedades de correção, selecione as propriedades que você deseja atualizar para os registros selecionados.

Campo	Descrição
Seleção de registro	○ **Itens selecionados** Atualiza somente os registros selecionados. ○ **Todos os itens** Atualiza todos os registros na lista.
Atribuições	Atualiza as atribuições no **Grupo de atribuição** De acordo com as Regras de atribuição mais recentes.
Pontuação de risco	Atualiza a pontuação de risco no **Pontuação de risco** De acordo com as Regras de pontuação de risco mais recentes.
Tarefas de correção	Atualiza as tarefas de correção de acordo com as regras de tarefa de correção mais recentes.
Exceções	Atualiza o status de adiamento dos registros de acordo com as regras de exceção mais recentes. Para obter mais informações sobre como o status de adiamento dos registros é atualizado, consulte Reavaliar as exceções para registros selecionados no Espaço do gerente de vulnerabilidade.
Data de meta de correção	Atualiza a data de destino de correção de acordo com as regras de destino de correção mais recentes.

Nota: Quando você seleciona uma propriedade, suas propriedades dependentes são selecionadas automaticamente.

6. Selecione **Aplicar**.

Resultado

As propriedades são atualizadas para os registros selecionados. Você pode verificar **Anotações de trabalho** dos registros dos valores anterior e mais recente das propriedades de correção atualizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adiamento direto de itens vulneráveis (Vits) por regras de exceção sem criação de tarefa de correção

As regras de exceção são aplicadas diretamente aos itens vulneráveis (VIT), eliminando o processo de criação de uma tarefa de correção. A coluna Regra de exceção automática é adicionada à exibição do formulário, o que preenche a regra de exceção atual aplicada ao item vulnerável (VIT)

Aprovação da regra de exceção/reaplicar:

Uma regra de exceção é criada para um item vulnerável (VIT) específico, que está em um **em aberto, sob investigação, aguardando implementação** estado inicialmente. Depois que a regra é aprovada, ela é processada por um trabalho programado diariamente e noturno que reaplica a regra de exceção.

Quando o trabalho agendado é executado, caso o VIT seja adiado (adiado) devido ao mapeamento incorreto do VIT para a regra de exceção, o trabalho agendado reabre o VIT para reaplicar uma nova regra de exceção.

Uma nova regra com uma ordem de execução posterior também pode ser ativada para substituir a anterior.

Nota: A data Adiado até é definida como 12 meses por padrão e você pode editar conforme necessário na página de definições de configuração da Gestão de exceções. Se você tentar selecionar uma data adiada além da data padrão, o sistema gerará um erro.

Tratamento de regras de exceção canceladas ou excluídas:

Se a regra de exceção antiga for cancelada ou excluída, ela acionará um trabalho em segundo plano para:

- Abra todos os Vits associados.
- Mova a regra de exceção para o estado de rascunho quando a regra for cancelada.
- Aplique uma nova regra de exceção aos Vits. (Se houver uma regra de exceção aplicável, a VIT será associada a ela e o status da VIT será adiado).

Nova criação de VIT (inserção):

Quando uma nova VIT é criada (como uma ingestão), ela é atribuída automaticamente à regra de exceção. O novo VIT também será adiado com o mesmo raciocínio e até a data, seguindo o mesmo processo de quando uma regra de exceção é cancelada.

Um link clicável está disponível no VM Manager Workspace para acessar a regra de exceção diretamente, permitindo que o usuário veja qual regra de exceção está afetando um determinado VIT.

Use a Exibição de lista no Espaço do gerente de vulnerabilidade

A exibição de lista no Espaço do gerente de vulnerabilidade Permite que gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção em registros, detalhem os registros de Resposta a vulnerabilidades e exibam o status de suas solicitações de aprovação e exceções.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na parte superior esquerda do espaço com a página inicial exibida, clique em **Lista** ícone.
3. **Opcional:** Clique em **Minhas listas** para criar uma lista.
   Para obter mais informações sobre como criar uma lista, consulte Crie uma lista personalizada de registros.
4. Consulte a tabela a seguir para obter as ações que você pode executar na página Lista.

Ação de IU	Descrição
Abra um esforço de correção	Com **Ativo** selecionado em **Esforços de correção** clique em um link de esforço de correção para abri-lo. Um esforço de correção é um conjunto de registros associados a um tópico de observação. Os registros listados em um esforço de correção são estáticos. Eles não são atualizados por novos dados de importação ou mudanças que você faz nos tópicos de observação. Os itens da lista relacionada no registro de esforço de correção permitem exibir o andamento geral da correção e o status nos registros associados a ele. Para obter mais detalhes e ações de IU que você pode executar a partir de um esforço de correção, consulte Usar registros de esforço de correção.
À esquerda da coluna numérica com uma lista exibida, passe o mouse sobre uma linha e clique no ícone de informações pequeno **(i)** para um registro.	Os detalhes sobre os registros são exibidos no painel lateral direito da página. Os detalhes incluem: ○ Grupo de atribuição ○ Vulnerabilidade ○ Atribuição a ○ Descrição resumida ○ Descrição Você pode editar os campos. Se a caixa de seleção Ativo for exibida, você poderá

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	ativar ou desativar o registro. Clique em **Atualização** para salvar suas mudanças.
Atualizar lista	Com o ícone de atualização no canto superior direito da página, recarregue a página atual.
Redefinir larguras	Clique no ícone de engrenagem para ajustar as larguras das colunas em suas listas. Uma cópia da lista original é salva em **Suas listas** .
Copie o URL da página exibida	Copie o URL para uso em outro lugar.
Exporte a página	No modal, insira o arquivo e os tipos de entrega e clique em **Exportação** .
Refine os filtros para os dados na página.	Selecione uma coluna e expanda o menu de três pontos verticais para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, você pode preferir filtrar a coluna Grupo de atribuição da lista Tarefas de correção ativas por um grupo de atribuição específico.
Filtre itens ou corresponda itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ○ Mostrar correspondência - exibe somente itens que correspondem à célula selecionada na coluna. ○ Descartar - Filtre os itens da coluna que correspondem à célula selecionada na coluna.

5. Crie um item vulnerável à aplicação a partir do **Ativo** ou **Todos** lista em *`Application Vulnerable items`*clicando em **Novo** botão no canto superior direito.

Crie uma lista personalizada de registros

Você pode criar uma lista personalizada no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione **Lista** e clique **Minhas listas** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Nova lista** .
4. No modal Nova lista, clique em **Começar a partir de existente** E pesquise na lista de seleção de lista uma lista existente para usar como modelo.
5. Edite o Nome da lista.
6. Adicionar filtros.
   Por exemplo, você pode criar uma lista de registros ativos para um scanner específico que você deseja monitorar para novas varreduras. Você pode usar os filtros: `Ativo é verdadeiro` e `A origem contém (nome do scanner)` .
7. Edite as colunas que você deseja exibir em sua lista.
8. Clique em **Criar**.
   Sua nova lista será exibida.
9. Como alternativa, clique em **Crie o seu próprio** , insira um nome, seguido por **Selecione Origem** .
10. Comece a digitar no campo e selecione uma das origens exibidas para sua nova lista.
11. Clique em **Criar**.
    Sua nova lista será exibida.

    Nota: Se você sair do módulo de lista, a lista exibida ao sair será a lista exibida ao retornar.

12. Para excluir uma lista, com a lista exibida, clique no ícone de engrenagem no canto superior direito da página.

Crie uma tarefa de correção manualmente no Espaço do gerente de vulnerabilidade

A partir da v25.0.4 de Resposta a vulnerabilidades, Você pode criar tarefas de correção manualmente a partir das listas de itens vulneráveis do host, itens vulneráveis da aplicação, itens vulneráveis do contêiner e resultados de teste de configuração na página Lista de Espaço do gerente de vulnerabilidade. Você também pode criar tarefas de correção a partir das listas de detalhamento que aparecem quando você clica nas visualizações na página inicial.

Antes de Iniciar

Função necessária:

- sn_vul.write_all, sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_write_all ou sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.write_all, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.write ou sn_vulc.admin para resultados de teste de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Criação manual de tarefas de correção (RTS) em Espaço do gerente de vulnerabilidade Oferece controle granular sobre a gestão de tarefas de correção, permitindo que você agrupe registros (Vits, CVITs, AVITs ou TRs) em tarefas de correção dinamicamente em tempo real.

Você pode criar uma tarefa de correção manualmente, quando quiser:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Agrupe itens vulneráveis por algo diferente dos critérios de regras da tarefa de correção. Por exemplo, você pode criar tarefas de correção para um gerente específico ou para novas explorações ativas, como ransomware que inclui diferentes vulnerabilidades.
- agrupar registros não agrupados.
- as regras da tarefa de correção estão inativas.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.
2. Na página Lista, abra **Ativo** ou **Todos** lista em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis da aplicação
   - Itens vulneráveis de contêiner
   - Resultados de testes de configuração
3. **Opcional:** Marque a caixa de seleção dos registros que você deseja atualizar e selecione Itens selecionados Opção no campo Seleção de registro no modal Criar tarefa de correção.
4. Selecione **Criar tarefa de correção** .
5. No modal Criar tarefa de correção, preencha os detalhes a seguir.

Criar modal de tarefa de correção

Campo	Descrição
Seleção de registro	○ **Itens selecionados** Atualiza somente os registros selecionados. ○ **Todos os itens** Atualiza todos os registros na lista.
Descrição resumida	Breve anotação sobre as tarefas de correção.
Critérios de agrupamento	As opções são: ○ **Grupo de atribuição** : Registros com o mesmo grupo de atribuição são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e item de configuração** : Registros com o mesmo grupo de atribuição e item de configuração são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e vulnerabilidade** : Registros com o mesmo grupo de atribuição e vulnerabilidade são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e classificação de risco** : Registros com o mesmo grupo de atribuição e classificação de risco são agrupados em uma tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Gerenciamento de registros em outras tarefas de correção	As opções são: ○ **Ignorar registros para novas tarefas de correção** Nenhuma ação é realizada nos registros que fazem parte de outras tarefas de correção. ○ **Mover para novas tarefas de correção** : Os registros que fazem parte de outras tarefas de correção são transferidos para novas tarefas de correção. ○ **Mantenha as tarefas de correção atuais e novas** : Os registros que fazem parte de outras tarefas de correção são mantidos em tarefas de correção antigas e novas.

6. Selecione **Criar tarefa de correção** .

Resultado

As tarefas de correção são criadas com base nos critérios de agrupamento. Uma notificação por e-mail é enviada aos responsáveis pela correção no grupo de atribuição, informando-os que uma tarefa de correção foi criada e atribuída ao grupo. Para obter exemplos de como as tarefas de correção são criadas com base nos critérios de agrupamento, consulte Exemplos de criação de tarefa de correção no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI.

Habilitar ou desabilitar a importação de resultados de teste para um Qualys grupo de teste

A partir da v23.0 de Resposta a vulnerabilidades controla a importação dos resultados de testes para os testes em um Qualys grupo de teste usando **Habilitar/Desabilitar importação** botão, que está disponível na exibição de registro do grupo de teste.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas**.
2. Em Bibliotecas, na lista Grupos de teste, abra um Qualys grupo de teste na exibição de registro.
3. Desabilite a importação dos resultados de teste associados a um Qualys grupo de teste selecionando **Desabilitar importação** botão.
   Da próxima ingestão de dados, os resultados do teste não são importados para Qualys grupo de teste.
   O valor em **Importação desabilitada** o campo muda para *verdadeiro* .
4. **Opcional:** Habilite a importação dos resultados do teste selecionando **Habilitar importação** botão.

Modifique a gravidade de um CVE ou TPE

Como gerente ou analista de vulnerabilidades, você pode modificar o nível de gravidade da CVE (Common Vulnerability Entry, entrada comum de vulnerabilidade) ou TPE (entrada de terceiros) no Espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager, sn_vul.app_developer para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas** > **Bibliotecas**.
2. Abra a entrada apropriada:
   - **CVEs (NVD)** : Para modificar a gravidade de um CVE.
   - **TPEs** : Para modificar a severidade de um TPE.
3. Selecione **Modificar severidade** em **Mais ações**ícone 
4. Selecione o novo nível de gravidade no menu suspenso.
5. Forneça uma justificativa para sua atualização.
6. Selecione **Enviar**.

Nota:

- Você pode reverter para a gravidade da origem original usando **Redefinir severidade** . **Mais ações** menu. Esta opção aparece somente depois que você modifica a gravidade.
- . **Severidade modificada** o campo aparece somente quando você muda a gravidade da origem. Se você redefinir o valor original, o campo será removido.
- O sistema usará o. **Severidade modificada** para cálculos de risco a partir do próximo trabalho agendado em diante. Se a gravidade for redefinida, a gravidade da origem original será aplicada.

Aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade

Aprovar ou rejeitar solicitações enviadas pelos responsáveis pela correção.

Antes de Iniciar

Funções necessárias:

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Aprovações falso-positivo	Um	• Função granular sn_vul.false_positive_approver para Itens vulneráveis (Vits). • Função sn_vul.app_false_positive_approver para itens vulneráveis à aplicação (AVITs)	-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
		• Função sn_vul_container.false_positive_approver para itens vulneráveis do contêiner (CVITs) • sn_vulc.false_positive_approver para obter resultados de teste de configuração Ou Os aprovadores devem estar no grupo de usuários Aprovador de falso positivo.	
Aprovações de exceção (adiamentos)	Dois	• Um aprovador é necessário no grupo Aprovador - Nível 1 • Um aprovador é necessário no grupo Aprovador - Nível 2	Uma solicitação de exceção para um registro ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível e fica visível na fila do aprovador 2.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Cancelar atribuição de aprovações	Um aprovador é necessário no grupo Aprovador - Nível 1	• sn_vul.unassign_appr para AVITs e Vits • sn_vul_container.unas para CVITs • sn_vulc.unassign_app para problemas de configuração (ICs)	**Nota:** Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação de cancelamento de atribuição é criado. Os usuários (Não atribuir aprovador - Nível 1) deste grupo podem aprovar a solicitação. Por padrão, este grupo contém uma função de aprovador de cancelamento de atribuição, sn_vul.unassign_approver. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar regras de aprovação, navegue até o respectivo módulo Regras de aprovação, selecione qualquer uma das regras de aprovação a seguir e navegue até a configuração de aprovação no **Configurações de aprovação** guia: • *Vulnerable item field change request* para um item vulnerável. • *Vulnerability field change request* para uma tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Aprovações de redução de risco	Dois	• Um aprovador é necessário no grupo Aprovador - Nível 1 • Um aprovador é necessário no grupo Aprovador - Nível 2	O fluxo de aprovação para redução de risco é o mesmo que as aprovações de exceção (adiamentos).

Consulte Resposta a vulnerabilidades personas e funções granulares e. Atribua o. Resposta a vulnerabilidades Funções de persona usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

Nota: Adicione usuários aos grupos de aprovação antes de enviar solicitações de aprovação. Se você criar solicitações antes de adicionar usuários aos grupos de aprovação, as solicitações poderão não estar visíveis para os usuários que têm a permissão de aprovação.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   Se um aprovador não tiver acesso ao espaço, as aprovações poderão ser processadas em **Resposta a vulnerabilidades** > **Minhas aprovações** no ambiente clássico.
2. Selecione o ícone Exibição de lista ( ).
   A página Lista é exibida.
3. Na lista Aprovações filtradas, selecione **Atribuído a mim** .
4. Localize uma solicitação que você deseja processar e selecione o link na coluna Estado.
   O registro de aprovação de mudança de estado de vulnerabilidade (nº VCA) é exibido.
5. Escolha uma das seguintes opções para aprovar ou rejeitar a solicitação.

Opção	Descrição
Clique na guia Detalhes, insira o texto no campo Comentários e clique em Rejeitar	○ Uma mensagem é exibida indicando que há uma aprovação rejeitada para o registro de aprovação de mudança de estado de vulnerabilidade. ○ O estado no registro de Aprovação de mudança de estado de vulnerabilidade muda para Rejeitado. ○ O estado na tarefa de correção ou no registro permanece o mesmo. ○ O registro de aprovação de mudança de estado de vulnerabilidade não é mais exibido na exibição da lista de aprovações no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Em **Solicitação** ou **Detalhes** Clique em Aprovar	○ Uma mensagem é exibida indicando que o registro de aprovação de mudança de estado de vulnerabilidade foi aprovado. ○ O estado na tarefa de correção ou no registro muda para Adiado. ○ Os registros ativos nas tarefas de correção fazem a transição para Adiados. ○ O registro de aprovação de mudança de estado de vulnerabilidade não é mais exibido na exibição da lista de aprovações.

Configurar notificações por e-mail no Resposta a vulnerabilidades Espaços de trabalho

Identifique usuários para lembretes de e-mail automáticos enviados aos usuários no grupo de usuários Proprietário da correção.

Antes de Iniciar

Função necessária: administrador

Este recurso gera automaticamente um resumo de e-mail para usuários no grupo de usuários Proprietário da correção. Adicione os usuários que você deseja que recebam notificações por e-mail, conforme descrito em Use o resumo de e-mail nos Espaços de resposta a vulnerabilidades.

Verifique se os usuários têm um endereço de e-mail ativo inserido no registro de usuário e se você os adicionou ao grupo de usuários Proprietário da correção.

Se você quiser mudar a frequência de entrega, o dia ou a hora dos e-mails ou desativar o recurso, siga estas etapas.

Procedimento

1. Navegar até **Tudo** > **Trabalhos agendados**.
2. Localize **Gerar resumo de correção** e clique nele para abrir o registro.

   Você pode preferir deixar os campos em suas configurações padrão até verificar se as notificações estão sendo enviadas. Por padrão, os e-mails são enviados semanalmente nas manhãs de segunda-feira às 9:00 no fuso horário da instância que está executando o trabalho.
3. Modifique os campos no formulário.
   Para mais informações sobre campos de formulário, consulte Gerar campos de formulário de resumo de correção.
4. Clique em **Atualizar**.

O que Fazer Depois

Caso você tenha verificado que todas as informações listadas anteriormente estão corretas e tenha usuários no grupo de usuários Proprietário da correção, mas os e-mails não sejam enviados conforme o esperado, verifique se há canais ativados para receber notificações por e-mail. Consulte Criar canais de notificação .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Correção de itens vulneráveis e resultados de testes no Espaço da gestão de exposição de segurança

Em Espaço do gerente de vulnerabilidade, você pode corrigir itens vulneráveis e resultados de teste em um tópico de observação definindo uma condição e rastrear o andamento da correção criando esforços de correção.

Usando a edição em massa no Espaço do gerente de vulnerabilidade

Em Espaço do gerente de vulnerabilidade, Você pode atualizar o estado dos registros, solicitar exceções e falsos positivos e atribuir registros a um grupo de atribuição de vários itens vulneráveis (Vits, AVITs ou CVITs) simultaneamente usando o recurso de edição em massa.

O recurso de edição em massa está disponível para:

- Itens vulneráveis do host (Vits) a partir de v21.0 de Resposta a vulnerabilidades.
- Itens vulneráveis à aplicação (AVITs) e Itens vulneráveis ao contêiner (CVITs) a partir da v22.0 de Resposta a vulnerabilidades.
- resultados do teste a partir da v23.0 de Resposta a vulnerabilidades.

Atualize o estado dos registros em massa no Espaço do gerente de vulnerabilidade

Atualize o estado de vários registros (Vits, AVITs ou CVITs) simultaneamente de acordo com o andamento da correção usando o recurso de edição em massa no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis do host
- sn_vul.app_sec_manager para itens vulneráveis da aplicação
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis do contêiner

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
3. Execute um dos seguintes procedimentos:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . **Seleção de registro** campo.
   - Aplique filtros se quiser usar **Todos os itens vulneráveis que correspondem ao filtro** . **Seleção de registro** campo.
4. Selecione **Edição em massa** botão.
5. No modal Edição em massa, preencha os seguintes campos para atualizar o estado dos registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente itens selecionados: Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ Todos os itens vulneráveis que correspondem ao filtro: Selecione esta opção se quiser atualizar os registros filtrados. ○ Tarefa de correção: Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ Entrada de vulnerabilidade: Selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecione o CVE no **Entrada de vulnerabilidade** campo. **Nota:** Registros com IC inválido ou IC desativado não são atualizados.
Estado	Mudança para **Estado** no registro. As opções são: ○ Não atualizar ○ Aberto ○ Sob Investigação ○ Aguardando Implementação ○ Adiado Para obter mais informações, consulteSolicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades. ○ Encerrado Para obter mais informações, consulte Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades. ○ Resolvido **Nota:** Somente os registros para os quais a transição de estado é válida são atualizados.
Anotações de trabalho	Texto inserido para descrever as mudanças.

6. Selecione **Editar** .

Um trabalho assíncrono de edição em massa atualiza os registros selecionados.

Editar itens vulneráveis do host em massa com patches e soluções

Recomende um patch ou solução para vários itens vulneráveis ao host simultaneamente usando o recurso de edição em massa no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin e qualquer função com a função granular sn_vul.bulk_edit.

Por Que e Quando Desempenhar Esta Tarefa

No modal de edição em massa, ao adicionar uma solução preferencial e um patch, você também pode cancelar ou atribuir vários itens vulneráveis do host (Vits) a um grupo de atribuição simultaneamente.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.

   Nota: Os registros selecionados devem estar no estado Aberto, Em investigação ou Aguardando implementação.

2. Na página Lista, em Itens vulneráveis ao host, abra a lista Ativo ou Todos.
3. Execute um dos seguintes procedimentos:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . **Seleção de registro** campo.
   - Aplique filtros se quiser usar **Todos os itens vulneráveis que correspondem ao filtro** . **Seleção de registro** campo.
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . Campo Seleção de registro do modal de edição em massa.
   - Aplique filtros se quiser usar **Todos os itens vulneráveis que correspondem ao filtro** . Campo Seleção de registro do modal de edição em massa.
4. Selecione **Edição em massa** botão.
5. No modal Edição em massa, preencha os campos para recomendar um patch ou solução para vários itens vulneráveis do host.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente itens selecionados: Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ Todos os itens vulneráveis que correspondem ao filtro: Selecione esta opção se quiser atualizar os registros filtrados. ◦ Tarefa de correção: Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ◦ Entrada de vulnerabilidade: Selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecione o CVE no **Entrada de vulnerabilidade** campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros (Vits) em Aberto, Em investigação ou Aguardando implementação os estados são atualizados.
Estado	Mudança para **Estado** dos itens vulneráveis do host. Você pode adicionar solução preferencial e patch somente quando escolher os estados a seguir. ◦ Não atualizar ◦ Aberto ◦ Sob Investigação ◦ Aguardando Implementação
Solução preferencial	Solução destinada a corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para **Solução preferencial** campo no item vulnerável. As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os Vits selecionados. **Nota:** ◦ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os Vits selecionados. ◦ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** Para uma edição em massa, todos os Vits da vulnerabilidade serão definidos como a solução preferencial selecionada. **Nota:** Esta operação não define **Solução preferencial** no nível de entrada da vulnerabilidade. Definindo o. **Solução preferencial** no nível de entrada de vulnerabilidade, definiria o. **Solução preferencial** Para todos os novos Vits daqui para frente. A edição em massa modifica somente o conjunto atual de Vits. ◦ Vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione Vits com critérios diferentes para definir o. **Solução preferencial** . ◦ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição da lista de itens vulneráveis.
Patch preferencial	Patch destinado a corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar a Orquestração de patches para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os patches potenciais em todos os Vits selecionados. ◦ Vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione Vits com critérios diferentes para definir o. **Patch preferencial** . ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Cancelar atribuição	Todos os itens selecionados não têm atribuição atribuída ao grupo de atribuição e ao responsável pela correção. **Nota:** ◦ Este campo aparece quando você seleciona o Estado como Não atualizar. ◦ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e enviada para aprovação. Para obter mais informações, consulte Remova atribuições de itens vulneráveis do host em massa.
Grupo de atribuição	Grupo de atribuição para os registros. Todos os grupos de atribuição ativos aparecem neste campo. **Nota:** Este campo é desativado quando você marca a caixa de seleção Cancelar atribuição.
Anotações de trabalho	Texto inserido para descrever as mudanças.

6. Selecione **Editar**.

Resultado

Um trabalho assíncrono de edição em massa atualiza os itens vulneráveis do host (Vits) selecionados. A solução preferencial e o patch são adicionados aos itens vulneráveis do host (Vits) relevantes. Abra um item vulnerável do host e exiba a solução preferencial e o patch na seção Correção da guia Detalhes.

Atribua registros a um grupo de atribuição em massa

Atribua vários registros (Vits, AVITs, CVITs ou TRs) simultaneamente a um grupo de atribuição usando o recurso de edição em massa no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute um dos seguintes procedimentos:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . Seleção de registro campo.
   - Aplique filtros se quiser usar **Todos os registros que correspondem ao filtro** . Seleção de registro campo.
4. Selecione **Edição em massa** botão.
5. No formulário, preencha os campos para atribuir os registros a um grupo de atribuição.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ *Somente itens selecionados* : Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ *Todos registros que correspondem ao filtro* : Selecione esta opção se quiser atualizar os registros filtrados. ○ *Tarefa de correção* : Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ *Entrada de vulnerabilidade* : Selecione esta opção se quiser atualizar os registros específicos de um vulnerabilidade . E, em seguida, selecione um CVE ou TPE em **Entrada de vulnerabilidade** campo. **Nota:** Este campo aparece para itens vulneráveis ao host, itens vulneráveis à aplicação e itens vulneráveis ao contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ *Teste de configuração* : Selecione esta opção se quiser atualizar os resultados de teste específicos para um teste e selecione um teste no **Teste de configuração** campo. **Nota:** Esta opção aparece somente para resultados de teste de configuração. **Nota:** ○ Registros com IC inválido ou IC desativado não são atualizados. ○ Somente os registros no estado Aberto, Em investigação, Aguardando implementação ou Adiado são atualizados.
Grupo de atribuição	Grupo de atribuição para os registros. Todos os grupos de atribuição ativos aparecem neste campo. **Nota:** Este campo é desativado quando você marca a caixa de seleção Cancelar atribuição Para Vits .
Anotações de trabalho	Texto inserido para descrever as mudanças.

6. Clique em **Editar** .

Resultado
Abra um registro para o qual você atualizou o grupo de atribuição e navegue até a guia Visão geral, o grupo de usuários ao qual o registro está atribuído aparece em **Grupo de atribuição** campo.

Remova atribuições de itens vulneráveis do host em massa

Remova a si mesmo ou seus grupos do **Atribuído a.** e. **Grupo de atribuição** Hospedar Itens vulneráveis (Vits) ou Tarefas de correção (VUL) se você determinar que os registros não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst e sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
O##recurso Cancelar atribuição é aplicável a registros em qualquer estado diferente de Encerrado ou Resolvido. Quando você remove atribuições de itens vulneráveis do host usando o recurso de edição em massa, somente os registros relevantes são atualizados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, em Itens vulneráveis ao host, abra a lista Ativo ou Todos.
3. Execute um dos seguintes procedimentos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marque a caixa de seleção ao lado de cada item se quiser usar o. **Somente itens selecionados** . Seleção de registro campo.
- Aplique filtros se quiser usar **Todos os itens vulneráveis que correspondem ao filtro** . Seleção de registro campo.

4. Selecione **Edição em massa** botão.
5. No formulário, preencha os campos para remover atribuições em massa.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente itens selecionados: Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ Todos os itens vulneráveis que correspondem ao filtro: Selecione esta opção se quiser atualizar os registros filtrados. ○ Tarefa de correção: Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ Entrada de vulnerabilidade: Selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecione o CVE no **Entrada de vulnerabilidade** campo. **Nota:** ○ Registros com IC inválido ou IC desativado não são atualizados. ○ Somente os registros no estado Aberto, Em investigação, Aguardando implementação ou Adiado são atualizados.
Estado	Selecione o estado como Não atualizar.
Cancelar atribuição	Todos os itens vulneráveis selecionados não são atribuídos ao grupo de atribuição e ao responsável pela correção. **Nota:** ○ Este campo aparece quando você seleciona o Estado como Não atualizar. ○ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e enviada para aprovação.
Anotações de trabalho	Texto inserido para descrever as mudanças.

6. Clique em **Editar** .
Uma tarefa de correção é criada com os Itens vulneráveis do host (Vits) selecionados.

Sua solicitação é enviada para aprovação e o aprovador recebe uma notificação por e-mail sobre sua solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O estado dos itens vulneráveis (Vits) do host e da tarefa de correção (VUL) são transições para Em revisão. Se uma tarefa de correção for atualizada com este recurso, o **Atribuído a.** e. **Grupo de atribuição** Os campos em todos os seus Vits associados também são limpos mediante a aprovação da sua solicitação.

Resultado
No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Solicitações de exceção** > **Tudo** E abra o registro de aprovação de mudança de estado correspondente (nº VCA) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado da aprovação	Resultado
Aprovadas	. **Atribuído a.** e. **Grupo de atribuição** todos os itens vulneráveis do host são limpos.
Rejeitado	. **Atribuído a.** e. **Grupo de atribuição** os campos de todos os itens vulneráveis do host não são atualizados.

Em **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades

Solicite uma exceção para vários registros (Vits, AVITs, CVITs ou TRs) simultaneamente usando o recurso de edição em massa em vez de selecionar manualmente cada registro.

Antes de Iniciar
Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa
Quando você solicita uma exceção para um ou mais registros do modal de edição em massa, uma tarefa de correção é criada com os registros selecionados.

Nota: Itens vulneráveis à aplicação (AVITs) dos scanners com **Gerencie exceções na ServiceNow** o conjunto de parâmetros como falso não foi atualizado.

- Se você selecionar AVITs em vários scanners, alguns com **Gerencie exceções na ServiceNow** Parâmetro definido como verdadeiro e outro definido como falso, os AVITs vinculados aos scanners com HE **Gerencie exceções na ServiceNow** o conjunto de parâmetros como falso não foi atualizado.
- Se você selecionar AVITs somente nos scanners com **Gerencie exceções na ServiceNow** parâmetro definido como falso, o. *Adiar* a opção não aparece em **Estado** Campo no modal Edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra Ativo Ou Todas as listas em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute um dos seguintes procedimentos:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. *Somente itens selecionados* . Seleção de registro campo.
   - Aplique filtros se quiser usar *Todos os registros que correspondem ao filtro* . Seleção de registro campo.
4. Selecione **Edição em massa** botão.
5. No formulário, preencha os campos a seguir para solicitar uma exceção para vários registros (Vits, AVITs, CVITs ou TRs) simultaneamente.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ *Somente itens selecionados* : Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ *Todos os registros que correspondem ao filtro* : Selecione esta opção se quiser atualizar os registros filtrados. ○ *Tarefa de correção* : Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ *Entrada de vulnerabilidade* : Selecione esta opção se quiser atualizar os registros específicos de uma vulnerabilidade E, em seguida, selecione um CVE ou TPE em **Entrada de vulnerabilidade** campo. **Nota:** Este campo aparece para itens vulneráveis ao host, itens vulneráveis à aplicação e itens vulneráveis ao contêiner. ○ *Teste de configuração* : Selecione esta opção se quiser atualizar os resultados de teste específicos para um teste e selecione um teste no **Teste de configuração** campo. **Nota:** Esta opção aparece somente para resultados de teste de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros no estado Aberto, Em investigação ou Aguardando implementação são atualizados.
Estado	Selecione *Adiado* estado para solicitar uma exceção para os registros selecionados. **Nota:** ◦ Quando você seleciona esta opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ◦ Quando você adia registros, uma tarefa de correção é criada e esta tarefa é enviada para aprovação.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro **Nota:** . **Motivo** O campo aparece quando você seleciona o Estado como Adiado.
Descrição resumida	Breve anotação descrevendo os motivos da solicitação de adiamento. Essas informações são refletidas em **Descrição** campo da tarefa de correção criada para uma solicitação de adiamento. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-Positivo.
Até	Data até a qual o registro permanece adiado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado.
Informações adicionais	Qualquer outra informação necessária. Essas informações são refletidas no campo Informações adicionais na guia Visão geral da tarefa de correção que é criada para solicitações adiadas e encerradas de falso-positivos. Se sua solicitação de adiamento for aprovada, essas informações adicionais serão exibidas como anotações de adiamento para VIT e tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-Positivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Anotações de trabalho	Texto inserido para descrever as mudanças.

6. Clique em **Editar** .
7. No modal Responder ao questionário, responda às perguntas e clique em **Enviar** .

   Uma tarefa de correção é criada contendo os registros que você selecionou. Sua solicitação é enviada para aprovação e o Estado dos registros muda para#Em revisão.

   Nota: . **Responder ao questionário** O modal aparece somente quando o questionário está habilitado para solicitações de exceção no formulário Gestão de exceções. Para obter mais informações sobre como configurar um questionário para solicitações de exceção, consulte Configure a Gestão de exceções para Resposta a vulnerabilidades, Configure a Gestão de exceções para Resposta a vulnerabilidades de aplicações e Configure a Gestão de exceções para Contêiner de Resposta a vulnerabilidades e Conformidade de configurações Visão geral da Gestão de exceções.

   O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultado

No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Exceções** > **Tudo**Abra o registro de aprovação de mudança de estado correspondente (nº VCA) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado da aprovação	Resultado
Aprovadas	O estado da tarefa de correção muda para Adiado com o motivo fornecido como subestado. O estado e o motivo são acumulados para os registros.
Rejeitado	O estado da Tarefa de Correção e seus registros não mudam.

Em **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades

Marque um ou mais registros (Vits, AVITs, CVITs ou TRs) como falso positivo simultaneamente usando o recurso de edição em massa do Espaço do Gerenciador de vulnerabilidades em vez de selecionar manualmente cada item.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Quando você gera uma solicitação de falso positivo para um ou mais registros do modal de edição em massa, uma tarefa de correção é criada com os registros selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando você gera uma solicitação de falso positivo para os itens vulneráveis à aplicação (AVITs) usando o recurso de edição em massa, os AVITs dos scanners com **Gerencie falso-positivo com a ServiceNow** o conjunto de parâmetros como falso não foi atualizado.

- Se você selecionar AVITs em vários scanners, alguns com **Gerencie falso-positivo com a ServiceNow** Parâmetro definido como verdadeiro e outro definido como falso, os AVITs vinculados aos scanners com **Gerencie falso-positivo com a ServiceNow** o conjunto de parâmetros como falso não foi atualizado.
- Se você selecionar AVITs somente nos scanners com **Gerencie falso-positivo com a ServiceNow** parâmetro definido como falso, o. *Falso-positivo* a opção não aparece em **Motivo** Campo no modal Edição em massa.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.

   Nota: Os registros selecionados devem estar no estado Aberto, Em investigação ou Aguardando implementação.

2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute um dos seguintes procedimentos:
   - Marque a caixa de seleção ao lado de cada item se quiser usar o. *Somente itens selecionados* . **Seleção de registro** campo.
   - Aplique filtros se quiser usar *Todos os registros que correspondem ao filtro* . **Seleção de registro** campo.
4. Selecione **Edição em massa** botão.
5. No formulário, preencha os campos para solicitar falso positivo para vários registros.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ *Somente itens selecionados* : Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ *Todos os registros que correspondem ao filtro* : Selecione esta opção se quiser atualizar os registros filtrados. ○ *Tarefa de correção* : Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ *Entrada de vulnerabilidade* : Selecione esta opção se quiser atualizar os registros específicos de uma vulnerabilidade E, em seguida, selecione um CVE ou TPE em **Entrada de vulnerabilidade** campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo aparece para itens vulneráveis ao host, itens vulneráveis à aplicação e itens vulneráveis ao contêiner. ○ *Teste de configuração* : Selecione esta opção se quiser atualizar os resultados de teste específicos para um teste e selecione um teste no **Teste de configuração** campo. **Nota:** Esta opção aparece somente para resultados de teste de configuração. **Nota:** ○ Registros com IC inválido ou IC desativado não são atualizados. ○ Somente os registros no estado Aberto, Em investigação ou Aguardando implementação são atualizados.
Estado	Selecione **Encerrado** estado.
Motivo	Selecione o motivo como Falso positivo. **Nota:** ○ Quando você seleciona esta opção, os campos Descrição resumida e Informações adicionais são exibidos. ○ Uma tarefa de correção é criada quando você marca os registros como falso-positivo e esta tarefa é enviada para aprovação. **Nota:** . **Motivo** O campo aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve anotação descrevendo os motivos da solicitação Encerrada-Falso-Positivo. Essas informações são refletidas em **Descrição** Campo da tarefa de correção que é criada para uma solicitação Encerrada-Falso-Positivo. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado-Falso-Positivo.
Informações adicionais	Qualquer outra informação necessária. Essas informações são refletidas no campo Informações adicionais na guia Visão geral da tarefa de correção que é criada para a solicitação Encerrado-Falso-Positivo. Se sua solicitação de falso-positivo for aprovada, essas informações adicionais serão exibidas como anotações para VIT e tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado-Falso-Positivo.
Anotações de trabalho	Texto inserido para descrever as mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Editar** .
7. No modal Responder ao questionário, responda às perguntas e selecione **Enviar** .
   Uma tarefa de correção é criada com os registros selecionados. Sua solicitação é enviada para aprovação e o Estado da tarefa de correção muda para#Em revisão.

   Nota: . **Responder ao questionário** O modal aparece somente quando o questionário está habilitado para solicitações falso-positivas no formulário Gestão de exceções. Para obter mais informações sobre como configurar um questionário para solicitações de falso positivo, consulte Configure a Gestão de exceções para Resposta a vulnerabilidades, Configure a Gestão de exceções para Resposta a vulnerabilidades de aplicações e Configure a Gestão de exceções para Contêiner de Resposta a vulnerabilidades.

   O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultado

No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Exceções** > **Tudo**Abra o registro de aprovação de mudança de estado correspondente (nº VCA) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado da aprovação	Resultado
Aprovadas	O estado da tarefa de correção muda para Encerrado com o motivo como Falso positivo. O estado e o motivo são acumulados para os registros.
Rejeitado	O estado da Tarefa de Correção e seus registros não mudam.

Em **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Feche registros em massa no Espaço do gerente de vulnerabilidade

Feche vários registros (Vits, AVITs ou CVITs) simultaneamente usando o recurso de edição em massa no Espaço do gerente de vulnerabilidade.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
3. Execute um dos seguintes procedimentos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marque a caixa de seleção ao lado de cada item se quiser usar a opção Somente itens selecionados no **Seleção de registro** campo.
- Aplique filtros se quiser usar a opção de filtro Todos os itens vulneráveis que correspondem em **Seleção de registro** campo.

4. Selecione **Edição em massa** botão.
5. No formulário, preencha os campos para fechar os registros selecionados.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente itens selecionados: Selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ○ Todos os itens vulneráveis que correspondem ao filtro: Selecione esta opção se quiser atualizar os registros filtrados. ○ Tarefa de correção: Selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecione a tarefa de correção desejada no **Tarefa de correção** campo. ○ Entrada de vulnerabilidade: Selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecione o CVE no **Entrada de vulnerabilidade** campo. **Nota:** ○ Registros com IC inválido ou IC desativado não são atualizados. ○ Somente os registros no estado Aberto, Em investigação ou Aguardando implementação são atualizados.
Estado	Selecione o estado como Encerrado.
Motivo	Motivo para fechar registros: ○ Falso-positivo **Nota:** Quando você seleciona esta opção para marcar os registros como falso-positivo, os campos Motivo, Descrição resumida e Informações adicionais são exibidos. Para obter mais informações sobre edição em massa para falso positivo, consulte Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades. ○ Cancelado(a) ○ Fixo **Nota:** Os motivos, Cancelado e Fixo não se aplicam a CVITs.
Anotações de trabalho	Texto inserido para descrever as mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Editar** .

Um trabalho assíncrono de edição em massa atualiza os registros relevantes.

Solicitar exceções para tarefas de correção e registros no Espaço do gerente de vulnerabilidade

Em Espaço do gerente de vulnerabilidade, Os gerentes de vulnerabilidades e analistas podem solicitar exceções e falsos positivos para uma tarefa de correção (VUL, avul, CVUL ou CRG) e registro (VIT, CVIT, AVIT ou CTR). Você também pode dividir uma tarefa de correção e criar solicitações de mudança.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para Itens vulneráveis do host (Vits)
- sn_vul.app_sec_manager para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para Itens vulneráveis ao contêiner (CVITs)
- sn_vulc.admin para resultados de teste de configuração (CTRs)

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Em Espaço do gerente de vulnerabilidade, você pode executar o seguinte nos registros e tarefas de correção:

- Divida uma tarefa de correção (VUL, avul, CVUL e CRG).
- Solicite uma exceção para um registro (VIT, AVIT ou CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).
- Solicite uma exceção de política para registros (VIT, AVIT ou CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).
- Solicitar redução de risco para um item vulnerável (VIT) do host e tarefa de correção (VUL)
- Crie uma solicitação de mudança para tarefa de correção (VUL, CVUL ou CRG).
- Solicite um falso positivo para registro (VIT, AVIT ou CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).

Nota: Você pode gerar solicitações falso-positivas para um conjunto de resultados de teste de uma tarefa de correção (CRG).

Você inicia essas ações de IU a partir de registros no Espaço do gerente de vulnerabilidade, da mesma forma que os responsáveis pela correção executam essas tarefas no Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte os tópicos a seguir:

- Solicite um falso positivo para um item vulnerável ou corrija a tarefa
- Solicite uma exceção no Espaço de correção de problemas de TI
- Solicitar redução de risco para um item vulnerável ou tarefa de correção
- Divida uma tarefa de correção no Espaço de correção de problemas de TI
- Crie uma solicitação de mudança no Espaço de correção de problemas de TI
- Solicite uma exceção usando GRC: Gestão de políticas e conformidade em Espaço de correção de problemas de TI
- Solicite um falso positivo para um conjunto de resultados de testes

Tópicos relacionados

Visão geral da Gestão de exceções

Conformidade de configurações Visão geral da Gestão de exceções

Solicitar exceção em massa no Espaço do Gerenciador de vulnerabilidades

Edição em massa para falso positivo no Espaço do gerenciador de vulnerabilidades

Solicite uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades

Solicite uma extensão para um item vulnerável adiado antes que ele atinja sua data de vencimento Adiado até. Como responsável pela correção, você não precisa mais aguardar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do ambiente clássico.

Use o mesmo procedimento para solicitar uma extensão para um item vulnerável à aplicação, item vulnerável ao contêiner, grupo de resultados de teste e uma tarefa de correção.

Procedimento

1. Navegar até **Espaços** > **Espaços do Gerenciador de vulnerabilidades**.
2. Selecione Listas.
3. Em Itens vulneráveis do host, selecione **Todos** .
4. Filtre a lista selecionando Adiado na coluna Estado.
5. Selecione um item vulnerável adiado.

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

6. Selecione **Extensão da solicitação** botão.
7. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até a qual o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Mitigação do controle em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

8. Selecione **Extensão da solicitação** .
   Um e-mail é acionado no envio da solicitação e na ação subsequente pelo aprovador.

   Nota:
   - A solicitação passa por dois níveis de aprovação.
   - Se um item vulnerável adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

9. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Espaço do gerente de vulnerabilidade informações de referência

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados em Espaço do gerente de vulnerabilidade.

Campos de formulário Criar tópico de observação

A tabela a seguir descreve os campos no formulário Criar tópico de observação no Espaço do gerente de vulnerabilidade.

Campo	Descrição
Nome	Nome do tópico de observação, por exemplo, VIS crítico .
Pertencente a	O nome do usuário proprietário do tópico de observação.
Ordem de exibição	Insira um valor entre 100 e 1000. 100 é o valor padrão. Valores inferiores que começam com 100 são exibidos em ordem crescente nas listas.
Grupo responsável	O nome do grupo proprietário do tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Ativar ou desativar o tópico de observação. O padrão é Selecionado (Ativo).
Participantes da lista de observação	Adicione nomes de usuários que recebem notificações e podem exibir o tópico de exibição.
Descrição	Texto que descreve seu tópico de observação. Este texto é exibido no campo Descrição quando você cria um esforço de correção a partir deste tópico de observação.
Categoria	Tipo de registro para o qual o tópico de observação está sendo criado.

Tópicos relacionados

Crie um tópico de observação no Espaço do gerente de vulnerabilidade

Campos do formulário Exceção de solicitação de GRC

A tabela a seguir mostra as descrições dos campos do formulário Exceção de solicitação de GRC.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começa. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e o estado do item vulnerável ou grupo muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder **Duração máxima da exceção (dias)** Que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Gerar campos de formulário de resumo de correção

A tabela a seguir mostra os campos no formulário Gerar resumo de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerar campos de resumo de correção

Campo	Descrição
Caixa de seleção Ativo	Esta caixa de seleção é ativada por padrão. Se você não quiser enviar notificações por e-mail, desative este campo.
Executar	Semanal é o padrão. Escolha uma opção na lista.
Dia	Monday é o padrão. Escolha uma opção na lista.
Hora	Defina um horário para entregar os e-mails. Selecione um fuso horário se quiser um fuso horário diferente do usado pela instância que executa o trabalho.

Impacto dos controles de compensação na pontuação de risco e na data de vencimento

Como responsável pela correção, você pode solicitar a redução de risco para um item vulnerável do host ou tarefa de correção. E o gerente ou analista de vulnerabilidades pode aprovar essas solicitações de redução de risco.

Para obter mais informações sobre como solicitar redução de risco e aprovar aprovação de redução de risco, consulte Solicitar redução de risco para um item vulnerável ou tarefa de correção e. Aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade respectivamente.

Quando uma solicitação de redução de risco é aprovada, a pontuação de risco é reduzida de acordo com **Valor desejado** (Classificação de risco) no registro Aprovação de mudança de estado (nº VCA). A pontuação de risco mais alta da classificação de risco desejada é atribuída ao registro quando sua solicitação de redução de risco é aprovada. O exemplo a seguir mostra como a pontuação de risco e a pontuação de risco original são atualizadas quando os controles de compensação são aplicados. As pontuações de risco mais altas padrão das classificações de risco são usadas no exemplo a seguir.

Impacto dos controles de compensação na pontuação de risco e na pontuação de risco original

Cenário	Classificação de risco	Pontuação de risco	Pontuação de risco original (pontuação de risco calculada)
Dados anteriores à v20.0	2 - Alta	80	O campo não está disponível antes da v20.0.
Após atualizar para v20.0	2 - Alta	80	Nulo
A pontuação de risco calculado muda para 90 durante a ingestão	1 - Crítico(a)	90	Nulo
Quando você aplica controles de compensação	3 – Médio	69	90
A pontuação de risco calculado muda para 70 durante a ingestão	3 – Médio	69	70
A pontuação de risco calculado muda para 50 durante a ingestão	3 – Médio	50	50

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impacto dos controles de compensação na pontuação de risco e na pontuação de risco original

Cenário	Classificação de risco	Pontuação de risco	Pontuação de risco original (pontuação de risco calculada)
A pontuação de risco calculado muda para 80 durante a ingestão	3 – Médio	50	80
Quando os controles de compensação expiram em **Até a data de redução de risco**	2 - Alta	80	Nulo

Impacto dos controles de compensação em uma tarefa de correção

Quando sua solicitação de redução de risco é aprovada para uma tarefa de correção, o impacto dos controles de compensação em seus itens vulneráveis é o seguinte:

- Os controles de compensação aplicados na tarefa de correção são aplicados em seus itens vulneráveis (exceto aqueles no estado Encerrado) que têm pontuação de risco maior do que a pontuação de risco correspondente a. **Valor desejado** no estado aprovação de mudança de uma tarefa de correção. E a pontuação de risco desses itens vulneráveis é reduzida de acordo com **Valor desejado** .
- . **Até a data de redução de risco** permanece inalterado para os itens vulneráveis nos quais um controle de compensação já está aplicado. Ele não é atualizado com **Até a data de redução de risco** Da tarefa de correção.
- . **Até a data de redução de risco** é revertido para os itens vulneráveis somente quando um controle compensatório não é aplicado em nenhum item vulnerável anteriormente. Se você aplicar os controles compensatórios na tarefa de correção novamente, o. **Até a data de redução de risco** não é revertido para os itens vulneráveis como o existente **Até a data de redução de risco** dos itens vulneráveis recebe prioridade.
- Quando um novo item vulnerável é adicionado a uma tarefa de correção na qual controles compensatórios já estão aplicados, o risco não é revertido para o item vulnerável.

Impacto de um controle de compensação em um item vulnerável

Quando sua solicitação de redução de risco é aprovada para um item vulnerável:

- Sua nova pontuação de risco é exibida no **Pontuação de risco** e a pontuação de risco antiga (pontuação de risco calculada) são movidos para **Pontuação de risco original** campo. Esta mudança é válida até a data especificada em **Até a data de redução de risco** campo.
- Quando um item vulnerável tem controles de compensação já aplicados, durante a ingestão:
  - Se a pontuação de risco calculada for maior do que a pontuação de risco, a pontuação de risco permanecerá a mesma e a pontuação de risco original será atualizada com a pontuação de risco calculada.
  - Se a pontuação de risco calculada for menor que a pontuação de risco, a pontuação de risco e a pontuação de risco original serão atualizadas com a pontuação de risco calculada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se um Item de configuração (IC) for alterado para um item vulnerável no qual um controle de compensação já está aplicado:
  - O IC é atualizado para um item vulnerável por padrão como *sn_sec_cmn.update_on_ci_change*a propriedade do sistema está definida como verdadeira.

    O controle de compensação ainda é aplicável ao item vulnerável.
  - O item vulnerável é encerrado e um novo item vulnerável é criado se *sn_sec_cmn.update_on_ci_change*a propriedade do sistema está definida como falsa.

    O controle de compensação aplicado ao item vulnerável antigo é aplicado ao novo item vulnerável e ao **Até a data de redução de risco** , **Pontuação de risco original** e. **Pontuação de risco** permanecer o mesmo.
- Quando um item vulnerável é reaberto pelo scanner e o controle de compensação já está aplicado a ele, o mesmo controle de compensação é aplicado depois que ele é reaberto.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Adicione um controle de compensação à biblioteca

Associe controles de compensação a CVEs ou TPEs para solicitações de redução de risco

Desabilite ou habilite a redução de risco para um CVE ou TPE

#unique_158_Connect_42_li-risk-reduction-vmws

Exemplos de criação de tarefa de correção no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI

Quando você cria tarefas de correção manualmente no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI, os registros são agrupados em uma tarefa de correção com base nos critérios de agrupamento selecionados.

Considere o exemplo a seguir em que 10 registros são selecionados para criação de tarefa de correção. Depois de fornecer os detalhes da seleção de registro e uma breve descrição, selecione **Critérios de agrupamento** de acordo com seu requisito e selecione como você deseja gerenciar os registros que já fazem parte das tarefas de correção existentes.

Example: Criação de tarefa de correção com base nos critérios de agrupamento

Itens vulneráveis selecionados para criação da tarefa de correção

ID do item vulnerável	Tarefas de correção existentes	Grupo de atribuição	Item de configuração	Vulnerabilidade	Classificação de risco
VIT10001	VUL10021, VUL10022	Gerenciador de correção	APSVR-NY-1672	CVE-2018-9020	4
VIT10002	-	Resposta a vulnerabilidades	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	Administradores LDAP	DEV-IBM-NY-682	CVE-2012-5357	1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens vulneráveis selecionados para criação da tarefa de correção

ID do item vulnerável	Tarefas de correção existentes	Grupo de atribuição	Item de configuração	Vulnerabilidade	Classificação de risco
VIT10004	-	Gerenciador de correção	CRMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Resposta a vulnerabilidades	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10006	-	Gerenciador de correção	CRMBK-SD-4210	CVE-2013-1710	2
VIT10007	-	Administradores LDAP	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008	-	Administradores LDAP	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009	-	Gerenciador de correção	CRMBK-SD-4210	CVE-2013-1710	2
VIT10010	-	Administradores LDAP	DEV-SAP-SD-9388	CVE-2013-3906	4

A lista a seguir mostra como os registros são agrupados em tarefas de correção com base nos critérios de agrupamento selecionados ao criar a tarefa de correção.

Cenário 1: Critérios de agrupamento são selecionados como "Grupo de atribuição" e Gerenciar registros em outras tarefas de correção é selecionado como "Ignorar registros para as novas tarefas de correção"

Os registros com o mesmo grupo de atribuição são agrupados em uma tarefa de correção. Os registros que já fazem parte das tarefas de correção existentes não são adicionados às novas tarefas de correção. Três tarefas de correção são criadas, cada uma contendo os registros atribuídos ao **Gerenciador de correção** , **Administradores LDAP** e **Resposta a vulnerabilidades** grupos de atribuição.

Tarefa de correção criada no cenário 1

Tarefas de correção criadas	Registros na tarefa de correção
Tarefa de correção 1 - VUL10001	Esta tarefa de correção contém os registros atribuídos ao **Gerenciador de correção** grupo de atribuição: • VIT10004 • VIT10006 • VIT10009 O registro VIT10001 não será movido para a tarefa de correção VUL10001.
Tarefa de correção 2 - VUL10002	Esta tarefa de correção contém o registro VIT10002 atribuído ao **Resposta a vulnerabilidades** grupo de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção criada no cenário 1

Tarefas de correção criadas	Registros na tarefa de correção
	O registro VIT10005 não será movido para a tarefa VUL10002.
Tarefa de correção 3 - VUL10003	Esta tarefa de correção contém os registros atribuídos ao **Administradores LDAP** grupo de atribuição: • VIT10007 • VIT10008 • VIT10010 O registro VIT10003 não será movido para a tarefa de correção do VUL10003.

Cenário 2: Critérios de agrupamento são selecionados como "Grupo de atribuição e item de configuração" e Gerenciar registros em outras tarefas de correção é selecionado como "Transferir registros para as novas tarefas de correção"

Os registros com o mesmo item de configuração atribuídos ao mesmo grupo de atribuição são agrupados em uma tarefa de correção. Os registros VIT10001, VIT10003 e VIT10005 são removidos de suas tarefas de correção antigas e movidos para as novas tarefas de correção. Cinco tarefas de correção são criadas.

Tarefas de correção criadas no cenário 2

Tarefas de correção criadas	Registra parte da tarefa de correção
Tarefa de correção 1 - VUL10004	Esta tarefa de correção contém os registros atribuídos a. **Responsável pela correção** grupo de atribuição e com **APSVR-NY-1672** item de configuração. • VIT10001 O registro VIT10001 será removido das tarefas de correção VUL10021 e VUL10022.
Tarefa de correção 2 - VUL10005	Esta tarefa de correção contém os registros atribuídos a. **Resposta a vulnerabilidades** grupo de atribuição e com **DEV-IBM-NY-682** item de configuração. • VIT10002 • VIT10005 O registro VIT10005 será removido da tarefa de correção VUL10022.
Tarefa de correção 3 - VUL10006	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de correção criadas no cenário 2

Tarefas de correção criadas	Registra parte da tarefa de correção
	de atribuição e com **DEV-IBM-NY-682** item de configuração. • VIT10003 • VIT10008 O registro VIT10003 será removido da tarefa de correção do VUL10021.
Tarefa de correção 4 - VUL10007	Esta tarefa de correção contém os registros atribuídos a. **Gerenciador de correção** grupo de atribuição e com **CRMBK-SD-4210** item de configuração. • VIT10004 • VIT10006 • VIT10009
Tarefa de correção 5 - VUL10008	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo de atribuição e com **DEV-SAP-SD-9388** item de configuração. • VIT10007 • VIT10010

Cenário 3: Critérios de agrupamento são selecionados como "Grupo de atribuição e vulnerabilidade" e Gerenciar registros em outras tarefas de correção é selecionado como "Manter registros nas tarefas de correção atuais e novas"

Os registros com a mesma vulnerabilidade atribuídos ao mesmo grupo de atribuição são agrupados em uma tarefa de correção. Os registros VIT10001, VIT10003 e VIT10005 serão adicionados às respectivas novas tarefas de correção sem serem removidos das tarefas de correção antigas.Aqui, cinco tarefas de correção são criadas.

Tarefas de correção criadas no cenário 3

Tarefas de correção criadas	Registra parte da tarefa de correção
Tarefa de correção 1 - VUL10009	Esta tarefa de correção contém os registros atribuídos a. **Responsável pela correção** grupo de atribuição e com **CVE-2018-9020** vulnerabilidade. • VIT10001 O registro VIT10001 permanecerá parte das tarefas de correção VUL10021 e VUL10022 também.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de correção criadas no cenário 3

Tarefas de correção criadas	Registra parte da tarefa de correção
Tarefa de correção 2 - VUL10010	Esta tarefa de correção contém os registros atribuídos a. **Resposta a vulnerabilidades** grupo de atribuição e com **CVE-2018-9020** vulnerabilidade. • VIT10002 • VIT10005 O registro VIT10005 também permanecerá parte da tarefa de correção do VUL10022.
Tarefa de correção 3 - VUL10011	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo de atribuição e com **CVE-2012-5357** vulnerabilidade. • VIT10003 O registro VIT10003 continuará a fazer parte da tarefa de correção do VUL10021 também.
Tarefa de correção 4 - VUL10012	Esta tarefa de correção contém os registros atribuídos a. **Gerenciador de correção** grupo de atribuição e com **CVE-2013-1710** vulnerabilidade. • VIT10004 • VIT10006 • VIT10009
Tarefa de correção 5 - VUL10013	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo de atribuição e com **CVE-2013-3906** vulnerabilidade. • VIT10007 • VIT10008 • VIT10010

Cenário 4: Agrupar critérios como "Grupo de atribuição e classificação de risco" e Gerenciar registros em outras tarefas de correção é selecionado como "Manter registros nas tarefas de correção atuais e novas"

Os registros com a mesma classificação de risco atribuídos ao mesmo grupo de atribuição são agrupados em uma tarefa de correção. Os registros VIT10001, VIT10003 e VIT10005 serão adicionados às respectivas novas tarefas de correção sem serem removidos das tarefas de correção antigas. Cinco tarefas de correção são criadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção criada no cenário 4

Tarefas de correção criadas	Registra parte da tarefa de correção
Tarefa de correção 1 - VUL10014	Esta tarefa de correção contém os registros atribuídos a. **Responsável pela correção** grupo de atribuição e com **4** classificação de risco. • VIT10001 • VIT10004 O registro VIT10001 continuará a fazer parte das tarefas de correção VUL10021 e VUL10022.
Tarefa de correção 2 - VUL10015	Esta tarefa de correção contém os registros atribuídos a. **Resposta a vulnerabilidades** grupo de atribuição e com **2** classificação de risco. • VIT10002 • VIT10005 O registro VIT10005 continuará a fazer parte da tarefa de correção do VUL10022.
Tarefa de correção 3 - VUL10016	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo de atribuição e com **1** classificação de risco. • VIT10003 • VIT10007 • VIT10008 O registro VIT10003 continuará a fazer parte da tarefa de correção do VUL10021.
Tarefa de correção 4 - VUL10017	Esta tarefa de correção contém os registros atribuídos a. **Gerenciador de correção** grupo de atribuição e com **2** classificação de risco. • VIT10006 • VIT10009
Tarefa de correção 5 - VUL10018	Esta tarefa de correção contém os registros atribuídos a. **Administradores LDAP** grupo de atribuição e com **4** classificação de risco. • VIT10010

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Crie uma tarefa de correção manualmente no Espaço do gerente de vulnerabilidade

Crie uma tarefa de correção manualmente no Espaço de correção de problemas de TI

Reavaliar as exceções para registros selecionados no Espaço do gerente de vulnerabilidade

Em Espaço do gerente de vulnerabilidade, Quando você avalia as regras de exceção para um conjunto de registros no modal Reavaliar e atualizar as propriedades de correção, o status de adiamento e Até a data de adiamento são atualizados de acordo com as regras de exceção mais recentes.

Cenários

Você pode se deparar com os seguintes cenários ao avaliar as exceções de um conjunto selecionado de registros no Reavaliar e atualizar o modal de propriedades de correção no Espaço do gerente de vulnerabilidade:

Cenário 1: Quando os registros selecionados já são adiados manualmente e correspondem à condição de uma regra de exceção, esses registros permanecem no estado Adiado sem mudanças.

Cenário 2: Quando os registros selecionados correspondem à condição nas regras de exceção e esses registros estão em um estado não adiado (como Aberto, Em revisão, Em investigação), esses registros são adiados até a data definida na regra de exceção.

Cenário 3: Quando os registros selecionados já estão no estado Adiado (que são adiados usando a regra de exceção A), eles permanecem no estado Adiado nos seguintes cenários:

- a regra de exceção expira e os registros não correspondem à condição
- a regra de exceção expira e os registros correspondem à condição
- A regra de exceção A expira e os registros correspondem à condição de outra regra de exceção B.

Cenário 4: Considere que os registros são adiados usando uma regra de exceção. Quando você altera a condição da regra de exceção para que o estado adiado dos registros não seja mais válido e reavalie as regras de exceção para esses registros:

- Os registros são movidos para o estado Aberto
- Até data, Data de adiamento, Contagem de adiamento e outros campos são atualizados.

Example: Considere que você está avaliando as exceções para os seguintes itens vulneráveis do host (Vits)

Considere a regra de exceção com os seguintes detalhes:

Detalhes da regra de exceção

Campo	Descrição	Valor
Nome	Nome da regra de exceção.	Adiando Vits críticos
Válida de	Data a partir da qual esta regra está ativa para adiar o VIS.	20-08-2024
Válida até	Data a partir da qual a tarefa de correção para de aceitar novos VIS.	30-11-2024

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes da regra de exceção

Campo	Descrição	Valor
Motivo	Motivo para criar esta regra de exceção.	Risco aceito
Grupo de atribuição	Grupo ao qual a tarefa de correção que foi criada para rastrear o VIS adiado está atribuída.	Grupo de correção 1
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.	Esta regra foi criada para adiar os Vits críticos automaticamente.
Condição	Condição do filtro para o VIS que pode ser definido durante o processamento do VIS.	Classificação de risco igual a 5 - Crítica
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.	Sim
Estado	Estado da regra de exceção.	Aprovadas
Ordem de execução	Ordem exclusiva para cada regra de exceção.	100
Adiado até	Data até quando os VULs e VIS são adiados. Nesta data, o VUL criado é encerrado, todos os VIS são movidos para fora do grupo e as regras do grupo são reaplicadas.	2024-12-23 16:10:29

A tabela a seguir mostra como o estado muda quando as regras de exceção são reavaliadas para vários Vits simultaneamente:

Registros para os quais as exceções são reavaliadas

Número de VIT	Estado	Pontuação de risco	Estado atualizado após reavaliar as exceções -1	Até a data - 1
VIT120067	Aberto	2 - Baixo(a)	Aberto	-
VIT120068	Em revisão	3 – Médio	Em revisão	-
VIT120069	Sob Investigação	5 - Crítico	Adiado	2024-12-23 16:10:29
VIT120070	Adiado	5 - Crítico	Adiado	2024-12-23 16:10:29
VIT120071	Adiado	2 - Baixo(a)	Adiado	2024-10-02 16:10:29 (adiado manualmente)
VIT120072	Encerrado	5 - Crítico	Encerrado	-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando a condição na regra de exceção anterior é modificada para Classificação de risco: 2 - Baixa e. **Adiado até** modificado para 2024-12-31 14:10:23 os registros são atualizados da seguinte forma:

Registros para os quais as exceções são reavaliadas

Número de VIT	Estado atualizado após reavaliar as exceções -1	Classificação de risco	Estado atualizado após reavaliar as exceções - 2	até a data - 2
VIT120067	Aberto	2 - Baixo(a)	Adiado	2024-12-31 14:10:23
VIT120068	Em revisão	3 – Médio	Em revisão	-
VIT120069	Adiado	5 - Crítico	Adiado	2024-12-23 16:10:29
VIT120070	Adiado	5 - Crítico	Adiado	2024-12-23 16:10:29
VIT120071	Adiado	2 - Baixo(a)	Adiado (nenhuma mudança no estado)	2024-10-02 16:10:29 (Nenhuma mudança na data Até)
VIT120072	Encerrado	5 - Crítico	Encerrado	-

Tópicos relacionados

Reavalie as propriedades de correção dos registros no Espaço do gerente de vulnerabilidade

Visão geral das regras de exceção

Conformidade de configurações Visão geral da Gestão de exceções

Espaço de correção de problemas de TI

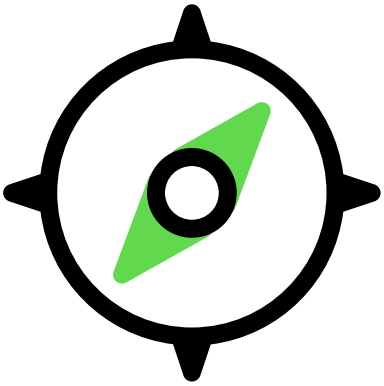
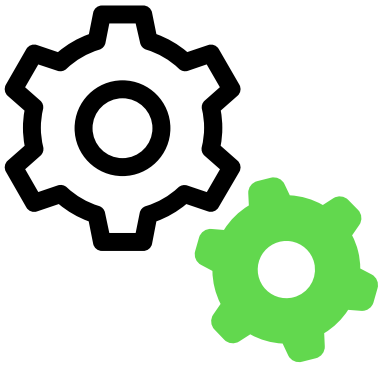
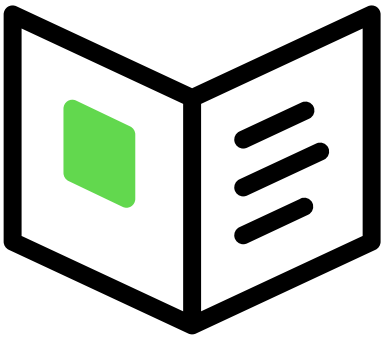
As equipes DE TI podem economizar tempo resolvendo vulnerabilidades relacionadas A TI criando facilmente solicitações de mudança, verificando novamente itens vulneráveis e enviando solicitações de exceção do Espaço de correção de problemas de TI.

Demonstração do Espaço de correção de TI v18.0

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar	Corrigir	Referência
		
Saiba mais sobre Espaço de correção de problemas de TI	Saiba como corrigir vulnerabilidades e configurações incorretas no Espaço de correção de problemas de TI	Obtenha informações adicionais que você usa para configurar e administrar Espaço de correção de problemas de TI

Solucionar problemas e obter ajuda

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

Explorar o. Espaço de correção de problemas de TI

. Espaço de correção de problemas de TI Destina-se a responsáveis pela correção de TI e grupos DE TI. Ele é composto por exibições de página inicial e de lista, bem como visualizações de dados nas quais você pode clicar que permitem ver as tarefas de correção atribuídas a você e quantos registros atribuídos a você têm soluções.

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

. Espaço de correção de problemas de TI consiste nas seguintes páginas, listas e formulários:

Página principal (Página inicial)

A página inicial consiste no cartão Tarefas de correção atribuídas, soluções preferenciais no cartão VIS, cartão de ICs afetados, patches preferenciais no cartão VIS e lista de tarefas de correção. Para obter mais informações sobre a página inicial, consulte Página inicial do Espaço de correção de problemas de TI.

Página Painéis

A página de painéis consiste no painel Correção de vulnerabilidades. Para obter mais informações sobre a página Painéis, consulte Página Painéis em Espaço de correção de problemas de TI.

Página da lista

Esta exibição consiste em listas padrão e personalizadas de tarefas de correção, itens vulneráveis do host, itens vulneráveis da aplicação, itens vulneráveis do contêiner, resultados de teste de configuração atribuídos a você e soluções, solicitações de exceções etc. Para obter mais informações sobre a página Lista, consulte Página de lista no Espaço de correção de problemas de TI. Para obter mais informações sobre o que você pode fazer nesta página, consulte Crie uma lista no Espaço de correção de problemas de TI.

Exiba um exemplo de fluxo de trabalho no Espaço de correção de problemas de TI

Exiba um exemplo de um fluxo de trabalho de ponta a ponta no Espaço de correção de problemas de TI. Veja como os especialistas DE TI podem usar o espaço para monitorar itens vulneráveis críticos (Vits, AVITs e CVITs) e resultados de testes (TRs) e corrigir as vulnerabilidades atribuídas a eles.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Procedimento

Clique na imagem a seguir para exibir as etapas do fluxo de trabalho.
Demonstração do Espaço de correção de TI

A imagem inclui as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na página inicial (página principal do responsável pela correção de TI), exiba as tarefas de correção atribuídas a você. Alterne entre o trabalho atribuído a você e ao seu grupo. Consulte as tarefas de correção do host que têm soluções. Para obter mais informações sobre a página inicial, consulte Página inicial do Espaço de correção de problemas de TI.
- Selecione **Lista** exibir para ver as listas do seu trabalho atribuído.
- Na Exibição de lista com **Atribuído ao meu grupo** Na lista Tarefas de correção, identifique e atribua trabalho a si mesmo. Para obter mais informações sobre a página Lista, consulte Página de lista no Espaço de correção de problemas de TI.
- Agrupar as tarefas de correção por tipo de registro: Selecione o menu de três pontos no **Tipo de registro** e selecione **Agrupar por tipo de registro** .
- Em uma tarefa de correção aberta (VUL, avul, CVUL e CRG):
  - Selecione **Visão geral** Para ver os registros (Vits, AVITs, CVITs e TRs) e os itens de configuração afetados (ICs) associados ao registro.
  - Selecione **Soluções** para ver as soluções preferenciais e potenciais para uma tarefa de correção de host.
  - Selecione **Detalhes** Para modificar campos editáveis, como Estado, Grupo de atribuição, Atribuído a e Descrição resumida, e exibir as ações realizadas em uma tarefa de correção.
  - Selecione **Aprovação de mudança de estado** Para exibir os registros de aprovação de mudança de estado (nº da CA) que ajudam você a rastrear o fluxo de trabalho de aprovação.
  - Selecione **Solicitações de mudança** para exibir o status de aprovação das solicitações de mudança e criar uma nova solicitação de mudança selecionando **Novo** botão.
  - Selecione as Ações de IU: **Marcar como falso positivo** , **Criar mudança** , **Tarefa dividida** , **Atualizar status Exceção de solicitação** , **Excluir** e assim por diante. Siga as instruções nas caixas de diálogo para ajudá-lo na correção.

Página inicial do Espaço de correção de problemas de TI

A página inicial do Espaço de correção de problemas de TI fornece uma lista consolidada de tarefas de correção de host, aplicação, contêiner e resultado de teste atribuídas a você e aos seus grupos de atribuição.

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

A página inicial consiste nos seguintes cartões e na lista de tarefas de correção atribuídas a você e aos seus grupos de atribuição, registros atribuídos a você com soluções.

Cartão Tarefas de correção atribuídas

Número de tarefas de correção ativas atribuídas a você. Selecione o bloco para exibir a lista de tarefas de correção.

Soluções preferenciais no cartão VIS

Número de soluções preferenciais disponíveis para corrigir os itens vulneráveis do host. A lista Soluções será exibida se a aplicação Gestão de soluções de vulnerabilidade estiver instalada. Este

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

cartão mostra dados da solução, soluções potenciais e preferenciais de fornecedores terceirizados sobre seus itens vulneráveis.

Cartão de ICs afetado

O número de itens de configuração que têm VIS atribuídos a você ou aos seus grupos. Para obter mais informações, consulte Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI.

Patches preferenciais no cartão VIS

Número de patches preferenciais disponíveis que podem ser usados para corrigir os itens vulneráveis do host.

Lista de tarefas de correção

A lista de tarefas de correção atribuídas a você e aos seus grupos de atribuição. Você pode filtrar os registros selecionando **Atribuído a mim** e. **Atribuído aos meus grupos** opções.

Você pode clicar em uma tarefa de correção para exibir os detalhes e iniciar uma investigação. Na exibição de listas, você pode exibir as Tarefas de correção, Itens vulneráveis, Resultados de teste de configurações e assim por diante. Você pode abrir uma tarefa de correção e clicar em **Atribuir a mim** para atribuir a tarefa a si mesmo e iniciar a investigação.

Nota: Se você não atribuir a tarefa a si mesmo na tarefa de correção, não poderá exibir nenhuma ação de IU no nível de registro.

Clique nas reticências Mais ações e clique em **Iniciar investigação** para resolver uma tarefa de correção.

Para obter mais informações sobre o que você pode fazer na página inicial, consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI.

Página Painéis em Espaço de correção de problemas de TI

A página Painéis no Espaço de correção de problemas de TI Fornece o painel Correção de vulnerabilidades no Next Experience IU que pode ser usada para se concentrar nas tarefas de correção e nos itens vulneráveis.

Como responsável pela correção (sn_vul.remediation_owner), você pode acessar **Correção de vulnerabilidade** navegando até **Espaços** > **Espaço de correção de TI** E selecionando o ícone Painéis. Para obter mais informações sobre o painel Correção de vulnerabilidades, consulte Usando o padrão Resposta a vulnerabilidades painéis.

Você pode criar um painel personalizado selecionando o ícone Mais opções ⋮ e selecionando **Criar novo** .

Página de lista no Espaço de correção de problemas de TI

A exibição de lista no Espaço de correção de problemas de TI Permite que os responsáveis pela correção exibam os registros (Vits, AVITs, CVITs e TRs) atribuídos a eles e seus grupos de atribuição e corrijam essas vulnerabilidades e configurações incorretas. Você também pode exibir a lista de soluções preferenciais recomendadas para corrigir os itens vulneráveis do host (Vits). Junto com essas listas, você pode exibir a lista de solicitações de exceção e solicitações de avaliação de teste de invasão levantadas por você, descobertas de teste de invasão associadas às suas solicitações de avaliação de teste de invasão, bibliotecas compatíveis e outros dados compatíveis.

Funções necessárias:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

As listas e os links na página Lista fornecem acesso fácil a registros e tarefas. Ele contém duas guias:

- **Listas** Guia: Exibe as listas padrão para esforços de correção, tarefas de correção, itens vulneráveis (Vits, AVITs ou CVITs), soluções, exceções e resultados de testes de configuração (TRs) etc. Para obter mais informações, consulte a tabela a seguir.
- **Minhas listas** Guia: Exibe todas as listas renomeadas na guia Lista e todas as listas que você criar.

  Você também pode criar sua própria lista de registros. Para obter mais informações, consulte Crie uma lista no Espaço de correção de problemas de TI.

Dica:

. *sn_vul_cmn_ws.navigate_to_workspace*a propriedade do sistema está definida como verdadeiro pelo administrador, ao selecionar os links de filtro predefinidos no Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades E Módulo Resultados de teste em Conformidade de configurações em **Todos** , esses links são abertos na página Lista do Espaço de correção de problemas de TI.

Por exemplo, se você selecionar **Atribuído a Meus grupos** navegando até **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuídos(as) aos meus grupos**este link é redirecionado para Espaço de correção de problemas de TI. A lista Atribuído ao meu grupo no módulo Tarefas de correção é aberta na página Lista do Espaço de correção de TI se você tiver uma função de responsável pela correção. Para exibir as tarefas de correção do host, agrupe as tarefas por **Tipo de registro** .

Você pode ocultar a contagem de registros em uma lista usando *glide.ui.list.seismic.omit.count*propriedade do sistema. Para obter mais informações sobre como ativar/desativar a exibição de contagem de registros em uma lista, consulte KBB0010402 artigo da base de conhecimento.

Guia Listas

As seguintes listas são exibidas:

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
Tarefas de correção	Exiba a lista de tarefas de correção e navegue até a tarefa desejada para começar a trabalhar nelas. As seguintes listas estão disponíveis: • **Atribuído a você** : Lista todas as tarefas de correção de host, aplicação, contêiner e	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.remediation_owner para Itens vulneráveis do host (Vits) • sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.remediation_owne para Itens

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
	resultado de teste atribuídas a você. • **Atribuído ao meu grupo** : Lista todas as tarefas de correção de host, aplicação, contêiner e resultado de teste atribuídas aos grupos de atribuição aos quais você pertence. Agrupe as tarefas por tipo de registro para categorizá-las em tarefas de correção de resultados de teste de host, aplicação, contêiner e configuração. As tarefas de correção criadas pelas regras de tarefa de correção na IU clássica têm um esforço de correção vazio.		vulneráveis do contêiner (CVITs) • sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)
Ativos afetados	Exiba a lista de ativos afetados. As seguintes listas estão disponíveis: • **Atribuído a você** : Lista de itens de configuração afetados atribuídos a você • **Atribuído ao meu grupo** : Lista de itens de configuração afetados atribuídos aos seus grupos de atribuição.	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.remediation_owner para Itens vulneráveis do host (Vits) • sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.remediation_owne para Itens vulneráveis do contêiner (CVITs) • sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
Itens vulneráveis de host	Exiba a lista de itens vulneráveis do host e navegue até o item desejado para começar a trabalhar neles. Estas listas estão disponíveis: • **Atribuído a mim** : Lista de itens vulneráveis do host atribuídos a você para correção. • **Atribuído ao meu grupo** : Lista de itens vulneráveis do host atribuídos aos grupos de atribuição aos quais você pertence.	Resposta a vulnerabilidades	sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
Itens vulneráveis à aplicação	Exiba a lista de itens vulneráveis do host e navegue até o item desejado para começar a trabalhar neles. As seguintes listas estão disponíveis: • **Atribuído a mim** : Lista de itens vulneráveis à aplicação atribuídos a você para correção. • **Atribuído ao meu grupo** : Lista de itens vulneráveis à aplicação atribuídos aos grupos de atribuição aos quais você pertence.	Resposta a vulnerabilidades de aplicações	sn_vul.app_security_champion
Itens vulneráveis de contêiner	Exiba a lista de itens vulneráveis ao contêiner e navegue até o item desejado para começar a trabalhar neles. Esta exibição de lista contém:	Contêiner de Resposta a vulnerabilidades	sn_vul_container.remediation_owner Exiba a lista de avaliações necessárias para executar a revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
	• **Atribuído a mim** : Lista de itens vulneráveis de contêiner atribuídos a você para correção. • **Atribuído ao meu grupo** : Lista de itens vulneráveis do contêiner atribuídos aos grupos de atribuição aos quais você pertence.		
Resultados de testes de configuração	Exiba a lista de resultados de testes e navegue até o registro desejado para começar a trabalhar neles. Esta exibição de lista contém: • **Atribuído a mim** : Lista de resultados de testes de configuração atribuídos a você para correção. • **Atribuído ao meu grupo** : Lista de resultados de teste de configuração atribuídos aos grupos de atribuição aos quais você pertence.	Conformidade de configurações	sn_vulc.remediation_owner
Soluções	Lista as soluções da aplicação de gestão de soluções. A lista Soluções será exibida se a aplicação Gestão de soluções de vulnerabilidade estiver instalada.	Resposta a vulnerabilidades	sn_vul.remediation_owner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
	• **Todos** Mostra todas as soluções disponíveis que você usa para corrigir os itens vulneráveis do host. • **Maior substituição** : Mostra todas as soluções que são usadas para preencher Soluções preferenciais. • **Com itens vulneráveis** : Mostra as soluções que estão sendo usadas como Solução preferencial em itens vulneráveis.		
Solicitações de exceção	• **Minhas solicitações** : Lista de todas as solicitações de aprovação de exceção, falso-positivo e cancelamento de atribuição geradas por você para itens vulneráveis de host, aplicação e contêiner e suas tarefas de correção. • **Minhas solicitações (conformidade de configuração)** : Lista de todas as solicitações de aprovação de exceção, falso-positivo e cancelamento de atribuição	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.remediation_owner para Itens vulneráveis do host (Vits) • sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.remediation_owne para Itens vulneráveis do contêiner (CVITs) • sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
	levantadas por você para os resultados de teste e suas tarefas de correção nas quais você está trabalhando.		
Bibliotecas	Contém as seguintes listas: • **NVDs** Uma biblioteca abrangente de inteligência contra vulnerabilidades mantida pelo National Institute of Standards and Technology (NIST). Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações. • **CWEs** : Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. • **Vulnerabilidades da aplicação** : Lista de todas as entradas de	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.remediation_owner para Itens vulneráveis do host (Vits) • sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.remediation_owne para Itens vulneráveis do contêiner (CVITs) • sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
	vulnerabilidade da aplicação de terceiros. • **TPEs** : Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs. • **Testes** : Testes importados das integrações de terceiros com as quais os resultados do teste devem estar em conformidade. • **Grupos de teste** : Lista de grupos/ políticas de teste importados de integrações de terceiros. Um grupo de testes contém um conjunto de testes.		
CMDB	• **Itens descobertos** : Lista de todos os itens descobertos. • **Imagens de contêiner descobertas** :	Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidades e Conformidade de configurações	• sn_vul.remediation_owner para Itens vulneráveis do host (Vits) • sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs) • sn_vul_container.remediation_owne para Itens vulneráveis do contêiner (CVITs) • sn_vulc.remediation_owner para resultados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
			de teste de configuração (CTRs)
Solicitações de avaliação de teste de invasão	Solicitações de avaliação de teste de invasão enviadas à equipe de segurança por você para executar uma avaliação de segurança de qualquer aplicação de negócios. Esta lista contém: • **Atribuído a mim** : Lista de solicitações de avaliação de teste de invasão feitas por você. • **Atribuído a Meus grupos** : Lista de solicitações de avaliação de teste de invasão geradas pelos usuários em seus grupos de atribuição.	Resposta a vulnerabilidades de aplicações	sn_vul.app_security_champion
Descobertas do teste de invasão	Lista de vulnerabilidades identificadas durante a Avaliação de teste de caneta realizada pela equipe de segurança: • **Atribuído a mim** : Lista de descobertas do teste de invasão atribuídas a você para correção. • **Atribuído a Meus grupos** : Lista de descobertas do teste de invasão atribuídas aos seus grupos de atribuição para correção.	Resposta a vulnerabilidades de aplicações	sn_vul.app_security_champion

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Aplicações necessárias	Função necessária
Dados de suporte	Esta exibição de lista contém: • **Fontes autorizadas** Lista de fontes autorizadas que fornecem as informações resumidas que são úteis para pesquisar as publicações de origem que foram usadas para criar o registro. • **.**: Lista de tecnologias que fornecem as informações resumidas sobre cada fonte autorizada e citação (também conhecidas, na Qualys, como uma estrutura).	Conformidade de configurações	sn_vulc.remediation_owner

Tópicos relacionados

Use a Exibição de lista no Espaço do gerente de vulnerabilidade

Usando o Espaço de correção de problemas de TI

. Espaço de correção de problemas de TI fornece uma lista consolidada de vulnerabilidades de host, vulnerabilidades de aplicações, vulnerabilidades de contêiner e configurações incorretas atribuídas a você e ao seu grupo. Você pode usar este espaço para corrigir e solicitar exceções para vulnerabilidades e configurações incorretas.

Abrir resultados da pesquisa em Espaço de correção de problemas de TI

Defina o escopo da aplicação como Espaço de correção de problemas de TI para abrir os resultados da pesquisa no Espaço de correção de problemas de TI Em vez da IU clássica, alterando o escopo da aplicação.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Por exemplo, se você pesquisar um item vulnerável do host com seu número em **Pesquisa** definindo o escopo da aplicação como Espaço de correção de problemas de TI, O VIT é aberto em sua exibição de registro no Espaço de correção de problemas de TI.

Procedimento

1. Na barra de navegação unificada, selecione o ícone de globo .
2. Selecione **Escopo da aplicação** e defina o escopo como **Espaço de correção de TI** .

Resultado

Quando você pesquisa registros como Vits, tarefas de correção, aprovações de mudança de estado e assim por diante, no **Pesquisa** na barra de navegação unificada, os registros são abertos no Espaço de correção de problemas de TI.

Quando o escopo não é Global, o ícone de globo é exibido com um anel vermelho . Selecione-o novamente para mudar o escopo.

Use o resumo de e-mail nos Espaços de resposta a vulnerabilidades

Use as notificações por e-mail para exibir o andamento da correção e lembrá-lo quando as tarefas estiverem próximas ou ultrapassarem o ANS.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Como responsável pela correção, entre em sua área de trabalho e veja sua notificação por e-mail como um resumo do seu trabalho. Veja o que você realizou, o que está se aproximando e o que está atrasado. Use a notificação para ajudá-lo a organizar e priorizar suas ações críticas de correção. Clique em um link no e-mail para levá-lo diretamente para o seu espaço. As notificações podem ajudar os especialistas DE TI com o status resumido do trabalho. Como gerente de vulnerabilidades, ajude seus especialistas DE TI a acessar a plataforma diretamente do serviço de e-mail para tarefas de correção.

Consulte Configurar notificações por e-mail no Resposta a vulnerabilidades Espaços de trabalho para obter mais informações sobre como configurar este recurso.

Por padrão, o e-mail mostra as tarefas encerradas, o total de tarefas ativas atribuídas a você e aos seus grupos, recém-atribuídas, Vits encerradas, além de outras informações.

Procedimento

1. Navegue até seu e-mail, localize uma notificação e clique para abri-la.
   A notificação é exibida com informações sobre seu status de trabalho.
2. Clique em **Ir para o espaço** para navegar até sua área de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma lista no Espaço de correção de problemas de TI

Com a exibição de lista no Espaço de correção de problemas de TI, você pode exibir tarefas de correção e registros atribuídos a você e aos seus grupos. Você também pode rastrear suas solicitações de exceção e falso positivo para tarefas de correção (VUL, AVUL, CVUL e CRG), itens vulneráveis (VIT, e CVIT) e resultados de testes (TRs) e exibir soluções.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Selecione o ícone de Lista ( ).
   A exibição de lista é exibida.
   - Clique em uma lista filtrada para exibir o número total de tarefas de correção ativas ou registros atribuídos a você ou ao seu grupo. Consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI para obter mais informações sobre o que você pode fazer a partir desses registros.
   - Exiba o número total de VIS atribuídos a você ou aos seus grupos que têm soluções. Clique em **Soluções preferenciais no VIS** cartão para exibir a lista.
   - Veja os ICs vulneráveis atribuídos a você e aos seus grupos que têm vulnerabilidades neles no **ICs vulneráveis** Na guia ou na lista ICs vulneráveis atribuídos a você e ao seu grupo na exibição de lista.
3. Selecione a guia **Minhas listas**.
4. Selecione **Adicionar nova lista**.
5. Crie a lista com base em uma lista existente ou em sua própria configuração.

Tipo de criação	Ações
Lista baseada em uma lista existente	**a.** Selecione **Começar a partir de existente** guia. **b.** Em **Lista** , selecione a lista existente a ser usada como modelo na lista suspensa. **c.** Forneça o nome da lista em **Nome da lis ta** campo.
Lista recém-criada	**a.** Selecione **Crie o seu próprio** **b.** Forneça o nome da lista em **Nome da lis ta** campo. **c.** Selecione a origem cujos dados você de– seja filtrar na lista.

6. **Opcional:** Crie uma lista filtrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em **Selecione colunas** determine quais colunas serão exibidas na lista excluindo todos os campos que você não deseja que apareçam.

b. Forneça condições para filtrar a lista.

(Optional) Para adicionar mais de uma condição, selecione **Novo conjunto de condições** .

Por exemplo, se você quiser criar uma lista de itens vulneráveis ativos para um scanner que deseja monitorar, poderá inserir as condições **[Ativo][is][true]** e. **[Origem][contém][scanner-name]** .

c. Selecione **Criar**.
Sua nova lista será exibida.

Nota: Se você sair do módulo de lista, a lista exibida ao sair será a lista exibida ao retornar. Para excluir as listas personalizadas que você cria, com a lista exibida, à direita do painel, selecione o ícone de engrenagem e selecione **Excluir** .

7. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista.

Tarefa	Descrição
Clique em Minhas listas	Crie novas listas e exiba as listas que você criou. No modal exibido, crie outra versão de uma lista existente ou uma nova. As listas que você cria são exibidas na guia Minha lista. Para excluir uma lista, com a lista exibida, na extrema direita da página, clique no ícone de engrenagem.
Atribua registros de tarefa de correção a você mesmo	Na guia Listas com **Atribuído ao meu grupo** Selecionado, clique em um registro de tarefa de correção (VUL) para abri-lo. No registro exibido, clique em **Atribuir a mim** . Esta opção só estará disponível se uma tarefa de correção ainda não estiver atribuída a você.
Abrir uma tarefa de correção (VUL)	Com um registro de tarefa de correção exibido, clique em um item de lista relacionado para abrir e exibir os seguintes detalhes: ○ Visão geral - Exibir o andamento da correção e outros detalhes da tarefa de correção. ○ Soluções - Exiba as soluções preferenciais e potenciais que você pode usar para corrigir a vulnerabilidade. Na guia Soluções, os itens da lista relacionada secundários mostram as soluções preferenciais e as possíveis soluções. ○ Detalhes - Mais informações de visão geral, incluindo a vulnerabilidade associada. Você pode editar esses campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	○ Solicitações de mudança - Exiba as solicitações de mudança associadas ao registro. ○ Aprovações solicitadas - Exiba as aprovações solicitadas. Se não houver aprovações de solicitação de mudança, este item de lista relacionado não será exibido. ○ Aprovações de mudança de estado - Exiba as solicitações de falso positivo e de exceção associadas a este registro. Se não houver solicitações, este item de lista relacionado não será exibido. Os registros abertos permanecem exibidos como guias até que você os feche. Consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI para o que você pode fazer a partir do registro da tarefa de correção.
Abra um registro de item vulnerável (VIT)	Com um registro de item vulnerável exibido, clique em um item da lista relacionada para abrir e exibir os seguintes detalhes: ○ Visão geral - O ativo afetado, a vulnerabilidade associada, a detecção inicial e outros detalhes sobre o estado e a data de destino. ○ Detalhes - Mais informações de visão geral, incluindo a solução preferencial, se disponível. Você pode editar esses campos. ○ Detecções - Informações encontradas pela primeira vez, pela última vez encontradas, endereço IP, porta, protocolo e prova, se disponíveis. ○ Serviços afetados - Criticalidade comercial, grupo de suporte e serviço ○ Tarefas de correção - As tarefas de correção às quais este VI está associado. Os registros de VIT abertos permanecem exibidos como guias até que você os feche. Consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI para o que você pode fazer a partir do registro da tarefa de correção.
Defina filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Por exemplo, em uma lista de itens vulneráveis selecionada, você pode preferir classificar a coluna de classificação de risco para que somente itens críticos sejam exibidos.
Filtre itens ou corresponda itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ○ Mostrar correspondência - Exibe somente itens que correspondem à célula selecionada na coluna. ○ Descartar - Filtre os itens da coluna que correspondem à célula selecionada na coluna.
Na exibição de lista, à esquerda da coluna Número com uma lista exibida, passe o mouse sobre uma linha e clique no ícone de informações pequeno (i) de um registro.	Os detalhes sobre os registros são exibidos no painel lateral direito da página.

Use registros no Espaço de correção de problemas de TI

Use registros para ajudá-lo a exibir o andamento da correção e o impacto de itens vulneráveis em seus ativos.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Procedimento

1. Em seu ServiceNow AI Platform instância, navegue até **Espaços** > **Espaço de correção de TI**.
   A página principal inicial da Página inicial é exibida.
2. Navegue até um registro de item vulnerável e abra-o na página principal inicial ou na exibição de lista.

   A guia de detalhes inclui informações no cabeçalho do formulário na parte superior relacionadas à natureza da vulnerabilidade, por exemplo, CVE-2013-5014 detectado no LINUX-DAL-4331 . No cabeçalho do formulário, os valores de Estado, classificação de risco e data de destino de correção são exibidos.
3. Consulte a tabela a seguir para obter as ações de IU que você pode executar no registro da tarefa de correção.

Tarefa	Descrição
Clique em um link de Itens relacionados	○ Visão geral - Exibir detalhes como estado, classificação de risco, pontuação de risco, origem, última localização, status de correção, vulnerabilidade associada,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	item de configuração afetado e informações de detecção inicial. ○ Detalhes - Mais informações de visão geral, incluindo a solução preferencial. Você pode editar esses campos. ○ Detecções - Exiba informações de detecção importadas de seus scanners. ○ Serviços afetados - Exibe os serviços afetados pela vulnerabilidade. ○ Tarefas de correção - Exiba as outras tarefas de correção associadas a este item vulnerável. Os registros abertos da VIT permanecem exibidos como guias nas guias de registro até que você os feche.
Clique em um link para abrir um registro	Na lista exibida em registros abertos nos links Itens relacionados, exiba mais detalhes sobre as tarefas de correção, detecções e serviços afetados.
Clique em uma ação de IU	○ Atribuir a mim - Esta opção só será exibida se a tarefa de correção ainda não estiver atribuída a você. ○ Marcar como falso positivo - Informe quando um scanner encontra uma vulnerabilidade, mas você determina que não existe nenhuma vulnerabilidade. Envie uma solicitação. ○ Se o item vulnerável for atribuído a você, você poderá verificar novamente o VI ○ Resolver - Resolve este item vulnerável. As tarefas de correção associadas são transferidas para Resolvidas quando todos os seus VIS são resolvidos. ○ Exceção de solicitação - Se uma data de destino for aprovada e você souber que precisa de mais tempo para resolver a vulnerabilidade, envie uma solicitação. ○ Salvar - Salva todas as mudanças e atualize o registro.
Adicione uma anotação de trabalho ou anexe um arquivo	Na extrema direita da tela, clique em **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.
Defina filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Por exemplo, com o item relacionado Detecções selecionado, você pode preferir classificar a coluna para que somente as detecções encontradas pela última vez em uma determinada data sejam exibidas.
Filtre itens ou corresponda itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ○ Mostrar correspondência - exibe somente itens que correspondem à célula selecionada na coluna. ○ Descartar - Filtre os itens da coluna que correspondem à célula selecionada na coluna.

Crie uma tarefa de correção manualmente no Espaço de correção de problemas de TI

A partir da v25.0.4 de Resposta a vulnerabilidades, Você pode criar tarefas de correção manualmente nas listas Itens vulneráveis do host, Itens vulneráveis da aplicação, Itens vulneráveis do contêiner e Resultados de teste de configuração na página Lista de Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.write_assigned ou sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_write_assigned ou sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.writer_assigned ou sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI** > **Lista**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis da aplicação
   - Itens vulneráveis de contêiner
   - Resultados de testes de configuração
3. Marque a caixa de seleção dos registros que você deseja atualizar e selecione Itens selecionados Opção no campo Seleção de registro no modal Criar tarefa de correção.
4. Selecione **Criar tarefa de correção** .
5. No modal Criar tarefa de correção, preencha os detalhes a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar modal de tarefa de correção

Campo	Descrição
Seleção de registro	**Itens selecionados** Atualiza somente os registros selecionados.
Descrição resumida	Breve anotação sobre as tarefas de correção.
Critérios de agrupamento	As opções são: ○ **Grupo de atribuição** : Registros com o mesmo grupo de atribuição são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e item de configuração** : Registros com o mesmo grupo de atribuição e item de configuração são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e vulnerabilidade** : Registros com o mesmo grupo de atribuição e vulnerabilidade são agrupados em uma tarefa de correção. ○ **Grupo de atribuição e classificação de risco** : Registros com o mesmo grupo de atribuição e classificação de risco são agrupados em uma tarefa de correção.
Gerenciamento de registros em outras tarefas de correção	As opções são: ○ **Ignorar registros para novas tarefas de correção** Nenhuma ação é realizada nos registros que fazem parte de outras tarefas de correção. ○ **Mover para novas tarefas de correção** : Os registros que fazem parte de outras tarefas de correção são transferidos para novas tarefas de correção. ○ **Mantenha as tarefas de correção atuais e novas** : Os registros que fazem parte de outras tarefas de correção são mantidos em tarefas de correção antigas e novas.

6. Selecione **Criar tarefa de correção** .

Resultado

As tarefas de correção são criadas com base nos critérios de agrupamento. Uma notificação por e-mail é enviada aos responsáveis pela correção no grupo de atribuição, informando-os que uma tarefa de correção foi criada e atribuída ao grupo. Para obter exemplos de como as tarefas de correção são criadas com base nos critérios de agrupamento e critérios de gestão de registros, consulte Exemplos de criação de tarefa de correção no Espaço do gerente de vulnerabilidade e. Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use registros de tarefa de correção no Espaço de correção de problemas de TI

As tarefas de correção são criadas e atribuídas automaticamente a partir dos esforços de correção. As equipes DE TI e os responsáveis pela correção podem exibir tarefas de correção no Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Quando gerentes e analistas de vulnerabilidades criam esforços de correção para orientar a correção, as tarefas de correção são criadas automaticamente e atribuídas às equipes DE TI com base no grupo associado aos registros em um esforço de correção.

Veja os ICs vulneráveis atribuídos a você e aos seus grupos que têm vulnerabilidades neles no **ICs vulneráveis** Na guia ou na lista ICs vulneráveis atribuídos a você e ao seu grupo na exibição de lista.

Procedimento

1. Em seu ServiceNow AI Platform instância, navegue até **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
   A página principal inicial da Página inicial é exibida.
2. Na seção Tarefas de correção, clique em uma tarefa de correção para abri-la.
3. **Opcional:** Como alternativa, você pode clicar no ícone Lista no canto superior esquerdo da página inicial para ver todas as tarefas de correção (VULs, AVULs, CVULs e CRGs) e registros (VITs, AVITs, CVITs e TRs) atribuído a você e aos seus grupos.
   Para obter mais informações sobre como usar a exibição de lista, consulte Crie uma lista no Espaço de correção de problemas de TI.
4. Na página inicial ou na exibição de lista, clique em uma tarefa de correção para abri-la.

   Em **Detalhes** , você pode atualizar algumas das informações no registro, como grupo de atribuição, estado, descrição resumida e assim por diante. Clique em **Salvar** para aplicar suas mudanças.
5. Consulte a tabela a seguir para obter as ações de IU que você pode executar a partir do registro da tarefa de correção.

Tarefa	Descrição
Clique em um link de Itens relacionados	○ Visão geral - Exiba o andamento da correção com % de VIS corrigidos, o estado, a classificação de risco, o grupo de atribuição, ICs afetados e outros detalhes da tarefa. Para ver os ICs afetados, consulte a imagem após a tabela. ○ Soluções - Exiba as soluções preferenciais e potenciais que você pode usar para corrigir a vulnerabilidade. No registro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	que é exibido, os itens da lista relacionada secundários mostram soluções preferenciais e possíveis soluções. Veja as imagens abaixo da tabela. ○ Detalhes - Mais informações de visão geral, incluindo a vulnerabilidade associada. Você pode editar esses campos. ○ Solicitações de mudança - Exiba as solicitações de mudança associadas ao registro. ○ Aprovações solicitadas - Exiba os envios de solicitações de mudança. Se não houver solicitações de aprovação de solicitação de mudança, este item de lista relacionado não será exibido. ○ Aprovações de mudança de estado - Exiba as solicitações de falso positivo e de exceção associadas a este registro. Se não houver solicitações, este item de lista relacionado não será exibido. Os registros abertos permanecem exibidos como guias até que você os feche.
Clique em um link para abrir um registro	Na lista exibida em registros abertos nos links Itens relacionados, exiba mais detalhes sobre os registros , As vulnerabilidades associadas, ICs afetados (ativos), dados de detecção, serviços afetados, e registros associados .
Clique em uma ação de IU	○ Atribuir a mim - Esta opção só será exibida se a tarefa de correção ainda não estiver atribuída a você. ○ Marcar como falso positivo - Envie uma solicitação se, por exemplo, um scanner encontrar uma vulnerabilidade, mas você determinar que não existe nenhuma vulnerabilidade. ○ Criar mudança - Você pode criar uma nova solicitação de mudança ou adicionar esta tarefa de correção a uma solicitação de mudança existente. ○ Tarefa dividida - Identifique um subconjunto de VIS que você deseja incluir em uma nova tarefa de correção ○ Exceção de solicitação: Envie uma solicitação se uma data de destino for aprovada e você souber que precisa de mais tempo para resolver a vulnerabilidade. ○ Resolver - Resolve este RT. A tarefa de correção faz a transição para Resolvido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	e todas as suas transições de VIS para Resolvido. ○ Salvar - Salva todas as mudanças e atu–alize o registro.
Adicione uma anotação de trabalho ou anexe um arquivo	Na extrema direita da tela, clique em **Atividade** (ícone de iluminação) e insira uma anotação de tra-balho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.
Defina filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu vertical de três pontos para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, com o item relacionado à Vi–são geral selecionado, você pode preferir classificar a coluna de classificação de ris–co para que somente os itens críticos se–jam exibidos.
Filtre uma coluna por uma linha selecionada	Selecione uma célula em uma coluna e refine os da-dos exibidos escolhendo uma: ○ Mostrar correspondência - exibe somen–te itens que correspondem à célula sele–cionada na coluna. ○ Filtrar - filtra os itens da coluna que cor–respondem à célula selecionada na colu–na.

A guia Soluções em uma tarefa de correção de host mostra informações de soluções preferenciais e potenciais que melhor correspondem à vulnerabilidade associada à tarefa de correção. As soluções são patches que suas equipes DE TI aplicam para resolver vulnerabilidades.

Se a aplicação Gestão de soluções de vulnerabilidade estiver instalada, *Soluções preferenciais* são as soluções de maior substituição que são aplicadas a itens vulneráveis. A lista de soluções é baseada nos itens vulneráveis na tarefa de correção do host.

Possíveis soluções são a lista de todas as soluções disponíveis para Vits em uma tarefa de correção de host.

Você pode exibir os ICs (ativos) afetados por esta vulnerabilidade na tarefa de correção navegando até **Visão geral** > **ICs afetados**.

Atribua uma tarefa de correção ou um registro a si mesmo no Espaço de correção de problemas de TI

Atribua uma tarefa de correção (VUL, avul, CVUL ou CRG) ou registro (VIT, AVIT, CVIT ou TR) a si mesmo na página Lista em Espaço de correção de problemas de TI espaço.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI** > **Lista** > **Tarefas de correção** > **Atribuído ao meu grupo**.
2. Abra uma tarefa de correção (VUL, avul, CVUL ou CRG) na lista Tarefas de correção.
3. Nos botões de ação de IU à direita, clique em **Atribuir a mim** .

   . **Atribuir a mim** o botão só estará disponível se o registro ainda não estiver atribuído a você.

   A tarefa de correção é exibida na lista Atribuído a mim em Tarefas de correção.
4. Você também pode atribuir um registro (VIT, AVIT, CVIT ou TR) a si mesmo seguindo as mesmas etapas de um registro aberto.
   . **Atribuir a mim** o botão só estará disponível se o registro ainda não estiver atribuído a você.

Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI

As melhorias a seguir foram adicionadas às tarefas de correção com a versão 16,1 do Resposta a vulnerabilidades aplicação.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

A função itil ou cmdb_read também será necessária se você quiser exibir dados de IC nos espaços de trabalho.

Por Que e Quando Desempenhar Esta Tarefa

Consulte os itens de configuração (ICs) atribuídos a você que têm vulnerabilidades neles. Clique em **ICs afetados** cartão de pontuação. Clique na lista Filtro no canto superior esquerdo para alternar entre **Atribuído a mim** e. **Atribuído aos meus grupos** . Na exibição de lista, clique nos links.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
   A página principal inicial da Página inicial é exibida.
2. Como alternativa, você pode exibir essas listas nos links na exibição de lista ou navegando até seus módulos, por exemplo, **Tudo** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
3. Escolha um para continuar.
   Dependendo do que estiver selecionado na alternância de filtro, exiba as listas dos seguintes registros atribuídos a você ou a você e aos seus grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Tarefas de correção atribuídas	Tarefas de correção (RT). Para obter mais informações sobre as ações que você pode executar de um RT, consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI.
Solução preferencial no VIS	Registros (Vits) que têm soluções preferenciais mapeadas para eles. Se a aplicação Gestão de soluções de vulnerabilidade estiver instalada, as Soluções preferenciais serão as soluções de maior substituição aplicadas aos registros. A lista de soluções é baseada nos registros no registro da tarefa de correção. Para ver o que você pode fazer a partir de registros de solução, consulte Use registros de tarefa de correção no Espaço de correção de problemas de TI.
ICs afetados	(IC)s com vulnerabilidades. Após o preenchimento inicial, este cartão de pontuação mostra contagens atualizadas de ICs vulneráveis após a adição de novos VIS com vulnerabilidades ou quando há mudanças de estado nos VIS existentes. Consulte as etapas a seguir para saber como exibir este registro e o que você pode fazer nesta lista.

4. Clique em **ICs afetados** cartão de pontuação.

   A lista de registros de IC é exibida.

5. Clique em um item de configuração para abrir seu registro.
   O registro é exibido.

   As listas relacionadas permitem exibir detalhes e vários registros associados. Os novos dados disponíveis neste registro com esta versão incluem:

   - Uma linha do tempo que mostra a atividade recente neste registro.
   - Todas as solicitações de mudança associadas a este IC.
   - Navegue facilmente até cartões de pontuação e exiba as tarefas de correção, os itens vulneráveis e as soluções preferenciais associadas a este IC.
   - Você pode navegar até os cartões de pontuação e exibir os patches preferenciais associados a este IC. Patches preferenciais são os patches associados aos itens vulneráveis. A guia Patches na lista relacionada exibe os patches instalados e ausentes para os ICs.
   - Informações sobre o IC que incluem Classe, Local, Conectado com a Internet, Ambiente e Programação de manutenção.

Crie uma solicitação de mudança no Espaço de correção de problemas de TI

Em uma tarefa de correção (VUL, avul, CVUL ou CRG), crie uma solicitação de mudança. Como alternativa, adicione uma tarefa de correção a uma solicitação de mudança existente.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Nota: A função ITLI será necessária se você quiser enviar solicitações de mudança do Espaço de correção de problemas de TI.

Por Que e Quando Desempenhar Esta Tarefa

Pode haver vários motivos pelos quais você deseja criar uma solicitação de mudança para uma tarefa de correção. Geralmente, é porque sua investigação requer intervenção manual para corrigir as vulnerabilidades.

Para obter mais informações sobre as solicitações de mudança e como criar solicitações de mudança no ambiente clássico, consulte Gestão de mudanças para Resposta a vulnerabilidades.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Selecione o ícone Lista.
3. Na página Lista, na lista Tarefas de correção, localize uma tarefa de correção (VUL, avul, CVUL ou CRG) para a qual você deseja criar uma solicitação de mudança.
4. Nos botões de ação de IU à direita, expanda a lista e escolha um:
   - Clique em **Criar mudança**
   - **Adicionar a uma mudança existente**
5. Para criar uma nova solicitação de mudança, no modal exibido, preencha os campos.
   Para obter informações sobre os campos de formulário, consulte Campos de formulário Criar solicitação de mudança.
6. Selecione **Criar solicitação de mudança** .
   O registro da tarefa de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada com sucesso.

   Clique no link relacionado Solicitações de mudança em um registro para exibir todas as solicitações de mudança associadas ao registro.
7. Como alternativa, para adicionar esta tarefa de correção a uma solicitação de mudança existente, siga estas etapas.

   a. Clique na seta para baixo para expandir a lista no **Criar mudança** botão.

   b. Selecione **Adicionar à mudança existente** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. No modal exibido, clique no ícone de pesquisa para exibir a lista de solicitações de mudança existentes.

d. Para adicionar condições à lista para focar a lista de solicitações de mudança, no canto superior direito do modal, clique no ícone de filtro (funil).

e. No novo painel exibido, clique em **Exibição avançada** .

f. Use o Construtor de condições para criar suas condições.

g. Selecione **Atualizar**.

h. Na lista, clique em uma solicitação de mudança para selecioná-la.
Um modal atualizado é exibido com sua escolha.

i. **Opcional:** No modal, marque a caixa de seleção Adicionar ICs à CR para adicionar itens de configuração de todos os itens vulneráveis ativos à solicitação de mudança.

j. Selecione **Adicionar mudança** .
O registro de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada e enviada com sucesso para aprovação.

- Clique em **Exibir mudança** Link na mensagem para abrir o registro de Solicitação de Mudança (CHG).
- Selecione **Solicitações de mudança** link do menu de item relacionado no registro da tarefa de correção para exibir todas as solicitações de mudança associadas ao registro.

Como alternativa, no ambiente clássico, navegue até **Autoatendimento** > **Minhas solicitações**. Depois que você enviar a mudança e ela for implementada, se a sincronização de estado estiver habilitada, a tarefa de correção será movida automaticamente para Resolvido . Para obter mais informações sobre estados e sincronização de estados em solicitações de mudança, consulte Crie uma solicitação de mudança a partir de uma tarefa de correção.

Divida uma tarefa de correção no Espaço de correção de problemas de TI

Em uma tarefa de correção (VUL, AVUL, CVUL ou CRG), identifique um subconjunto de registros e crie uma nova tarefa de correção para eles.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Você pode selecionar registros individuais na guia Visão geral de uma tarefa de correção e movê-los para uma nova tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os casos de uso para dividir registros (Vits, AVITs, CVITs ou CTRs) de tarefas de correção existentes em novas tarefas podem incluir os seguintes exemplos:

- Você deseja criar uma solicitação de mudança ou solicitações de mudança para uma tarefa dividida.
- Reatribuir uma tarefa dividida para outro usuário em seu grupo de atribuição.
- Você solicita um adiamento ou exceção para uma tarefa dividida, porque sabe que algumas vulnerabilidades em itens de configuração (ICs) específicos não podem ser corrigidas até a data de destino.

Para obter mais informações sobre solicitações de mudança e dividir uma tarefa de correção no ambiente clássico e para versões de Resposta a vulnerabilidades anterior à v15.0, consulte Divida uma tarefa de correção.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Abra uma tarefa de correção (VUL, avul, CVUL ou CRG) na página inicial ou na página Lista.
3. Na guia Visão geral, selecione os registros (Vits, AVITs, CVITs ou CTRs) que você deseja mover para uma nova tarefa de correção.
4. Clique em **Tarefa dividida** .
5. Na caixa de diálogo exibida, o número de registros (Vits, AVITs, CVITs ou CTRs) selecionados na lista é exibido.
6. Clique em **Tarefa dividida** novamente.
   Uma mensagem de confirmação é exibida com um link para a nova tarefa de correção.

   Como alternativa, você pode usar o Construtor de condições para filtrar registros (Vits, AVITs, CVITs ou CTRs).
7. Localize uma tarefa de correção que você deseja dividir.
8. Nos botões de ação de IU à direita, clique em **Tarefa dividida** .
   Depois de alguns momentos, o construtor de condições é exibido.
9. No modal exibido, use o construtor de condições para identificar o subconjunto de registros (Vits, AVITs, CVITs ou CTRs) desejado . adicione a uma nova tarefa de correção.
10. Clique em **Tarefa dividida** .
    Se uma mensagem for exibida informando que nenhum registro corresponde às suas condições, você deverá ajustar seus critérios e clicar em **Tarefa dividida** novamente. Edite o campo Descrição resumida conforme necessário. Este campo pode ajudar você a encontrar sua nova tarefa de correção depois que ela é criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se os registros corresponderem às suas condições, o número de registros correspondentes será exibido em uma mensagem.

11. **Opcional:** Clique em **Visualizar itens** link para exibir os registros que correspondem às condições do filtro.
A nova tarefa de correção é exibida como uma nova guia.

Solicite um falso positivo para um item vulnerável ou corrija a tarefa

Indique uma solicitação falso-positiva para item vulnerável ao host (VIT), item vulnerável à aplicação (AVIT), item vulnerável ao contêiner (CVIT) ou tarefa de correção (VUL, avul, CVUL ou CRG) no Espaço de correção de problemas de TI. Um falso-positivo é uma condição em que um scanner relata incorretamente que existe uma vulnerabilidade no sistema devido a situações como uma classificação incorreta, lógica inadequada ou um algoritmo no scanner.

Antes de Iniciar
Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa
Para obter informações sobre como solicitar um falso positivo para um conjunto de resultados de testes, consulte Solicite um falso positivo para um conjunto de resultados de testes.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Ícone Selecionar lista ( ).
3. Selecione a tarefa de correção (VUL, avul, CVUL ou CRG) ou o item vulnerável (VIT, AVIT ou CVIT).
4. Selecione **Marcar como falso positivo** .
5. Insira informações sobre a solicitação.
6. Selecione **Aprovação da solicitação** .
7. Forneça informações adicionais sobre sua solicitação ao aprovador e selecione **Enviar** .

> **Nota:** O modal Responder questionário aparece somente quando **Habilite o questionário para marcar falso-positivo** Está marcada no formulário Configuração de gestão de exceções. Para obter mais informações, consulte Configure a Gestão de exceções para Resposta a vulnerabilidades, Configure a Gestão de exceções para Resposta a vulnerabilidades de aplicações, Configure a Gestão de exceções para Contêiner de Resposta a vulnerabilidades e Configure a Gestão de exceções para Conformidade de configurações.

Resultado
O estado do item vulnerável (VIT, AVIT ou CVIT) ou da tarefa de correção (VUL, AVUL ou CVUL) muda para Em revisão.

Sua solicitação é enviada para aprovação e o aprovador recebe uma notificação por e-mail sobre sua solicitação.

Você receberá uma notificação por e-mail após a aprovação ou rejeição de sua solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

No Espaço de correção de TI, na página Lista, navegue até **Solicitações de exceção** > **Minhas solicitações** E abra o registro de aprovação de mudança de estado correspondente (nº VCA) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado da aprovação	Registro (VIT, AVIT ou CVIT)	Tarefa de correção (VUL, avul, CVUL ou CRG)
Aprovadas	O Estado do registro muda para Encerrado com Motivo como Falso positivo.	O Estado da tarefa de correção muda para Encerrado com Motivo como Falso positivo. O estado é revertido para os registros na tarefa de correção de acordo. Navegue até a guia Detalhes de uma tarefa de correção e defina a data de expiração para falso positivo em **Até** se necessário. A tarefa de correção é revertida para o estado Aberto após a data especificada e o estado é revertido para os resultados do teste.
Rejeitado	O estado do registro não muda.	O estado da tarefa de correção e seus registros são revertidos para o estado anterior.

Em **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da solicitação de falso positivo.

Tópicos relacionados

Falso-positivo visão geral

Solicite um falso positivo para um conjunto de resultados de testes

Gere uma solicitação falso-positivo para um conjunto de resultados de teste em uma tarefa de correção no Espaço de correção de problemas de TI.

Por Que e Quando Desempenhar Esta Tarefa

As seguintes condições devem ser atendidas para que você solicite um falso positivo para um conjunto de resultados de teste em uma tarefa de correção:

- Versão 22,0 de Resposta a vulnerabilidades deve ser instalado.
- Pelo menos um resultado de teste selecionado deve estar no estado Ativo
- A tarefa de correção deve ter pelo menos dois resultados de teste
- Pelo menos um resultado de teste está desmarcado

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Selecione o ícone de Lista ( ).
3. Na página Lista, selecione Conformidade de configurações Tarefa de correção.
4. Na lista relacionada Visão geral, na guia Resultados de teste, selecione os resultados de teste que você deseja marcar como falso-positivo.
5. Selecione **Marcar como falso positivo** Na guia Resultados do teste de configuração.
6. Na caixa de diálogo exibida, insira informações sobre a solicitação e selecione **Aprovação da solicitação** .
7. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação ao aprovador e selecione **Enviar** .

> **Nota:** O modal Responder questionário aparece somente quando **Habilite o questionário para marcar falso-positivo** Está marcada no formulário Configuração de gestão de exceções. Para obter mais informações sobre como um questionário é configurado, consulte Configure a Gestão de exceções para Conformidade de configurações.

Resultado

Os resultados de teste selecionados são movidos para uma nova tarefa de correção e sua solicitação é enviada para aprovação. O número da tarefa aparece em **Fluxo de atividades** Da tarefa de correção antiga. O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Você receberá uma notificação por e-mail sobre a aprovação ou rejeição de sua solicitação. Em **Fluxo de atividades** de um resultado de teste ou tarefa de correção, você pode exibir todo o fluxo de trabalho da solicitação de falso-positivo.

O que Fazer Depois

1. Em Espaço de correção de problemas de TI, Na página Lista, navegue até **Solicitações de exceção** > **Minhas solicitações**.
2. Abra o registro de aprovação de mudança de estado correspondente (nº VCA) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado da aprovação	Resultado
Aprovadas	O Estado da nova tarefa de correção muda para Encerrado com Motivo como Falso positivo.
Rejeitado	O estado da nova tarefa de correção muda para Aberto.

3. Depois que a solicitação for aprovada, navegue até a guia Detalhes da nova Tarefa de correção e defina a data de expiração para falso-positivo em **Até** se necessário.

   A tarefa de correção será revertida para o estado Aberto após a data especificada e o Estado será revertido para os resultados do teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicite uma exceção no Espaço de correção de problemas de TI

Solicite uma exceção para o item vulnerável do host (VIT), o item vulnerável da aplicação (AVIT), o item vulnerável do contêiner (CVIT) e a tarefa de correção (VUL, AVUL, CVUL ou CRG) do Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Ou você pode determinar que uma tarefa de correção não pode ser resolvida até a data de destino. Quando sua correção não pode estar em conformidade com um gerenciamento de vulnerabilidades publicado ou política de segurança, padrão ou diretriz, você pode solicitar uma exceção.

Você pode solicitar exceções para tarefas de correção (VUL, AVUL, CVUL ou CRG) e itens vulneráveis (VIT, AVIT ou CVIT) do Espaço de correção de problemas de TI atribuídos a você.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18,0 , você pode solicitar exceções para itens de vulnerabilidade da aplicação e itens de vulnerabilidade do contêiner.

Para obter mais informações sobre como solicitar exceções no ambiente clássico, consulte Solicite uma exceção para uma tarefa de correção.

Procedimento

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Selecione o ícone Lista.
3. Na lista Tarefas de correção, abra uma tarefa de correção (VUL, avul, CVUL ou CRG) ou registro (vits, AVITs ou CVITs) para o qual você deseja solicitar uma exceção.
4. Nos botões de ação de IU à direita, clique em **Exceção de solicitação** .
5. Na caixa de diálogo exibida, preencha a data de término da exceção, selecione um motivo na lista e adicione outras informações necessárias.
6. Clique em **Exceção de solicitação** .
7. Em **Responder ao questionário** modal, responda às perguntas e clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Responder ao questionário** o modal aparece somente quando **Habilite o questionário para solicitar exceção** a caixa de seleção está marcada em **Configuração da Gestão de exceções** formulário.

Uma mensagem é exibida informando que sua solicitação foi enviada com sucesso para aprovação.

Uma solicitação de exceção para uma tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de nível 2.

- A tarefa de correção ou o registro faz a transição para Em revisão enquanto a solicitação de exceção está aberta.
- A tarefa de correção ou o registro muda para Adiado se a solicitação for aprovada.
- O registro de solicitação de exceção (nº VCA) é encerrado depois que sua solicitação de exceção é aprovada.

Para exibir o status de suas solicitações de aprovação, em Solicitações de exceção na página Lista, clique em **Minhas solicitações** . O número da solicitação (nº VCA) é exibido quando você abre o registro ou a tarefa de correção na lista.

- Se a solicitação for rejeitada, o registro de solicitação (nº VCA) será exibido **Rejeitado** Na coluna Estado de aprovação na exibição de lista em Minhas solicitações.
- Você deverá enviar uma nova solicitação de exceção se ainda quiser adiar este item.

Solicite uma exceção usando GRC: Gestão de políticas e conformidade em Espaço de correção de problemas de TI

Solicite uma exceção de política para o item vulnerável do host (VIT), item vulnerável da aplicação (AVIT), item vulnerável do contêiner (CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG) do Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para Itens vulneráveis do host (Vits)
- sn_vul.app_security_champion para Itens vulneráveis à aplicação (AVITs)
- sn_vul_container.remediation_owner para Itens vulneráveis do contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de teste de configuração (CTRs)

Por Que e Quando Desempenhar Esta Tarefa

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de teste	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. No navegador de aplicações, selecione o ícone Lista ( ).
3. Na página Lista, em Itens vulneráveis ao host, Itens vulneráveis à aplicação, Itens vulneráveis ao contêiner ou Tarefas de correção (VUL, AVUL, CVUL ou CRG), selecione o registro para o qual você deseja solicitar uma exceção.
   O registro selecionado deve estar no estado Aberto, Em investigação ou Aguardando implementação.
4. Selecione **Exceção de solicitação** botão.
5. No formulário, preencha os campos.
   Para mais informações sobre campos de formulário, consulte Campos de formulário Solicitar exceção para exceções de política.
6. Selecione **Exceção de solicitação** .
7. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar** .

   Nota: O modal Responder questionário aparece somente quando os detalhes do questionário são adicionados ao respectivo registro de integração.

   É exibida uma mensagem informando que sua solicitação foi enviada com sucesso para aprovação.

   Para obter mais informações sobre a Integração de exceção de política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Solicitar redução de risco para um item vulnerável ou tarefa de correção

Solicite uma redução no risco de um item vulnerável do host ou uma tarefa de correção no Espaço de correção de problemas de TI.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
A partir de v21.0 de Resposta a vulnerabilidades, você pode solicitar redução de risco somente para os seguintes itens :

- . tarefa de correção apenas se todos os itens vulneráveis estiverem associados a. . Mesma entrada de vulnerabilidade comum (CVE) Independentemente de sua redução de risco estar habilitada para CVEs.
- Um terceiro (TPE) para o qual a redução de risco está habilitada.

Nota: O recurso Controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Selecione o ícone de Lista ( ).
3. Na página Lista, abra um item vulnerável do host ou uma tarefa de correção.
4. Selecione o ícone Mais opções e selecione **Exceção de solicitação** .
5. No formulário Exceção de solicitação, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter uma descrição dos valores de campos, consulte Formulário Solicitar exceção para redução de risco.

6. Selecione **Exceção de solicitação** .
7. Se um modal Responder questionário for exibido, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar** .

> **Nota:** O modal Responder questionário aparece somente quando o questionário está habilitado para gestão de exceções. Para obter mais informações, consulte Configure a Gestão de exceções para Resposta a vulnerabilidades.

Resultado

Uma mensagem é exibida informando que sua solicitação foi enviada com sucesso para aprovação. Uma notificação é enviada ao aprovador sobre sua solicitação.

- Se sua solicitação for para um adiamento e redução de risco:
  - Duas aprovações de mudança de estado (nº VCA) são criadas para adiamento e redução de risco.
  - O estado do registro muda para Em revisão.
- Se sua solicitação for somente para redução de risco:
  - Uma aprovação de mudança de estado (nº VCA) é criada.
  - O estado não muda.

Na aprovação ou rejeição da sua solicitação, você receberá uma notificação. Para obter mais informações sobre o processo de aprovação, consulte Aprovar ou rejeitar solicitações no Espaço do gerente de vulnerabilidade.

Para obter mais informações sobre como **Até a data de redução de risco** é atualizado para uma tarefa de correção e item vulnerável quando uma solicitação de redução de risco é aprovada, consulte Impacto dos controles de compensação na pontuação de risco e na data de vencimento.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Desabilite ou habilite a redução de risco para um CVE ou TPE

Adicione um controle de compensação à biblioteca

Impacto dos controles de compensação na pontuação de risco e na data de vencimento

Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Iniciar novas varreduras do Espaço de correção de problemas de TI em seu ServiceNow AI Platform sob demanda.

Novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas com sucesso em seus itens de configuração (ICs).

A nova verificação é compatível com as seguintes integrações no Espaço de correção de problemas de TI. Para obter mais informações, consulte os tópicos a seguir:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Nova verificação Qualys itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho
- Nova verificação Rapid7 itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho
- Nova verificação Tenable.io e. Tenable.sc itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho

Funções necessárias: sn_vul.remediation_owner para Espaço de correção de problemas de TI.

Nova verificação Qualys itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Iniciar novas varreduras no Qualys produto sob demanda do Espaço de correção de problemas de TI em seu ServiceNow AI Platform instância.

Antes de Iniciar

Para iniciar uma nova verificação para Qualys produto do ambiente clássico, consulte Iniciar uma nova verificação para Qualys Vulnerability Integration.

. Qualys os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm essas aplicações como origem, o. **Nova verificação** o botão não está disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto do scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem nos registros de item vulnerável e tarefa de correção após a próxima importação, e. **Nova verificação** Está disponível como uma ação de IU.

Para obter mais informações sobre como configurar seu Qualys scanner, consulte Configurar dispositivos de scanner e. Avançado Qualys configurações e modificações.

- Você pode iniciar novas varreduras sob demanda para itens vulneráveis e tarefas de correção que tenham Qualys produto como a origem do Espaço de correção de problemas de TI em seu ServiceNow AI Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ser do Qualys produto.
- Para iniciar novas verificações no espaço de correção de TI a partir de registros de item vulnerável e tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para Espaço de correção de problemas de TI.
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin no Espaço do Gerenciador de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção atribuída a você e abra-a.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os VIS associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Nova verificação** .

3. No modal Nova verificação, escolha um perfil de opção.
   Um perfil de opção é necessário quando você inicia um Qualys digitalize a partir do ServiceNow AI Platform®. Os perfis de opção contêm Qualys configurações de verificação.

Opção	Descrição
Usar perfil de opção padrão	Este é o perfil de opção definido como padrão para a instância de integração. Você seleciona este perfil ao configurar seu Qualys scanner. Para obter mais informações, consulte Configurar dispositivos de scanner.
Especificar perfil de opção	Na lista de perfis de opção, escolha um perfil a ser usado para a verificação. Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

4. No modal Nova verificação, clique em **Nova verificação da solicitação** .
   A mensagem, A solicitação de verificação está sendo processada é exibido.

5. Clique em **Exibir status** link na mensagem para exibir o andamento da verificação.

   O registro de verificação (nº VSCAN) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária será concluído.
   - A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração associado e a vulnerabilidade, o estado do VI e seu status de correção.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro.

   O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida.

   Todos os VIS que fizeram a transição, ou farão a transição, para Encerrado/Fixo são importados com a próxima importação programada do Qualys integrações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nova verificação Rapid7 itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Iniciar novas varreduras no Rapid7 Produto sob demanda do Espaço de correção de TI em seu ServiceNow AI Platform instância.

Antes de Iniciar

Para iniciar uma nova verificação do produto no ambiente clássico, consulte Iniciar uma nova verificação para Rapid7 Integração de vulnerabilidades. Este tópico também inclui informações sobre como programar verificações com os parâmetros de integração no Rapid7 instância de integração.

. Rapid7 os scanners são desativados por padrão no Resposta a vulnerabilidades aplicação. Se você tentar executar uma nova verificação dos itens vulneráveis ou tarefas de correção que têm Rapid7 aplicação como origem, o. **Nova verificação** o botão não está disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Tudo** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto do scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem nos registros de item vulnerável e tarefa de correção após a próxima importação, e. **Nova verificação** Está disponível como uma ação de IU.

- Você pode iniciar novas varreduras sob demanda para itens vulneráveis e tarefas de correção que tenham Rapid7 InsightVM Produto como a origem do Espaço de correção de TI em seu ServiceNow AI Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ser do Rapid7 produto.
- Para iniciar novas verificações no espaço de correção de TI a partir de registros de item vulnerável e tarefa de correção, esses registros precisam ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para o espaço de correção de TI
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin no Espaço do Gerenciador de vulnerabilidades

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção atribuída a você e abra-a.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os VIS associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Nova verificação** .
3. No modal Confirmar nova verificação, clique em **Nova verificação da solicitação** .
   A mensagem, A solicitação de verificação está sendo processada é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Exibir status** link na mensagem para exibir o andamento da verificação.

   O registro de verificação (nº VSCAN) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária será concluído.
   - A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração associado e a vulnerabilidade, o estado do VI e seu status de correção.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro.

   O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida.

   Todos os VIS que fizeram a transição, ou farão a transição, para Encerrado/Fixo são importados com a próxima importação programada do Rapid7 integrações.

Nova verificação Tenable.io e. Tenable.sc itens vulneráveis do Resposta a vulnerabilidades espaços de trabalho

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Iniciar novas varreduras no Tenable.io e. Tenable.sc Produtos sob demanda do Espaço de correção de TI em seu ServiceNow AI Platform instância.

Antes de Iniciar

Para iniciar uma nova verificação para Tenable.io e. Tenable.sc produtos do ambiente clássico de Resposta a vulnerabilidades, consulte Iniciar uma nova verificação para Tenable.sc integração e. Iniciar uma nova verificação para Tenable.io integração.

Para executar novas varreduras do seu ServiceNow AI Platform, Você precisa de suas credenciais do Tenable. Para obter mais informações sobre como configurar seu Tenable.io e. Tenable.sc E importação de suas credenciais da Tenable, consulte Configure a Integração de vulnerabilidades do Tenable usando o Assistente de configuração.

- Você pode iniciar novas varreduras sob demanda para itens vulneráveis e tarefas de correção que tenham Tenable.io ou Tenable.sc Produto como a origem do Espaço de correção de TI em seu ServiceNow AI Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado** E todos os VIS associados devem ser do Tenable.io ou Tenable.sc produto.
- Para iniciar novas varreduras no Espaço de correção de problemas de TI de itens vulneráveis e registros de tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para Espaço de correção de problemas de TI
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin no Espaço do Gerenciador de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção atribuída a você e abra-a.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os VIS associados a esse registro serão verificados.

2. No canto superior direito de um registro, clique em **Nova verificação** .
   Você será solicitado a escolher a instância ou instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pelo Tenable.io e. Tenable.sc Verificar integrações de credenciais.

3. No modal, clique no ícone de pesquisa.

   No modal Selecione uma credencial de verificação exibido, use os filtros nos cabeçalhos de coluna para selecionar o nome, a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Consulte a tabela a seguir para obter mais informações.

Coluna	Descrição
Nome	Escolha o nome das credenciais desejadas. Passe o mouse sobre o título da coluna. Use o menu vertical de três pontos no título da coluna para filtrar os nomes das suas credenciais.
Instância de integração	Escolha um Tenable.io ou, se for Tenable.sc. Tenable.sc instância de integração da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io ou Tenable.sc são exibidos. Se existir uma VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar. **Nota:** Se você optar por verificar novamente o VIS de um registro de tarefa de correção para uma única instância de integração, somente os VIS ativos associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas, serão verificados.
Tipo	Estas são as credenciais do scanner disponíveis importadas do Tenable.io ou Tenable.sc produtos. Passe o mouse sobre o título da coluna. Use o menu vertical de três pontos no título da coluna para abrir o modal e selecionar os tipos de credencial desejados.

4. No modal de nova verificação atualizado, clique em **Nova verificação da solicitação** .
   A mensagem, A solicitação de verificação está sendo processada é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Exibir status** link na mensagem para exibir o andamento da verificação.

   O registro de verificação (nº VSCAN) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária será concluído.
   - A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração associado e a vulnerabilidade, o estado do VI e seu status de correção.

   . ServiceNow AI Platform® a instância rastreia o status da nova verificação até que ele seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que ocorrer primeiro.

   O tempo limite não interrompe a verificação. O tempo limite se refere a quando ServiceNow AI Platform® o acompanhamento do status da nova verificação foi interrompido, não quando a nova verificação foi interrompida.

   Todos os VIS que fizeram a transição, ou farão a transição, para Encerrado/Fixo são importados com a próxima importação programada do Tenable.io ou Tenable.sc integrações.

Espaço de correção de problemas de TI informações de referência

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados em Espaço de correção de problemas de TI.

Campos de formulário Criar solicitação de mudança

A tabela a seguir mostra os campos e sua descrição no formulário Criar solicitação de mudança.

Campo	Descrição
Tipo de mudança	Normal - Normal é o padrão. Padrão- Dois campos adicionais são exibidos: Categoria de mudança padrão - Selecione uma categoria na lista Modelo de mudança padrão - Selecione um modelo na lista de seleção a ser usado para esta solicitação de mudança Prioridade crítica
Adicionar ICs à solicitação de mudança	O padrão é Habilitado. Se habilitada, a solicitação de mudança adicionará todos os itens de configuração (IC) que pertencem a itens vulneráveis ativos neste esforço

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de correção e serão adicionados a esta solicitação de mudança.
Prioridade	Alto é o padrão. Selecione uma prioridade na lista.
Grupo de atribuição	Por padrão, o grupo de atribuição é obtido do tópico de observação. Clique no ícone de pesquisa e, no modal, escolha outro grupo de atribuição.
Data de término planejada	Clique no ícone de calendário para selecionar uma data de término planejada.
Atribuição a	Por padrão, o usuário atual é atribuído à tarefa de correção. Clique no ícone de pesquisa e, no modal, escolha outro usuário.
Descrição resumida	A descrição resumida é obtida da tarefa de correção. Clique no texto para editá-lo.
Descrição	A descrição é obtida da tarefa de correção. Clique no texto para editá-lo.
Justificativa	A justificativa obtida da tarefa de correção. Clique no texto para editá-lo.
Plano de implementação	Preenchido previamente com informações de solução preferencial, se disponível. Exiba a solução ou insira um plano de justificativa.

Tópicos relacionados

Crie uma solicitação de mudança no Espaço de correção de problemas de TI

Campos de formulário Solicitar exceção para exceções de política

A tabela a seguir mostra os campos que você deve preencher no formulário Exceção de solicitação para exceções de política.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de Gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válida de	Data em que a exceção começa. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até o(a)	Data em que a exceção de política expira e o estado do item vulnerável ou grupo muda de Adiado para Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	Nota: O número de dias em que a exceção de política é válida não pode exceder o valor em **Duração máxima da exceção (dias)** campo definido para a política. Para obter mais informações, consulte Crie uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta exceção está sendo solicitada. Este campo deve ser preenchido pelo responsável pela correção.

Tópicos relacionados

Solicite uma exceção usando GRC: Gestão de políticas e conformidade em Espaço de correção de problemas de TI

Formulário Solicitar exceção para redução de risco

A tabela a seguir mostra os campos que você deve preencher no formulário Exceção de solicitação para solicitações de redução de risco.

Formulário Solicitar exceção

Campo	Descrição
Motivo	Motivo da sua solicitação de exceção. Selecione *Mitigação do controle em vigor* para solicitação de redução de risco. Para ver como adicionar novas opções de motivo, consulte Defina o mapeamento do motivo da política.
Solicitação de adiamento	Derfer o registro. Este campo é selecionado por padrão. **Nota:** Este campo aparece somente quando *Mitigação do controle em vigor* a opção está selecionada em **Motivo** campo.
Solicitação de redução de risco	Permite que você solicite a redução da pontuação de risco. **Nota:** Esta caixa de seleção aparece somente quando *Mitigação do controle em vigor* a opção está selecionada em **Motivo** campo.
Classificação de risco atual	Gravidade atual do risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	Nota: Este campo aparece somente quando **Solicitação de redução de risco** a caixa de seleção está marcada.
Classificação de risco desejada	Nova classificação de risco que você deseja atribuir ao registro. A pontuação de risco mais alta neste intervalo de classificação de risco é aplicada ao registro quando sua solicitação é aprovada. **Nota:** Este campo aparece somente quando **Solicitação de redução de risco** a caixa de seleção está marcada.
Selecione Controles de compensação	Motivo da sua solicitação para reduzir a classificação de risco.
Até	Data em que a solicitação de adiamento ou redução de risco expira. Quando a solicitação de exceção expira: • O registro é revertido para o estado Aberto. • Os controles de compensação expiram. • A pontuação calculada substituirá uma pontuação reduzida.
Observações de justificativas	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

Tópicos relacionados

Solicitar redução de risco para um item vulnerável ou tarefa de correção

Explorar o Espaço de avaliação de vulnerabilidade

O Espaço de avaliação de vulnerabilidades foi projetado para que o gerenciador de eventos de vulnerabilidade execute a avaliação de exposição e gerencie proativamente eventos de vulnerabilidade crítica, especialmente durante os eventos de vulnerabilidade crítica, como um evento de dia zero.

Depois que uma vulnerabilidade crítica é identificada, os gerentes de eventos de vulnerabilidade podem avaliar o possível impacto e o risco associados à vulnerabilidade. Os analistas podem analisar o sistema afetado, as aplicações ou os componentes de rede para entender a gravidade e os possíveis vetores de ataque na organização.

O Espaço de avaliação de vulnerabilidades contém:

Página Avaliação de exposição

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fornece visibilidade detalhada dos ativos expostos a vulnerabilidades e software vulnerável. A funcionalidade de avaliação de exposição fornece:

- Visibilidade dos ativos afetados para vulnerabilidade e software afetado
- Capacidade de executar avaliações independentes para um único CVE ou software vulnerável
- Visibilidade de ativos afetados para CVEs de vulnerabilidades exploradas conhecidas pela CISA
- Visibilidade para exposição de ativos e modelos de descoberta adicionais.
- Capacidade de criar itens vulneráveis

Página Avaliação de vulnerabilidades

A página Avaliação de vulnerabilidades na qual você pode lidar com eventos de crise de vulnerabilidade, da avaliação à resolução, usando o fluxo de trabalho Gestão de crises de vulnerabilidade. O fluxo de trabalho permite rastrear eventos de vulnerabilidade de interesse, analisar o risco associado a eles, executar avaliação de exposição em vários inventários (por exemplo, inventário de instalações de software) e declará-lo como uma crise para compromisso de resposta elevado. Em seguida, você pode associar o registro de avaliação de vulnerabilidade a um incidente de segurança grave e permitir que a equipe de resposta a incidentes de segurança responda à crise.

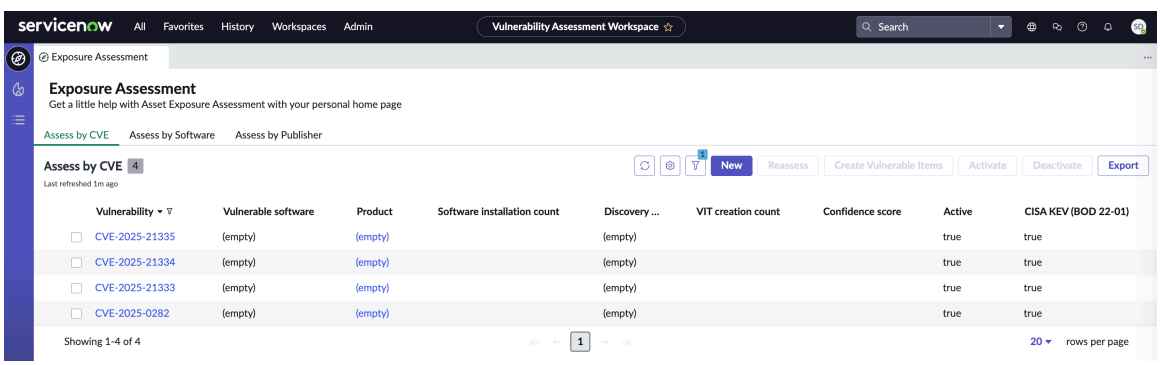
- Crie e modifique avaliações de vulnerabilidade para eventos de vulnerabilidade críticos
- Registre os principais atributos da vulnerabilidade para calcular o risco
- Execute a avaliação de vulnerabilidade para determinar o nível de exposição e a prioridade
- Declare a avaliação de vulnerabilidade como um evento crítico
- Associe a avaliação de vulnerabilidade a um incidente de segurança grave vinculando, propondo ou promovendo a avaliação de vulnerabilidade a um incidente de segurança grave.

Página de lista

A página Lista é composta por uma biblioteca que contém:

- CVEs
- TPEs
- CWEs

A imagem a seguir mostra a página inicial do Espaço de avaliação de vulnerabilidades.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorando a avaliação de exposição

A avaliação de exposição usa a estrutura CPE (Common Platform Enumeration, enumeração de plataforma comum), que faz parte do sistema CVEs (Common Vulnerabilities and Exposures, vulnerabilidades comuns e exposições), para avaliar a exposição a vulnerabilidades de seus ativos ao software de vulnerabilidade. Esta avaliação é realizada usando um modelo de descoberta de software.

Ao empregar um algoritmo de correspondência, os CPEs relevantes são associados e mapeados para o modelo de descoberta de software, permitindo a identificação de possíveis exposições.

Você pode usar a avaliação de exposição por CVE ou software para identificar a exposição a possíveis vulnerabilidades nos seguintes cenários:

- Vulnerabilidades que podem não ser identificadas por scanners tradicionais
- Vulnerabilidades de dia zero antes que o scanner forneça a assinatura para detecção de vulnerabilidades

A avaliação de exposição fornece um aviso antecipado para corrigir essas vulnerabilidades e melhorar a maturidade do programa de gestão de vulnerabilidades.

Pré-requisitos para avaliação de exposição

Versões disponíveis

Aplicação	Versão
Plug-in Gestão de crises de vulnerabilidade	1.0
Resposta a vulnerabilidades	20,0
Resposta a vulnerabilidades Com NVD	1,3
Vulnerability Response integration with CISA	1.2
Integração de Resposta a vulnerabilidades com NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações de NVD.	1,3
Software Asset Management	Plug-in Software Asset Management Foundation ou Software Asset Management Professional plug-in

Casos de uso

Para obter exemplos de como a organização Analistas de vulnerabilidades usaria o espaço Avaliação de exposição a vulnerabilidades, consulte estes casos de uso.

Tipo de avaliação	Uso
Avaliar por CVE	Avalie vulnerabilidades por CVE para obter uma compreensão completa do impacto e da exposição dos sistemas afetados usando Software Asset Management(SAM) e. Descoberta dados. Execute ações de correção imediatas criando Vits manuais e atribuindo-os aos responsáveis pela correção. Avaliar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de avaliação	Uso
	por CVEs é benéfico porque os scanners podem não detectar todos os sistemas afetados, enquanto Descoberta identifica normalmente a maior parte do software na superfície de ataque.
Avaliar por software	Avalie o impacto do software quando o CVE não estiver disponível para identificar o número de ICs em que o software está instalado. Ao avaliar por software, você pode agir proativamente em vulnerabilidades críticas ou de dia zero criando uma VIT manual e atribuindo-a ao responsável pela correção antes que ela seja publicada oficialmente ou antes que os scanners as identifiquem.
Avaliar por fornecedor	Avalie as vulnerabilidades de um fornecedor de software para entender o impacto e a exposição dos sistemas afetados para os CVEs publicados pelo fornecedor dentro de um intervalo de tempo. Avaliar por fornecedor ajuda a avaliar o risco do fornecedor e as vulnerabilidades críticas, permitindo a correção proativa.

Compatibilidade e requisitos do sistema

. Resposta a vulnerabilidades a aplicação está disponível no ServiceNow Store. . Gestão de ativos de software do ITSM A aplicação (com.snc.asset_management) é necessária para o módulo Avaliação de exposição. Este aplicativo gerencia todos os seus ativos e licenças de software e SAM Foundation a versão desta aplicação faz parte do Resposta a vulnerabilidades aplicativo que você baixa do ServiceNow Store.

Importante: A aplicação Avaliação de exposição funciona com os seguintes plug-ins:

- Plug-in Software Asset Management Foundation (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Plug-in Software Asset Management (com.snc.software_asset_management)

Para verificar SAM Foundation a aplicação está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e pesquise por com.snc.asset_management. Se a aplicação não estiver instalada, selecione **Instalar** . . Vulnerabilidade A aplicação Avaliação de exposição requer acesso aos dados do ativo no seu ServiceNow AI Platform® as aplicações de gestão de ativos devem ter dados para referência. A tabela Modelos da Descoberta de software (cmdb_sam_sw_discovery_model) e as Instalações de software (cmdb_sam_sw_install) exigem dados.

Campos de algoritmo correspondentes para modelos de descoberta de software

. Software Asset Management Professional A aplicação permite que você edite um modelo de descoberta de software para normalizar manualmente o software descoberto que não foi totalmente normalizado (parcialmente normalizado, fornecedor normalizado ou correspondência não encontrada) no formulário Modelos de Descoberta de software

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para que ele possa ser reconciliado. A partir da versão 20,0 de Resposta a vulnerabilidades oferece suporte ao modelo de descoberta normalizado que vem de Software Asset Management Professional. Os campos a seguir são usados para o algoritmo de correspondência para modelos de descoberta de software.

CPE (Modelo de software)	SAM fundações	SAM Professional
Fornecedor	Chave primária	Chave primária
Produto	Nome de exibição	Nome de exibição
Versão	Fornecedor descoberto	Fornecedor descoberto
Edição	Produto descoberto	Produto descoberto
	Versão Descoberta	Versão Descoberta
		Fornecedor Normalizado
		Produto normalizado
		Versão normalizada

Nota: A aplicação SAM Professional não faz parte do núcleo Resposta a vulnerabilidades produto do ServiceNow Store e requer uma assinatura separada.

Propriedade do sistema

Para processar as vulnerabilidades exploradas pela CISA automaticamente para avaliação de exposição, defina a propriedade do sistema *sn_vul_analyst.enable_exposure_for_cisa*. *true*. O valor padrão é *false*.

Trabalhos agendados

A seguir estão os trabalhos agendados.

Nome do trabalho agendado	Descrição
Verifique a possível exposição a vulnerabilidades	Processa os delta CVEs, o software e as instalações para obter a exposição. **Nota:** Este trabalho agendado é executado a cada 12 horas. Ele é executado por um período mais longo do que os outros trabalhos agendados.
Insira CVE explorado da CISA na configuração de exposição	Sob demanda. Insere os CVEs da CISA na tabela Configuração de exposição para calcular a exposição.
Execute a avaliação de exposição para CVEs configurados	Sob demanda. Calcula a exposição de todos os registros CVE na tabela Configuração de exposição.
Executar exposição de software	Sob demanda. Calcula a exposição de todos os registros de software na tabela Configuração de exposição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termos principais

- **Pontuação de confiança:** Uma pontuação de confiança é uma medida da confiabilidade no fornecimento de uma recomendação para um campo. Quanto maior a pontuação, mais confiável será a recomendação. Para obter exemplos de cálculos, consulte Exemplo de cálculo de pontuação de confiança.
- **Contagem de instalações de software:** Número de ativos de software afetados pela vulnerabilidade.
- **Modelo de software:** Modelo de software associado ao produto. Detalhar o modelo de software para ver o resultado do modelo de software. Para obter mais informações, consulte Plug-in Software Asset Management Foundation modelos de descoberta e instalações de software .

. **Contagem de instalações de software** o campo fornece o número total de instalações de software, independentemente do status ativo ou inativo no modelo de descoberta. A partir da v22.0 de Resposta a vulnerabilidades, uma nova propriedade do sistema, *sn_vul.filter_inactive_sw_installs*foi introduzido para determinar se instalações de software inativas devem ser filtradas para avaliação de exposição . Por padrão, a propriedade está habilitada no sistema de base. Quando o filtro está habilitado, somente as instalações ativas são exibidas.

. **Modelo da Descoberta** O campo mostra especificamente a contagem de instalações de software ativas, já que as inativas são filtradas com base no filtro ativo-verdadeiro padrão na tabela Modelo de Descoberta de Software. A contagem neste campo deve corresponder à contagem filtrada exibida em **Contagem de instalações de software** campo. A contagem em **Instalação do software** o campo persiste mesmo se você atualizar a propriedade do sistema. Para obter a contagem atualizada, você deve executar os trabalhos agendados *Run exposure assessment for configured CVEs*e. *Run software exposure that updates the count*.

Avaliação de exposição por CVE

A avaliação de exposição usa Vulnerabilidades e exposições comuns (CVEs) para avaliar a exposição de seus ativos usando o modelo de descoberta de software. Você pode usar a avaliação de exposição por CVE para identificar a exposição a possíveis vulnerabilidades.

Para obter informações sobre como avaliar a exposição por CVE, consulte:

- Adicione CVEs para avaliar a exposição
- Criar VIS para CVEs para avaliação de exposição
- Ativar ou desativar CVEs para avaliação de exposição
- Exporte ICs afetados para avaliação de exposição
- Exemplo de cálculo de pontuação de confiança

Adicione CVEs para avaliar a exposição

Adicione Vulnerabilidades e exposições comuns (CVEs) à lista de configuração de exposição de CVEs na Avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione **Adicionar**.
3. Na caixa de diálogo Adicionar CVE, selecione os CVEs que você deseja adicionar à lista e selecione **Adicionar** opção.
   CVEs que já estão na lista não são adicionados novamente. O restante é adicionado à lista de CVEs.

   Nota: Selecione o ícone de filtro para navegar até **Exibição avançada** E especifique os CVEs que você deseja exibir.

4. Para avaliar o impacto dos CVEs que já estão na lista:

   a. Marque a caixa de seleção dos CVEs que você deseja reavaliar.

   b. Selecione **Reavaliar** botão.
      Os detalhes atualizados aparecem nas respectivas colunas.

Criar VIS para CVEs para avaliação de exposição

Crie Itens vulneráveis (VIS) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de VIS e recomendam soluções e patches que ajudam a equipe DE TI a corrigir essas vulnerabilidades.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Depois que a exposição é avaliada, a lista da avaliação potencial é exibida no registro de avaliação de exposição com a contagem de itens de configuração (ICs). Você pode selecionar os registros e, na ação de lista, selecione **Criar itens vulneráveis** Criar itens vulneráveis (VIS) para os ICs em que o software vulnerável está presente e nas Vulnerabilidades e exposições comuns (CVEs). Os VIS são criados em segundo plano. Este processo pode levar algum tempo. Depois que os itens são criados, você pode navegar até a tabela VI para exibir os registros criados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs necessários e selecione **Criar itens vulneráveis** opção.
3. Na caixa de diálogo Criar itens vulneráveis, selecione **Criar itens vulneráveis** opção.
4. Selecione **Exibir status** Link para exibir o status do trabalho em segundo plano usado para criar o VIS.

Ativar ou desativar CVEs para avaliação de exposição

Para o processamento delta de um CVE, você pode ativá-lo, adicionando-o à lista ativa de CVEs.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da versão 4.0.1 da Avaliação de exposição a vulnerabilidades, se uma Entrada de vulnerabilidade comum (CVE) não tiver sido atualizada ou tiver Itens vulneráveis (Vits) criados nos últimos 30 dias, o registro de avaliação de exposição desse CVE será marcado automaticamente como inativo. No entanto, você pode ativar ou desativar manualmente esses registros. Além disso, o trabalho agendado `Check potential vulnerability exposure` Executado continuamente para verificar esses CVEs para designá-los como inativos.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs ativos necessários e selecione **Desativar** opção.
   Os CVEs estão desativados.

   Nota: Para ativar o software, siga o mesmo processo e selecione **Ativar** opção.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exporte ICs afetados para avaliação de exposição

Você pode rastrear a lista de ativos afetados de um novo CVE exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione o modelo de Descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados no **Instalado em** coluna.
3. Selecione **Exportação** opção.
4. Na caixa de diálogo Exportar, selecione o Tipo de arquivo e o Tipo de entrega para exportar os ICs relacionados.
5. Selecione **Exportação** opção.

Exemplo de cálculo de pontuação de confiança

Exemplo de cálculo da confiança de uma vulnerabilidade de dia zero com base em suas informações de CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns).

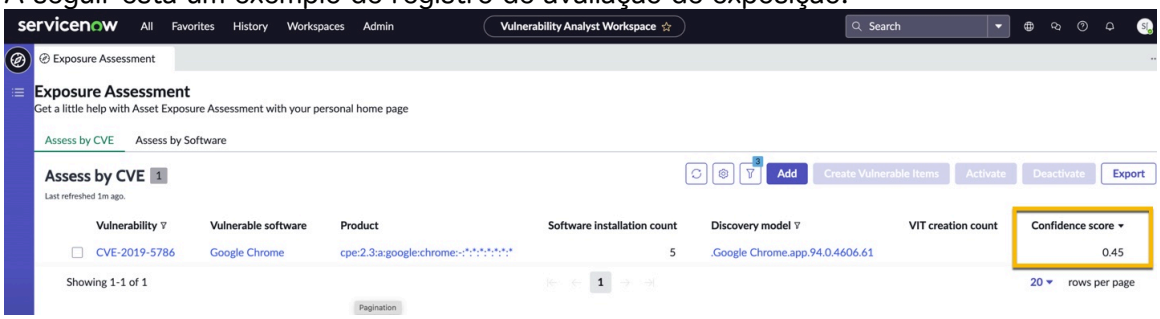
A seguir está um exemplo de cálculo da pontuação de confiança a partir das informações de CPE (Common Platform Enumeration, enumeração de plataforma comum) de **CVE-2019-5786** .

Nota: Para exibir os CPEs, você pode agrupar a coluna Vulnerabilidade por vulnerabilidade. Para obter detalhes sobre como exibir os detalhes do software vulnerável, consulte Exibir detalhes do software vulnerável.

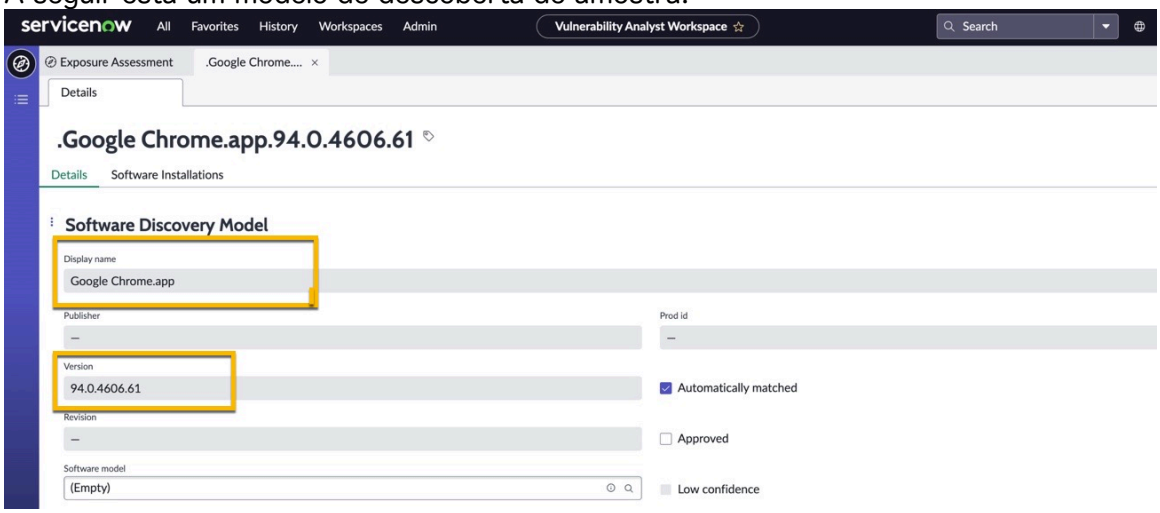
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de registro de avaliação de exposição:



A seguir está um modelo de descoberta de amostra:



Como calcular a pontuação de confiança

O intervalo de pontuação de confiança é de 0 a 1. Com base nas informações do CPE, a pontuação de confiança é calculada usando a seguinte fórmula:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

```
.45
```

Nota: Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

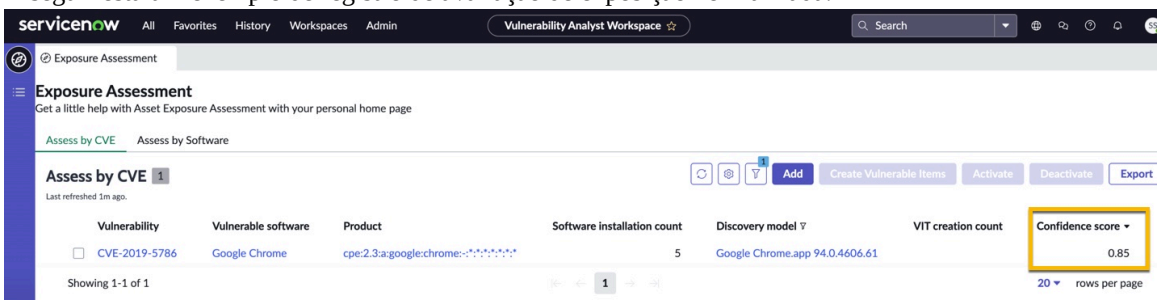
Calcular pontuação de confiança quando o modelo de software é correspondido ao modelo de descoberta normalizado

Se você estiver usando o modelo de descoberta normalizado, as informações adicionais disponíveis para o modelo de descoberta de software fornecerão uma pontuação de confiança aprimorada. A seguir está o cálculo de amostra:

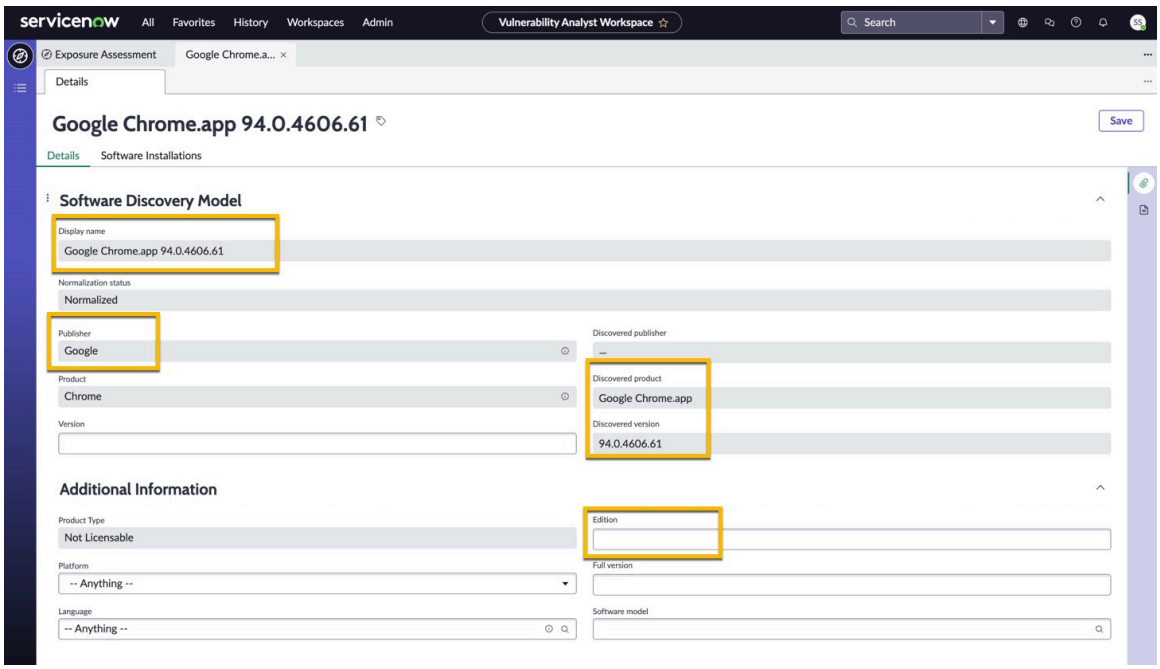
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de registro de avaliação de exposição normalizada.



A seguir está um exemplo de modelo de descoberta normalizado.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) +
 (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Nota: Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

Exibir detalhes do software vulnerável

Exiba os detalhes do software vulnerável, neste caso, o Google Chrome. Ele é comparado com o modelo de descoberta e a CPE (Common Platform Enumeration, enumeração de plataforma comum). Esta versão do CPE afeta todas as versões do Google Chrome.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** e digite *sn_vul_software.LIST*.
2. Na lista de software vulnerável, pesquise **cpe:2,3:a:google:chrome:-:*:*:*:*:*:*:*:*** para exibir as informações.

Tabelas de referência de pontuação de confiança para avaliação de exposição

Valores de referência usados para calcular a pontuação de confiança.

Tabelas de referência

Tabela de referência de cálculo de pontuação de confiança

Segmento de software vulnerável	Segmento do modelo da Descoberta	Pontuação	Segmento de correspondência exata do modelo da Descoberta	Pontuação de correspondência exata
Fornecedor	Nome de exibição	15	Fornecedor	5
Modelo	Nome de exibição	15	Modelo	5
Versão	Nome de exibição	10	Versão	5
Edição	Nome de exibição	3	Edição normalizada	2
Nome de exibição	Nome de exibição	10	Nome de exibição	5

Tabela de resumo da pontuação de confiança

Pontuação	Valor
Soma de todas as pontuações	75
Pontuação base **Nota:** Pontuação mínima fornecida a todos os modelos de descoberta correspondentes.	25
Pontuação total	100

Avaliação de exposição por software

Avaliação de exposição para vulnerabilidades de dia zero, quando Vulnerabilidades e exposições comuns (CVEs) para o ativo ou item de configuração não está disponível. Ele usa as informações de software para avaliar a exposição, usando o modelo de descoberta de software.

Para obter informações sobre como avaliar a exposição por software, consulte:

- Adicione software para avaliação de exposição
- Criar VIS para software para avaliação de exposição
- Ativar ou desativar o software para avaliação de exposição
- Exporte ICs afetados para software no espaço Avaliação de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione software para avaliação de exposição

Adicione um novo software ao módulo Avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software** > **Adicionar**.
2. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software.
Produto	Nome do produto do software.
Versão	Versão do produto de software.
Edição	Edição do software

Nota: Se você tentar adicionar exposição para o software que existe na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

3. Selecione **Adicionar** opção.
4. Para avaliar o impacto do software que já está na lista:
   a. Marque a caixa de seleção do software que você deseja reavaliar.
   b. Selecione **Reavaliar** botão.
   Os detalhes atualizados aparecem nas respectivas colunas.

Criar VIS para software para avaliação de exposição

Crie Itens vulneráveis (VIS) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de VIS e recomendam soluções e patches que ajudam a equipe DE TI a corrigir essas vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione os registros para os quais você deseja criar o VIS.
3. Selecione **Criar itens vulneráveis** opção.
4. Na caixa de diálogo Criar itens vulneráveis, selecione:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidade Existente
- Nova Vulnerabilidade

5. Selecione **Criar itens vulneráveis** opção.

Ativar ou desativar o software para avaliação de exposição

Para interromper o processamento delta adicional do software, você pode optar por desativá-lo, removendo-o da lista ativa de software.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Para desativar, selecione o software ativo necessário e selecione **Desativar** opção.
   O software está desativado.

   Nota: Para ativar o software, siga o mesmo processo e selecione **Ativar** opção.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exporte ICs afetados para software no espaço Avaliação de vulnerabilidades

Você pode rastrear a lista de ativos afetados para o novo software exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione o modelo de descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados no **Instalado em** coluna.
3. Selecione **Exportação** opção.
4. Na caixa de diálogo Exportar, selecione **Tipo de arquivo** e. **Tipo de entrega** Para exportar os ICs relacionados.
5. Selecione **Exportação** opção.

Avaliação de exposição por software do fornecedor

Avalie a exposição para vulnerabilidades de dia zero quando as vulnerabilidades e exposições comuns (CVEs) do ativo ou item de configuração não estiverem disponíveis. Ele usa as informações de software para avaliar a exposição, usando o modelo de descoberta de software.

Para obter informações sobre como avaliar a exposição por software, consulte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adicione software de um fornecedor para avaliação de exposição
- Criar VIS para software por um fornecedor para avaliação de exposição
- Ativar ou desativar software por um fornecedor para avaliação de exposição
- Exporte ICs afetados para software por um fornecedor no espaço Avaliação de vulnerabilidades

Adicione software de um fornecedor para avaliação de exposição

Adicione software de um fornecedor ao módulo Avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por fornecedor** > **Novo**.
2. Em Nova avaliação , selecione o fornecedor para o qual você deseja executar a avaliação.
3. Selecione uma data em **CVE publicado de** campo.
   Se qualquer uma das Entradas de Vulnerabilidade Comum (CVEs) associadas ao software for modificada após a data selecionada, esse software será considerado para avaliação de exposição.
4. Selecione o nível de gravidade do CVE em **Gravidade de CVE** seção.
5. Selecione **Iniciar avaliação** .
   Quando o trabalho é concluído, os registros selecionados são criados.

Criar VIS para software por um fornecedor para avaliação de exposição

Crie Itens vulneráveis (VIS) na página Avaliação de exposição para analisar a lista de VIS e recomendar soluções e patches que podem ajudar a equipe DE TI a corrigir as vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por fornecedor**.
2. Selecione os registros para os quais você deseja criar o VIS.
3. Selecione **Criar itens vulneráveis** opção.
4. Na caixa de diálogo Criar itens vulneráveis, selecione:
   - Vulnerabilidade Existente
   - Nova Vulnerabilidade
5. Selecione **Criar itens vulneráveis** opção.

Ativar ou desativar software por um fornecedor para avaliação de exposição

Ative ou desative o software por um fornecedor para interromper o processamento delta do software e removê-lo da lista ativa de software.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por fornecedor**.
2. Para desativar, selecione o software ativo necessário por um fornecedor e selecione **Desativar** opção em **Reavaliar** botão.
   O fornecedor está desativado.

   Nota: Para ativar o software por um fornecedor, siga o mesmo processo e selecione **Ativar** opção.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exporte ICs afetados para software por um fornecedor no espaço Avaliação de vulnerabilidades

Você pode rastrear a lista de ativos afetados para o novo software exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por fornecedor**.
2. Selecione o modelo de descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados no **Instalado em** coluna.
3. Selecione **Exportação** opção.
4. Na caixa de diálogo Exportar, selecione **Tipo de arquivo** e. **Tipo de entrega** Para exportar os ICs relacionados.
5. Selecione **Exportação** opção.

Explorando a avaliação de vulnerabilidades

O Espaço de avaliação de vulnerabilidades foi projetado para que o Gerenciador de eventos de vulnerabilidade crie um evento de vulnerabilidade e execute avaliação de vulnerabilidade, especialmente durante a análise de vulnerabilidade de dia zero.

Você pode usar o espaço de avaliação de vulnerabilidades para gerenciar vulnerabilidades críticas, como:

- Vulnerabilidades de dia zero de gravidade crítica ou alta
- Nova ameaça identificada para uma vulnerabilidade
- Exploração rápida de uma vulnerabilidade de gravidade crítica ou alta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Espaço de avaliação de vulnerabilidades e Gestão de crises de vulnerabilidade

Como gerente de eventos de vulnerabilidade, identifique e crie um registro de evento de vulnerabilidade para vulnerabilidades de interesse. Depois de criar o evento vulnerável, você pode executar a avaliação de risco, atualizar manualmente os atributos de risco e calcular a pontuação de risco automaticamente. Usando o Espaço de avaliação de vulnerabilidades, você pode executar as seguintes ações para lidar com o evento de crise de vulnerabilidade desde a criação até a resolução.

- Crie um registro de avaliação de vulnerabilidade
- Modifique o registro de avaliação de vulnerabilidade
- Execute uma avaliação de vulnerabilidade
- Revise os detalhes da avaliação
- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicione ICs afetados ao registro de avaliação
- Crie itens vulneráveis para o IC afetado ou o componente de software afetado
- Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave em Gestão de incidentes graves de segurança

Pré-requisitos para avaliação de vulnerabilidades

Versões disponíveis

Aplicação	Versão
Plug-in Gestão de crises de vulnerabilidade	1.0
Resposta a vulnerabilidades	20,0
Resposta a vulnerabilidades Com NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações de NVD.	1.4.2
Vulnerability Response integration with CISA	1.2
Modelo de dados para SBOM	1.1.2
Lista de materiais de software Núcleo	2.0.2
Software Asset Management	Plug-in Software Asset Management Foundation ou Software Asset Management Professional plug-in
Gestão de incidentes graves de segurança	2.2.5

Trabalhos agendados

A seguir estão os trabalhos agendados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do trabalho agendado	Descrição
Avaliação de vulnerabilidade	Atualiza a tabela de itens de configuração afetados e a origem do IC se itens vulneráveis (Vits ou AVITs) forem criados após a avaliação. **Nota:** Este trabalho agendado é executado diariamente. Ele é executado por um período mais longo do que os outros trabalhos agendados.

Tópicos relacionados

Gestão de crises de vulnerabilidade

Crie um registro de avaliação de vulnerabilidade

Crie registros de avaliação para vulnerabilidades de interesse. Depois de criar a avaliação, você pode iniciar a avaliação de risco inicial, atualizar manualmente o registro e calcular a pontuação de risco automaticamente.

Antes de Iniciar

Você precisa fazer parte do grupo de atribuição do Gerenciador de eventos de avaliação de vulnerabilidades do sistema de base para poder executar as tarefas associadas à avaliação de vulnerabilidades.

Função necessária: sn_vul_analyst.vul_event_manager, sn_vul_analyst.emergency_response

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar um registro de avaliação de vulnerabilidade para vulnerabilidades de interesse associando o registro de evento a um CVE primário ou a um produto afetado.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione **Avaliação de vulnerabilidades** ícone.
3. Selecione **Novo**.
4. Insira um título apropriado em **Título** campo.
5. **Opcional:** Selecione um CVE primário para associar ao novo registro de avaliação do **CVE primário** campo.

   Nota: Todos os detalhes preliminares no registro de avaliação são preenchidos com base no produto selecionado ou criado ou no CVE primário que você associa ao registro.

6. Selecione **Enviar**.
   O registro de avaliação de vulnerabilidade com o título inserido é criado e exibido em uma nova guia de avaliação de vulnerabilidade. Por padrão, o registro de avaliação de vulnerabilidade é exibido no **Detalhes** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Por padrão, os detalhes do CVE primário associado/mapeado são exibidos.

- Se nenhum CVE primário for selecionado durante a criação do registro do evento de avaliação de vulnerabilidade, um registro padrão será criado.
- Se o CVE primário tiver CVEs associados, os CVEs relacionados serão preenchidos no **Entradas de vulnerabilidade** guia. Você pode adicionar mais CVEs associados do **Entradas de vulnerabilidade** guia.

7. Navegue até **Produtos afetados** guia.

a. Selecione **Novo**.

b. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software. Este é um campo obrigatório.
Produto	Nome do produto do software. Este é um campo obrigatório.
Versão	Versão do produto de software.
Edição	Edição do software

Nota: Se você tentar adicionar a vulnerabilidade para o software que existe na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

c. Selecione **OK**.

8. Selecione **Save** (Salvar).

Atualize o registro de limpeza automática da avaliação de vulnerabilidades

Atualize o registro de limpeza automática da avaliação de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

No sistema de base, o período de retenção de registros de avaliação de vulnerabilidade é definido como 6 meses. Se qualquer estado de registro de avaliação de vulnerabilidade for Encerrado, os registros de avaliação de vulnerabilidade serão armazenados somente até o período de retenção definido e os registros relacionados dessa avaliação serão removidos após 6 meses de todas as tabelas relacionadas.

Procedimento

1. Navegar até **Tudo** > **Limpezas automáticas**.

2. Abrir o registro com a tabela, sn_vul_analyst_vulnerability_assessment .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Ativo** caixa de seleção para ativar a opção de limpeza automática do registro de avaliação de vulnerabilidade.
4. Clique em **Atualizar**.

Modifique o registro de avaliação de vulnerabilidade

Atualize o registro de Avaliação de vulnerabilidades e publique sua criação. Com base nos valores do campo, você pode calcular a pontuação de risco .

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

Depois que o CVE primário é adicionado à avaliação de vulnerabilidade, o registro é movido para um estado Avaliação pendente. Você pode adicionar outros CVEs relacionados em **Entradas de vulnerabilidade** ou adicione os produtos afetados por esta vulnerabilidade do **Produtos afetados** guia. Você pode fazer modificações adicionais no **Avaliação de risco** e **Pontuação de risco** para o registro de avaliação é atualizado automaticamente de acordo.

Procedimento

1. Navegar até **Tudo** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Em **Detalhes** atualize os campos.

Campo	Descrição
Título	Título que descreve o evento de vulnerabilidade registro.
CVE primário	CVE primário associado ao registro de evento.
Estado	Estado atual do registro do evento.
Prioridade	Prioridade do registro do evento em uma escala de 1 a 5.
Origem do alerta	Origem do possível evento de vulnerabilidade.
Pontuação de Risco	Pontuação de risco calculada automaticamente. Não editável por padrão.
Nível de exposição	O nível de exposição do evento de vulnerabilidade em uma escala de 1 a 5.
Grupo de Atribuição	O grupo de atribuição ao qual o registro de evento está atribuído.
Atribuição a	O usuário ao qual o registro de evento está atribuído.
Descrição	Descrição detalhada do registro do evento.

3. Navegue até **Entradas de vulnerabilidade** Para adicionar CVEs associados ou relacionados.
   a. Selecione **Novo**.
   b. PESQUISE o registro no **Entrada de vulnerabilidade** campo.
   c. Selecione o registro de vulnerabilidade que você deseja associar ao registro de avaliação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Opcional: Selecione **Procurar** para procurar e anexar um arquivo.

e. Selecione **Save** (Salvar).
Os registros de vulnerabilidade selecionados são adicionados ao registro de avaliação e exibidos no **Entradas de vulnerabilidades** guia.

4. **Opcional:** Adicionar produtos afetados.
5. Adicione um link relacionado ao registro de avaliação.
6. Modifique o. **Atributos de risco** Para o CVE primário associado ao registro de evento de avaliação de vulnerabilidade.

Campo	Descrição
Corrupção de memória	Indica se este registro de evento pode corromper a memória.
Executável de código remoto	Indica se a execução remota de código é possível.
Escalação de privilégio local	Indica se existe vulnerabilidade de escalação de privilégio local.
Acesso não autorizado	Indica se existe vulnerabilidade de acesso não autorizado.
DDOS	Indica se o possível evento pode envolver negação de serviço distribuído.
Complexidade do ataque	Indica a complexidade do anexo. As opções são Baixo, Médio ou Alto.
Vetor de ataque	Indica o possível caminho ou método de ataque. As opções são: Rede, Rede adjacente, Local, Físico, Nenhum.
Privilégios necessários (PN):	Indica o nível de privilégios que um invasor precisa para explorar a vulnerabilidade. As opções são Nenhum, Baixo ou Alto.
Interação do usuário	Indica se a interação do usuário é necessária ou não para explorar a vulnerabilidade.
Impacto da confidencialidade	Indica a medida do possível impacto na confidencialidade da vulnerabilidade. As opções são Nenhum, Baixo ou Alto
Mudança de escopo	Indica se o escopo da avaliação foi alterado.
Impacto na disponibilidade	Indica o possível impacto na disponibilidade de uma vulnerabilidade de uso indevido explorada com sucesso. Disponibilidade refere-se à acessibilidade dos recursos de informação. As opções são Nenhum, Baixo ou Alto
Impacto na integridade	Indica o possível impacto na integridade de uma vulnerabilidade de uso indevido explorada com

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	sucesso. A integridade refere-se à confiabilidade e veracidade garantida das informações. As opções são Nenhum, Baixo ou Alto
Nível de correção	Indica o status ou a disponibilidade de correção da vulnerabilidade. As opções são Correção oficial, Correção temporária, Solução alternativa, Indisponível, Não definido.
Maturidade do código de exploração	Indica a probabilidade de a vulnerabilidade ser explorada com base no estado existente das técnicas de exploração e na disponibilidade do código. As opções são Não comprovada, Prova de conceito, Funcional, Alto e Não definido.
Confiança do relatório	Indica o quanto você tem certeza de que a vulnerabilidade existe.

7. Insira comentários relevantes em **Compor** campo.
   - Insira suas anotações de trabalho no **Anotações de trabalho (privadas)** campo.
   - Insira seus comentários (visíveis para todos) em **Comentários** campo.
8. **Salvar** o registro de avaliação.
   Com base nas atualizações feitas no **Atributo de risco** Campos para o CVE primário ou o produto afetado associado ao registro de avaliação, o. **Pontuação de risco** o campo é atualizado automaticamente.

   Nota: Para modificar as regras ou critérios da calculadora de pontuação de risco do sistema de base, navegue até **Tudo** > **Calculadoras de avaliação de vulnerabilidade** > **Calculadora de risco da avaliação de vulnerabilidade** > **Regra de risco de avaliação de vulnerabilidade**. Você pode adicionar critérios e modificar a ponderação no nível do campo para critérios existentes conforme necessário.

O que Fazer Depois
Execute uma avaliação inicial do registro do evento.

Exclua CVEs associados ou produtos afetados do registro de avaliação de vulnerabilidade

Exclua um registro de evento de vulnerabilidade se ele não for mais necessário.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Você pode excluir CVEs ou produtos afetados associados ao registro de avaliação de vulnerabilidade. Você só pode excluir entradas de vulnerabilidade/CVEs associados ou produtos afetados se eles estiverem em **Novo** ou **Avaliação pendente** estados.

Procedimento
1. Navegar até **Tudo** > **Espaços** > **Avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Entradas de vulnerabilidade** ou **Produtos afetados** guia.
4. Selecione o CVE associado ou o registro do produto afetado.
5. Selecione **Excluir**.

Nota: . **Excluir** o botão é exibido somente para um registro de avaliação quando eles estão em **Novo** ou **Avaliação pendente** estados.

Adicione um link relacionado ao registro de avaliação

Adicione links e informações adicionais relacionados ao registro de avaliação.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione a entrada de registro de avaliação.
3. Selecione **Links relacionados** guia.
4. Insira uma descrição relevante em **Descrição** campo.
5. Insira o URL no **Link** campo.
6. Selecione **OK**.
   O link relacionado é adicionado e listado na guia Links relacionados.

Execute uma avaliação

Depois de criar o registro de avaliação de vulnerabilidade e atualizar os campos de atributo de risco, execute uma avaliação do registro de evento.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Execute uma avaliação inicial depois que um evento de uma vulnerabilidade de interesse tiver sido criado e determinado como apresentando risco para sistemas e dados. O objetivo desta atividade é analisar melhor a ameaça atualizando a avaliação de risco com uma avaliação de exposição detalhada.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Selecione o registro relevante na lista de registros de eventos de avaliação de vulnerabilidade.
3. Selecione **Avaliar** para executar a avaliação de vulnerabilidade.
   . Resposta a vulnerabilidades - Evento de avaliação de vulnerabilidade do processo o trabalho em segundo plano é iniciado e uma notificação relevante é exibida.
4. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
5. Selecione **Save** (Salvar).

. **Avaliações** exibe detalhes da avaliação. Quando a avaliação é processada, os Vits ou AVITs associados às entradas vulneráveis ou CVEs são exibidos no **Itens vulneráveis** ou **Itens vulneráveis à aplicação** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

- Itens vulneráveis ou TPEs relacionados aos CVEs associados são obtidos durante a avaliação. Os ICs relacionados aos itens vulneráveis também são identificados e exibidos na tabela Itens de configuração afetados.
- Se os ICs associados não existirem na tabela de ICs afetados, os ICs identificados serão adicionados à tabela e ao **Tem item vulnerável** o valor do campo está definido como **Verdadeiro** e **Origem** O valor do campo é definido como Scanner.
- Se o IC já existir na tabela de IC afetado, somente **Tem item vulnerável** o valor do campo está definido como **Verdadeiro** e o. **Origem** O valor dos campos do IC permanece o mesmo de quando o registro de avaliação foi criado.
- Se itens vulneráveis forem criados após a avaliação, um Avaliação de vulnerabilidades O trabalho agendado é executado para atualizar a tabela de ICs afetados e a origem do IC.

O que Fazer Depois

- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicione ICs afetados ao registro de avaliação
- Crie itens vulneráveis para o IC afetado ou o componente de software afetado
- Adicione um link relacionado ao registro de avaliação

Tópicos relacionados

Guia Avaliação

Guia "Visão geral"

Guia Avaliação

Revise os resultados da avaliação na guia Avaliação. Depois de executar uma avaliação do evento de vulnerabilidade, o registro é correlacionado com os dados de Lista de materiais de software e. Software Asset Management e exibidos com visualizações.

A guia Avaliação preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações de Software Asset Management e. Lista de materiais de software Dados do componente no CMDB.

Como a avaliação funciona

Ao selecionar **Avaliar** Uma avaliação para todos os CVEs relacionados e produtos afetados usando ambos Software Asset Management e. SBOM os dados são iniciados. Um trabalho em segundo plano é acionado e, quando a avaliação é processada, os Vits ou AVITs associados às entradas vulneráveis ou CVEs são exibidos no **Itens vulneráveis** e. **Itens vulneráveis à aplicação** guias.

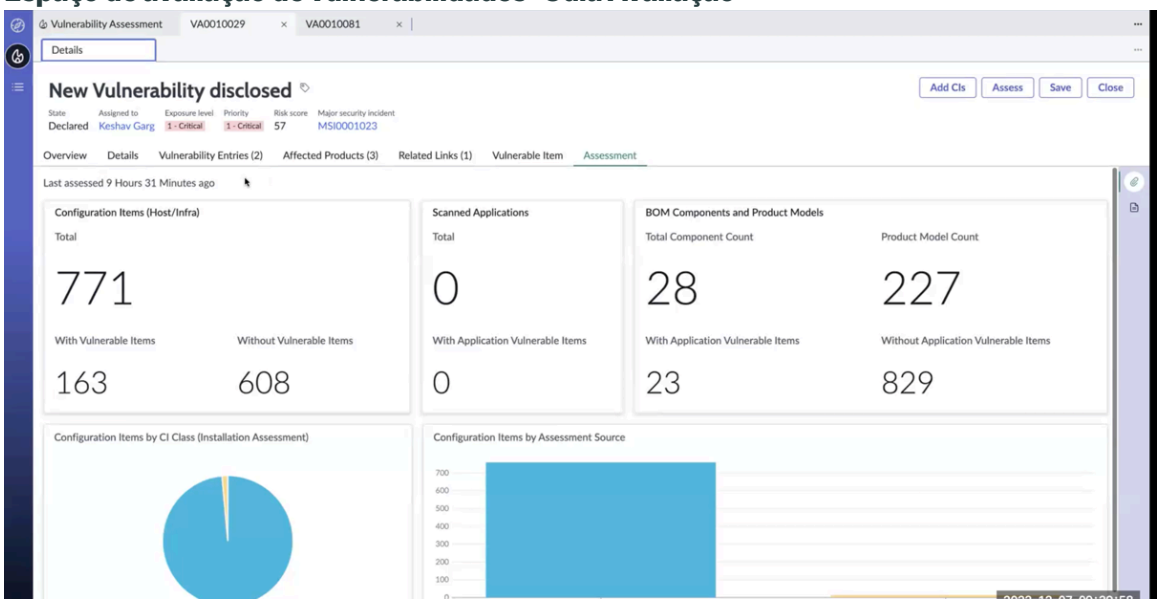
- Todos os itens vulneráveis ou TPEs relacionados ao CVE são identificados.
- Os itens de configuração (ICs) relacionados aos itens vulneráveis também são identificados e exibidos na tabela de itens de configuração afetados.
- Se os ICs não estiverem presentes na tabela de ICs afetados, os ICs identificados serão adicionados à tabela e ao **Tem item vulnerável** o sinalizador é transformado em verdadeiro e o **Origem** O valor do campo é definido como Scanner.
- Se o IC já existir na tabela de itens de configuração afetados, somente **Tem item vulnerável** o sinalizador está definido como verdadeiro e **Origem** permanece inalterado desde quando o registro de avaliação foi criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se itens vulneráveis forem criados após a avaliação, um Avaliação de vulnerabilidades O trabalho agendado é executado para atualizar a tabela de ICs afetados e a origem do IC.
- No espaço Avaliação, você pode exibir carimbos de data/hora para ver a última avaliação dos eventos. . **Avaliação** a guia fica visível somente quando as novas avaliações são criadas. Se a avaliação estiver no estado Em andamento, o status da última avaliação aparecerá como a avaliação está Em andamento. Para exibir o status da avaliação atualizado, você precisa atualizar a página. Quando a avaliação for concluída, o usuário poderá ver todas as guias relacionadas a essa avaliação.

Espaço de avaliação de vulnerabilidades- Guia Avaliação



Os detalhes da avaliação são exibidos para os widgets a seguir.

- Itens de configuração (host/infraestrutura)
- Aplicações escaneadas
- Componentes da BOM e modelos de produto
- Itens de configuração por classe de IC (avaliação de instalação)
- Itens de configuração por origem de avaliação - Exibe a lista de itens de configuração afetados.

Visualizações de dados

Nome	Tipo	Descrição
Itens de configuração (host/ infraestrutura)	Pontuação Única	Exibe a contagem de ICs com e sem VIS. O widget Itens de configuração exibe a contagem total de ICs encontrados para serem associados ao registro de avaliação. O widget exibe ainda os itens de configuração com itens

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		vulneráveis e sem itens vulneráveis.
Aplicações escaneadas	Contagem	Contagem total de aplicações verificadas com AVITs. **Nota:** Você pode exibir a contagem de aplicações verificadas para CVEs primários e secundários.
Componentes da BOM e modelos de produto	Pontuação Única	Contagem total de componentes, Contagem de modelos de produto, com itens vulneráveis à aplicação, sem contagem de itens vulneráveis à aplicação.
Itens de configuração por origem de avaliação	Barras empilhadas	Itens de configuração afetados empilhados pela origem de avaliação.
Itens de configuração por classe de IC (avaliação de instalação)	Gráfico de pizza	Itens de configuração empilhados por classe de IC.

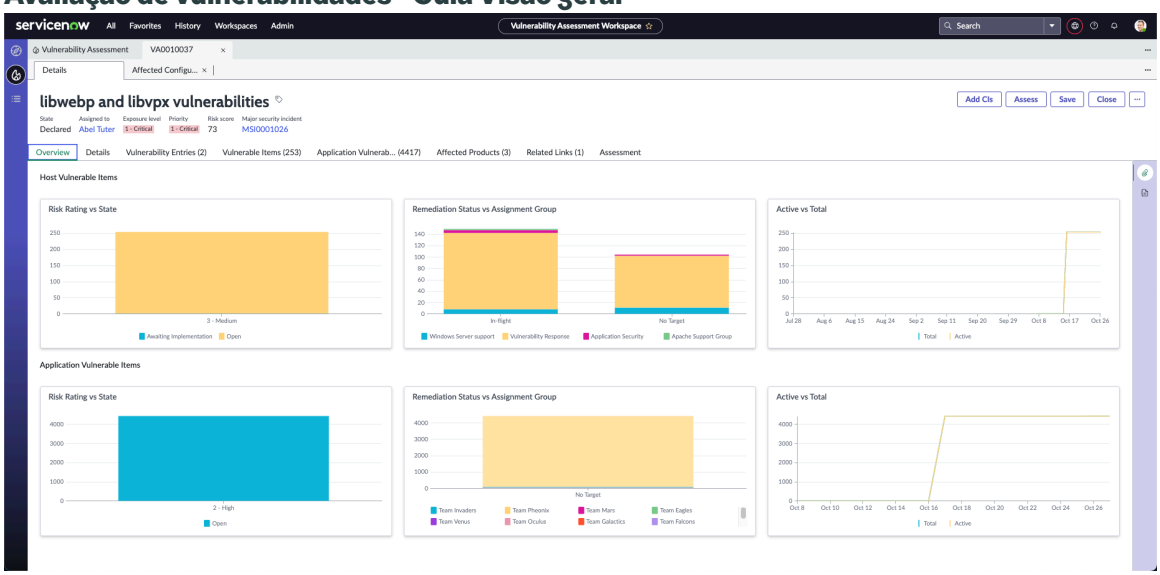
Guia "Visão geral"

A visão geral dos detalhes da avaliação é exibida na guia Visão geral. Depois de executar a avaliação inicial, o registro é correlacionado com os dados do Lista de materiais de software e. Software Asset Management e exibidos com visualizações.

Guia "Visão geral"

A guia Visão geral preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações de Software Asset Management e. Lista de materiais de software Dados no CMDB. O

Avaliação de vulnerabilidades - Guia Visão geral



Os detalhes da avaliação são exibidos para os widgets a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Itens vulneráveis do host (host/infraestrutura)
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total
- Itens vulneráveis da aplicação
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total

Visualizações de dados

Itens vulneráveis de host

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável empilhado por seu grupo de atribuição.
Ativo x Total	Lista e Linha	Total de itens vulneráveis associados a esta entrada versus itens vulneráveis ativos.

Itens vulneráveis da aplicação

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis à aplicação empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável da aplicação empilhado por seu grupo de atribuição.
Ativo x Total	Lista e Linha	Total de itens vulneráveis da aplicação associados a esta entrada versus itens vulneráveis ativos.

Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade

Atribua manualmente prioridade e nível de exposição ao registro de avaliação de vulnerabilidade.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de Avaliação de vulnerabilidades**.
2. Selecione um registro de avaliação de vulnerabilidade.
3. Navegue até **Atributos de risco** em **Detalhes** guia.
4. Selecione um **Prioridade** na lista de opções.
5. Selecione um **Nível de exposição** na lista de opções.
6. Selecione **Save** (Salvar).

Adicione ICs afetados ao registro de avaliação

Adicione manualmente os ICs em sua organização que você acha que devem ser associados ao registro de avaliação de vulnerabilidade, mas não serão exibidos nos ICs afetados após inicial avaliação.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

Adicione ICs que você sabe que podem ter sido afetados, mas que não aparecem após a conclusão da avaliação. Você só pode adicionar ICs quando o registro de avaliação está em **Declarado** ou **Avaliação pendente** estado.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação necessário na lista.
3. Selecione **Adicionar ICs** .
4. Selecione os itens de configuração na caixa de diálogo Itens de configuração.
5. Selecione **Adicionar ICs** .
   . Resposta a vulnerabilidades- Adicionar itens de configuração ao evento o trabalho em segundo plano é iniciado e uma notificação relevante é exibida.
6. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.

Resultado

Registros são adicionados à tabela Itens de configuração afetados com **Origem** . `Manual` .

O que Fazer Depois

Navegue até **Avaliação** e atualize **Itens de configuração (host/infraestrutura)** Widget para exibir os ICs que você adicionou.

Crie itens vulneráveis para o IC afetado ou o componente de software afetado

Crie Itens vulneráveis (VIS) ou Itens vulneráveis à aplicação (AVITs) no Espaço de avaliação de vulnerabilidades. Os analistas de vulnerabilidades analisam a lista de VIS e recomendam soluções e patches que ajudam a equipe DE TI a corrigir essas vulnerabilidades.

O gerenciador de eventos de vulnerabilidade deve ser capaz de selecionar um, muitos ou todos os resultados da pesquisa de exposição para criar Itens de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Item vulnerável à aplicação para resultados de avaliação de SBOM que não têm AVITs associados
- Itens vulneráveis para itens de configuração que não têm Vits associados
- Associe CVE primário aos itens de vulnerabilidade.

Criar VIS para itens de configuração sem itens vulneráveis associados

Crie Vits de itens vulneráveis para itens de configuração identificados por meio da avaliação de vulnerabilidade, mas não tenham Vits associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione **Avaliação** guia.
4. Selecione **Itens de configuração** contar a partir de **Itens de configuração (infraestrutura do host)** widget.
5. Selecione os Itens de configuração para os quais você deseja criar Vits a partir de **Itens de configuração afetados** lista.
6. Selecione **Criar item vulnerável** .
   . Resposta a vulnerabilidades - Criar avaliação de Vul manual o trabalho em segundo plano é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Itens vulneráveis para os itens de configuração afetados que você selecionou são criados.

   . **Itens de configuração (infraestrutura do host)** O widget exibirá o mesmo IC no **Com itens vulneráveis** contagem.

Crie itens vulneráveis à aplicação (AVITs) para modelos ou componentes de produtos afetados sem itens vulneráveis à aplicação associados

Crie itens vulneráveis à aplicação (AVITs) para produtos afetados ou itens de componentes identificados por meio da avaliação de vulnerabilidade, mas não têm AVITs associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione **Avaliação** guia.
4. Selecione **Itens vulneráveis à aplicação** contar a partir de **Componentes DA BOM e Modelos de produto** widget.
5. Selecione os modelos de produto afetados para os quais você deseja criar AVITs a partir de **Modelos de Produto Afetados** lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Criar item vulnerável à aplicação** .
   . Resposta a vulnerabilidades - Criar avaliação de Vul manual o trabalho em segundo plano é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Os itens vulneráveis à aplicação para os modelos de produto afetados que você selecionou são criados. Para o CVE primário associado ao registro.

   . **Componentes DA BOM e Modelos de produto** o widget exibirá o mesmo modelo de produto ou componente no **Com itens vulneráveis à aplicação** contagem.

Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave em Gestão de incidentes graves de segurança

Você pode vincular, propor ou promover o registro de avaliação para um Incidente grave de segurança desde que você tenha acesso ao Gestão de incidentes graves de segurança aplicação.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode mover o registro de avaliação para ser associado a um incidente de segurança grave existente, criar um novo MSI a partir do registro de avaliação ou promover o registro de avaliação de vulnerabilidade a um incidente de segurança grave. Aproveite o. Gestão de incidentes graves de segurança recursos como as integrações com Microsoft Teams e. Microsoft SharePoint.

Você também pode exibir o link para incidentes de segurança graves no Espaço do gerenciador de vulnerabilidades para itens vulneráveis. . MSIM o link será associado à avaliação vulnerável que será mostrada nos itens de vulnerabilidade e nos outros espaços de trabalho do Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação que você deseja vincular a um incidente de segurança grave.
3. Selecione **Mais ações** ícone, no **Detalhes** guia.
4. Selecione uma das seguintes opções.

Opção	Descrição
Link para o incidente de segurança grave	Selecione o registro MSI existente na lista de incidentes de segurança graves. O registro de avaliação de vulnerabilidade está vinculado ao incidente de segurança grave existente.
Propor como incidente de segurança grave	Insira os seguintes detalhes e selecione **Propor** . ○ Data de detecção ○ Justificativa ○ Impacto potencial
Promover como incidente de segurança grave	Insira os seguintes detalhes e selecione **Promover** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Data de detecção ○ Data de resolução estimada ○ Justificativa ○ Impacto potencial

5. Selecione **Save** (Salvar).

O que Fazer Depois

Selecione o registro MSI para abrir o registro no Gestão de incidentes graves de segurança exibir.

Tópicos relacionados

Vincular a Incidente grave de segurança

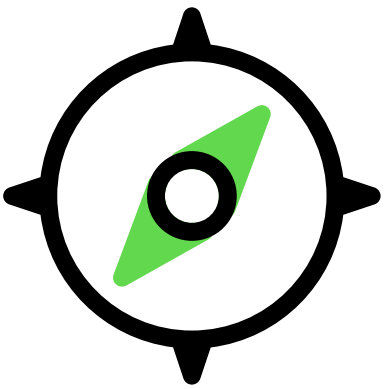
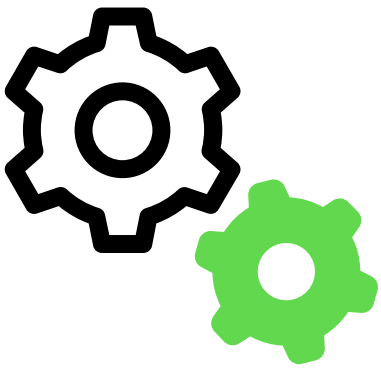
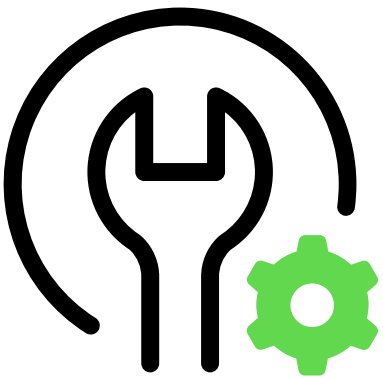
Propor como um Incidente grave de segurança

Promover para um Incidente grave de segurança

Lista de materiais de software

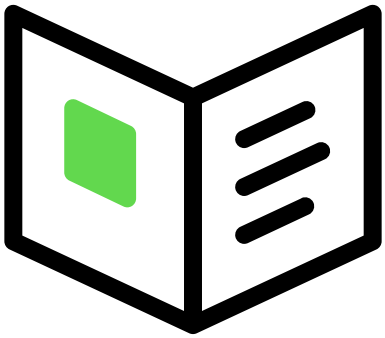
Exiba uma lista dos componentes de software de código aberto e de terceiros que você está usando no desenvolvimento de aplicações. Obtenha informações sobre licenças de software, informações de versão e as vulnerabilidades conhecidas em seus componentes no Lista de materiais de software(SBOM) arquivos que você carrega em sua instância.

Primeiros passos

Explorar	Configurar	Uso
		
Saiba mais sobre SBOM conceitos e recursos.	Configurar SBOM aplicações.	Saiba como importar SBOM e exibir dados no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Referência  Obter detalhes sobre SBOM formulários, campos, tabelas e propriedades.	

Solucionar problemas e obter ajuda

- Comunidade de Operações de segurança
- CycloneDX - Lista de materiais de software (SBOM) .
- SPDX .
- PESQUISE artigos de erros conhecidos no Portal de erros conhecidos .
- Contato Suporte e atendimento ao cliente.

Explorando Lista de materiais de software

Identifique os componentes usados nas aplicações da sua organização de Lista de materiais de software(SBOM arquivos que você carrega em sua instância. Entenda todos os riscos associados ao uso de software de código aberto para ajudar você a determinar sua possível exposição, exibir a conformidade de licença e corrigir vulnerabilidades.

Visão geral Lista de materiais de software

Componentes de terceiros e de código aberto oferecem muitas vantagens para a rápida criação e lançamento de seus projetos de software. No entanto, em alguns casos, há riscos associados ao uso de componentes acessíveis publicamente, como os seguintes:

- Falta de visibilidade da integridade do componente
- Vulnerabilidades no software de código aberto
- Inteligência de pacote para software de código aberto
- Licenças de software fora de conformidade

Você pode carregar seus arquivos de lista de materiais de software por meio de uma API ou manualmente. Exiba os arquivos que você importa como entidades, que são inventários das bibliotecas de componentes de terceiros usadas em seu software, incluindo dependências transitivas e informações de licenciamento disponíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre o que está incluído nos inventários de software no CycloneDX e SPDX SBOMs, consulte CycloneDX - Lista de materiais de software (SBOM) e. SPDX .

Lista de materiais de software usuários

Usuários

Usuário	Descrição
Gerentes e analistas de vulnerabilidades	Exiba arquivos de lista de materiais de software carregados em registros, visualizações de dados, bem como inteligência de vulnerabilidades aprimorada no Lista de materiais de software(SBOM) Espaço. Gerentes e analistas de vulnerabilidades usam essas informações para ajudá-los a determinar sua conformidade de licenciamento de software e a possível exposição a riscos com o uso de software de código aberto.
Usuários que podem incluir, mas não estão limitados a: • Advogados de tecnologia ou software • Gerentes DE TI • Auditores • Gerentes e equipes de ativos de software	Exibir licenças de software proprietárias e de código aberto carregadas para componentes do carregados SBOM arquivos. Crie um banco de dados de licenças de software proprietárias e de código aberto para os componentes. Revise e classifique licenças com informações ausentes de acordo com suas políticas internas ou regulatórias. Corresponda seus componentes às licenças e determine a conformidade geral da licença e veja sua possível exposição a risco a licenças proibidas, restritas ou ausentes.

Fluxo de trabalho do Lista de materiais de software

As aplicações SBOM permitem carregar arquivos e exibir detalhes de entidades, inventários de componentes, vulnerabilidades e informações de licença de software no Espaço da Lista de materiais de software (SBOM).

- Upload SBOM Arquivos com uma API ou manualmente.
- Revise os componentes em SBOM arquivo carregado no SBOM Espaço.
- Revise as informações de licença do componente carregadas SBOM e classificá-los para ajudar você a identificar sua exposição a licenças restritas ou proibidas.
- Avalie sua exposição ao risco e crie itens vulneráveis para componentes que têm vulnerabilidades associadas.
- Exiba relatórios e painéis, bem como a conformidade geral da licença para carregado SBOM Componentes na página inicial do SBOM Espaço.

Benefícios do Lista de materiais de software

Três aplicações de Lista de materiais de software permitem exibir um inventário preciso de seus componentes de software e riscos associados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Modelo de dados para SBOM
- SBOM Núcleo
- SBOM Resposta

Para obter informações de compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .

Benefícios do SBOM

Benefício	Aplicação	Versões com suporte
Esta aplicação fornece as tabelas usadas para armazenar SBOM dados. Esta aplicação é necessária. Ele inclui as tabelas, ACLs e funções que precisam ser lidas SBOM dados.	Modelo de dados para SBOM	v4.0, v3.0, v2.0
Esta aplicação é necessária. Ele inclui a API necessária para carregar SBOM e a lógica de negócios necessários para analisar e importar os dados desses documentos para sua instância. Você pode exibir um inventário de seus componentes de software no SBOM, mas você não pode exibir as visualizações de dados na página principal . Carregue, analise e processe seus arquivos de lista de materiais de software nos padrões CycloneDX e SPDX. Consulte a coluna Versões compatíveis para obter os formatos de arquivo compatíveis e as versões desses produtos. Exiba entidades da lista de materiais (BOM) e um inventário dos componentes de software. Uma entidade de BOM é o componente de nível raiz em um arquivo SBOM. Por exemplo, para um CycloneDX SBOM, O componente listado nos metadados é considerado a entidade de BOM.	SBOM Núcleo	v6.0, v5.0, v4.0 A partir da versão 4,0, SBOM O Core oferece suporte a: • XML e JSON versões 1,0 a 1,6 do CycloneDX. • JSON versões 2,2 a 2,3 do SPDX.
• SBOM A resposta será necessária se você quiser acessar os recursos e os dados visualizações na página principal em SBOM Espaço. • SBOM A resposta requer Resposta a vulnerabilidades aplicação. • Exiba seu inventário de componentes e avalie sua exposição ao risco no SBOM Espaço. Configure regras para criar itens vulneráveis à aplicação (AVITs) automaticamente e corrija-os com Resposta a vulnerabilidades de aplicações fluxo de trabalho. • Exiba as informações de licença do componente carregadas com seu	SBOM Resposta	v6.0, v5.0, v4.0

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Benefícios do SBOM

Benefício	Aplicação	Versões com suporte
SBOM arquivos no Módulo de administração de licenças . Classifique e resolva (corresponda) os componentes que você carrega em Resposta a vulnerabilidades de aplicações arquivos para licenças para que você possa ver o estado da conformidade de licença geral. • A partir da versão 4,0 de Resposta a vulnerabilidades de aplicações Resposta, você pode exibir componentes identificados como obsoletos ou abandonados como "fora de conformidade" na interface Política como Mecanismo de código (Pace) que está disponível em SBOM Espaço. • As integrações de OSV.dev e Deps.dev são incluídas durante a instalação SBOM Resposta. ○ OSV.dev é uma API de código aberto que fornece informações de inteligência contra vulnerabilidades para uma determinada versão de um pacote ou biblioteca. ○ O Deps.dev é uma API de código aberto que fornece uma lista de versões para um determinado pacote ou biblioteca e identifica os componentes que estão no **Obsoleto** e. **Abandonado** estados. Para obter mais informações, consulte Configuração das integrações de Deps.dev, OSV.dev e Pace para Lista de materiais de software. Consulte Integração do PaCE a outras aplicações Para obter mais informações sobre as políticas de ritmo e ritmo.		
Gerar e carregar Lista de materiais de software(SBOM arquivos de software durante toda a integração contínua e os ciclos de desenvolvimento de implantação contínua.	SBOM Resposta	• Modelo de dados para SBOM v1.4 e posterior. • SBOM Core: V3.0 e posterior. • SBOM Resposta: V4.0 e posterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades aplicações e. CSDM tabelas

. Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações integrações de vulnerabilidades de terceiros e Lista de materiais de software gerenciar aplicações (contribuir com dados para) CSDM tabelas. Esses aplicativos também usam dados do CSDM tabelas geradas por outras aplicações. Vários ServiceNow os produtos, portanto, se beneficiam e agregam valor a eles Operações de segurança aplicações. Para obter mais informações, consulte Resposta a vulnerabilidades aplicações e. CSDM tabelas.

O que explorar a seguir

Para saber mais sobre como configurar e usar o Lista de materiais de software, consulte:

- Explorar aplicações compatíveis com Lista de materiais de software
- Configuração da Lista de materiais de software
- Carregando e exibindo seu SBOM arquivos no SBOM Espaço
- Exibição de relatórios e painéis no Lista de materiais de software espaço

Explorar aplicações compatíveis com Lista de materiais de software

Inteligência de vulnerabilidades de terceiros e outras integrações com Lista de materiais de software as aplicações podem aprimorar os dados dos arquivos carregados.

Benefícios das aplicações compatíveis

Inteligência de vulnerabilidades de terceiros e outras integrações com Lista de materiais de software as aplicações permitem exibir contagens de componentes considerados obsoletos e abandonados, bem como informações sobre se você pode corrigir vulnerabilidades associadas a componentes.

. ServiceNow® as aplicações e integrações de terceiros listadas na tabela a seguir são compatíveis com SBOM aplicações. Esses aplicativos fornecem dados de vulnerabilidade aprimorados, inteligência contra vulnerabilidades e outras informações importantes que podem ajudar a exibir e priorizar as vulnerabilidades associadas aos arquivos SBOM. Todas essas aplicações e integrações estão disponíveis no ServiceNow® Store.

Aplicações compatíveis e integrações de terceiros

Benefício	Aplicação	Versões com suporte	Usuários
Resposta a vulnerabilidadesé necessário se você instalar o. SBOM Aplicação de resposta. Instale o. Resposta a vulnerabilidades Aplicação antes de instalar a Resposta do SBOM. Resposta a vulnerabilidades de	Resposta a vulnerabilidades	Para obter informações de compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações compatíveis e integrações de terceiros

Benefício	Aplicação	Versões com suporte	Usuários
aplicações os recursos são instalados com Resposta a vulnerabilidades. Esses recursos permitem o acesso ao Espaço do gerenciador de vulnerabilidades no Resposta a vulnerabilidades E o fluxo de trabalho de vulnerabilidade para ajudar a corrigir itens vulneráveis à aplicação (AVIT)			
Exiba dados aprimorados de vulnerabilidade e gravidade do NVD. Exiba dados importados das integrações de NVD e CWE para enriquecer todos os dados de vulnerabilidade que você possa encontrar em seus dados de SBOM. Para obter mais informações, consulte Importação de dados com as integrações NVD e CWE e gerenciamento de bibliotecas de terceiros.	Integração de Resposta a vulnerabilidades com Resposta de NVD e SBOM	Para obter informações de compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .	
Importe arquivos de listas de materiais de software com Integração de Resposta a vulnerabilidades com Veracode. . Integração de Resposta a vulnerabilidades com Veracode o inclui os seguintes aprimoramentos com Veracode Arquivos SBOM: • Se você tiver instalado SBOM Resposta, você tem a opção de incluir	Integração de vulnerabilidades Veracode e resposta do SBOM	A partir da versão 4,3 do Integração de Resposta a vulnerabilidades com Veracode. . Integração de Resposta a vulnerabilidades com Veracode já instalado, você também pode carregar importados Veracode SBOM Dados nos formatos CycloneDX (JSON e XML) e SPDX (XML) a partir da	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações compatíveis e integrações de terceiros

Benefício	Aplicação	Versões com suporte	Usuários
vulnerabilidades encontradas por SBOM para SBOM arquivos que você carrega. • SBOMÉ mapeado para o campo Origem para registros na tabela Lista de materiais [sn_sbom_doc] para SBOM SBOM arquivos que você carrega. Para obter mais informações, consulte Integração de Resposta a vulnerabilidades com Veracode.		versão v3.0 de SBOM Núcleo. Para obter informações de compatibilidade, consulte KB0856498 Mudanças na Matriz de compatibilidade de resposta a vulnerabilidades e no esquema de versão .	
Upload SBOM arquivos para ServiceNow AI Platform Dos repositórios do GitHub. Determine se SBOM Os arquivos gerados em seus pipelines de IC/CD (integração contínua e entrega/ implantação contínua) foram enfileirados com sucesso em seu ServiceNow AI Platform instância. Proteja seus ambientes contra componentes potencialmente prejudiciais durante os ciclos de desenvolvimento de software com ações do GitHub que você inicia no seu ambiente do GitHub.	Obtenha todas as ações do GitHub necessárias para SBOM Carregue no GitHub Marketplace.	A partir da versão 4,0 de SBOM Núcleo.	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração da Lista de materiais de software

Baixe e ative as aplicações necessárias para Lista de materiais de software(SBOM) antes de carregar SBOM arquivos.

Visão geral da configuração

1. Baixe o necessário SBOM E quaisquer aplicações e integrações adicionais compatíveis que você deseja da ServiceNow Store para sua instância da ServiceNow. Consulte Explorando Lista de materiais de software e. Baixar uma aplicação do ServiceNow Store pela primeira vez para obter mais informações sobre aplicações compatíveis.

   A aplicação Resposta a vulnerabilidades é necessária para SBOM Resposta. Instale a aplicação Resposta a vulnerabilidades antes de instalar SBOM Resposta.

2. Localize as aplicações SBOM que você baixou e selecione Instalar para ativá-las junto com suas dependências na ordem a seguir. Consulte Instale os aplicativos compatíveis para Lista de materiais de software.

   - Resposta a vulnerabilidades e suas dependências
   - Integração de Resposta a vulnerabilidades com NVD
   - Modelo de dados para SBOM
   - SBOM Núcleo
   - SBOM Resposta, que inclui as integrações de OSV.dev e Deps.dev e acesso aos recursos da Política como Mecanismo de código (Pace) no Espaço do SBOM.

3. Configure as integrações de Deps.dev e OSV.dev. Essas integrações estão incluídas com SBOM E são instalados e ativados automaticamente. Você deve iniciar a Integração OSV.dev - abrangente sob demanda do registro de integração. Consulte Configuração das integrações de Deps.dev, OSV.dev e Pace para Lista de materiais de software e. Explorando Lista de materiais de software para obter mais informações.

   A integração Deps.dev fornece informações sobre os componentes que estão no **Obsoleto** e. **Abandonado** estados de uma determinada versão de um pacote ou biblioteca que você carrega em SBOM arquivos.

   O OSV.dev extrai dados de vulnerabilidade de um banco de dados de código aberto para uma versão de um pacote ou biblioteca que você carrega em SBOM arquivos.

4. Consulte a documentação do produto para configurar todas as aplicações e integrações compatíveis adicionais que você instalou. Consulte Integrações do Resposta a vulnerabilidades e Integração do Resposta a vulnerabilidades de aplicações a outras aplicações.

Instale os aplicativos compatíveis para Lista de materiais de software

Baixe e ative as aplicações necessárias para Lista de materiais de software(SBOM) antes de carregar arquivos.

Antes de Iniciar
Funções necessárias: administrador para download, instalação e ativação de todas as aplicações e atribuições de função em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Baixe o necessário SBOM aplicações do ServiceNow Store em seu ServiceNow instância.

   Esses aplicativos permitem que você carregue e importe SBOM em sua instância. Você pode exibir dados de entidade e componente da BOM no SBOM Espaço, se você tiver SBOM Núcleo instalado.

   Você pode exibir a entidade da BOM, os dados do componente e as visualizações de dados no SBOM Espaço, se você tiver SBOM Resposta instalada.

   - Modelo de dados para SBOM
   - SBOM Núcleo

   Para obter mais informações sobre como baixar e ativar aplicações, consulte o seguinte:

   - Instale um ServiceNow Store aplicação
   - Instale uma atualização em um ServiceNow Store aplicação

2. **Opcional:** Se você quiser exibir seu SBOM dados no SBOM, Exiba inteligência de vulnerabilidades de terceiros importada, avalie sua exposição a riscos e corrija vulnerabilidades com o. Resposta a vulnerabilidades de aplicações e. Resposta a vulnerabilidades fluxos de trabalho, baixe os seguintes aplicativos:

   - Resposta a vulnerabilidades e suas dependências
   - Integração de Resposta a vulnerabilidades com NVD
   - SBOM Resposta

   Para obter mais informações sobre esses e outros compatíveis SBOM aplicações, consulte Explorando Lista de materiais de software.

3. Depois de baixar os aplicativos, navegue até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
4. Localize SBOM aplicações que você baixou e selecionou **Instalar** para ativá-los junto com suas dependências.

   Uma mensagem é exibida depois que uma aplicação é ativada com sucesso. Ative as aplicações na seguinte ordem:

   - Resposta a vulnerabilidades e suas dependências
   - Integração de Resposta a vulnerabilidades com NVD
   - Modelo de dados para SBOM
   - SBOM Núcleo
   - SBOM Resposta, que inclui as integrações de OSV.dev e Deps.dev e oferece suporte à interface Política como Mecanismo de código (Pace) no SBOM Espaço.

   Consulte Configuração das integrações de Deps.dev, OSV.dev e Pace para Lista de materiais de software para obter mais informações sobre como configurar esses aplicativos de integração após a instalação do SBOM Resposta.

5. **Opcional:** Navegue até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo** e selecionando **Instalar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Para obter mais informações sobre essas integrações e os recursos que elas fornecem, consulte Explorando Lista de materiais de software.

- Integração do Vulnerability Response com o Veracode. Para obter mais informações, consulte Instale o. ServiceNow Integração de Resposta a vulnerabilidades com Veracode.
- Integração de Resposta a vulnerabilidades com NVD, que é necessária se você quiser exibir os dados aprimorados para vulnerabilidades associadas a componentes carregados. Para obter mais informações, consulte Noções básicas sobre as integrações de NVD.
- Integração abrangente do CWE 2000. Consulte Configure e execute o trabalho agendado para atualizar registros CWE para obter mais informações sobre como ativar este trabalho agendado.

Uma mensagem é exibida depois que uma aplicação é ativada com sucesso.

6. Atribua as seguintes funções aos usuários.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolvedor
7. **Opcional:** Atribua usuários ao grupo Gerenciador da App-Sec se você estiver criando itens vulneráveis à aplicação para vulnerabilidades no importado SBOM dados.

   (Optional) Os usuários atribuídos ao grupo Gerenciador da App-Sec priorizam e gerenciam itens vulneráveis da aplicação. Os usuários deste grupo herdam muitas das funções necessárias para ler e editar registros e configurar as aplicações compatíveis com Resposta a vulnerabilidades de aplicações e seus fluxos de trabalho de correção.

8. **Opcional:** Reabrir AVITs se detectados (*sn_sbom_resp.reopen_avits_if_detected*propriedade do sistema) se você não quiser **Encerrado** AVITs para fazer a transição de volta para **Aberto** estado automaticamente.

   (Optional) . **Encerrado** O item vulnerável à aplicação (AVIT) de um componente com uma vulnerabilidade associada é reaberto (definido como **Aberto** Automaticamente e visível no Espaço do SBOM se as seguintes condições existirem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O AVIT com a vulnerabilidade associada é detectado novamente por verificações de vulnerabilidade de integração de terceiros ou o componente com a vulnerabilidade faz parte de um carregamento subsequente do SBOM.
- Reabrir AVITs não foi desabilitado se detectado (*sn_sbom_resp.reopen_avits_if_detected*propriedade do sistema). Esta propriedade do sistema é ativada por padrão.
- O subestado do **Encerrado** Avit não é um dos seguintes: **Controle de mitigação em vigor** , **Não afetado** ou **Falso-positivo** . AVITs com esses subestados não são reabertos pela propriedade do sistema.

O que Fazer Depois

Carregue seu SBOM arquivos. Para obter mais informações, consulte Upload Lista de materiais de software arquivos manualmente e Carregando Lista de materiais de software Arquivos que usam uma REST API.

Configuração das integrações de Deps.dev, OSV.dev e Pace para Lista de materiais de software

Você pode editar alguns dos parâmetros das integrações de Deps.dev e OSV.dev. Também há duas versões de gatilho de código dessas integrações que são usadas estritamente para fluxos de trabalho internos, e você não deve iniciar essas integrações sob demanda. Além disso, você pode ativar um trabalho agendado para criar políticas usando Política como Mecanismo de código (Pace).

Integrações de gatilho de código para fluxos de trabalho internos

A partir da v3.2 de SBOM Melhorias de desempenho incluídas a adição de dois OSV.dev e Deps.dev. gatilho de código integrações:

- Integração OSV (gatilho de código sob demanda)
- Integração Deps.dev (gatilho de código sob demanda)

Essas integrações são iniciadas automaticamente por fluxos de trabalho internos e são somente para uso interno. Embora você possa localizá-los, você não deve iniciar essas integrações sob demanda com **Executar agora** de seus registros de integração.

Configurar a programação de execução da integração Deps.dev.

A integração Deps.dev. instalado com SBOM Resposta. A integração está ativada (caixa de seleção Ativo marcada no registro de integração) por padrão e programada para ser executada semanalmente. Observe que esta não é a integração do gatilho de código Deps.dev sob demanda e você pode editar a programação e iniciar o trabalho agendado sob demanda a partir do registro de integração. .

Para modificar a programação, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações** > **Integração Deps.dev**. A função sn_vul.app_configure_integrations é necessária para editar a programação desta integração.

Esta integração de Deps.dev é usada para identificar os componentes que estão no **Obsoleto** e. **Abandonado** estados. A versão de um componente obsoleto é mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. Um componente abandonado não foi atualizado há mais de dois anos. Os limites de dois anos e duas versões podem ser editados com as propriedades do sistema. Para editar esses parâmetros, navegue até **Tudo** > **Propriedades do sistema** > **Todas as Propriedades** e localize os seguintes registros:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Os valores de limite para abandonado e obsoleto estão em meses. O valor limite da versão é numérico.

Você pode exibir dados importados na página inicial do espaço e no módulo Fila da BOM. Os dados importados são armazenados na tabela Grupos de pacotes [sn_sbom_pkg_group].

Configuração e início da Integração OSV.dev - Abrangente

Integração OSV.dev - Abrangente a integração é instalada com SBOM Resposta. A integração está ativada (caixa de seleção Ativo marcada no registro de integração) por padrão. Observe que esta não é a integração do gatilho de código OSV.dev sob demanda e você deve iniciar essa integração sob demanda a partir do registro de integração.

Para configurar e iniciar esta integração, navegue até **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações** > **Integração OSV.dev - Abrangente**. A função sn_vul.app_configure_integrations é necessária.

Você pode exibir dados importados na página inicial do espaço na guia Vulnerabilidade em registros da lista Entidades e no módulo Bibliotecas. Os dados importados são armazenados nas tabelas Entradas vulneráveis à aplicação [sn_vul_app_vul_entry] e Entradas do banco de dados nacional de vulnerabilidades [sn_vul_nvd_entry].

Nota: Você pode configurar o OSV.dev's *batchSize*Parâmetro de integração na guia Parâmetros de integração no **Instância de vulnerabilidades de código aberto** localizado em **Tudo** > **Resposta a vulnerabilidades** > **Administração** > **Integrações** > **Integrações de Vulnerabilidade** > **Instância de vulnerabilidades de código aberto**. O padrão é 75 Purls por chamada de API.

Você pode preferir deixar este valor em sua configuração padrão. Alterar o valor pode afetar o desempenho.

Ativando o ritmo

A partir da versão 4,0 de SBOM Resposta, você pode exibir componentes identificados como obsoletos ou abandonados como "fora de conformidade" na interface Política como Mecanismo de código (Pace) que está disponível em SBOM Espaço.

- Determine se os componentes estão obsoletos ou abandonados com *Run PaCE policies for SBOM Response*trabalho agendado. Este trabalho agendado está desativado por padrão.
- Exiba componentes identificados como obsoletos ou abandonados como fora de conformidade na interface do Pace que está disponível e exibido no SBOM Espaço.

Consulte Integração do PaCE a outras aplicações Para obter mais informações sobre as políticas de ritmo e ritmo.

Carregando e exibindo seu SBOM arquivos no SBOM Espaço

. SBOM As aplicações permitem que você carregue arquivos e exiba detalhes de entidades, inventários de componentes, informações de licença e outros detalhes no Espaço de lista de materiais do software.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral de carregando SBOM arquivos

Você pode carregar seus arquivos de lista de materiais de software por meio de uma API ou manualmente. Exiba os arquivos que você importa como entidades, que são inventários das bibliotecas de componentes de terceiros usadas em seu software, incluindo dependências transitivas.

- Carregando Lista de materiais de software Arquivos que usam uma REST API.

  A API de carregamento é usada para carregar e ingerir um SBOM Arquivo (CycloneDX/SPDX) em sua instância.

- Upload Lista de materiais de software arquivos manualmente.

  Carregue arquivos de lista de materiais de software manualmente. O método que você usa para carregar seus arquivos depende de você ter o SBOM Núcleo ou SBOM Aplicações de resposta instaladas.

- Carregando Lista de materiais de software Para DevOps SBOM arquivos.

  Gerar e carregar SBOM arquivos para software durante toda a integração contínua e os ciclos de desenvolvimento de implantação contínua.

- Classifique e resolva licenças de componente no módulo Administração de licenças.

  Revisão classificar e resolver (atribuir) informações de licença para os componentes que você carrega em SBOM arquivos de acordo com suas políticas internas ou regulatórias. Você pode corresponder seus componentes às licenças e determinar a conformidade geral da licença para ver sua possível exposição ao risco a licenças proibidas, restritas ou ausentes.

- Exibição de relatórios e painéis no Lista de materiais de software espaço

  Os analistas e gerentes de vulnerabilidades podem exibir arquivos de lista de materiais de software carregados e dados importantes em registros, visualizações de dados, bem como inteligência de vulnerabilidades aprimorada e informações de licença Lista de materiais de software(SBOM) Espaço.

  Nota: Você deve instalar SBOM Resposta se você quiser exibir as visualizações de dados na página principal (Página inicial) do espaço.

Tradução automática

Carregando Lista de materiais de software Arquivos que usam uma REST API

Revise as seguintes informações antes de carregar Lista de materiais de software Arquivos que usam uma API.

Usando a REST API

Para carregar um arquivo SBOM com uma API, a função sn_sbom_core.sbom_ingest é necessária.

Carregar API.

Esta API é usada para carregar e ingerir um arquivo SBOM (CycloneDX/SPDX) em sua instância.

Versão 4,0 de SBOM O Core oferece suporte a:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- XML e JSON no CycloneDx (versões 1.0 - 1.6).
- JSON no SPDX (versões 2,2-2,3)

- **Nota:** Arquivos com mais de 32 MB podem não ser carregados corretamente.

Método HTTP: (POST)

URL DA API: `<host_name>/api/sbom/core/upload`

Nota: `<host_name>` é seu ServiceNow nome da instância.

Todos os parâmetros de solicitação abaixo são opcionais; o corpo da solicitação é o conteúdo do arquivo SBOM. Se você estiver usando DevOps como parte do seu processo de desenvolvimento, o valor de "questedBy" deve ser "devots". Consulte Carregando Lista de materiais de software Para DevOps SBOM arquivos Para obter mais informações gerais sobre DevOps. Se o valor de "questedby" for "devops" (operações de desenvolvimento), estes parâmetros serão obrigatórios:

- Criado
- Fase de Vida

Além disso, se "questedBy" for "devops", os dados de fetchVulenrabilityInfo e fetchPackageInfo serão incluídos.

- Cadeia de caracteres buildid- que você envia
- LifecycleStage- Dois valores, production ou pre_production
- FetchVulenrabilityInfo- t/f
- FetchPackageInfo-t/f

Parâmetros da solicitação	Valores possíveis	Descrição
productModelId	SYS ID	SYS ID do modelo de produto a ser mapeado com a aplicação raiz de fornecida SBOM.
BusinessApplicationId	SYS ID	SYS ID da aplicação de negócios a ser mapeada com a aplicação raiz de fornecida SBOM.
BusinessApplicationName (descontinuado)	Seu nome da aplicação de negócios	Nome da aplicação de negócios a ser mapeada com a aplicação raiz de fornecida SBOM.
SbomSource	Um produto como Veracode, por exemplo	A origem do seu SBOM arquivo.
requestedBy	Uma ferramenta, ou nome de uma metodologia, Jenkins. Se você usar "devops", buildid e lifecycleStage serão obrigatórios.	Carregamento solicitado por
Criado	Um solicitante de cadeia de caracteres envia.	ID de compilação do SBOM compilação.
Fase de Vida	produção ou pre_production	Fase do ciclo de vida da entidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros da solicitação	Valores possíveis	Descrição
FetchVulenrabilityInfo	t/f	Se verdadeiro, aciona a integração de inteligência de vulnerabilidades.
FetchInformações do pacote	t/f	Se verdadeiro, aciona a integração de inteligência de pacote.

Carregar resposta da API: Sucesso/falha "status", "message" (cadeia de caracteres), "bomRecordId" incluído (este é o sys ID do SBOM retornado por meio da API de upload para um carregamento bem-sucedido do SBOM).

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```

API de status

Esta API obtém o status e o resumo de um SBOM que está enfileirado para ingestão.

- URL DA API: `/api/sbom/core/upload/status`
- Método HTTP (GET)

Parâmetros da solicitação	Valores possíveis	Descrição
BomRecordId	SYS ID	ID do registro do SBOM que é retornado por meio da API de carregamento para um carregamento bem-sucedido do SBOM.

Exemplo de resposta padrão da API de status.

```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    }
}
```

Exemplo de resposta da API de status com parâmetros adicionais. Se você solicitou fetchVulenrabilityInfo para esse SBOM, obterá o detalhamento da vulnerabilidade como parte da resposta.

```
{
 "result": {
  "bomRecordId": "93af349b4393c290629aa597cbb8f258",
  "uploadStatus": "processed",
  "additionalInfoStatus": "complete",
  "uploadSummary": {
    "components": {
     "added": 0,
     "removed": 0,
     "total": 3
   },
   "vulnerabilityInfo": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "none": 0
   }
  },
  "buildId": "1"
 }
}
```

Se você solicitou fetchPackageInfo para esse SBOM, obterá contagens obsoletas e abandonadas como parte da resposta.

Depois de um SBOMé processado com sucesso, onde você exibe os registros carregados depende das aplicações que está usando.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se você estiver usando SBOM Resposta, o registro da entidade da BOM é exibido no SBOM Lista Status de ingestão no módulo Fila da BOM no SBOM Espaço.
- Se você estiver usando o SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Melhorias no compatíveis SBOM padrões e informações gerais de uso

Versão 4,0 de SBOM O Core oferece suporte a:

- XML e JSON no CycloneDx (versões 1.0 - 1.6).
- JSON no SPDX (versões 2,2-2,3)

- **Nota:** Arquivos com mais de 32 MB podem não ser carregados corretamente.

A partir da v4.0 de SBOM Core, as seguintes melhorias foram feitas para oferecer suporte aos padrões CycloneDx para as versões 1,0 a 1,6:

- Importe informações adicionais nos arquivos SBOM do CycloneDX com a propriedade (sn_sbom_core.collect_properties). Esta propriedade está desativada por padrão. Ative a propriedade para importar informações que geralmente não são compatíveis. Todas as informações importadas dessas propriedades são carregadas na tabela Propriedade do componente SBOM [sn_sbom_comp_property] para o seguinte:
  - Arquivos SBOM carregados
  - Metadados
  - Vulnerabilidades individuais
  - Componentes
- Exiba dados de componentes importados para licenças declaradas e concluídas para arquivos SBOM nas versões 1,4 e posteriores do CycloneDX em dois novos campos de licença:
  - **Declarado**
  - **Concluído**
- O suporte à análise do SBOM foi estendido para os seguintes tipos de componente do CycloneDX:
  - Versão 1,5: Plataforma, dados, driver de dispositivo, modelo de aprendizado de máquina
  - Versão 1,6: Criptográfico

Versão 3,0 de SBOM O Core oferece suporte a:

- XML e JSON no CycloneDx (até e incluindo a versão 1,4).
- JSON em SPDX (até e incluindo v2.3).

Se o usuário chamador for autenticado com sucesso e tiver a função sn_sbom_core.sbom_ingest em seu ServiceNow, você pode acessar a API de fora da sua instância para carregar o. SBOM dados.

Depois que os dados são carregados, eles são analisados. Antes que os dados sejam analisados, os seguintes requisitos são verificados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os dados de entrada são verificados se são JSON ou XML válidos.
- O formato da BOM é compatível. A partir da v2.1 de SBOM Os formatos Core, CycloneDX (JSON e XML) e SPDX (XML) são compatíveis.
- Os campos mínimos estão disponíveis para que os dados possam ser analisados.

Depois que essas verificações são verificadas, uma entrada é feita na tabela Lista de materiais [sn_sbom_doc] com a entrada SBOM dados como um anexo.

. *Process BOM file*a regra de negócio é acionada automaticamente como resultado da inserção de registro e da análise de dados.

Nota: Esta regra de negócio é ativada durante a instalação de SBOM Core por padrão.

Todos os componentes listados em um SBOM definido tipo .

- Componentes para os quais SBOM Os arquivos carregados são considerados entidades de BOM.
- Componentes listados como tipo: biblioteca são considerados componentes de terceiros.

Tópicos relacionados

Exibir status de carregamento para Lista de materiais de software arquivos

Exibição de relatórios e painéis no Lista de materiais de software espaço

Upload Lista de materiais de software arquivos manualmente

Upload Lista de materiais de software(SBOM) arquivos manualmente.

Antes de Iniciar

A partir da versão 4,0, o SBOM Core oferece suporte a:

- XML e JSON nas versões 1,0 - 1,6 do CycloneDX.
- JSON nas versões 2,2 a 2,3 do SPDX.

Função necessária: sn_sbom_core.sbom_ingest

Procedimento

1. Carregar arquivos manualmente.

   O método que você usa para carregar seus arquivos depende de você ter o SBOM Núcleo ou SBOM Aplicações de resposta instaladas.

Opção	Descrição
Se você tiver instalado SBOM Núcleo	**a.** Navegar até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**. **b.** Na lista Lista de materiais, selecione **No vo** . **c.** Selecione **Clique para adicionar** link. Você pode carregar um SBOM arquivo de cada vez.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	d. Selecione **Escolha o arquivo** e localize o arquivo desejado. O nome do arquivo é exibido na página Escolher um arquivo de anexo. **e.** Selecione **OK**.
Se você tiver instalado SBOM Resposta que começa com v4.0	**a.** Navegar até **Tudo** > **Espaços** > **Espaço de SBOM** > **Fila de lista de materiais**. **b.** Selecione **Carregar BOM** . O modal Carregar arquivo SBOM é exibido. **c.** Selecione **Anexar arquivo** link. **d.** Localize o arquivo desejado e selecione **Aberto** . Após o carregamento do arquivo, um link para o arquivo é exibido junto com três ícones que fornecem as seguintes opções: ▪ Baixe o arquivo. ▪ Edite o nome do arquivo. ▪ Exclua o arquivo do carregamento. **e.** Selecione **Upload** para continuar. Você pode carregar um SBOM arquivo de cada vez. **f.** (Opcional) Selecione uma aplicação de negócios e um modelo de produto nas listas. Esses valores ajudam você a associar isso SBOM para uma aplicação de negócios ou modelo de produto em sua organização. Essas informações são exibidas no registro de entidade da BOM após o carregamento. **g.** Selecione **Carregar**. A página da fila da BOM é exibida e o arquivo é listado na seção Ingestão do SBOM junto com o status de carregamento de outras informações sobre o arquivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Opcional:** Upload SBOM arquivos importados pelo Integração de Resposta a vulnerabilidades com Veracode.

> **Nota:** Você pode carregar Veracode Arquivos nos formatos CycloneDX (JSON e XML) e SPDX (XML) somente se você tiver instalado e ativado o. Veracode integração com Resposta a vulnerabilidades de aplicações. Consulte Integração de Resposta a vulnerabilidades com Veracode para obter mais informações.

Resultado

Depois de um SBOMé processado com sucesso, onde você exibe o status de carregamento depende das aplicações que está usando.

- Se você estiver usando SBOM Resposta, o registro da entidade da BOM é exibido no SBOM Lista Status de ingestão no módulo Fila da BOM no SBOM Espaço.
- Se você estiver usando SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Tópicos relacionados

Carregando Lista de materiais de software Arquivos que usam uma REST API

Carregando Lista de materiais de software Para DevOps SBOM arquivos

Gerar e carregar Lista de materiais de software SBOM arquivos para software durante toda a integração contínua e os ciclos de desenvolvimento de implantação contínua.

DevOps e. SBOM arquivos

SBOM Os arquivos podem ser gerados em várias fases ao longo do ciclo de vida de desenvolvimento de integração contínua de software e implantação contínua (CI/CD). A maioria das operações de desenvolvimento de software (DevOps) nas organizações usa algum tipo de processo de CI/CD para ajudá-las a identificar e evitar erros caros que podem surgir após o lançamento. Em todo o pipeline de CI/CD, o DevOps pode gerar arquivos SBOM e verificar proativamente se há vulnerabilidades e componentes em risco. Essas verificações podem ajudar as organizações a alcançar melhor qualidade de software e evitar manutenção dispendiosa posteriormente. Gerando SBOM Arquivos são essenciais para implementar e automatizar com sucesso avaliações de compilação precisas durante o desenvolvimento de IC/CD.

O carregamento de arquivos SBOM de pipelines de desenvolvimento é compatível a partir das seguintes versões do SBOM aplicações.

Versões com suporte

Aplicação	Versões com suporte
Modelo de dados para SBOM	v3.0, v2.0
SBOM Núcleo	v5.0, v4.0, v3.0
SBOM Resposta	v5.0, v4.0, v3.2, 3,1

Casos de uso

Gerando SBOM Os arquivos e o envio deles por meio da API de carregamento do SBOM como parte do pipeline de compilação do DevOps podem fornecer contagens para o seguinte para determinar se o pipeline deve ser bem-sucedido ou falhar:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Componentes adicionados
- componentes removidos
- Informações sobre vulnerabilidades
- Informações do pacote (componentes abandonados/obsoletos)

As políticas e regras de DevOps para o sucesso ou falha de um pipeline podem ser definidas pelas contagens de vulnerabilidades e limites de contagem de componentes obsoletos e abandonados que são recebidos do SBOM API de status.

Para um pipeline com falha, os usuários do DevOps podem acessar informações sobre a compilação com falha em ServiceNow® instância para ajudá-los a entender melhor a causa raiz e a origem das vulnerabilidades.

Consulte Carregando Lista de materiais de software Arquivos que usam uma REST API Para obter mais informações sobre parâmetros (POST) e (GET) e URLs para as APIs de Upload e Status.

Separação de domínios

Todas as tabelas nas aplicações SBOM são separadas por domínio.

Classificando licenças e resolvendo licenças de componente no Lista de materiais de software espaço

Classifique licenças e resolva (corresponda) a componentes ou crie licenças no módulo Administração de licenças no SBOM espaço. Classificar e corresponder licenças aos seus componentes permite que você determine a conformidade da licença para os componentes de software proprietários, de código aberto e fornecidos pelo fornecedor que você carrega no SBOM arquivos.

Dados de licença e software de terceiros

À medida que as organizações criam mais de seus próprios aplicativos de software, elas estão usando componentes de código aberto e software fornecido pelo fornecedor. O uso de componentes de terceiros e de código aberto oferece muitas vantagens para a rápida criação e lançamento de seus projetos de software. No entanto, o uso desses componentes traz riscos de licenciamento:

- Componentes de software de código aberto e fornecidos pelo fornecedor às vezes dependem de outros componentes, e cada componente pode ter seus próprios requisitos de licenciamento.
- Se você não estiver em conformidade com os termos de suas licenças para os componentes e software em suas aplicações, poderá enviar inadvertidamente código que viola suas políticas internas e requisitos de licenciamento regulatório.

O módulo Administração de licenças

O módulo Administração de licenças no Espaço do SBOM permite que você execute as tarefas a seguir.

- Classifique as licenças que exigem isso para os componentes que você carrega com seu SBOM arquivos.
- Resolva cada licença que você classificar para um componente específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Veja qual porcentagem dos componentes que você está usando está fora de conformidade em uma visualização de dados na página inicial. Você pode usar essas informações para ajudar a determinar sua postura geral de segurança e possível exposição a riscos.

. SBOM Os arquivos carregados incluem informações de licença, o banco de dados de licenças cresce automaticamente conforme licenças exclusivas são observadas em cada carregamento do SBOM. Com cada carregamento do SBOM, você pode criar um banco de dados de licenças carregadas e classificá-las, se necessário, com o módulo Administração de licenças no SBOM Espaço. Você cria um inventário de licenças para poder atribuí-las a componentes depois de classificá-las em uma das seguintes categorias:

- Permitido
- Restrito(a)
- Banido
- Não classificado

Os funcionários jurídicos, gerentes de licença, gerentes de conformidade e regulatórios executam tarefas no módulo Administração de licenças.

Exibindo dados de licença carregados

Você tem as seguintes opções para exibir todas as informações de licença carregadas com seus componentes no Espaço do SBOM.

- Navegar até **Espaços** > **Espaço de SBOM** > **Componentes**.

  Na página Componentes, o cartão Classificação de licença de componentes exibe uma visualização da conformidade geral da licença com as seguintes categorias.

Categoria	Descrição
Banido	O uso licenciado não é permitido.
Classificação necessária	A licença ainda não foi classificada e requer uma revisão.
Permitido	O uso licenciado é permitido sem restrições.
Restrito(a)	O uso licenciado não é permitido em casos de uso específicos.

  Este snapshot usa as classificações e as informações de licença resolvidas que você insere no módulo Administração de licenças para calcular sua conformidade de licença geral.

  Se você selecionar um registro de componente nesta lista, poderá exibir as informações de licença do componente junto com outras informações no campo Estado.

- Como alternativa, navegue até **Espaços** > **Espaço de SBOM** > **Administração de licenças** > **Classificação de licença**.

  Esta página rastreia o número total de licenças exclusivas que foram detectadas nos arquivos SBOM que você carregou. Também os filtra em cartões na parte superior da página nas categorias a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Não classificado - A licença requer revisão e classificação.
- Proibido - O uso de licença não é permitido.
- Restrito - A licença não é permitida em casos de uso específicos.
- Permitido - O uso da licença é permitido sem restrições.
- Todas as licenças - Contagem total de licenças.

Todos os componentes da sua organização estão usando uma das licenças listadas nesta página. Quando uma nova licença é detectada a partir de um carregamento do SBOM, um registro é criado e armazenado na tabela Licença do SBOM [sn_sbom_license] e adicionado a esta lista. Sua classificação por padrão é, **Classificação necessária** . Os registros de licença neste estado devem ser revisados e classificados antes que você possa resolvê-los (corresponder) aos componentes para que a conformidade geral da licença seja calculada com precisão.

Para obter informações sobre como classificar licenças, consulte Classificar licenças importadas no Lista de materiais de software Espaço.

Funções

Novas licenças devem ser classificadas por um usuário com a função sn_sbom_response.managelicense. Este usuário exibe as informações de licença carregadas e determina quais licenças são permitidas e quais são proibidas. Usuários com esta função não podem exibir o módulo de resolução de licença do componente, a menos que tenham a função sn_sbom_response.licenseresolver.

Após a classificação, as licenças devem ser resolvidas por um usuário com a função sn_sbom_response.licenseresolver para que sua conformidade de licença geral possa ser determinada. Este usuário resolve licenças para componentes. Usuários com esta função não podem exibir o módulo Classificação de licença, a menos que tenham a função sn_sbom_response.managelicense.

Classificar novas informações de licença é um processo contínuo. Você pode preferir manter o número total exibido no cartão não classificado baixo. Como gerente de licenças, você pode preferir verificar se há licenças que precisam de classificação a cada poucos dias e depois de carregar arquivos SBOM.

Como resolvedor de licença, você pode preferir verificar se há licenças classificadas atualizadas a cada poucos dias.

Classificar licenças importadas no Lista de materiais de software Espaço

Classifique as licenças de componente que você carrega com seu SBOM Arquivos com o recurso Classificação de licença.

Antes de Iniciar

Classificar novas informações de licença é um processo contínuo. Você pode preferir manter o número total exibido no cartão não classificado baixo. Como gerente de licenças, você pode preferir verificar se há licenças que precisam de classificação a cada poucos dias e depois de carregar arquivos SBOM.

Função necessária: sn_sbom_response.managelicense

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de SBOM** > **Administração de licenças** > **Classificação de licença**.

   Nota: A menos que você também tenha a função sn_sbom_response.licenseresolver, somente a guia Classificação de licença ficará visível.

2. **Opcional:** Selecione um cartão para filtrar licenças por suas classificações.
3. Para classificar licenças, escolha uma.

Opção	Descrição
Edite registros em massa ou edite mais de um registro na lista.	**a.** Selecione vários registros. **b.** Clique duas vezes no cabeçalho da coluna Classificação. **c.** Atualize a classificação.
Edite e atualize a classificação no registro.	**a.** Selecione um registro da lista para abri-lo. **b.** Adicione anotações de trabalho e anexos, se necessário. **c.** Selecione **Save** (Salvar).

4. Depois de classificar as licenças, você está pronto para Resolva licenças classificadas para componentes .

Resolva licenças para componentes no Lista de materiais de software Espaço

Resolver (atribuir) licenças classificadas a componentes específicos com o recurso Resolução de licença de componente. Atribua licenças a componentes com informações ausentes ou incorretas ou crie novas licenças para que a conformidade geral da licença possa ser calculada.

Antes de Iniciar

Função necessária: sn_sbom_response.licenseresolver

Procedimento

1. Navegar até **Espaços** > **Espaço de SBOM** > **Administração de licenças** > **Resolução de licença do componente**.

   Nota: A menos que você também tenha a função sn_sbom_response.managelicense, somente a guia Resolução de licença do componente ficará visível.

   Esta página rastreia o número total de licenças exclusivas e uma exibição resumida dos totais de licenças que foram detectados nos arquivos SBOM que você carregou. As licenças exibidas nesta página se enquadram em duas categorias amplas, pois estão relacionadas a componentes.

   - Todas as instâncias do componente concordam com uma licença.
   - Uma única licença é discordada e há mais de uma licença para um componente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No segundo caso, você deve reconciliar essas licenças para que uma única licença seja resolvida para um único componente. A conformidade da licença é calculada com base em uma licença resolvida por componente.

As licenças nesta página são filtradas nas seguintes categorias para ajudar você a resolvê-las.

Valor	Descrição
Componentes com licenças não resolvidas	Nenhuma licença foi atribuída ao componente e ele requer resolução. (vazio) É exibido na coluna Licença resolvida para esses componentes. Os totais de licenças ausentes e múltiplas são listados como parte desta categoria.
Componentes com licenças ausentes.	Componentes com informações de licença ausentes que exigem resolução.
Componentes com várias licenças	Componentes visíveis em várias entidades que têm licenças diferentes e exigem resolução.
Todos os componentes	Lista total de componentes rastreados em sua organização. Você pode mudar licenças nesta lista filtrada.

2. Selecione um cartão.
3. Escolha um para resolver uma licença.

Opção	Descrição
Atribua uma licença existente a um componente.	**a.** Clique duas vezes em um campo na coluna Licença resolvida de um componente. **b.** Selecione uma licença na lista Licença resolvida. **c.** Sua edição é salva e o cartão associado na parte superior é atualizado. **d.** Como alternativa, selecione o registro na coluna Nome para abri-lo. Ele é aberto em uma nova guia. **e.** Clique em **Entidades DE BOM** para ver onde o componente está sendo usado. **f.** Selecione um na lista Licença resolvida. **g.** Insira uma justificativa. **h.** Selecione **Save** (Salvar). **i.** Atualize a página para atualizá-la.
Mude uma licença para um componente que já tem um.	Você pode escolher esta opção se determinar que uma licença foi atribuída incorretamente a um componente ou precisa ser alterada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Selecione **Todos os componentes** cartão. **b.** Localize o componente que você deseja modificar. **c.** Selecione o registro na lista para abri-lo. **d.** Selecione um na lista Licença resolvida. **e.** Selecione **Save** (Salvar). **f.** Atualize a página para atualizá-la.
Crie uma licença.	Você pode usar esta opção se souber que uma licença específica é usada em sua organização, mas um registro não foi detectado de um anterior SBOM E não há registro para ele listado no módulo Classificação de licença. **a.** Selecione **Novo** Na guia Classificação de licença e preencha os campos. **b.** Nome- Nome exclusivo desta licença. **Nota:** O nome de exibição é baseado no campo ID. Se o campo ID não estiver definido, o nome de exibição será baseado no campo Nome. Se o campo Nome não estiver definido, o nome de exibição será baseado no campo Expressão. **c.** Classificação. Selecione uma: ▪ Não classificado - A licença requer revisão e classificação. ▪ Proibido - O uso de licença não é permitido. ▪ Restrito - A licença não é permitida em casos de uso específicos. ▪ Permitido - O uso da licença é permitido sem restrições. **d.** Tipo de licença. Essas informações não são usadas pelo sistema ou para um fluxo de trabalho. Essas informações são fornecidas para ajudar você a armazenar informações adicionais e categorizar suas licenças. **e.** Site da origem da licença. Não é usado por um fluxo de trabalho ou um sistema. **f.** Expressão: Combine aritmeticamente licenças. Por exemplo, Apache-2,0 COM GPL-2,1-or-later são combinados para uma expressão. Combinações ou expressões de licença são tratadas como uma licença no ServiceNow AI Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	g. Anexos. Adicione anexos ou anotações de trabalho. **h.** Selecione **Save** (Salvar). Esta licença é adicionada ao seu banco de dados, é exibida na página Classificação de licença e agora pode ser detectada em componentes durante SBOM carregamentos.
Carregue várias licenças e classificações.	Você pode escolher esta opção se tiver um arquivo com várias licenças e classificações para as quais deseja criar registros. Você pode carregar arquivos no formato especificado e armazená-los na tabela Licença do SBOM [sn_sbom_license]. **a.** Navegue até SBOM tabela licença [sn_sbom_license]. **b.** Selecione **Mais opções** menu de qualquer coluna. **c.** Selecione **Importar**. Na página exibida, carregue um modelo compatível existente ou baixe o modelo gerado pela Plataforma (**Criar modelo do Excel**). Você carrega os dados neste modelo que é inserido na tabela. **d. Escolha o arquivo** e localize seu arquivo. **e.** Selecione **Carregar**. Seu arquivo é carregado e os registros são criados na tabela Licença do SBOM [sn_sbom_license] e podem ser visualizados no SBOM Espaço na página Classificação de licença.

Tradução automática

4. Navegue até a página inicial no Espaço do SBOM para ver qual porcentagem dos componentes que você está usando está fora de conformidade na classificação de licença da visualização de componentes.
   Os dados desta visualização são atualizados diariamente pelo trabalho programado Detalhamento de licença de componentes da BOM. Este trabalho faz parte do trabalho agendado do Coletor de dados de relatórios do SBOM que é executado diariamente.

Exibição de relatórios e painéis no Lista de materiais de software espaço

Os analistas de vulnerabilidades exibem arquivos de lista de materiais de software carregados em registros, visualizações de dados, bem como inteligência de vulnerabilidades aprimorada no Lista de materiais de software(SBOM) Espaço.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SBOM Núcleo

Você pode exibir entidades de BOM e uma lista de componentes que você carregou na página inicial (principal) e no módulo Componentes no SBOM Espaço.

SBOM Resposta

. SBOM A aplicação de resposta fornece visualizações de dados com informações detalhadas sobre entidades de BOM, entidades com vulnerabilidades e itens vulneráveis da aplicação ativa na página inicial (principal) no SBOM Espaço. O espaço com SBOM A resposta inclui os seguintes módulos:

- Página inicial - Visualizações de dados e detalhes aprimorados da vulnerabilidade.
- Componentes - Informações de versão e correção dos componentes e. classificação de licença de componentes .
- Regras de criação de AVIT (item vulnerável à aplicação) - Condições para quando itens vulneráveis à aplicação (AVITs) são criados.
- Fila DA BOM - Status e histórico de carregamento de arquivo.
- Lista - Registros do AVIT para seus componentes vulneráveis e bibliotecas (vulnerabilidades de aplicações e NVD).

Os tópicos a seguir fornecem mais informações sobre como localizar detalhes sobre seus componentes no Lista de materiais de software Espaço.

- Revise a Página inicial no Lista de materiais de software Espaço
- Revisando o módulo Componentes no Lista de materiais de software Espaço
- Exibir status de carregamento para Lista de materiais de software arquivos
- Verificando um Lista de materiais de software entidade para vulnerabilidades
- Classificando licenças e resolvendo licenças de componente no Lista de materiais de software espaço

Revise a Página inicial no Lista de materiais de software Espaço

Os dados carregados são acumulados para as visualizações na página principal (Página inicial) no Lista de materiais de software(SBOM) Espaço. Os dados são modificados depois que você carrega arquivos para que os analistas de vulnerabilidade possam ver tendências e revisar informações atuais sobre seus componentes.

Antes de Iniciar

Funções necessárias: sn_sbom_resp.sbom_analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de SBOM**.
   Por padrão, a página principal (Página inicial) é exibida.

   O que você pode ver no módulo depende dos aplicativos instalados.

   Os dados importados não são calculados e preenchidos por consultas em tempo real. As pontuações nas páginas Página inicial e Componentes são atualizadas uma vez por dia com melhorias de desempenho para emissão de relatórios. Este aprimoramento pode fornecer tempos de carregamento mais rápidos para os cartões de pontuação nos módulos Página inicial e Componentes no SBOM Espaço.

   Esses aprimoramentos não afetam como ou onde os dados são armazenados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
Se você tiver instalado SBOM Núcleo	Todas as entidades da BOM. A lista inclui o Nome, o Classificador (Aplicação, Contêiner, Biblioteca e assim por diante) e a contagem de componentes de cada entidade. Uma entidade de BOM se refere ao componente de nível raiz em um SBOM arquivo para o qual um SBOM o documento foi gerado e carregado. Navegue até a página inicial no espaço Para exibir a lista de entidades da BOM.
Se você tiver instalado SBOM Resposta	As visualizações de dados a seguir são exibidas. ○ Todas as entidades da BOM - Um detalhamento das entidades da BOM por tipo: Aplicação, contêiner, biblioteca e outros. Uma entidade de BOM se refere ao componente de nível raiz em um SBOM arquivo para o qual um SBOM o documento foi gerado e carregado. ○ Entidades DA BOM com vulnerabilidades - Entidades que têm uma vulnerabilidade associada a qualquer componente do qual dependem. Se uma dependência de entidade tiver uma **Crítico** a gravidade da entidade é considerada crítica. ○ AVIS ativos - A tendência do número de itens vulneráveis à aplicação (AVI) criados a cada dia. As visualizações de dados exibem dados dos últimos 30 dias. O intervalo de 30 dias não é editável. Esses dados ficam disponíveis depois que você revisou e configurou as regras de criação para itens vulneráveis da aplicação. Para obter mais informações, consulte Criação de regras para itens vulneráveis à aplicação no Lista de materiais de software Espaço.

2. Selecione um cartão de visualização de dados para ver sua lista de registros.
3. Selecione **Página inicial** para retornar à página principal.
4. Como alternativa, selecione um registro em **Entidades DE BOM** lista.

   O nome e a versão da entidade são exibidos na parte superior do registro, por exemplo, SNC-SECOPS-SIR2.0 .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Com o módulo Administração de licenças, o relacionamento entidade-licença não é exibido nesta lista. Para exibir as entidades em que um componente é usado, navegue até o módulo Componentes e abra um registro de componente. No registro do componente, você pode exibir o Estado: Não resolvido ou Não classificado.

5. Selecione as guias no registro da entidade para revisar os dados.

   a. Se não estiver selecionado, selecione **Visão geral** guia.

   Revise os dados. Se um campo não estiver preenchido neste registro, os dados não serão incluídos com SBOM arquivos que você carregou.

Nome	Descrição
Nome	Nome da entidade.
Classificador	Tipo de entidade, por exemplo, uma aplicação, componente ou biblioteca.
Versão	Número da versão da entidade.
Fornecedor	O produto que forneceu a entidade.
Modelo do produto	Se não houver nenhum modelo de produto existente ou se você não incluir um no momento do seu SBOM Carregado por meio da API, um é criado. O nome da entidade é usado para o registro do modelo do produto, por exemplo SNC-SECOPS-SIR2.0 .

   b. Selecione **Depende de** guia.

   Todas as dependências desta entidade são listadas, bem como classificadores, por exemplo, Biblioteca . O número da versão, Licenças e outras informações são exibidas.

   Selecionar um link nesta lista abre um registro. Sua guia é exibida abaixo das guias de registro Página inicial e Entidade. O registro que você abre pode incluir as seguintes listas relacionadas que você pode revisar: Visão geral, hashes, entidades de BOM, vulnerabilidades e itens vulneráveis à aplicação (AVITs).

   A lista relacionada Entidades da BOM exibe todas as entidades nas quais este item exibido é usado.

   c. Selecione **Vulnerabilidades** para ver as vulnerabilidades associadas a uma dependência desta entidade.

   Para obter mais informações sobre as vulnerabilidades exibidas para uma entidade, consulte Exibir status de carregamento para Lista de materiais de software arquivos.

   d. Selecione **Avis** para ver se há itens vulneráveis à aplicação para esta entidade.

6. **Opcional:** Depois de revisar os registros, você pode excluir um ou mais registros de entidade da BOM se determinar que não precisa mais deles.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Excluir registros de entidade da BOM remove permanentemente eles e seus relacionamentos de componente. Todos os itens vulneráveis à aplicação (AVIT) associados às entidades da BOM fazem a transição para **Encerrado** . Mais tarde, você decidir que deseja que os registros e os relacionamentos de componente excluídos novamente na lista Entidades da BOM e fiquem disponíveis no espaço, será necessário carregar essas entidades da BOM novamente.

a. Se não estiver na página inicial, selecione **Página inicial** para retornar a ela.

b. Selecione o(s) registro(s) em **Entidades DE BOM** lista que você deseja excluir.

c. Selecione **Excluir**.

Revisando o módulo Componentes no Lista de materiais de software Espaço

O módulo Componentes no Lista de materiais de software(SBOM) Exibe informações atuais sobre combinações vulneráveis, obsoletas, abandonadas e de alto risco para os componentes importados.

Exibindo o módulo Componentes

Função necessária: sn_sbom_resp.sbom_analyst

Navegar até **Espaços** > **Espaço de SBOM** > **Componentes**.

O que você pode ver no módulo depende dos aplicativos instalados.

Os dados importados não são calculados e preenchidos por consultas em tempo real. As pontuações nas páginas Página inicial e Componentes são atualizadas uma vez por dia com melhorias de desempenho para emissão de relatórios. Este aprimoramento pode fornecer tempos de carregamento mais rápidos para os cartões de pontuação nos módulos Página inicial e Componentes no SBOM Espaço.

Esses aprimoramentos não afetam como ou onde os dados são armazenados.

Aplicação instalada	Descrição
Se você tiver instalado SBOM Núcleo	Um inventário de todos os componentes carregados que inclui as seguintes informações: • Nome • Descrição • Versão • Contagem de entidades da lista de materiais
Se você tiver instalado SBOM Resposta	Selecione um gráfico ou um número no gráfico para exibir uma lista de registros associados. **Todos os componentes** A lista de **Obsoleto** e. **Abandonado** componentes, bem como aqueles com pelo menos uma vulnerabilidade na contagem total de componentes. Essas contagens podem ajudar você a identificar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	componentes que exigem sua atenção. Esses subconjuntos de componentes podem não corresponder à contagem total de componentes porque todos os componentes podem não se encaixar nessas categorias. • A versão de um componente obsoleto é mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. • Um componente abandonado não foi atualizado há mais de dois anos. • Componentes vulneráveis são componentes que têm vulnerabilidades com severidade de **Alto** ou maior. **Combinações de alto risco** Componentes de alto risco podem exigir sua atenção imediata. A integração de Deps.dev, que é instalada quando você instala o. SBOM Aplicação de resposta, fornece a inteligência de pacotes para componentes no **Obsoleto** e. **Abandonado** estados. As combinações importadas e de alto risco são compostas por componentes obsoletos e abandonados com pelo menos um grave (**Crítico** ou **Alto** vulnerabilidade que você pode corrigir com atualizações, substituição ou outro tipo de reparo. . **Completamente corrigível** o status significa que um componente tem uma versão disponível que pode corrigi-lo. A porcentagem do número total de componentes de alto risco que têm versões fixáveis é anotada. **Fixação de componentes vulneráveis** Totais e detalhamentos dos componentes com **Crítico** , **Alto** , **Médio** e **Baixo** vulnerabilidades e se algumas ou todas as vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	podem ser corrigidas. Se um componente tiver mais de uma vulnerabilidade, a vulnerabilidade mais crítica terá precedência. O status de fixabilidade: • Concluído - Existem versões de correção para todas as vulnerabilidades associadas à versão atual do componente. • Parcial - Há uma versão de correção para pelo menos uma, mas não todas as vulnerabilidades associadas à versão atual do componente. **Classificação de licença de componentes** Totais e detalhamentos de componentes por suas classificações de licença. A Lista de componentes nas visualizações permite que você veja o nome, a descrição, a versão e as contagens de entidades. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões. Vulnerabilidades e exposição comuns (**CVE** e. **Fixabilidade** colunas também são exibidas.

Avaliar seu risco com inteligência contra vulnerabilidades

Consulte Verificando um Lista de materiais de software entidade para vulnerabilidades para obter mais informações sobre como revisar dados de inteligência de vulnerabilidades no espaço, .

Avaliar seu risco com conformidade de licença

Consulte Classificando licenças e resolvendo licenças de componente no Lista de materiais de software espaço para obter mais informações sobre como licenciar os dados importados com seus componentes e como exibir a conformidade de licença geral no espaço de trabalho.

Criação de regras para itens vulneráveis à aplicação no Lista de materiais de software Espaço

Antes que você possa ver itens vulneráveis à aplicação (AVITs) na Lista de materiais do software (SBOM), você deve configurar as condições sob as quais os AVITs são criados.

AVITs no SBOM Espaço

Se você instalou e ativou o. SBOM Aplicação de resposta, AVITs são criados para SBOM Se algum dos dados importados corresponder às condições das regras de criação do AVIT existentes.

. SBOM Resposta e. Resposta a vulnerabilidades As aplicações devem configurar regras para criar itens vulneráveis à aplicação (AVITs) automaticamente e corrigi-los com o. Resposta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a vulnerabilidades de aplicações fluxo de trabalho. Para obter mais informações, consulte Explorando Lista de materiais de software.

Como um usuário com a função sn_sbom_resp.manage_avi_rule, você deve adicionar regras de criação do AVIT no SBOM Antes que você possa criar AVITs para as vulnerabilidades encontradas em seu ingerido SBOM dados. AVITs permitem que você avalie a integridade dos componentes de terceiros em suas aplicações. Um AVIT é criado em sua instância quando uma aplicação corresponde a um componente que tem uma vulnerabilidade associada.

Em SBOM, você pode exibir somente AVITs do SBOM. No entanto, você pode exibir SBOM AVITs junto com outros tipos de itens vulneráveis no Espaço do Gerenciador de vulnerabilidades em Resposta a vulnerabilidades. Você pode exibir todos os AVITs que foram criados no Espaço do SBOM no Módulo de lista. O módulo de lista também inclui todas as entradas NVD e CWE e Vulnerabilidades da aplicação.

Você também pode atribuir AVITs para correção com base em recomendações de listas de vulnerabilidades conhecidas, como o National Vulnerability Database (NVD). Um trabalho agendado é acionado e, se as condições das regras de criação corresponderem aos dados ingeridos, os AVITs serão criados.

Você pode rastrear e corrigir AVITs configurando regras personalizadas.

Consulte Crie uma regra de item vulnerável à aplicação no Lista de materiais de software Espaço para obter informações sobre como criar uma regra.

SBOM AVITs em Espaço do gerente de vulnerabilidade em Resposta a vulnerabilidades

Você pode exibir qualquer um SBOM AVITs que são criados no SBOM Espaço no Espaço do gerente de vulnerabilidade se você tiver acesso a ele.

Nota: Somente para exibir SBOM AVITs da lista de itens vulneráveis à aplicação em Espaço do gerente de vulnerabilidade Em vez de todos os AVITs, defina a condição **[Origem] [IS] [SBOM] E. [Tipo de verificação] [IS] [SBOM-SCA]** Na tabela Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item]. Para exibir a tabela, navegue em sua instância até **Todos** e insira **sn_vul_app_vulnerable_item.list** no navegador de filtros.

Para obter mais informações sobre o Espaço do gerenciador de vulnerabilidades, como exibir tópicos de observação, esforços de correção de aplicações e regras de tarefa de correção de aplicações para AVITs configurados no Resposta a vulnerabilidades aplicação no Espaço do gerente de vulnerabilidade, consulte Usar tópicos de observação no Espaço do gerente de vulnerabilidade.

As tarefas de correção (AVULs) são criadas a partir de AVITs e atribuídas automaticamente a grupos para correção com base em suas regras de atribuição. Para obter mais informações sobre como criar essas regras, consulte os seguintes tópicos:

- Criar ou editar Resposta a vulnerabilidades regras de atribuição
- Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção e Crie um esforço de correção no Espaço do gerente de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reabrindo itens vulneráveis da aplicação na resposta do SBOM

. **Encerrado** AVIT (Application Vulnerable Item, item vulnerável à aplicação) de um componente com uma vulnerabilidade associada é reaberto automaticamente e visível no SBOM Se existirem as seguintes condições:

- O AVIT com a vulnerabilidade associada é detectado novamente por verificações de vulnerabilidade de integração de terceiros ou o componente com a vulnerabilidade faz parte de um subsequente SBOM upload.
- Reabrir AVITs não foi desabilitado se detectado (*sn_sbom_resp.reopen_avits_if_detected*propriedade do sistema). Esta propriedade do sistema é ativada por padrão.
- O subestado do **Encerrado** Avit não é um dos seguintes: **Controle de mitigação em vigor** , **Não afetado** ou **Falso-positivo** . AVITs com esses subestados não são reabertos pela propriedade do sistema.

Desative esta propriedade do sistema somente se não quiser **Encerrado** AVITs a serem reabertos automaticamente.

Exibir status de carregamento para Lista de materiais de software arquivos

Verifique o status de carregamento da Lista de materiais do software (SBOM Arquivos que você carrega no módulo Fila da BOM no Lista de materiais de software(SBOM) Espaço. Rastreie os arquivos que você carregou com sucesso, seu histórico de carregamentos e erros.

Antes de Iniciar

Função necessária: sn_sbom_resp.sbom_analyst

Procedimento

1. Exiba seu status de carregamento.

   O método usado para exibir o status de carregamento depende das aplicações instaladas.

Opção	Descrição
SBOM Núcleo	**a.** Navegar até **Tudo** > **Núcleo de SBOM** > **Status de ingestão da lista de materiais**. **b.** Na lista Lista de materiais, revise as colunas como **Status** , **Tempo de geração DA BOM** e **Criado** colunas para obter detalhes.
SBOM Resposta	**a.** Navegar até **Tudo** > **Espaço de SBOM** > **Fila de lista de materiais**. **b.** Selecione um cartão de visualização para revisar os seguintes detalhes das categorias dos arquivos carregados: ▪ Atualizações DE BOM nos últimos 30 dias - Total de entidades de BOM carregadas e analisadas com sucesso nos últimos 30 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ Origem do carregamento - Total de carregados com sucesso SBOM Arquivos e um detalhamento dos métodos usados para ingeri-los (API ou manual). ▪ Erros de carregamento por categoria - As cinco principais categorias de erros de carregamento. Se nenhum dado aparecer nesta visualização, todos os seus SBOM arquivos carregados com sucesso.

As informações de status na tabela Lista de materiais [sn_sbom_doc_list] e no módulo Fila da BOM incluem formatos da BOM, status de ingestão e tempo de geração da BOM. A coluna Status da ingestão da BOM inclui os seguintes estados:

- Em fila - SBOM os dados foram carregados.
- Processamento - Os dados do componente estão sendo processados como parte da importação.
- Processado - A ingestão de dados foi concluída com sucesso.
- Erro - Ocorreu um erro durante o processamento.

Além do status dos arquivos carregados, você pode exibir listas de componentes que ingeriu selecionando um registro de entidade de BOM.

2. **Opcional:** Acesse mais informações sobre erros e status de carregamento selecionando o ícone de engrenagem e adicionando campos como **Categoria de erro** e. **Detalhe do erro** .

Verificando um Lista de materiais de software entidade para vulnerabilidades

Determine se alguma vulnerabilidade está associada aos componentes em um carregado Lista de materiais de software(SBOM).

As seguintes aplicações devem ser instaladas e ativadas antes que você possa exibir as vulnerabilidades e os dados aprimorados de vulnerabilidade:

- SBOM Resposta
- Integração de Resposta a vulnerabilidades com trabalhos de NVD e CWE
- Resposta a vulnerabilidades

Para obter mais informações, consulte Explorando Lista de materiais de software.

Função necessária: sn_sbom_resp.sbom_analyst

1. Navegar até **Tudo** > **Espaço de SBOM** > **Componentes**.
2. você pode exibir informações de vulnerabilidade por meio de uma visualização ou de um registro de componente.

Método	Ações
Visualização de entidades DE BOM com vulnerabilidades	Selecione **Entidades DE BOM com vulnerabilidades** gráfico de visualização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Método	Ações
	○ Se vulnerabilidades estiverem associadas a este componente, os totais serão exibidos nas colunas CVE e CWE na lista. Um componente pode ter mais de uma vulnerabilidade. Se disponível, você pode verificar a coluna Fixabilidade nesta lista para entradas. ○ Se nenhuma vulnerabilidade estiver associada a este componente, essas colunas serão exibidas 0 ou nenhum valor para o componente. Se as colunas CVE, CWE e Fixibilty não forem exibidas, você poderá adicioná-las à página selecionando o ícone de engrenagem no canto superior direito da página e. **Editar colunas** . Selecione-os na lista Coluna disponível e selecione **OK** .
Registro do componente	**a.** Selecione um registro na lista abaixo das visualizações. **b.** Selecione **Vulnerabilidades** no registro. **i.** Se nenhum dado for exibido, nenhuma vulnerabilidade relatada será associada ao registro. **ii.** Se os dados forem exibidos, consulte Revisando o módulo Componentes no Lista de materiais de software Espaço e siga as etapas no fluxo de trabalho de correção para Resposta a vulnerabilidades de aplicações para lidar com a vulnerabilidade. Para obter mais informações, consulte Correção Resposta a vulnerabilidades de aplicações vulnerabilidades.

Tradução automática

Avaliar seu risco com inteligência contra vulnerabilidades

Exibir mais dados de vulnerabilidade aprimorados com SBOM Resposta em registros de componente. . SBOM Aplicação de resposta, Resposta a vulnerabilidades, Integração do banco de dados de vulnerabilidade nacional (NVD) e trabalhos agendados de enumeração de pontos fracos comuns (CWE) descritos em Aplicações compatíveis deve ser instalado e ativado.

1. Selecione **Todos os componentes** visualização para exibir sua lista de registros associados.
2. Selecione um link no **Nome** coluna para abrir um registro.

   Os estados, **Obsoleto** , **Abandonado** e **Vulnerável** são exibidos sob o nome do componente. Um componente pode ter qualquer combinação desses estados. Se nenhum estado for exibido, o componente não será obsoleto, abandonado ou vulnerável.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revise a versão atual e a versão publicada mais recente. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões e sua localização na lista pode fornecer informações sobre o motivo pelo qual um componente está **Obsoleto** , **Abandonado** e **Vulnerável** . Por exemplo, você pode estar usando uma versão mais antiga de um componente.

3. Selecione **Visão geral** , **Hashes** , **Entidades DE BOM** , **Vulnerabilidades** e **Avis** guias relacionadas no registro.
   - Visão geral - Um resumo dos detalhes do componente.
   - Entidades DA BOM - Uma lista das entidades associadas a este componente.
   - Hashes - Se importados, os hashes serão exibidos.
   - Vulnerabilidades - Informações sobre vulnerabilidades conhecidas associadas a este componente. Se esta lista estiver vazia, não haverá vulnerabilidades conhecidas.

     Se a lista estiver preenchida, selecione a guia para exibir IDs de vulnerabilidade, resumos e outras informações de vulnerabilidade para dados CVE (Common Vulnerabilities and Exposures) e CWE (Common Weakness Enumeration) associados a este registro. CVEs são divididos por gravidade, CVEs são divididos por quão provável o componente pode ser explorado. Você pode exibir os registros de vulnerabilidade aprimorados no Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações Selecionando o link de ID da vulnerabilidade.

   - AVITs (AVITs) - Itens vulneráveis à aplicação associados a este componente se você tiver criado regras de criação do AVIT que correspondam ao componente a uma vulnerabilidade conhecida. A aplicação de resposta a vulnerabilidades da aplicação (AVR) relaciona uma vulnerabilidade a uma aplicação para criar um registro AVI. Para obter mais informações, consulte Criação de regras para itens vulneráveis à aplicação no Lista de materiais de software Espaço.

Componentes instalados com Lista de materiais de software aplicações

Vários tipos de componentes são instalados com a ativação do Lista de materiais de software aplicações, incluindo tabelas, funções de usuário e trabalhos agendados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_sbom_response.managelicense	Esta função é instalada com SBOM Aplicação de resposta. Esta função permite que você resolva licenças para componentes.	Nenhum(a)
sn_sbom_response.licenseresolvedor	Esta função é instalada com SBOM Aplicação de resposta. Esta função permite exibir informações de	Nenhum(a)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	licença carregadas e determina quais licenças são permitidas e quais são proibidas.	
SBOM gravação [sn_sbom_dm.app_write], SBOM criar [sn_sbom_dm.app_create], SBOM leitura [sbom_dm.app_read]	Essas funções são instaladas com o Modelo de dados para SBOM aplicação. Eles permitem que você leia, crie e edite registros no SBOM tabelas.	Nenhum(a)
SBOM Os núcleos ingere [sn_sbom_core.sbom_ingest] e. SBOM Administrador principal [sn_sbom_core.admin]	Essas funções são instaladas com SBOM Aplicação principal. A função sn_sbom_core.sbom_ingest permite carregar SBOMs manualmente e por meio da REST API. A função sn_sbom_core.admin permite criar, ler, editar dados e carregar SBOMs. Esta função também lhe dá acesso ao SBOM Módulos principais em sua instância. Herda as funções do Modelo de dados para SBOM aplicação.	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read
Analista de SBOM [sn_sbom_resp.sbom_analyst]	Esta função é instalada com SBOM Aplicação de resposta. Herda a função sn_sbom_core.admin e permite que você acesse SBOM Espaço.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • tabela sn_sbom_config_rule

Tradução automática

Tabelas instaladas com SBOM aplicações

As tabelas listadas na tabela a seguir são instaladas com o Modelo de dados para SBOM aplicação.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de dados para SBOM tabelas

Tabela	Descrição
Documento de SBOM [sn_sbom_doc]	Contém as entidades de BOM que você carregou.
Componente do SBOM [sn_sbom_component]	Importados SBOM classificadores e versões incluídos no componente primário.
SBOM relacionamento de componente [sn_sbom_comp_relationship]	Contém componentes e suas dependências.
SBOM componente de bom m2m [sn_sbom_m2m_bom_comp]	Contém os mapeamentos do componente da BOM.
Licença do SBOM [sn_sbom_license]	Contém os IDs de licença de código aberto usados para componentes.
SBOM fornecedor [sn_sbom_supplier]	Contém a organização que forneceu o componente, que pode ser um fabricante, distribuidor ou reempacotador.
SBOM ID do componente [sn_sbom_comp_id]	Contém os identificadores de componente.
SBOM propriedades do componente [sn_sbom_comp_property]	Contém as propriedades name-value do componente.
SBOM hash [sn_sbom_hash]	Contém algoritmos de hash de componente.
SBOM contato [sn_sbom_contact]	Contém informações de contato do fornecedor.
SBOM referências externas	Contém componentes, tipos de componente e URLs externos que documentam sistemas, sites e informações que podem ser relevantes, mas não estão incluídos com SBOM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de dados para SBOM tabelas

Tabela	Descrição
[sn_sbom_comp_external_ref]	
SBOM grupo de pacotes [sn_sbom_pkg_group]	Contém as informações do grupo de pacotes para cada componente. Várias versões das bibliotecas podem ser usadas em todas as aplicações. Versões dos mesmos componentes são agrupadas e adicionadas a esta tabela para evitar extrair os mesmos dados várias vezes.

As tabelas listadas na tabela a seguir são instaladas com SBOM Aplicação de resposta

SBOM Tabelas de resposta

Tabela	Descrição
SBOM configuração da regra de criação [sn_sbom_config_rule]	Contém regras de criação do AVIT usadas no SBOM Espaço.
SBOM vulnerabilidades do componente m2m [sn_sbom_m2m_comp_vuln]	Contém os componentes e as vulnerabilidades associadas.
Informações de correção de vulnerabilidade do componente [sn_sbom_comp_vuln_fix_info]	Contém as versões de correção para cada vulnerabilidade de terceiros associada a uma versão do componente.
Informações do relatório do componente [sn_sbom_comp_report_insight]	Contém informações sobre dados obsoletos, abandonados e de fixabilidade para componentes.
Importações de integrações de Deps [sn_sbom_deps_integration_import]	Contém informações da lista de versões importadas para um determinado pacote ou biblioteca.
Importações de integrações de OSV [sn_sbom_osv_integration_import]	Contém informações de inteligência contra vulnerabilidades para uma determinada versão de um pacote ou biblioteca.
Listas de versão de componentes [sn_sbom_st_version_list]	Contém informações de versão e datas publicadas para componentes.

Trabalhos agendados

Trabalho	Descrição
Calcular Fixabilidade e Vulnerabilidade do Componente	Calcula informações sobre como corrigir componentes com vulnerabilidades e a probabilidade de você corrigir componentes.
Novos componentes de integração do OSV	Recupera todas as vulnerabilidades conhecidas publicamente associadas a pacotes (bibliotecas)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
	que foram importados após a última execução de integração.
Integração abrangente do OSV	Recupera todas as vulnerabilidades conhecidas publicamente associadas a todos os pacotes que foram importados.
Integração Deps.dev	Recupera todas as versões publicamente conhecidas de pacotes e usadas com para identificar componentes em **Obsoleto** e. **Abandonado** estados.
Atualize vuln_based_criticality nos componentes da BOM	Atualiza a criticidade de componentes com vulnerabilidades.

Crie uma regra de item vulnerável à aplicação no Lista de materiais de software Espaço

Configure as condições sob as quais os itens vulneráveis à aplicação (AVITs) são criados automaticamente no módulo Regras de criação de AVI no Lista de materiais de software(SBOM) Espaço.

Antes de Iniciar

. SBOM A aplicação de resposta será necessária se você quiser criar itens vulneráveis à aplicação. Para obter mais informações, consulte Explorando Lista de materiais de software.

Função necessária: sn_sbom_resp.manage_avi_rule.

Procedimento

1. Navegar até **Espaço de SBOM** > **Regras de criação de AVI**.
2. Selecione **Novo**.
3. Preencha os campos.

Campo	Descrição
Nome	Nome da regra.
Ativo	Indica se a regra de criação está ativada.
Ordem de execução	Ordem na qual as regras são avaliadas. A regra com o menor valor numérico é executada primeiro. Por exemplo, você pode criar regras de prioridade mais alta para itens que precisam de tratamento especial ou onde o risco é crítico, para que eles sejam executados primeiro. Em seguida, crie regras gerais para itens que não exigem manipulação especial. Por fim, crie uma regra padrão para detectar todos os componentes que tenham vulnerabilidades.
Descrição	Descrição da regra para ajudá-lo a distingui-la de outras regras.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condições	Crie as condições sob as quais os itens vulneráveis à aplicação (Avis) são criados. Por exemplo, você pode selecionar **[Vulnerabilidade > Severidade][is][1-Crítica]** Para criar AVITs para componentes que têm vulnerabilidades de alto risco e que podem afetar gravemente você. Observe que você pode adicionar mais condições.

4. Selecione **Save** (Salvar).
   Sua regra de criação é executada automaticamente após o próximo carregamento e cria Avis para componentes que correspondem às suas condições. Você também pode executar a regra sob demanda no módulo Regras de criação de AVI selecionando **Executar agora** .

Resultado

Depois de criados, você pode verificar se um AVIT foi criado especificamente para SBOM verificando os valores em **Origem** e. **Tipo de verificação** Campos em um registro AVI.

Campo	Valor
Origem	SBOM
Tipo de verificação	SBOM-SCA

Aplicações de gestão de casos de segurança empresarial

As aplicações de gestão de casos de segurança empresarial incluem Resposta a incidentes de segurança Uma solução SOAR (Security Orchestration and Automation Response, orquestração de segurança e resposta de automação) que ajuda você a responder rapidamente às ameaças em evolução, otimizando e orquestrando as operações de segurança empresarial. Elimina os erros e o atrito inerentes às transferências manuais entre sistemas, equipes e responsabilidades.

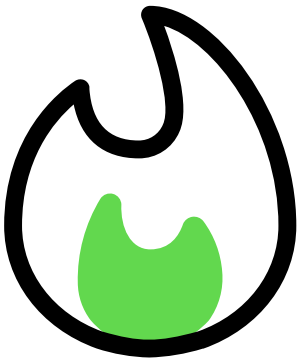
Primeiros passos

A seguir Resposta a incidentes de segurança as aplicações estão disponíveis com assinaturas separadas do ServiceNow® Store. Consulte Operações de segurança e o ServiceNow Store para obter mais informações sobre como localizar, obter direito e baixar aplicativos em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança



Saiba mais sobre a aplicação Resposta a incidentes de segurança

Gestão de incidentes graves de segurança



Saiba mais sobre a aplicação Gestão de incidentes de segurança graves

Inteligência contra ameaças



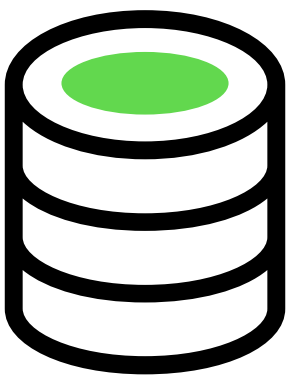
Saiba mais sobre a aplicação Inteligência contra ameaças

Central de segurança de inteligência contra ameaças



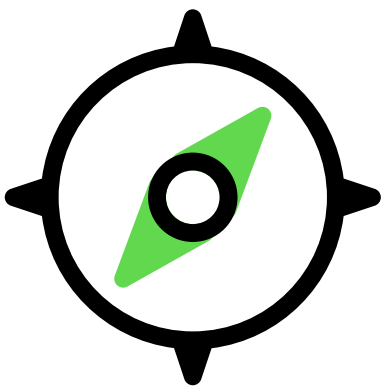
Saiba mais sobre a aplicação Central de segurança do Inteligência contra ameaças

Data Loss Prevention Incident Response



Saiba mais sobre a aplicação Prevenção contra perda de dados

Recursos compartilhados de aplicações de resposta a incidentes de segurança



Saiba mais sobre os recursos compartilhados entre as aplicações Resposta de incidentes de segurança

Tradução automática

Solucionar problemas e obter ajuda

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

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança

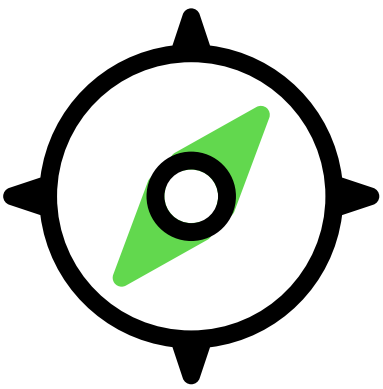
. ServiceNow® Resposta a incidentes de segurança a aplicação rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão final pós-incidente, a criação e o fechamento do artigo da base de conhecimento.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

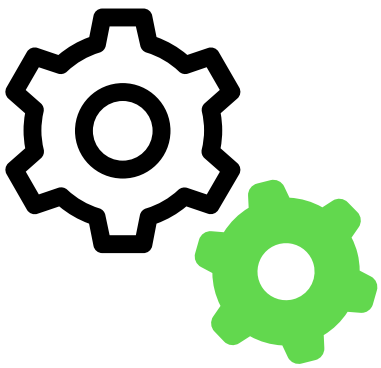
Resposta a incidentes de segurança

Explorar



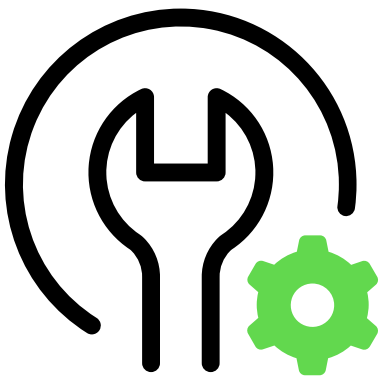
Saiba mais sobre os recursos da Resposta a incidentes de segurança

Configurar e Configurar



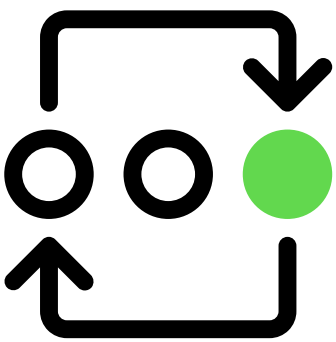
Instale e configure sua aplicação de Resposta a incidentes de segurança

Administrar



Gerencie e personalize seus incidentes de segurança

Integrar



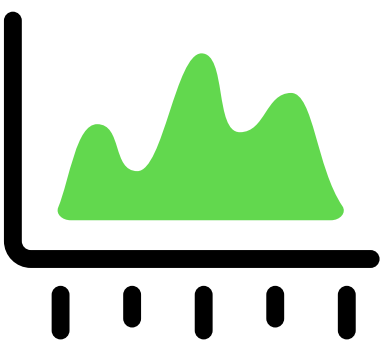
Estenda a Resposta a incidentes de segurança integrando-a a outras aplicações

Use o Espaço de resposta a incidentes de segurança



Saiba como usar os espaços de Resposta a incidentes de segurança e Correção de TI

Análise e emissão de relatórios



Monitorar o andamento da correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Obtenha informações adicionais sobre Resposta a incidentes de segurança

Solicitar um aplicativo Operações de segurança na Store

Se você é um novo Operações de segurança cliente em London Patch 6 ou posterior, visite ServiceNow Store site para exibir todos os apps disponíveis e obter informações sobre como enviar solicitações para a loja.

Solucionar problemas e obter ajuda

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

Noções básicas do Resposta a incidentes de segurança

Com Resposta a incidentes de segurança(SIR), gerencie o ciclo de vida de seus incidentes de segurança, desde a análise inicial até a contenção, erradicação e recuperação. A Resposta a incidentes de segurança permite que você obtenha uma compreensão abrangente dos procedimentos de resposta a incidentes realizados por seus analistas e entenda tendências e gargalos nesses procedimentos com painéis e relatórios orientados por análise.

Uma introdução à Resposta a incidentes de segurança, mostrando como começar a usar a aplicação .

Assista a este vídeo de nove minutos para saber mais sobre o processo SIR, usando Resposta a incidentes de segurança para impedir ataques e exibir atividades de segurança no Resposta a incidentes de segurança Explorador.

Integrações integradas com soluções de segurança cibernética de terceiros e integrações desenvolvidas por parceiros da ServiceNow Habilite a automação e a orquestração da segurança para uma resposta eficiente e precisa a incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para proteger suas investigações e manter os incidentes de segurança privados, Resposta a incidentes de segurança Fornece os meios para restringir o acesso ao sistema a funções e ACLs específicas relacionadas à segurança. Administradores que não sejam de segurança podem ser restritos ao acesso, a menos que você permita expressamente a entrada deles.

Nota: Os administradores do sistema DE TI [admin] podem representar usuários da ServiceNow. No entanto, ao representar um usuário com uma função de administrador de aplicação para Resposta de incidente de segurança, um administrador não pode acessar recursos concedidos por essa função, incluindo incidentes de segurança e informações de perfil. O acesso a módulos e aplicações na barra de navegação também é restrito. Além disso, o administrador não pode mudar a senha de nenhum usuário com uma função de administrador da aplicação para Resposta a incidentes de segurança.

Fluxo de informações de Resposta do incidente de segurança

O Security Incident Response emprega o seguinte fluxo de informações, desde a integração até a investigação e, em seguida, a resolução e a revisão.

Nota: Este é um infográfico interativo, portanto, você pode tentar clicar em qualquer um dos ícones ou etapas na imagem para saber mais sobre esse processo ou tarefa.



1. Clique nesta imagem para saber mais sobre as integrações DE SIR
2. Clique nesta imagem para saber mais sobre a criação de incidentes de segurança
3. Clique nesta imagem para saber mais sobre Inteligência contra ameaças
4. Clique nesta imagem para saber mais sobre o Espaço SIR
5. Clique nesta imagem para saber mais sobre os recursos do ataque MITRE
6. Clique nesta imagem para saber mais sobre as atividades de revisão pós-incidente

Descoberta

Os incidentes de segurança podem ser registrados ou criados das seguintes maneiras.

- No formulário Incidente de segurança
- De eventos gerados internamente ou criados por monitoramento externo ou sistemas de acompanhamento de vulnerabilidades por meio de regras de alerta ou manualmente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- De monitoramento externo ou sistemas de rastreamento
- Do catálogo de serviços

Análise

Dependendo da exibição selecionada que você está usando (Padrão, Segurança não relacionada à TI, ITIL de segurança e assim por diante), o formulário Incidente de segurança pode mostrar qualquer combinação de vulnerabilidades, incidentes, mudanças, problemas, tarefas no IC afetado e grupos de IC afetados. O sistema pode identificar malware, vírus e outras áreas de vulnerabilidade cruzando o banco de dados do National Institute of Standards and Technology (NIST) ou outro software de detecção de terceiros. Conforme os incidentes de segurança são resolvidos, você pode usar qualquer incidente para criar um artigo da base de conhecimento de segurança para referência futura.

Execute análises adicionais usando um mapa de serviços de negócios para localizar outros sistemas afetados ou serviços de negócios que podem ser infectados.

Contenção, Erradicação e Recuperação

Ao monitorar e analisar vulnerabilidades, você pode criar e atribuir tarefas a outros departamentos. Você pode usar um mapa de serviço de negócios para criar tarefas, problemas ou mudanças para todos os sistemas afetados, documentos, atividades, mensagens SMS, chamadas de ponte, e assim por diante.

Revisão

Depois que o incidente é resolvido, outras etapas podem ocorrer antes do fechamento. Você pode executar uma revisão pós-incidente. Criar artigos da base de conhecimento pode ajudar com incidentes semelhantes futuros. Incidentes significativos podem exigir uma revisão de resolução pós-incidente. Esta revisão pode assumir várias formas. Por exemplo:

- Conduza uma reunião para discutir o incidente e coletar respostas.
- Escreva e distribua para as equipes que trabalharam em um incidente uma lista de perguntas de revisão de resolução projetadas para cada categoria ou prioridade de incidente.
- Os gerentes de incidentes podem escrever o relatório e coletar informações por conta própria.

Um relatório de revisão de resolução de incidentes pode ser gerado automaticamente, incluindo:

1. um resumo do que foi feito
2. a linha do tempo
3. o tipo de incidente de segurança encontrado
4. Todos os incidentes, mudanças, problemas, tarefas e grupos de IC relacionados
5. os detalhes da resolução

Um sistema automatizado de pesquisa de revisão de resolução de incidentes de segurança está disponível. Ele reúne os nomes de todos os usuários atribuídos a um incidente de segurança e envia uma pesquisa personalizada para coletar dados sobre o tratamento do incidente. Esses dados podem ser disponibilizados em um relatório de revisão de incidente de segurança gerado, que você pode editar em um rascunho final. Dados semelhantes podem ser adicionados a um artigo da base de conhecimento para conter as lições aprendidas e as etapas a serem seguidas para resolver problemas semelhantes no futuro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Terminologia de resposta do incidente de segurança

Os termos a seguir são usados em Resposta a incidentes de segurança.

Termo	Definição
Ativo	Qualquer incidente de segurança que não esteja no estado Encerrado ou Cancelado.
Bloqueio do administrador	A capacidade de restringir Resposta a incidentes de segurança Acesso à equipe com funções relacionadas à segurança e ACLs.
Solicitações de segurança de entrada	Solicitações enviadas para demandas de segurança de baixo impacto, como solicitar um novo crachá eletrônico.
Gerenciar atividades pós-incidente	Uma revisão das origens e manipulação de um incidente de segurança. O produto final é um relatório pós-incidente, que documenta todas as ações realizadas e os motivos para fazê-las.
Tarefas de resposta	Tarefas atribuídas a um incidente de segurança para rastrear ações em resposta à ameaça.
Noções básicas sobre calculadoras de incidentes de segurança	Calculadoras usadas para atualizar valores de registro quando as condições pré-configuradas são atendidas.
Mapas em árvore de incidentes de segurança	Tipo de gráfico que mostra hierarquicamente dados de incidentes de segurança na forma de retângulos aninhados.
Pesquisa de ameaças	Uma solicitação enviada do catálogo de incidentes de segurança para verificar arquivos, URLs e endereços IP em busca de malware.
Verificação de vulnerabilidades	Uma solicitação iniciada no formulário Incidente de segurança para verificar recursos afetados (servidores, computadores e outros itens de configuração) em busca de vulnerabilidades.

Separação de domínios e Resposta a incidentes de segurança

Separação de domínios é compatível com Resposta a incidentes de segurança. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui todos os aspectos de **Básico** suporte de nível.
- As propriedades da aplicação reconhecem domínio conforme necessário.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

Em Resposta a incidentes de segurança A separação de aplicações e domínios permite que os provedores de serviço (SPs) padronizem os procedimentos SOC (Security Operations Center, Centro de operações de segurança) e de Resposta a incidentes de segurança (SIR) em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço mais alta. Espaços separados do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garantem que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte ao Domain Separation na Resposta a incidentes de segurança por versões

Versão	Nível de suporte	Anotações
Genebra, Helsinki	Sem suporte	Início da separação de domínio no nível de dados
Istambul	Somente dados	
Jakarta	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos** Suporte a integrações de terceiros com separação de domínio de nível 2 em uma única instância de integração, incluindo integrações de Inteligência contra ameaças
Kingston	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos** A integração da Pesquisa de vistas para SIR está habilitada com várias instâncias, mas todas as instâncias ainda estão em um único domínio. Exemplo: Se houver duas instâncias de uma integração do Splunk configuradas (SplunkCLOUD e SplunkCORP), ambas ainda serão aproveitadas para atividades de resposta a incidentes em um único domínio, onde a implementação foi configurada originalmente.
Londres	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos** : Todas as integrações residem em vários domínios
Madri	Nível 2 (Dados, Solicitante, Executante)	Agora, todas as integrações podem residir em vários domínios. No exemplo acima, SplunkCloud pode ser domain1 e SplunkCORP domain2.
Nova York	Nível 2 (Dados, Solicitante, Executante)	Todas as integrações residem em vários domínios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suporte ao Domain Separation na Resposta a incidentes de segurança por versões

Versão	Nível de suporte	Anotações
Orlando	Padrão	Todas as integrações residem em vários domínios.
Paris	Padrão	Todas as integrações residem em vários domínios.

Separação de domínio para Resposta a incidentes de segurança a aplicação abrange as seguintes funcionalidades do produto:

- Os alertas de segurança são direcionados para o domínio apropriado do usuário cujo ID/credencial/escopo gera o incidente e está registrado como um Incidente de segurança.
- Os alertas geram "observáveis", que representam propriedades com estado ou eventos mensuráveis: Fluxos de trabalho de segurança no domínio do incidente de segurança são usados para orquestrar a resposta.
- As integrações são configuradas no domínio do incidente de segurança para automação de resposta.
- Os recursos são configurados no domínio do incidente de segurança para automação de resposta. Estes recursos (a partir da versão Kingston) incluem:
  - Pesquisa de ameaças
  - Aprimorar observável
  - Item de configuração de aprimoramento
  - Obter processo em execução
  - Obter estatísticas de rede
  - Solicitação de bloqueio
  - Isolar Host
  - Pesquisa de Vistas
  - Pesquisa e exclusão de e-mails
  - Publicar na lista de observadores
- Os resultados da Automação de resposta (como Pesquisa de ameaças ou Pesquisa de vistas) são armazenados no domínio do incidente de segurança.
- Outros incidentes de segurança têm referência cruzada no mesmo domínio do incidente de segurança com base em um conjunto compartilhado de observáveis.
- Outros usuários têm referência cruzada no domínio do incidente de segurança.
- Os itens de configuração têm referência cruzada no mesmo domínio que o incidente de segurança.
- Tarefas de resposta manual são adicionadas ao domínio do incidente de segurança.
- Artigos da base de conhecimento e manuais de execução são referenciados no domínio do incidente de segurança.
- As métricas de Resposta a incidentes de segurança pertinentes a incidentes no domínio são exibidas em painéis e na emissão de relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Nos casos anteriores, os princípios abrangentes de visibilidade em domínios separados na NOW Platform se aplicam. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como a separação de domínio funciona na Resposta a incidentes de segurança

. Resposta a incidentes de segurança a aplicação gerencia o ciclo de vida de um incidente de segurança de ponta a ponta Os seguintes casos de uso reconhecem a separação de domínios:

- **Ingestão de eventos e alertas** Para criar incidentes de segurança para o analista no SOC do cliente ou no MSP responder:
  - Analisadores de e-mail (baseados em plataforma, phishing relatado pelo usuário, personalizados)
  - Alertas/eventos de desduplicação antes da criação do incidente
  - Extração automática de observáveis
  - Aplicações no armazenamento SIEM de terceiros
- **Aprimoramento** De artefatos envolvidos nos incidentes (IP, URLs, domínios, hashes de arquivo):
  - Aprimoramento de ativos (CMDB)
  - Usuários (plataforma)
  - Aprimoramento de observável (por exemplo: WHOIS)
- **Investigar** os incidentes com a ajuda dos artefatos e sua reputação ou associação com ameaças conhecidas
  - Orquestrar: Playbooks e artigos da base de conhecimento
  - Pesquisa de ameaças (por exemplo: Virustotal), pesquisa de detecções (por exemplo: Splunk), obter processos em execução (por exemplo: Carbon Black)
- **Erradicar** os artefatos relacionados à ameaça envolvidos no incidente com base na investigação realizada
  - Orquestrar: Playbooks e artigos da base de conhecimento
  - Pesquisa e exclusão de e-mail (por exemplo: Microsoft Exchange), bloquear IP (por exemplo: Firewall Palo Alto)
- **Medida** A eficiência ou as operações de resposta do incidente
  - Painéis do Performance Analytics: Produtividade e tendências de incidentes
  - Reconstrução de etapas de investigação de incidente a partir de anotações de trabalho
  - Revisão pós-incidente

Configuração do Domain Separation

Configuração do Domain Separation para Resposta a incidentes de segurança não requer etapas adicionais. Todos Resposta a incidentes de segurança As tabelas adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os incidentes de segurança em um domínio não podem ser exibidos de outros domínios.
- Observáveis extraídos do incidente de segurança são colocados no mesmo domínio e não podem ser exibidos de outros domínios.
- Até a versão Kingston, as integrações de terceiros configuradas existem no domínio global e podem ser acessadas por todos os outros domínios na instância.
- Na versão Madrid, as integrações de terceiros podem ser configuradas e ativadas por domínio. Isso significa que a integração ativada e configurada em um domínio não pode ser aproveitada em outro domínio.
- As automações executadas nos observáveis usando integrações de terceiros (para investigação, contenção ou erradicação de ameaças) colocam seus resultados no domínio do incidente de segurança e os resultados não podem ser exibidos de outro domínio.
- Os fluxos de trabalho de Orquestração criados em um domínio não estão visíveis em outro domínio.
- As capacidades (conforme delineadas na lista de funções de capacidades de avanço) que são invocadas permanecem genéricas em domínios com implementação específica do domínio da capacidade que está sendo chamada. Por exemplo, uma Pesquisa de avistamento em um IP pode invocar uma implementação Splunk em um domínio e uma implementação QRadar em outro.

Configuração

Todos os aspectos da configuração do produto são independentes em um ambiente separado por domínio. A configuração pode ser personalizada para domínios individuais.

Nota: A lógica de negócios e os processos em nº 2-5 abaixo podem ser administrados no domínio do locatário.

As seguintes tarefas devem ser configuradas:

1. Administração do Sistema
   - Atribuir funções a usuários e grupos de usuários: Funções de usuário instaladas com a Resposta de incidente de segurança
   - Instale um ou mais plug-ins de integração de terceiros com os quais trabalhar Resposta a incidentes de segurança: Integrações do Resposta a incidentes de segurança
2. Resposta a incidentes de segurança Administration
   - Adicionar ou revisar funções: Componentes instalados com Resposta a incidentes de segurança
   - Configurar grupos e usuários: Crie um grupo de incidentes de segurança
   - Configurar escalações de incidente: Escalar um incidente de segurança
   - Configurar calculadoras de pontuação de risco de incidente de segurança: Noções básicas sobre calculadoras de incidentes de segurança
   - Configurar acordos de nível de serviço: Crie um Resposta a incidentes de segurança ANS
   - Configurar definições de processo de incidente de segurança: Noções básicas sobre a definição do processo de resposta a incidentes de segurança
   - Configurar processos de revisão pós-incidente: Gerenciar atividades pós-incidente
3. Configurações de e-mail de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Defina a caixa de entrada de análise de e-mail: Operações de segurança análise de e-mail
- Configurar analisadores de e-mail para ingestão de alertas: Crie analisadores de e-mail em Operações de segurança
- Configure regras de correspondência de e-mail para phishing relatado pelo usuário: Crie regras para validar ataques de phishing relatados pelo usuário
- Configurar ações de entrada de e-mail: Ações de e-mail de entrada

4. Configurações do playbook de incidentes de segurança
   - Revisar e configurar documentos de runbook: Crie um runbook de resposta a incidentes de segurança
   - Configurar fluxos de trabalho de incidentes de segurança: Operações de segurança funcionalidade comum
5. Configurações de capacidade
   - Solicitação de bloqueio: Integração de operações de segurança - capacidade de solicitação de bloqueio
   - Pesquisa e exclusão de e-mail: Integração de operações de segurança - Recurso de pesquisa e exclusão de e-mail
   - Enriquecer item de configuração: Integração de operações de segurança- Enrich a capacidade de IC
   - Enriquecer observável: Integração de operações de segurança- Enrich a capacidade observável
   - Obter estatísticas de rede: Integração de operações de segurança- Obtenha a capacidade de estatísticas de rede
   - Obter processos em execução: Integração de operações de segurança- Obtenha a capacidade de processos em execução
   - Isolar host: Integração de operações de segurança- Isolar capacidade do host
   - Publicar na lista de observação: Integração de operações de segurança- Publicar na lista de observação
   - Pesquisa de vistas: Integração de operações de segurança - Capacidade de pesquisa de vistas
   - Pesquisa de ameaças: Integração de operações de segurança - Recurso de pesquisa de ameaças

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários do domínio do locatário criam suas próprias regras de análise de e-mail para ingerir incidentes de segurança.
- Os proprietários do domínio do locatário podem configurar integrações específicas exclusivamente para uso no domínio.
- Os proprietários do domínio do locatário podem criar seus próprios fluxos de trabalho de resposta a incidentes.
- Os proprietários do domínio do locatário podem criar suas próprias categorias de incidentes, artigos da base de conhecimento de resposta a incidentes e runbooks a serem associados a fluxos de trabalho de resposta a incidentes.
- Os usuários do domínio do locatário criam e encerram seus próprios incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Resposta a incidentes de segurança usuários e grupos
- Resposta a incidentes de segurança Integrações (a partir da versão Madrid)
- Regras de análise de e-mail para criação de incidente
- Regras de negócios para consolidar vários eventos ou alertas em um incidente de segurança
- Fluxos de trabalho para orquestração de resposta a incidentes
- Calculadoras de pontuação de risco de incidente de segurança
- Caminho de escalação de incidente de segurança
- ANS de incidente de segurança
- Definições de processo de incidente de segurança
- Processos de revisão pós-incidente de segurança

Tópicos relacionados

Domain Separation para provedores de serviço

Configuração do Resposta a incidentes de segurança

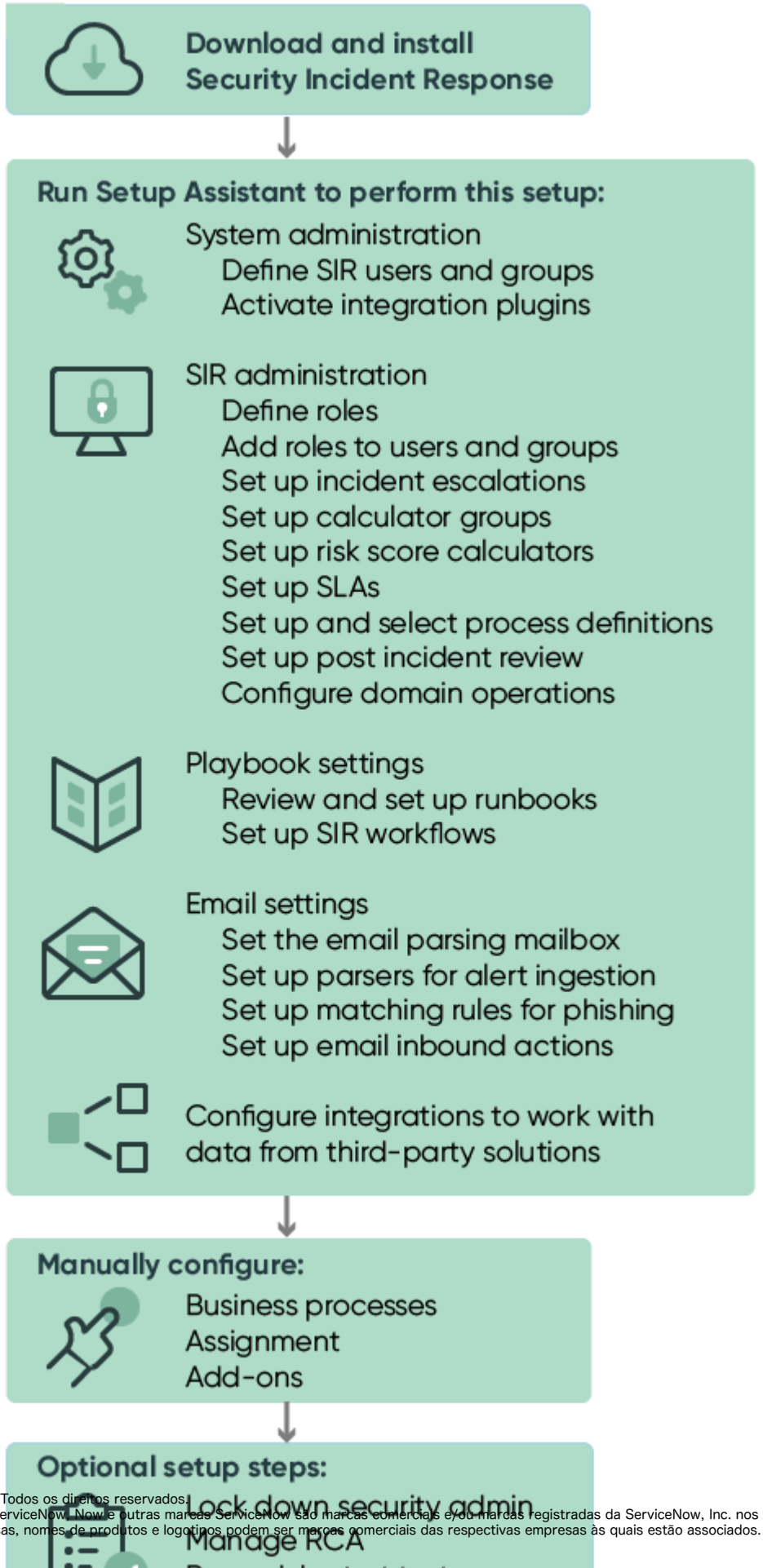
Configuração para Resposta a incidentes de segurança envolve algumas etapas obrigatórias e várias etapas opcionais, dependendo de seus requisitos específicos. Depois de ter baixado Resposta a incidentes de segurança em ServiceNow Store E instalado, você está pronto para executar o Assistente de configuração para executar a configuração básica do Resposta a incidentes de segurança e integrações de terceiros.

. Resposta a incidentes de segurança processo de configuração

O diagrama a seguir ilustra o processo de configuração. Ele é separado em dois subprocessos, baixando e configurando o. Resposta a incidentes de segurança aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A primeira etapa de configuração é a. baixe o. Resposta a incidentes de segurança aplicação do ServiceNow Store. Quando o download é concluído, vários aplicativos dependentes, incluindo o Assistente de configuração, são carregados e prontos para uso para configurar Resposta a incidentes de segurança.

Assistente de configuração

. Resposta a incidentes de segurança Assistente de configuração é uma aplicação semelhante a um assistente que orienta você, passo a passo, durante a configuração da sua base Resposta a incidentes de segurança instância.



As etapas de configuração são bastante autoexplicativas; no entanto, se você precisar de explicações adicionais, poderá encontrar assistência adicional em Referência do Assistente de configuração . Depois de concluir a configuração usando o Assistente de configuração, você pode executar outros procedimentos de configuração opcionais , conforme necessário. Estes procedimentos incluem opções para:

- Configuração do ciclo de vida da solicitação
- Criação de catálogos e solicitações
- Configurar notificações
- Configuração de atribuição manual e automática
- Habilitação da base de conhecimento, documentos gerenciados e atividades de tarefa

Um novo e aprimorado Espaço de resposta a incidentes de segurança está disponível. Para obter mais informações, consulte Espaço de resposta a incidentes de segurança.

Instalar e configurar Resposta a incidentes de segurança

Antes de executar Resposta a incidentes de segurança em sua instância, você deve baixá-lo do ServiceNow Store e conclua as etapas de configuração.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

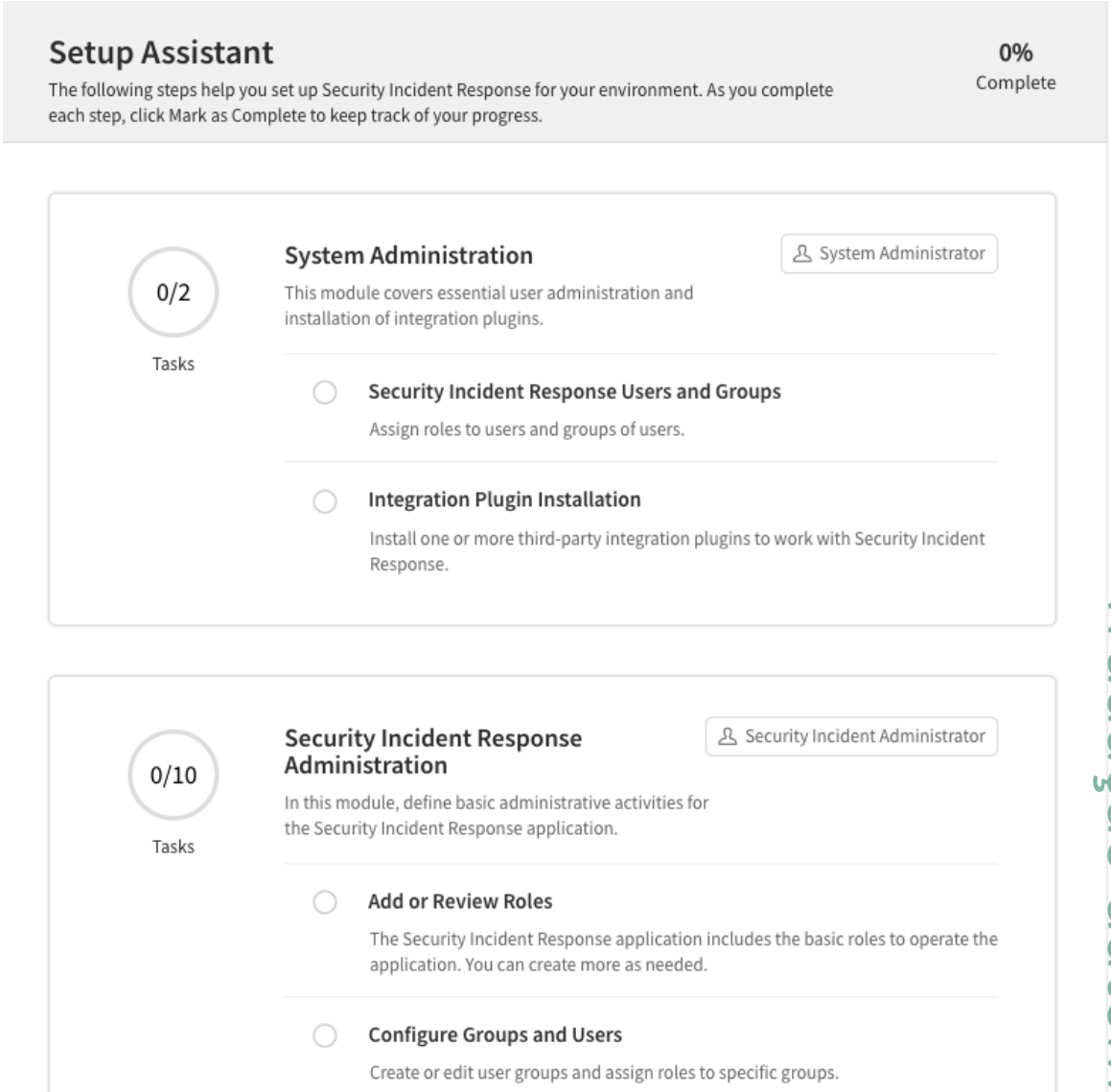
- Instalando o. Resposta a incidentes de segurança versão 13.4.5 ou posterior do ServiceNow Store instalará automaticamente o. Espaço de resposta a incidentes de segurança(sn_si_aw) versão 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte Espaço SIR plug-ins e funções seção.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/upgrade do Resposta a incidentes de segurança e não podem ser instaladas independentemente.
- Os recursos mais recentes do Resposta a incidentes de segurança estão disponíveis exclusivamente em Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para o mais recente Resposta a incidentes de segurança ou Espaço de resposta a incidentes de segurança Versão para acessar e aproveitar recursos como transferência de turno, calculadora de pontuação de risco etc.

Procedimento

1. Siga as instruções para baixando uma aplicação do ServiceNow Store.
2. Depois de baixar o. Resposta a incidentes de segurança e todas as suas aplicações de dependência, navegue até **Incidente de segurança** > **Configuração do Espaço do analista** > **Assistente de configuração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Siga as instruções nos formulários para configurar o. Resposta a incidentes de segurança sistema de base. Para obter informações adicionais sobre algumas das tarefas de configuração mais complicadas, consulte Referência do Assistente de configuração, conforme necessário.

Baixe e instale o Espaço do analista de segurança

Antes de executar o. Resposta a incidentes de segurança Nova IU em sua instância, você deve baixá-la do ServiceNow® Store e instale-o.

Antes de Iniciar

Para garantir uma instalação tranquila, verifique se você tem o necessário ServiceNow funções para sua instância. As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados:

- Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá a função Administrador de resposta a incidentes de segurança [sn_si.admin].
- O administrador de resposta a incidentes de segurança [sn_si.admin] supervisiona a configuração e verifica os resultados esperados.

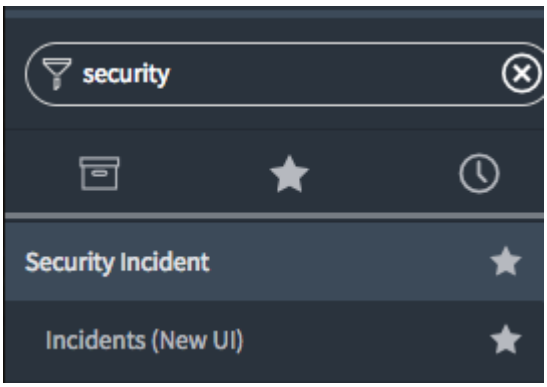
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga as instruções para baixando uma aplicação do ServiceNow Store e instale o. **IU de resposta do incidente de segurança** aplicação.
2. Após a conclusão da instalação, você pode abrir o Espaço do analista de segurança navegando até **Incidente de segurança** > **Incidentes (Nova IU)**



Componentes instalados com Resposta a incidentes de segurança

Vários tipos de componentes são instalados com o download e a ativação da aplicação Resposta a incidentes de segurança, incluindo funções de usuário, tabelas, propriedades e trabalhos agendados.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Propriedades instaladas

Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Propriedade	Uso
Os nós de categoria padrão que são exibidos na guia Gráfico de relacionamento no Espaço. Os valores padrão representam os nomes das tabelas correspondentes aos registros relacionados. sn_si_aw.defaultCategories	• **Tipo**: cadeia de caracteres • **Valor padrão** : sn_ti_m2m_task_observables,sn_si_m2m_task_affected_user,s
Hora de início padrão para todos os agentes quando nenhuma programação estiver definida, no formato 8:00 sn_si.default.start.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 08:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
Hora de término padrão para todos os agentes quando nenhuma programação estiver definida, no formato 17:00 sn_si.default.end.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 17:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Incluir observáveis do tipo de destino junto com outros observáveis de tipo de contexto no usuário de incidentes de segurança e relacionamentos de IC sn_si.link_dest_ip	Determina se um observável de incidente de segurança com um tipo de contex é exibido nas guias **Itens de configuração** ou **Usuários afetados**. Por p observáveis com um tipo de contexto de destino são excluídos. Para incluir os escolha Sim.
Permitir personalização ao criar um Problema ou uma Solicitação de mudança com base em um Incidente de segurança sn_si.popup	Quando um problema ou uma mudança são criados, esta propri uma janela pop-up para modificar a solicitação. Se essas propriedades estiverem definidas como **false**, o probl solicitação de mudança tem a mesma prioridade, descrição resu descrição do incidente de segurança sem a opção de adicionar esses campos. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Associe resultados de pesquisa de detecções a ICs no CMDB. sn_si.associate_ci_with_sighting_search	Quando definido como verdadeiro, os resultados da pesquisa de vistas incluem configuração associados que estão no seu CMDB. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
A pontuação de risco no intervalo é realçada em verde, no formato 0 - 49 sn_si.risk.score.green	Na lista Incidentes de segurança, os incidentes de segurança com uma pontua entre 0 e 49 são marcados com um ponto verde.
A pontuação de risco no intervalo é realçada em laranja, no formato 50 a 79 sn_si.risk.score.orange	Na lista Incidentes de segurança, os incidentes de segurança com uma pontua entre 50 e 79 são marcados com um ponto laranja.
A pontuação de risco no intervalo é realçada em vermelho, no formato 80 a 100 sn_si.risk.score.red	Na lista Incidentes de segurança, os incidentes de segurança com uma pontua entre 80 e 100 são marcados com um ponto vermelho.
Este parâmetro ativa ou desativa as configurações de pesquisa de detecções que têm esse recurso implementado.	Quando definido como verdadeiro, as pesquisas de detecções podem ser reali integrações ativadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_si.enable_sighting_search	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
O número de linhas de dados brutos é salvo quando for realizada uma pesquisa de detecções. Intervalo de 0 a 100 sn_si.sighting_search_raw_data_rows	Esta propriedade tem como padrão 50 linhas de dados brutos. Metade das linh resultados são relatadas a partir do início do intervalo de tempo de pesquisa e do final do intervalo de tempo de pesquisa. Portanto, se você selecionar 50 lin do início do intervalo de tempo de pesquisa e 25 do fim do intervalo de tempo
Avançar automaticamente o Estado do Incidente para Conter quando uma Tarefa de Resposta avançar para Trabalho em Andamento sn_si.rollup_task_state	Ao usar fluxos ou fluxos de trabalho, considere definir esta propriedade como permite que você controle o Estado do incidente de dentro de fluxos ou fluxos Também ajuda a evitar possíveis conflitos durante a transição de um estado d outro. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Propriedades de atribuição do Security Incident Response	
Peso do local sn_si.location.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o local for consi uma tarefa, o valor do peso do local será adicionado à classificação do analist • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso das Habilidades sn_si.skills.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, habilidades fore para uma tarefa, o valor do peso das habilidades será adicionado à classificaçã de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Definir o número máximo de analistas de segurança a serem processados pela atribuição automática de uma vez sn_si.max.agents.processed	O sistema tem um limite absoluto de 300 analistas de segurança. Se você espe 300, ele definirá o valor para esse nível. O sistema não pode expedir automati tarefa para um grupo de expedição que contém mais analistas de segurança do configurado. • **Tipo**: inteiro • **Valor padrão**: 100 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso do Fuso horário	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o fuso horário d

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_si.timezone.weight	segurança for considerado para uma tarefa, o valor do peso do fuso horário se classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Quantidade de tempo (em minutos) para adicionar entre o final de uma tarefa e o início da próxima viagem. sn_si.work.spacing	Um exemplo de valor de tempo válido é 10. • **Tipo**: inteiro • **Valor padrão**: 0 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Campos de diário especificados que contenham marcadores de código que renderizem o conteúdo como HTML. sn_si.journal_field.html_enabled	• **Tipo**: cadeia de caracteres • **Valor padrão**: work_notes, comentários • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Calcule os serviços afetados em segundo plano. sn_si.refresh_impacted.event	A lista relacionada Serviços afetados/ICs afetados é gerada por meio de event habilitada, a atualização é executada em segundo plano e marcadores de segu adicionados ao incidente. Defina o valor como **verdadeiro** para executar a operação em se plano. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Recupere o serviço crítico de dados pré-calculados. sn_si.critical_service.calculator.use_cache	Permite que a calculadora de serviço crítico use dados pré-calc itens de configuração. Defina o valor como **verdadeiro** para pesquisar a partir de dado calculados • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de incidentes de segurança [sn_si.admin]	Controle total sobre todos os dados de Resposta a incidentes de segurança. Também gerencia territórios e habilidades, conforme necessário.	• assessment_admin • catalog_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	Nota: No sistema de base, o administrador também tem acesso a sn_si.admin. Resposta a incidentes de segurança pode ser restringido pelo administrador, desde que pelo menos outro usuário tenha a função de administrador de segurança atribuída.	• decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.ingestion_profile_admin • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Administrador de perfil [sn_si.ingestion_profile_admin]	Configure os plug-ins, crie, edite, exclua e gerencie perfis para a aplicação Splunk, Splunk ES e Azure Sentinel Integration for Security Operations. **Nota:** Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão. A função sn_si.ingestion_profile_admin é atribuível aos usuários pelo sn_si.admin.	N/D

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Analista de incidentes de segurança [sn_si.analyst]	Gerenciar incidentes de segurança. Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_access
Incidente de segurança básico [sn_si.basic]	Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• canvas_user • document_management_user • email_composer • flow_operator • Inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user
Diretoria de segurança da informação (CISO) [sn_si.ciso]	Exibir e manipular o painel do CISO. Além disso, se o plug-in Resposta a vulnerabilidades estiver ativado, os usuários com esta função poderão adicionar mapas de árvore de definição de significância de vulnerabilidade ao painel. Você também pode fazer o mesmo com Resposta a incidentes de segurança plug-in.	• pa_viewer • sn_si.basic • sn_si.read
Incidente de segurança externo [sn_si.external]	Exiba todos os incidentes de segurança que pertencem ao grupo específico.	service_fulfiller

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	Nota: As duas regras a seguir são aplicáveis em ServiceNow independentemente do administrador com escopo ou do app do escopo. • Ao adicionar qualquer usuário a um grupo, você também está atribuindo funções a esse grupo. Da mesma forma, quando você remove um usuário de um grupo, as funções herdadas também são removidas. • Cada função é atribuível por alguma função de precedência mais alta.	
Usuário de integração de incidente de segurança [sn_si.integration_user]	Ferramentas externas podem fornecer novos registros de incidentes de segurança e atualizar registros de incidentes de segurança.	import_transformer
Administrador de conhecimento do incidente de segurança [sn_si.knowledge_admin]	Gerencie, atualize e exclua as informações na base de conhecimento do Incidente de Segurança.	• knowledge_admin • sn_si.read
Gerente de incidenets de segurança [sn_si.manager]	Mesmo acesso que os analistas de segurança.	• pd_author • pd_operator • sn_si.basic
Leitura de incidente de segurança [sn_si.read]	Ler incidentes de segurança.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet • sn_ti.observable.read • workspace_user
Gerenciador de acesso de restrição de segurança [sn_si.restriction_access_manager]	Permite que usuários ou grupos "imponham restrições" em incidentes de segurança. Aplicável somente para mudança de campo.	N/D
Acesso especial a incidentes de segurança sn_si.special_access	Fornece acesso a incidentes de segurança específicos para usuários fora da organização do Security Operations.	N/D

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Ativador de acesso especial de segurança [sn_si.special_access_enabler]	Fornece função de acesso especial a um usuário fora da organização Operações de segurança a incidentes de segurança específicos.	N/D
Gerenciador de leitura de acesso especial de incidente de segurança [sn_si.special_access_read_manager]	Gerencie a função Acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o. **Acesso de leitura** campo no formulário de incidente de segurança. Esta função pode ser atribuída por sn_si.admin.	sn_si.special_access_enabler
Gerenciador do gravador de acesso especial a incidentes de segurança [sn_si.special_access_write_manager]	Gerencie a função Acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o. **Acesso privilegiado** campo no formulário de incidente de segurança. Esta função pode ser atribuída por sn_si.admin.	sn_si.special_access_enabler

Trabalhos agendados instalados

Trabalho agendado	Descrição
Pesquisar observáveis de incidente de segurança	Executa uma pesquisa de observáveis em uma programação definida pelo usuário.

Tabelas instaladas

Tabela	Descrição
Configuração do Feed de Notícias [sn_si_feed_configuration]	Registros de configuração usados para definir o conteúdo exibido no feed de notícias de incidentes de segurança.
Regra de Atribuição de Análise Pós-incidente [sn_si_pir_condition]	Automatiza a seleção de participantes de uma pesquisa de revisão pós-incidente quando um incidente de segurança é encerrado.
Incidente de Segurança [sn_si_incident]	Armazena um incidente de segurança, as respostas ao incidente, todas as tarefas vinculadas, mudanças, problemas e incidentes relacionados a este incidente de segurança.
Vetores de Ataque do Incidente de Segurança [sn_si_attack_vector]	Opções de vetor de ataque.
Log de Auditoria de Incidentes de Segurança [sn_si_audit_log]	Armazena logs de auditoria de aprimoramento de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Calculadora de Incidentes de Segurança [sn_si_calculator]	Uma calculadora para definir determinados campos de incidente de segurança quando certas condições são atendidas.
Grupo de Calculadoras de Incidentes de Segurança [sn_si_calculator_group]	Um agrupamento de calculadoras de incidente de segurança. A ordem do grupo de calculadoras determina qual grupo é avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Firewall de aprimoramento de incidente de segurança [sn_si_enrichment_firewall]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do Firewall da Palo Alto Networks.
Resultados de malware de aprimoramento de incidente de segurança [sn_si_enrichment_malware]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do malware.
Estatísticas de Rede de Aprimoramento de Incidente de Segurança [sn_si_enrichment_network_statistics]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos das estatísticas de rede.
Processos em execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running _processes]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para processos em execução.
Serviços de Execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running_service]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para serviços em execução.
Pesquisa de E-mail de Incidente de Segurança [sn_si_m2m_incident_email_search]	Mapeia registros de pesquisa de e-mail para incidentes de segurança.
Importação de incidentes de segurança [sn_si_incident_import]	Tabela de importação para incidentes de segurança. Usado para criar incidentes de segurança a partir de sistemas externos.
Definição do Processo de Incidentes de Segurança [sn_si_process_definition]	Armazena a configuração dos fluxos do processo de incidente de segurança.
Seletor de Definição do Processo de Incidentes de Segurança [sn_si_process_definition_selector]	Armazena a definição do processo de incidente de segurança a ser usada para incidentes de segurança.
Caso do Atendimento ao cliente relacionado ao incidente de segurança [sn_si_m2m_incident_customerservice_case]	Mapeia casos de atendimento ao cliente e incidentes de segurança
Dados de aprimoramento relacionados ao Incidente de Segurança	Mapeia incidentes de segurança e registros de dados de aprimoramento relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_si_m2m_incident_enrichment]	
Tarefa Resposta a incidentes de segurança [sn_si_task]	Gerencia subtarefas relacionadas à manipulação de um incidente de segurança. Essas tarefas podem ser atribuídas ao pessoal de segurança ou a pessoas em outros departamentos, para gerenciar a comunicação entre departamentos e o acompanhamento de tarefas.
Modelo de tarefas Resposta a incidentes de segurança [sn_si_task_template]	Usado para criar uma tarefa Resposta a incidentes de segurança. Esses modelos geralmente são usados em entradas do catálogo para criar automaticamente um conjunto de subtarefas apropriadas para um tipo específico de incidente de segurança.
Documento de runbook de incidente de segurança [sn_si_runbook_document]	Associa condições ou filtros de incidente de segurança a um artigo de conhecimento. Usado para especificar procedimentos de runbook para correção de incidente de segurança.
Modelo de Incidente de Segurança [sn_si_incident_template]	Usado para criar um incidente de segurança. Esses modelos geralmente são usados em entradas do catálogo para criar um incidente de segurança pré-criado.
Requisição de Segurança [sn_si_request]	Uma solicitação relacionada à segurança para a equipe de segurança.
Solicitação de Verificação de Segurança [sn_si_scan_request]	Uma solicitação de pesquisa de ameaças.
Calculadora de Gravidade sn_si_severity_calculator	Define os valores de severidade, impacto, risco e criticalidade de um incidente de segurança.
Usuário Afetado pela Tarefa [sn_si_m2m_task_affected_user]	Uma tabela muitos para muitos que associa incidentes de segurança aos usuários afetados.
Avaliador de Resultado de Atividade de Fluxo de Trabalho de Modelo [sn_si_wf_activity_outcome_evaluator]	Mapeia um recurso com um script de avaliação. Um novo subfluxo pode ser adicionado a um fluxo de trabalho de modelo para definir um resultado de tarefa de resposta em vez de ter um analista para defini-lo manualmente.

Adicional Resposta a incidentes de segurança tarefas de configuração

Se você for um administrador no domínio global, configure como Resposta a incidentes de segurança lida com operações diárias.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Essas opções são padrão para muitas aplicações de gestão de serviços e, como tal, usam a terminologia de gestão de serviços. Por exemplo, Solicitação é usada para a tarefa principal (ou seja, o incidente de segurança) e Tarefa é usada para subtarefas ou tarefas de resposta.

Se você for um administrador em um domínio inferior ao domínio global, poderá exibir a tela Configurações, mas não poderá modificar as configurações.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Configuração**.
   As opções para configurar as aplicações estão organizadas nestas guias:
   - . **Processo de negócios** contém opções para configurar o ciclo de vida da solicitação, criar catálogos e solicitações e configurar notificações.
   - . **Atribuição** contém opções para configurar atribuição manual e automática.
   - . **Complementos** contém opções para habilitar a base de conhecimento, documentos gerenciados e atividades de tarefa.
2. Preencha os campos em **Processo de negócios** guia.

Tela de configuração - Guia Processo de negócios

Campo	Descrição
Ciclo de vida	
As anotações de trabalho são necessárias para fechar ou cancelar uma solicitação ou tarefa	Habilite esta opção para exigir que o usuário insira anotações de trabalho antes que um incidente de segurança ou tarefa de resposta possa ser encerrado ou cancelado.
Copiar anotações de trabalho da tarefa para solicitação	Habilite esta opção para sincronizar as anotações de trabalho da tarefa de resposta com as anotações de trabalho no incidente de segurança. Portanto, quando anotações de trabalho na tarefa são adicionadas, as mesmas anotações de trabalho aparecem no incidente de segurança primário.
Criação de Solicitação e Catálogo	
Criar ou atualizar solicitações por e-mail de entrada	Habilite esta opção para criar ou atualizar incidentes de segurança a partir de e-mails de entrada.
As solicitações são criadas usando	Selecione **formulário de catálogo ou regular** para ativar o catálogo e habilitar a publicação automática de modelos de incidentes de segurança no catálogo. Selecione **formulário regular somente** para desativar o catálogo e desabilitar a publicação automática de modelos de incidente de segurança no catálogo.
Os modelos criam um item do catálogo dedicado	Habilite esta opção para ativar a publicação automática de itens do catálogo para a aplicação.
Notificações	

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Para uma solicitação ou tarefa, quando o campo selecionado mudar, envie uma notificação aos destinatários	Você pode configurar notificações para serem enviadas a destinatários específicos quando os campos selecionados em incidentes de segurança e tarefas de resposta mudarem. **a.** De **Tabela** , selecione **Solicitação (incidente de segurança** ou **Tarefa (tarefa de resposta)** . **b.** De **Campo** , selecione o campo a ser usado para gerar notificações. Quando uma mudança é feita no campo selecionado, uma notificação é enviada aos destinatários identificados. **c.** De **Destinatários** selecione um ou mais destinatários. **d.** Se você selecionar **um usuário específico** ou **um grupo específico** , você será solicitado a selecionar um usuário ou grupo. **e.** Para definir mais notificações usando outros campos ou destinatários, repita as etapas anteriores para o próximo conjunto de configurações de notificação. **f.** Para remover uma notificação, clique em ícone à direita da notificação.

3. Clique em **Atribuição** e preencha os campos.

Tela de configuração - Guia Atribuição

Campo	Descrição
Método de atribuição para solicitações	Selecione o método para atribuir incidentes de segurança: ○ **usando atribuição automática** : Incidentes de segurança são atribuídos automaticamente. ○ **usando um fluxo de trabalho** : Incidentes de segurança são atribuídos pelo fluxo de trabalho selecionado. ○ **manualmente** : Incidentes de segurança são atribuídos manualmente.
Use este fluxo de trabalho para atribuir solicitações	Selecione o fluxo de trabalho para expedir incidentes de segurança. Este campo aparece quando **usando um fluxo de trabalho** selecionado em **Método de atribuição para solicitações** lista.
Método de atribuição para tarefas	Selecione o método para atribuir tarefas de resposta: ○ **usando atribuição automática** Tarefas de resposta são atribuídas automaticamente. ○ **usando um fluxo de trabalho** Tarefas de resposta são atribuídas pelo fluxo de trabalho selecionado. ○ **manualmente** Tarefas de resposta são atribuídas manualmente.
Use este fluxo de trabalho para atribuir tarefas	Selecione o fluxo de trabalho para atribuir tarefas de resposta. Este campo aparece quando **usando um fluxo de trabalho** selecionado em **Método de atribuição para tarefas** lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuir solicitações ou tarefas com base nas áreas cobertas do grupo de atribuições	Habilite esta opção para limitar a atribuição de incidentes de segurança e tarefas de resposta a grupos que cobrem o local da tarefa.
Programando	
A seleção automática de agentes considera o fuso horário para tarefas	Habilite esta opção para considerar o fuso horário do agente ao atribuir uma tarefa. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Fatores adicionais	
A seleção automática de agentes considera a localização dos agentes	Habilite esta opção para dar preferência aos agentes que estão mais próximos do local da tarefa ao atribuir tarefas. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
A seleção automática de agentes requer tarefas que eles estejam aptos a realizar	Selecione o grau em que as habilidades do agente devem ser correspondidas a uma tarefa ao determinar a atribuição automática. ○ Selecione **todos** exigir que um agente atribuído tenha todas as habilidades para executar a tarefa. Um agente que não tem uma habilidade é eliminado. ○ Selecione **alguns** se você quiser agentes que tenham a maioria das habilidades necessárias para executar a tarefa. ○ Selecione **nenhum** se você quiser atribuir agentes automaticamente sem levar em conta as habilidades. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Tentativa de seleção automática de atribuir o mesmo agente a todas as tarefas em uma solicitação	Habilite esta opção para atribuir automaticamente todas as tarefas de resposta de um incidente de segurança ao mesmo agente.

4. Clique em **Complementos** e preencha os campos.

Guia Configuração - Guia Complementos

Campo	Descrição
Documentação	
Habilitar uma base de conhecimento dedicada	Habilite esta opção para ativar a base de conhecimento para Resposta a incidentes de segurança.
Habilitar documentos gerenciados	Habilite esta opção para adicionar uma lista relacionada a documentos gerenciados.
Habilitar atividades da tarefa	Habilite esta opção para registrar interações e comunicações de tarefas, como chamadas telefônicas e mensagens de e-mail.

5. Clique em **Salvar**.

Bloquear administração de segurança

Para proteger as investigações e manter os incidentes de segurança privados, você pode restringir Resposta a incidentes de segurança Acesso a funções e ACLs específicas de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administradores que não sejam de segurança podem ser restritos ao acesso, a menos que você permita expressamente a entrada deles.

Antes de Iniciar

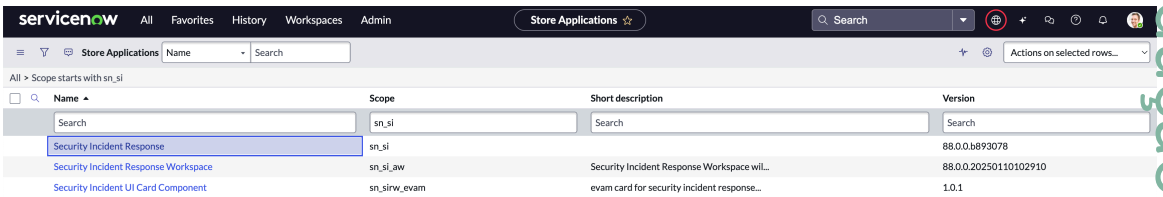
. Resposta a incidentes de segurança A aplicação está ativada, o usuário Administrador do sistema recebe a função sn_si.admin por padrão. O Administrador do sistema é o único administrador que pode configurar grupos de segurança e usuários.

Uma função de segurança é necessária para ter acesso a. Resposta a incidentes de segurança recursos e registros.

Função necessária: sn_si.admin

Procedimento

1. Após Resposta a incidentes de segurança O plug-in foi ativado, um usuário com a função de administrador atribui a função de administrador com escopo (sn_si.admin) a pelo menos um usuário.
2. O usuário com a função de administrador muda para o escopo do Incidente de segurança.
3. Navegar até **Tudo** > **sys_store_app.list**.
4. Tipo **sn_si** em **Escopo** campo.



5. Clique em **Resposta a incidentes de segurança** .
6. Role para baixo até **Links relacionados** e clique em **Remover da função contida pelo administrador** .
7. Logout e login novamente.
   O usuário administrador não pode acessar o. Resposta a incidentes de segurança aplicação.

Tópicos relacionados

Administração da aplicação

Gerenciar acesso restrito do solicitante

O recurso RCA (Restricted Caller Access, acesso restrito do solicitante) permite que um administrador defina o acesso entre escopos a uma aplicação ou recurso de aplicação e permita ou negue solicitações de acesso. Este recurso está habilitado em Resposta a incidentes de segurança por padrão, os analistas de segurança podem proteger informações confidenciais relacionadas à segurança.

Um campo chamado **Acesso do solicitante** foi adicionado a todas as tabelas e inclusões de script em Resposta a incidentes de segurança e o campo é padronizado como **Acompanhamento do solicitante** . Esta configuração significa que os escopos da aplicação têm permissão de acesso a. Resposta a incidentes de segurança tabelas e inclusões de script. No entanto, um registro de acompanhamento é criado para cada registro e armazenado na tabela Privilégio de acesso de solicitante restrito [sys_restricted_caller_access].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Tome cuidado ao mudar registros de **Acompanhamento do solicitante** . **Solicitante restrito** . Registros com este status não podem ser acessados até que um administrador permita o acesso a ele manualmente. O administrador deve navegar até **Aplicações do sistema** > **Acesso de chamador restrito a aplicação**, localize a tabela ou inclusão de script para a qual o acesso foi solicitado e altere **Status** campo de **Solicitado** . **Permitido** .

Tópicos relacionados

Configurações de privilégio de acesso de solicitante restrito

Defina o escopo da aplicação, o recurso da aplicação e o acesso ao evento

Execute testes de início rápido para Resposta a incidentes de segurança

Valide isso Resposta a incidentes de segurança ainda funciona depois que você faz mudanças de configuração, como aplicar um upgrade ou desenvolver uma aplicação. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

Os testes de início rápido Resposta a incidentes de segurança exigem a ativação do plug-in Resposta a incidentes de segurança (com.snc.security_incident) e o carregamento dos dados de demonstração.

Testes Resposta a incidentes de segurança

Teste	Descrição	Versão de lançamento
SIR: criar incidente de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Madrid
SIR: criar incidente de segurança por meio do catálogo de incidentes de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Madrid
SIR: ciclo de vida do incidente de segurança	Valide as tarefas de resposta do fluxo de trabalho de violação de política.	Madrid
SIR: Teste de configuração OOTB de avaliações PIR	Use este teste para validar avaliações de PIR e configurações de sistema de base.	Tokyo
SIR: Testes de configuração condicional de avaliações de PIR	Verifique se incidentes de segurança correspondentes à regra condicional obrigatória não são encerrados sem a conclusão da avaliação pós-incidente. Verifique se os incidentes de segurança correspondentes à regra condicional opcional podem ser encerrados sem a conclusão da avaliação pós-incidente. Verifique se as avaliações não são geradas para os	Tokyo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a incidentes de segurança

Teste	Descrição	Versão de lançamento
	incidentes de segurança que não correspondem a nenhuma regra.	
PIR: Experiência de tempo de execução do PIR	Verifique se os relatórios PIR estão configurados e anexados aos incidentes de segurança de acordo com o novo design.	Tokyo
PIR Design Time Experience	Verifique se o incidente de segurança está mapeado com o modelo de relatório baseado na configuração do administrador.	Tokyo
SIR: Vincular o incidente de segurança a um importante incidente de segurança existente	Vincule um Incidente de Segurança a um Incidente de Segurança Importante existente e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Tokyo
SIR: promover o incidente de segurança como um incidente de segurança importante	Promova um Incidente de Segurança como um Incidente de Segurança Importante e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Tokyo
SIR: propor Incidente de Segurança como Incidente de Segurança Importante	Proponha um Incidente de Segurança como Incidente de Segurança Importante e valide os dados de Incidente de Segurança implementados no Incidente de Segurança Importante.	Tokyo
SIR: ciclo de vida do incidente de segurança	Valide um ciclo de vida de incidente de segurança com o fluxo de trabalho de tarefas de resposta à violação de política.	Yokohama
SIR: Criar caso de segurança	Crie um caso de segurança no formulário Incidente de segurança.	Yokohama
Verifique se somente Membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ATIVADA	Verifique se somente membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ativada.	Yokohama
Verifique se o incidente de segurança habilitado com "Impor restrição" não está visível para nenhum usuário	Verifique se o incidente de segurança habilitado com "Impor restrição" não está visível para nenhum usuário.	Yokohama
Validar acesso de leitura	Valide o acesso de exibição.	Yokohama
Validar acesso de gravação	Valide o acesso de edição.	Yokohama

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a incidentes de segurança

Teste	Descrição	Versão de lançamento
Espaço SIR: Acesso de leitura	Verifique se o usuário de acesso de leitura pode exibir o incidente de segurança sem ter funções de segurança, mesmo no espaço.	Yokohama
Espaço SIR: Acesso de gravação	Verifique se o usuário de acesso de gravação pode atualizar o incidente de segurança sem ter funções de segurança.	Yokohama
Espaço SIR: Criar novo incidente de segurança	Crie um novo incidente de segurança a partir do espaço.	Yokohama
Espaço SIR: Criar tarefa de resposta	Crie uma nova tarefa de resposta a partir de um incidente de segurança existente.	Yokohama
Now Assist para segurança: Resumo de incidente de segurança ativo	Resuma um incidente de segurança ativo e valide as seções exibidas.	Zurich
Now Assist para segurança: Resumo do incidente de segurança_share para anotações de trabalho	Compartilhe o resumo gerado com anotações de trabalho.	Zurich
Now Assist para segurança: Resumo de incidente de segurança encerrado	Resuma um incidente de segurança encerrado e valide as seções exibidas.	Zurich

Tópicos relacionados

Testes de início rápido

Referência do Assistente de configuração

O Assistente de configuração orienta você pelas etapas que você precisa executar para configurar o. Resposta a incidentes de segurança sistema de base. Esta seção fornece informações adicionais sobre as etapas complicadas para as quais você pode precisar de mais explicações.

Crie um Resposta a incidentes de segurança definição do processo

Você pode criar uma definição de processo para definir como os incidentes de segurança fazem a transição de um estado para o próximo. As definições de processo fornecem às centrais de serviços e aos usuários finais ajuda a rastrear o problema durante todo o ciclo de vida.

Antes de Iniciar

Função necessária: sn.si_admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Definição de processo**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos, se for o caso.

Criando definições de processo

Campo	Descrição
Nome	Nome do registro que descreve o processo codificado no arquivo de inclusão de script. O nome é exibido como uma opção no **Seletor de definição de processo** lista.
Inclusão de script	O nome (incluindo `sn_si` . prefixo) da inclusão de script que contém a definição do processo. O script deve estar no Incidente de segurança (`sn_si` escopo da aplicação. Para obter mais informações, consulte Criar um personalizado Resposta a incidentes de segurança inclusão de script de definição de processo. Se este campo não contiver um nome de inclusão de script válido, a definição padrão ProcessDefinition_NIST_Stateful será usada.
Descrição	Informações úteis sobre a inclusão de script.
Ordem	Determina a posição na lista de definição de processo.
Ativo	Quando marcado, torna esta definição de processo selecionável no **Seletor de definição de processo** página.

4. Clique em **Enviar**.

Tópicos relacionados

Seleção do processo de resposta do incidente de segurança

Noções básicas sobre a definição do processo de resposta a incidentes de segurança

Noções básicas sobre a definição do processo de resposta a incidentes de segurança

Resposta a incidentes de segurança Definição de processo substitui fluxos de estado e fornece aos usuários finais e às centrais de serviços o status de um problema. Uma definição de processo ajuda a rastrear o problema durante seu ciclo de vida. Resposta a incidentes de segurançaÉ uma aplicação de Gestão de serviços (SM), que tem seu próprio conjunto de estados. estados inválidos são relatados como parte de Seleção de processo.

Definição do processo de resposta do incidente de segurança

A definição de processo padrão (NIST Stateful) define os seguintes estados de incidente:

Nota: os estados disponíveis variam com base no estado atual do incidente.

estados de definição do processo de incidente de segurança

Estado	Descrição
Rascunho	O iniciador da solicitação adiciona informações sobre o incidente de segurança, mas ele ainda não está pronto para ser trabalhado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estados de definição do processo de incidente de segurança

Estado	Descrição
Análise	O incidente foi atribuído e o problema está sendo analisado.
Contém	O problema foi identificado e a equipe de segurança está trabalhando para contê-lo e executar o controle de danos. Essas ações podem incluir colocar servidores off-line, desconectar equipamentos da Internet e verificar se há backups.
Erradicar	O problema foi contido e a equipe de segurança está tomando medidas para corrigir o problema.
Recuperar	O problema foi resolvido e a prontidão operacional dos sistemas afetados está sendo verificada.
Revisão	O incidente de segurança está concluído e todos os sistemas estão de volta à função normal, no entanto, uma revisão pós-incidente ainda é necessária.
Encerrado	O incidente está concluído, mas antes que um incidente de segurança possa ser encerrado, você deve preencher as informações no **Informações de fechamento** guia.

Definições de processo de tarefa de Incidente de segurança

As definições de processo a seguir são usadas para tarefas de incidente de segurança.

estados de definição do processo de tarefa

Estado	Descrição
Pronto	A tarefa está pronta para ser trabalhada depois que é atribuída a um agente.
Atribuída	A tarefa é atribuída a um agente.
Trabalho em andamento	O agente atribuído está trabalhando na tarefa.
Concluídas	A tarefa está concluída.
Cancelado	A tarefa foi cancelada.

O NIST oferece suporte aos dois modelos a seguir:

- **NIST Stateful**

  Esta definição de processo permite que os analistas se movam de um estado para outro em uma ordem sequencial sem ignorar nenhuma etapa. Por exemplo, se o analista começar com **Rascunho** , a ordem sequencial desta definição de processo é **Rascunho** > **Análise** > **Conter** > **Erradicar** > **Recuperar** . Portanto, a definição do Processo Stateful do NIST é unidirecional e permite que os analistas progridam somente para os estados futuros.

  Outro exemplo: Se o analista começar com o estado Análise, a ordem sequencial desta definição de processo será **Análise** > **Conter** > **Erradicar** > **Recuperar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **NIST aberto**

  Esta definição de processo permite que os analistas se movam de um estado para outro, para frente ou para trás. Por exemplo, se o analista começar com **Análise** , a ordem da definição do processo pode ser **Análise** > **Conter** > **Erradicar** > **Recuperar** ou **Análise** > **Rascunho** . Portanto, a definição de processo em aberto do NIST é bidirecional e permite que os analistas se movam para os estados de avanço ou retrocesso, dependendo de seus requisitos.

Seleção do processo de resposta do incidente de segurança

Resposta a incidentes de segurança A Seleção de processos lista processos com estados inválidos para incidentes de segurança e tarefas de resposta.

Um administrador pode corrigir o incidente ou a tarefa para estados válidos manualmente ou usando um script. Uma lista relacionada vazia (sem incidentes; sem tarefas) indica que todas as tarefas ativas estão em um estado válido. os estados disponíveis variam com base no estado atual do incidente. Para obter mais informações, consulte Corrija um incidente de segurança inválido ou estado de tarefa com a definição do processo.

Selecione um Resposta a incidentes de segurança definição do processo

Você pode selecionar a definição do processo a ser usada para os estados apropriados para os incidentes de segurança e tarefas de resposta da sua empresa.

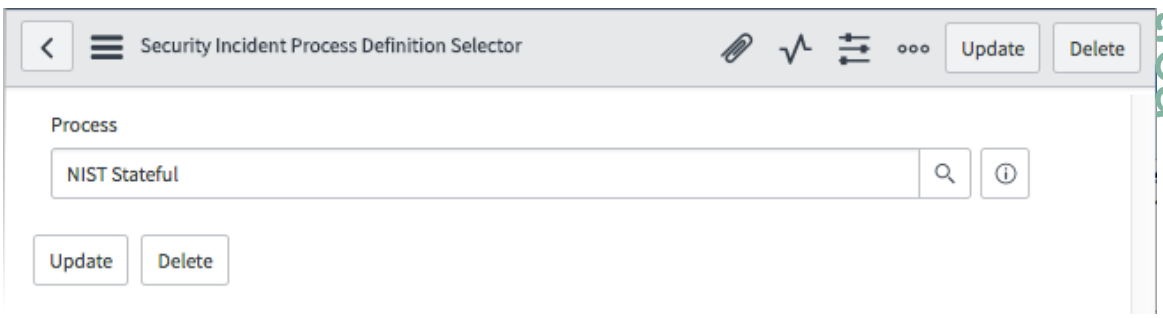
Antes de Iniciar

Função necessária: administrador e sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Tudo** > **Resposta a incidentes de segurança** > **Administração** > **Seleção de processo**.
2. Clique no ícone de pesquisa para listar as definições de processo disponíveis.



3. Selecione uma definição de processo.
4. Clique em **Atualizar**.

Criar um personalizado Resposta a incidentes de segurança inclusão de script de definição de processo

Crie um script de Definição de processo personalizado para os estados apropriados para os incidentes de segurança e tarefas de resposta da sua empresa.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O script principal sn_si.ProcessDefinition inclui definições de processo de controles. **Definição do processo** determina qual definição está em uso (usando **Seleção de processo**). Chama o arquivo de inclusão de script apropriado para determinar os estados iniciais e as transições para incidentes de segurança e tarefas de resposta.

Procedimento

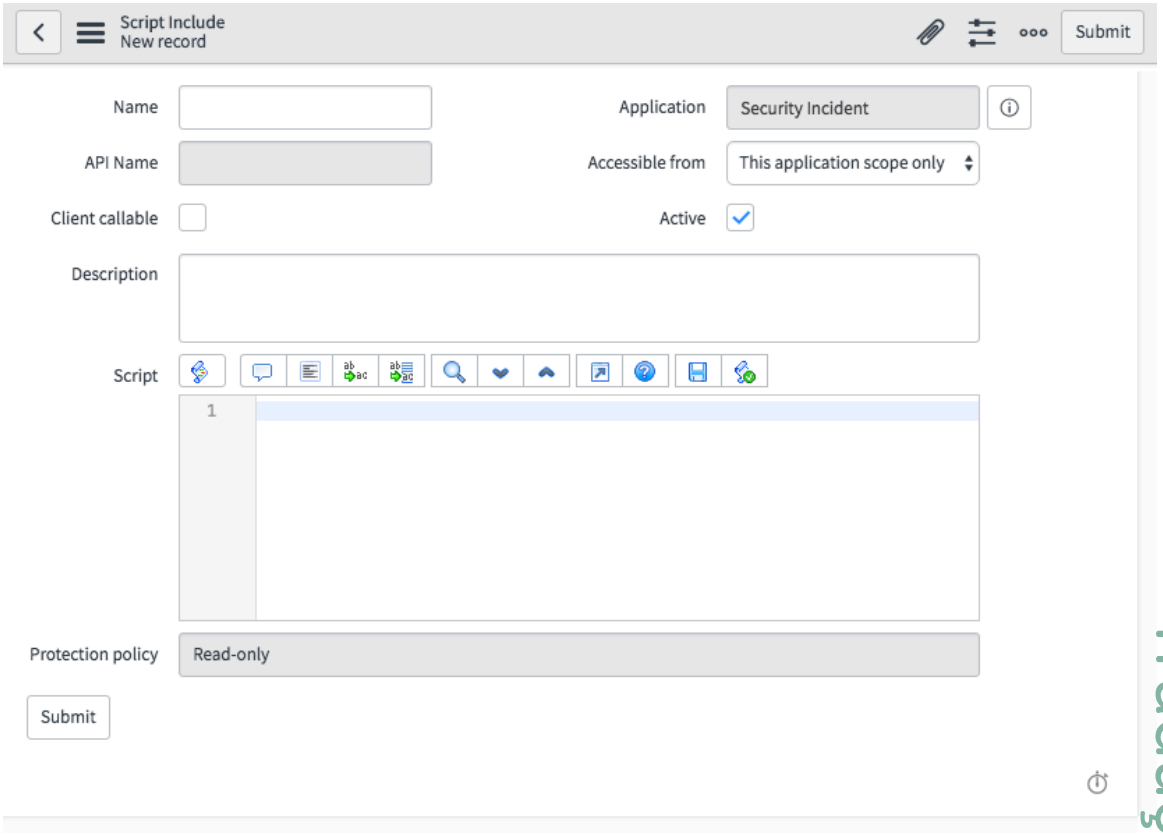
1. Navegar até **Tudo** > **Definição do Sistema** > **Inclusões de script**.
2. Clique em **Novo.**
3. Preencha os campos, se for o caso.

Criando definições de processo

Campo	Descrição
Nome	Nome desta inclusão de script.
Nome da API	Criado com base no nome da inclusão de script.
Cliente chamável	Disponibiliza a inclusão de script para scripts de cliente, filtros de lista e relatório, qualificadores de referência ou , se especificado , Como parte do URL.
Aplicação	Incidente de segurança
Acessível de	Escolha **Somente este escopo da aplicação** .
Ativo	Quando marcado, ele torna esta inclusão de script selecionável no **Definição do processo** página.
Descrição	Informações úteis sobre a inclusão de script.
Script	Define o script do lado do servidor a ser executado quando chamado de outros scripts. O script deve definir uma única classe JavaScript ou uma função global. O nome da classe ou função deve corresponder ao campo Nome. Para obter informações sobre o conteúdo do script, consulte Inclusão de script de Definição de processo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Enviar**.

Tópicos relacionados

Inclusão de script de Definição de processo

Inclusão de script de Definição de processo

A inclusão de script de Definição de processo fornece métodos para definir uma definição de processo.

Implemente as constantes, atributos, matrizes e chamadas de método descritas aqui para personalizar uma inclusão de script de definição de processo.

Onde usar

Use esta inclusão de script para criar uma definição de processo.

Corpo de inclusão de script

O corpo de inclusão de script é composto por três seções:

- Constantes: Definições de estado inicial
- Incidente de segurança e tarefa de resposta: Matrizes de definição do processo
- Chamadas de método: Recuperando informações

Constantes

As constantes são usadas para definir os estados iniciais de incidentes de segurança e tarefas de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O uso de constantes é opcional, mas incentivado para legibilidade. Por exemplo:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Que são usados posteriormente pelos seguintes métodos:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

O próximo conjunto de constantes define os estados para incidentes de segurança e tarefas de resposta.

Cada matriz também contém a definição de quais estados estão disponíveis quando o incidente ou a tarefa está em um estado específico.

Por exemplo:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

O exemplo é uma matriz de objetos. Cada objeto define um estado e possíveis estados de transição.

A ordem do objeto do estado determina a ordem desejada para o fluxo.

Quando a tarefa está no estado "Rascunho" (valor 1), os estados possíveis são: 1 (Rascunho, que não é mudança) e 10 (Pronto, a próxima etapa do processo).

Não há limite para o número de transições fora de um estado. "Encerramento concluído" e "Cancelado" são estados finais e, portanto, não têm transições de estado possíveis.

A ordem dos atributos no objeto não é importante. Se isso tornar a definição mais clara, coloque o rótulo primeiro.

Atributos

Os atributos obrigatórios em um objeto de definição de estado são:

- estado: valor numérico do estado
- rótulo: texto legível associado ao estado
- opção: uma matriz de valores de estado para os quais o estado pode fazer a transição (determina o conteúdo do menu suspenso de estado)

Os atributos opcionais são:

- Obrigatório: Lista de IDs de campo que se tornam obrigatórios neste estado
- somente leitura: Lista de IDs de campo que se tornam somente leitura neste estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Visível: Lista de IDs de campo que se tornam visíveis neste estado
- Não obrigatório: Lista de IDs de campo que se tornam não obrigatórios neste estado
- Notvisible: Lista de IDs de campo que não estariam mais visíveis neste estado

Nota:

Se atributos opcionais forem usados, é responsabilidade do autor garantir que os campos sejam tornados visíveis/invisíveis, obrigatórios/não obrigatórios, visíveis/ocultos ou somente leitura adequadamente entre os estados.

Ocultar um campo em um estado não o torna visível em outro estado posteriormente, a menos que o atributo "visível" seja usado.

Matrizes de definição de fluxo do processo

Para definir as informações exibidas no formatador de fluxo do processo (a barra na parte superior dos formulários de tarefa Incidente de segurança e Resposta), o sistema requer informações sobre o que exibir para cada estado.

Por exemplo:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

A matriz TASK_pf é uma coleção de rótulos, condições e descrições usadas para determinar o texto exibido na barra do formatador de processos (incluindo ordem e atividade).

No exemplo, o texto "Pronto" é o segundo item exibido. É realçado quando a tarefa atende à condição "estado: 10 EQ".

Quando o ponteiro passa o mouse sobre o texto, a descrição "Tarefa de resposta do incidente de segurança está pronta para ser atribuída" é exibida.

Nota:

Os estados podem ser combinados em um único estado do formatador.

No exemplo, os estados "Encerramento concluído" e "Cancelado" aparecem como "Encerrado" na barra superior.

Chamadas de método

Os seguintes métodos devem estar presentes na inclusão de script, pois são usados por sn_si.ProcessDefinition:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de retorno	Resumo do método	Descrição
Cadeia de caracteres	GetInitialIncidentState: Function()	retorna o valor numérico do estado do incidente inicial
Cadeia de caracteres	GetInitialTaskState: Function():	retorna o valor numérico do estado da tarefa inicial
Matriz de cadeia de caracteres	GetIncidentstates: Função():	retorna a matriz do estado do incidente
Matriz de cadeia de caracteres	GetTaskStates: Função():	retorna a matriz do estado da tarefa
Matriz de objetos	GetIncidentProcessFlows: Função():	retorne a matriz de definição de fluxo do processo de incidente
Matriz de objetos	GetTaskProcessFlows: Função():	retorne a matriz de definição de fluxo do processo de tarefa

O próximo conjunto de métodos é chamado sempre que um incidente ou uma tarefa é atualizado e permite que ações sejam tomadas em transições de mudança específicas.

Tipo de retorno	Resumo do método	Descrição
vazio	PerformIncidentStateChange: Função(atual, anterior)	Este método é usado para definir valores relacionados ao SM e garantir que um incidente saia do "Rascunho" depois que alguém for atribuído a ele.
vazio	PerformTaskStateChange: Função(atual, anterior)	No exemplo, este método é usado para atualizar carimbos de data/hora (na atribuição e no fechamento) e avançar a tarefa de "Pronto" para "Atribuído" depois que o campo assigned_to for preenchido.

As mesmas ações executadas por esses dois métodos podem ser realizadas usando uma regra de negócio. Ao defini-las na inclusão de script, a alternância de definições de processo é mais fácil.

Corrija um incidente de segurança inválido ou estado de tarefa com a definição do processo

Um administrador pode corrigir o incidente de segurança ou a tarefa para estados válidos, manualmente ou usando um script. os estados disponíveis variam com base no estado atual do incidente.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois de alternar as definições de processo, a nova definição pode não oferecer suporte a alguns dos estados antigos. Para corrigir o incidente órfão ou os estados da tarefa, você pode mude a definição do processo , edite sua inclusão de script ou abra manualmente cada incidente ou tarefa para atualizar o estado. Atualizar o estado (que pode ser feito em massa) é a solução mais fácil.

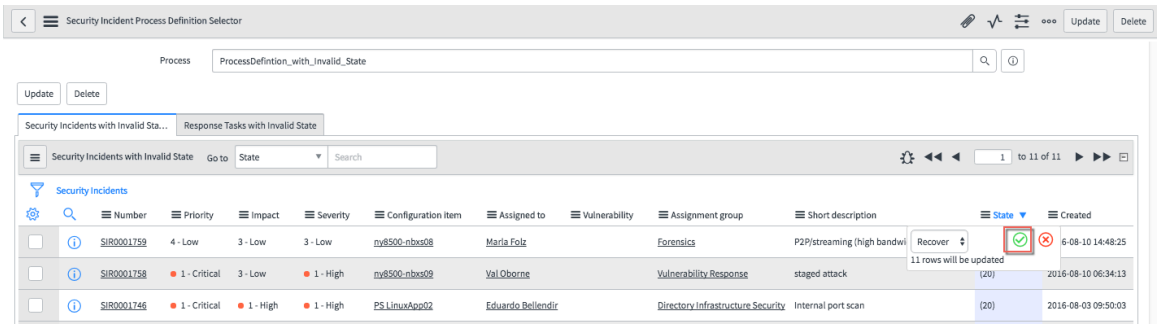
Para mudar estados em massa, faça o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Seleção de processo**.
2. Realce **Estado** campo para os incidentes ou tarefas que você deseja mudar.
3. Duplo- clique em **Estado** no primeiro registro, selecione o novo **Estado,** e clique na marca de seleção verde ( ) para concluir a mudança.



4. Clique em **Atualizar**.

Crie um grupo de incidentes de segurança

Configure um grupo de incidentes de segurança e atribua as funções e usuários apropriados ao grupo.

Antes de Iniciar

Funções necessárias:

- Se você tiver a função user_admin, poderá criar grupos de atribuição de incidentes de segurança.
- Se você tiver a função sn_si.admin, poderá criar e editar grupos de atribuição de incidentes de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Os usuários em um grupo herdam as funções do grupo, portanto, você não precisa atribuir funções a cada usuário separadamente.

Criar quantos grupos forem necessários em sua organização é uma prática recomendada. Também é uma prática recomendada criar um grupo para administradores e atribuir a função de administrador somente a este grupo.

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos** ou **Incidente de segurança** > **Configuração** > **Grupos**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Nota:

Para obter mais informações, consulte Crie um grupo de usuários .

4. Certifique-se de selecionar **incidente de segurança** tipo para este grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. . **Tipo** o campo não está visível, configure o formulário para adicioná-lo.

b. Clique no ícone de cadeado ao lado de **Tipo** campo.

c. Clique no ícone de pesquisa de referência ()

d. PESQUISE e selecione **incidente de segurança** tipo.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
6. Em **Funções** lista relacionada, adicione as funções que cada membro deste grupo recebe.
   Por exemplo, se você estiver criando um grupo para Resposta a incidentes de segurança membros da equipe, adicione sn_si.analyst. Se você estiver criando um grupo para Resposta a incidentes de segurança administradores, adicione sn_si.admin.
7. Em **Membros do grupo** lista relacionada, adicione usuários a este grupo.
8. Clique em **Atualizar**.

Crie um grupo de calculadora de incidentes de segurança

Os grupos de calculadoras de incidentes de segurança são usados para agrupar calculadoras.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidentes de segurança.
Aplicação	A aplicação que contém este registro.
Ordem	A ordem na qual a calculadora de incidentes de segurança é executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Descrição	Uma descrição deste grupo de calculadoras.
Criada por	Insira o nome do usuário que criou

4. Clique em **Enviar**.

Crie uma calculadora de incidentes de segurança

As calculadoras de incidentes de segurança permitem calcular a gravidade de um incidente de segurança com base em fórmulas predefinidas. Você pode definir suas próprias calculadoras de incidentes de segurança, conforme necessário.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Ou clique no nome do grupo para o qual você deseja criar uma calculadora, ou você pode crie um grupo de calculadoras .
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidentes de segurança.
Grupo de Calculadoras	Nome do grupo ao qual esta calculadora pertence. **Nota:** Criar ou alterar o grupo de calculadora se torna disponível depois que você insere um **Nome** e. **Tabela** .
Tabela	Selecione a tabela a ser usada para esta calculadora. Ao adicionar calculadoras a tabelas diferentes de Vulnerabilidade [sn_vul_vulnerability] e Item vulnerável [sn_vul_vulnerable_item], você deve adicionar regras de negócio e ações de IU a essas tabelas. Para ver exemplos: ○ Navegar até **Definição do Sistema** > **Regras de negócio**e localize **Calcule a gravidade** Regra de negócio na tabela Item vulnerável [sn_vul_vulnerable_item]. ○ Navegar até **IU do Sistema** > **Ações de IU**e localize **Calcule a gravidade** Ação de IU na tabela Item vulnerável [sn_vul_vulnerable_item]. Além disso, a função de administrador de vulnerabilidade deve receber recursos completos de leitura, gravação (ou save_as_template) em qualquer tabela usada por uma calculadora para ver corretamente os valores a serem aplicados ao modelo.
Aplicação	A aplicação com escopo à qual a calculadora pertence.
Ordem	A ordem em que a calculadora de incidentes de segurança é executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Ativo	Ligar ou desligar a calculadora.
Descrição	Uma descrição desta calculadora.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
. **Condições** e. **Valores a serem aplicados** as guias são exibidas.
6. Preencha os campos em **Condições** , conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou crie um novo grupo de filtros para definir os critérios da calculadora.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir uma calculadora. Este campo aparecerá somente se você selecionou **Usar grupos de filtros** caixa de seleção.
Usar a condição avançada	Marque esta caixa de seleção para indicar que uma condição de script é usada para determinar quando esta calculadora é aplicada. Quando você marca a caixa de seleção, um **Condição avançada** o campo de script é exibido. Se você selecionou **Usar grupo de filtros** caixa de seleção, este campo está oculto. **Nota:** Antes de definir condições avançadas e gravar scripts para determinar quando as calculadoras de incidentes de segurança são aplicadas, retorne à lista Calculadoras de incidentes de segurança. Explore os registros da calculadora enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora é usada. Se você selecionou um dos **Usar grupo de filtros** ou **Use condições avançadas** este campo está oculto.

7. Clique em **Valores a serem aplicados** e preencha os campos no formulário, conforme apropriado. Você tem a opção de criar um script para definir os valores a serem aplicados ao cálculo ou definir um modelo com base nos campos na tabela selecionada.

Campo	Descrição
Usar valores de script	Marque esta caixa de seleção para definir valores de campo com um script.
Valores de Script	Define a quais valores os cálculos serão aplicados. Este campo aparecerá somente se você selecionou **Use valores de script** caixa de seleção.
Modelo	Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**. Selecione os campos e valores que você deseja usar para a calculadora.

8. Quando tiver concluído todas as entradas, clique em **Enviar** .

Noções básicas sobre calculadoras de incidentes de segurança

Calculadoras de incidentes de segurança são usadas para atualizar valores de registro quando as condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

. Resposta a incidentes de segurança o sistema de base inclui os seguintes grupos de calculadoras de incidentes de segurança e calculadoras. Em cada grupo, a primeira calculadora que corresponde às condições será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidentes de segurança	Calculadoras incluídas no grupo	Descrição
Impacto nos negócios	Agregar de calculadoras de gravidade	Esta calculadora delega à Calculadora de criticidade de segurança que determina a criticidade ponderando os valores de outros campos.
Gravidade	Negócios impactados	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples.
	Serviço crítico afetado	Esta calculadora de severidade define seus critérios de seleção usando uma condição avançada. . Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios altamente crítico, o. **Pontuação de risco** , **Impacto nos negócios** e **Prioridade** os campos são elevados conforme definido pela calculadora.
	Mudanças em serviço crítico	Esta calculadora de severidade define seus critérios de seleção usando uma condição avançada. Se o incidente de segurança atender às condições, um script será executado para definir para quais níveis os campos serão elevados. . Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios mais crítico ou um pouco crítico, o. **Pontuação de risco** , **Impacto nos negócios** e **Prioridade** os campos são elevados conforme definido pela calculadora.
	Vetores de vários ataques	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples. Se o item de configuração no incidente de segurança estiver associado a vetores de ataque da Web, e-mail e representação, o. **Pontuação de risco** , **Impacto nos negócios** e **Prioridade** os campos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidentes de segurança	Calculadoras incluídas no grupo	Descrição
		são elevados conforme definido pela calculadora.
	Definir prioridade com categoria e serviços	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condições avançado. A prioridade do incidente de segurança está definida como **1 - Crítico** quando as seguintes condições são atendidas: • O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso **Nota:** Esta calculadora está disponível no sistema de base quando você tem o nível de preço de Operação de segurança inicial.
	Definir prioridade com observáveis	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condições avançado. A prioridade do incidente de segurança está definida como **1 - Crítico** quando as seguintes condições são atendidas: • O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso • Um dos observáveis ou indicadores associados tem uma contagem de avistamentos que excede dois avistamentos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidentes de segurança	Calculadoras incluídas no grupo	Descrição
		com indicadores ativos (ou seja, os observáveis ou indicadores são confirmados como ruins de várias fontes). **Nota:** Esta calculadora está disponível no sistema de base quando você tem o nível de preço Advanced Security Operation e ativa o plug-in Threat Feeds.
Criticidade do usuário	Obter criticidade do usuário	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples. Esta calculadora de gravidade faz com que a criticalidade comercial do usuário mude para **1 - Crítico** . **Departamento** o campo foi alterado para **Finanças** .
	Obter criticidade do grupo de usuários	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condições avançado. Esta calculadora de gravidade fornece um exemplo de uma calculadora que é executada em dados em uma lista relacionada.

Calculadoras de gravidade

Ao criar um incidente de segurança, o **Pontuação de risco** , **Impacto nos negócios** e **Prioridade** os campos contêm valores padrão. Quando você salva o incidente, uma regra de negócios valida automaticamente as informações no incidente de segurança em relação às condições definidas em cada uma das calculadoras de gravidade ativas. Eles são validados uma calculadora de segurança por vez, na ordem definida pelo **Pedido** em cada calculadora. Se as informações no incidente de segurança corresponderem às condições definidas em uma das calculadoras, os valores do campo Severidade serão atualizados de acordo com as regras configuradas na calculadora.

Por exemplo, suponha que você crie um incidente de segurança para um IC afetado e o IC seja altamente crítico. Quando o incidente de segurança é salvo, as informações do IC são comparadas com as condições definidas nas calculadoras de gravidade. Quando o incidente de segurança é validado em relação a. **Serviço crítico afetado** calculadora de gravidade, os campos de gravidade são atualizados automaticamente e uma mensagem semelhante à seguinte aparece na parte superior do incidente de segurança.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar essas calculadoras de gravidade como estão ou editá-las para atender melhor às necessidades do seu negócio. Por exemplo, se você quiser identificar ameaças da Web e de e-mail específicas da unidade de negócios Finanças, poderá mudar as condições do **Vários vetores de ataque** calculadora:

- [Vetor de ataque] [Contém] [Web]
- [Vetor de ataque] [Contém] [E-mail]
- [Unidade de negócios] [Contém] [Finanças]

Você também pode atualizar os valores de gravidade em um incidente de segurança existente a qualquer momento abrindo o registro e clicando em **Calcule a gravidade** link relacionado.

Calculadoras de pontuação de risco de incidente de segurança

. **Defina prioridade com categoria e serviços** e. **Definir prioridade com observáveis** calculadoras são usadas para calcular uma pontuação de risco para um incidente de segurança.

Calculadoras de criticalidade do usuário

As duas calculadoras no **Criticidade do usuário** grupo (**Obter criticidade do usuário** e. **Obter criticidade do grupo de usuários** forneça exemplos de como você pode orientar a criticidade com base em critérios definidos em um registro de usuário ou com base no grupo ao qual um usuário pertence.

Eles podem ser editados conforme necessário ou novas calculadoras de criticidade do usuário podem ser criadas.

. **Obter criticidade do usuário** a calculadora faz com que a criticalidade comercial do usuário mude para **1 - Crítico** . **Departamento** o campo foi alterado para **Finanças** .

. **Obter criticidade do grupo de usuários** a calculadora faz com que a criticalidade comercial do usuário mude para **1 - Crítico** quando o usuário é adicionado ao **Banco de dados** grupo.

Nota: **Obter criticidade do grupo de usuários** é um exemplo de uma calculadora executada em dados em uma lista relacionada. Se você quiser adicionar mais grupos para iniciar uma mudança de criticidade, adicione uma lista separada por vírgulas de sys_ids do grupo na primeira linha do script. Exemplo: `Var CRITICAL_GROUPS: [Group1_sys_id, group2_sys_id, group3_sys_id]` .

Cálculos de pontuação de risco de incidente de segurança

A pontuação de risco é calculada como uma média aritmética que representa o risco com base na prioridade de um incidente de segurança, no tipo de incidente de segurança (negação de serviço, spear Phishing ou atividade de código mal-intencionado) e no número de origens que acionaram uma pontuação de reputação com falha em um indicador.

A pontuação de risco ajuda a priorizar o trabalho de incidentes de segurança para os analistas.

Importante: Se você quiser usar a nova Calculadora de pontuação de risco, consulte Defina as novas regras da calculadora de pontuação de risco.

. **Defina prioridade com categoria e serviços** e. **Definir prioridade com observáveis** calculadoras de incidentes de segurança são usados para calcular uma pontuação de risco para um incidente de segurança. Além disso, as seguintes regras de negócios acionam o cálculo automático de pontuações de risco:

Tradução automática

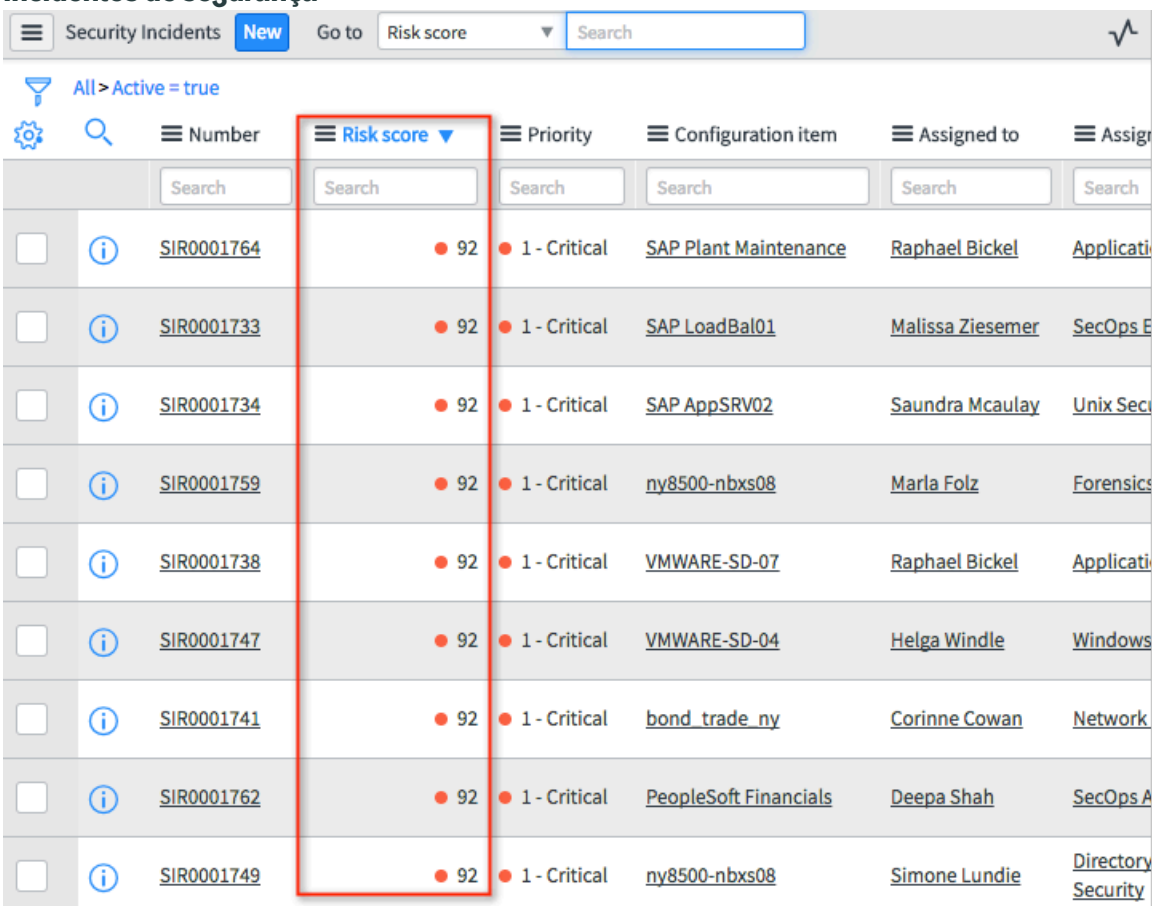
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Calcular Gravidade
- Atualizar pontuação de risco
- Atualizar pontuação de risco de SI

Nota: A calculadora de risco disponível no sistema de base depende do nível de preço de Operações de segurança.

Ao observar uma lista de incidentes de segurança no sistema de base, observe **Pontuação de risco** coluna.

Incidentes de segurança

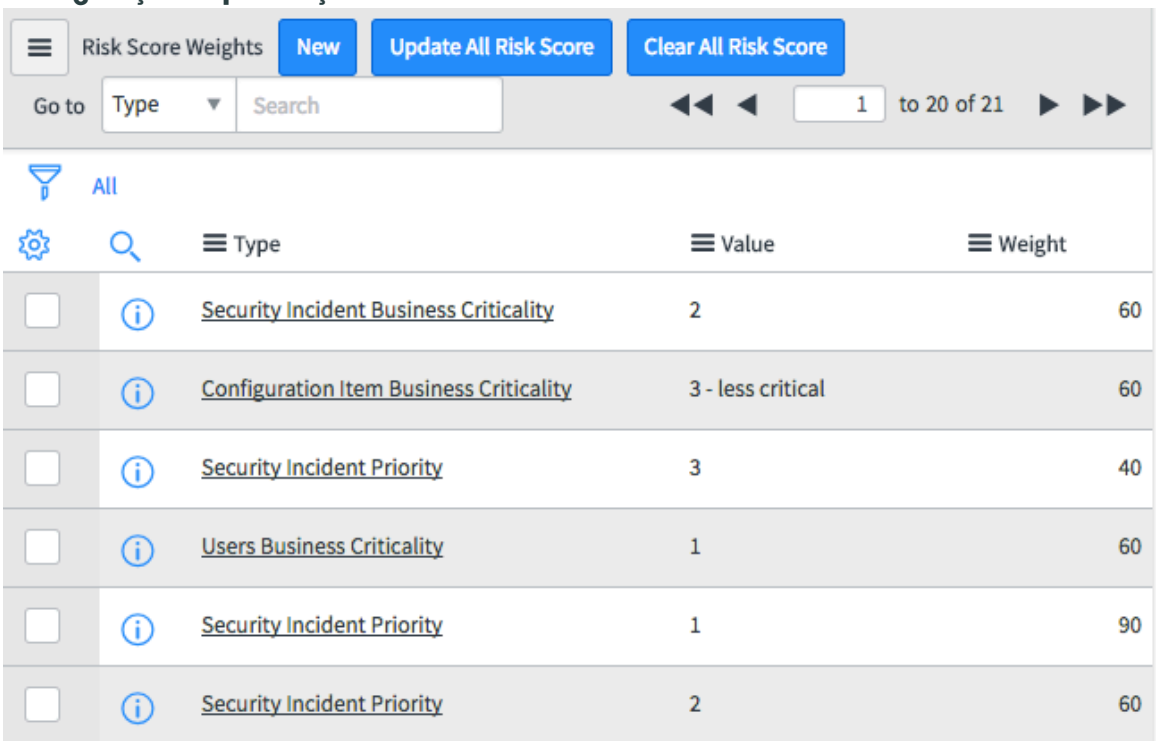


A pontuação de risco é calculada usando pesos definidos em **Configuração da pontuação de risco** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de pontuação de risco



Por exemplo, se um incidente de segurança tiver um **Impacto nos negócios** definido como **2-Alto** e um **Prioridade** definido como **3-Moderado** , Os respectivos pesos na tabela Ponderações da pontuação de risco são pesquisados e calculados da seguinte forma:

Incidente de segurança nos negócios com um valor de 2 é um peso de 60.

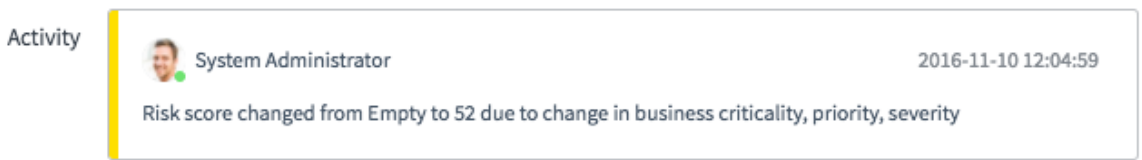
Prioridade do incidente de segurança com um valor de 3 é um peso de 40.

(60 e 40)/2 é uma pontuação de risco de 50.

A posição do incidente de segurança na lista de incidentes de segurança é reordenada com base em sua pontuação de risco atualizada.

Se, no exemplo acima, o **Impacto nos negócios** ou **Prioridade** do incidente de segurança são alterados, a pontuação de risco é recalculada e as mudanças são refletidas nas anotações de trabalho.

Anotações de trabalho



As anotações de trabalho são atualizadas quando os seguintes campos são alterados (fazendo com que a pontuação de risco seja atualizada):

- **Impacto nos negócios** No formulário Incidente de segurança
- **Prioridade** No formulário Incidente de segurança
- **Gravidade** No formulário Incidente de segurança (oculto por padrão)
- **Impacto nos negócios** em **Usuários afetados** lista relacionada

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Impacto nos negócios** em **Serviços afetados** lista relacionada
- **Impacto nos negócios** em vulnerabilidades no **Itens vulneráveis** lista relacionada

Além disso, as anotações de trabalho são atualizadas nas seguintes situações:

- Quando uma associação entre usuários afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre serviços afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre itens vulneráveis e um incidente de segurança é criada ou modificada

As anotações de trabalho também são atualizadas sempre que **Atualize todas as pontuações de risco** e. **Limpar todas as pontuações de risco** em Pesos da pontuação de risco formulário clicado.

Manter pesos de pontuação de risco

Os pesos de pontuação de risco usados para calcular pontuações de risco em incidentes de segurança podem ser removidos ou atualizados individualmente. Eles também podem ser removidos ou atualizados para todos os incidentes de segurança. A capacidade de removê-los de incidentes de segurança é útil ao alterar valores de ponderação.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Nota: Usuários com a função sn_si.read podem exibir a configuração da pontuação de risco em Resposta a incidentes de segurança.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Configuração** > **Configuração da pontuação de risco**.

   Nota: Usuários com a função sn_si.read podem exibir a configuração da pontuação de risco navegando até **Incidente de segurança** > **Alertas e eventos** > **Configuração de pontuação de risco**.

2. Para adicionar um novo peso de pontuação de risco, clique em **Novo** e insira informações nos campos.

Campo	Descrição
Tipo	Selecione o tipo de pontuação de risco que você está definindo.
Valor	Especifique o valor associado ao tipo selecionado. Se vários valores estiverem disponíveis para o tipo, convém definir vários registros de peso de pontuação de risco. Exemplo: Prioridade de incidente de segurança com um valor de 1, Prioridade de incidente de segurança com um valor de 2 e assim por diante.
Peso	O peso associado ao par de tipo/valor selecionado. As entradas válidas estão entre 0 e 100, sendo 0 o peso mais baixo e 100 o mais alto.

3. Clique em **Enviar**.
4. Execute qualquer uma dessas etapas, conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para limpar um registro de peso de pontuação de risco, abra-o na lista e clique em **Excluir** .
- Para limpar todos os registros de peso da pontuação de risco, clique em **Limpar todas as pontuações de risco** .
- Para atualizar todos os registros de peso da pontuação de risco, clique em **Atualize todas as pontuações de risco** .

Crie um Resposta a incidentes de segurança ANS

Você pode definir um Acordo de nível de serviço (ANS) para Resposta a incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Configuração** > **ANS**.
2. Clique em **Nova**.
   Para obter descrições de campos e instruções detalhadas, consulte Criação de uma definição do ANS .

Repare ANS de incidentes de segurança

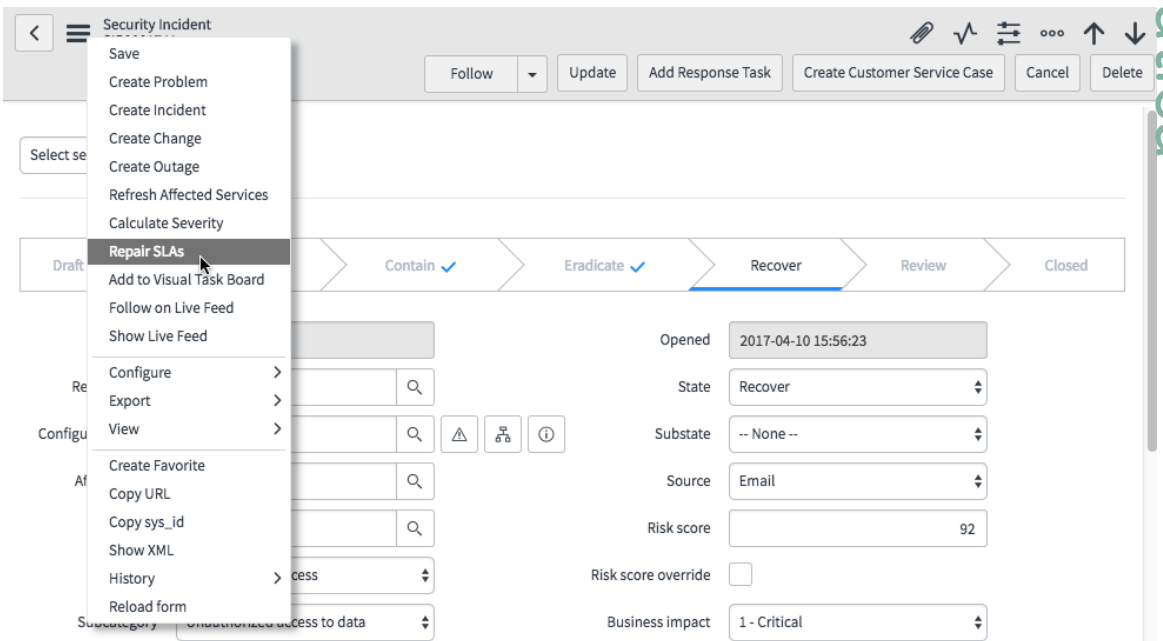
Você pode reparar registros de ANS para garantir que as informações de tempo e duração do ANS sejam precisas.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança para o qual você deseja reparar os SLAs.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Repare ANS** :



3. Clique em **OK** Na caixa Confirmação de aviso.
   Para obter mais informações, consulte Repare ANS .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um runbook de resposta a incidentes de segurança

Um runbook é uma associação entre um artigo de conhecimento publicado e uma tarefa específica. Enquanto você executa a tarefa, um artigo de conhecimento no runbook é aberto automaticamente, fornecendo informações pertinentes à tarefa.

Antes de Iniciar

Deve haver artigos de conhecimento existentes no Resposta a incidentes de segurança Base de conhecimento do runbook. Quando você crie um artigo de conhecimento de incidente de segurança certifique-se de selecionar **Runbook de resposta do incidente de segurança** em **Base de conhecimento** campo. Depois de publicar o artigo, você pode clicar em **Criar runbook** botão.

Função necessária: sn.si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar runbooks durante os processos de criação de incidente de segurança ou tarefa de resposta ou associar os artigos da base de conhecimento em um runbook a tarefas no playbook.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Runbook manual** > **Criar novo runbook**.
2. Preencha os campos, se for o caso.

Campo	Descrição
Artigo de conhecimento	Selecione um artigo de conhecimento para incluir no runbook.
Ativo	Marque a caixa para disponibilizar o runbook no **Navegador de filtros** .
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou crie um novo grupo de filtros para definir os critérios do runbook.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir um runbook. Este campo aparecerá somente se **Usar grupos de filtros** a caixa de seleção está marcada.
Tabela	Selecione Incidente de segurança [sn_si_incident] ou Resposta a incidentes de segurança Tarefa [sn_si_task]. Se você selecionou **Usar grupo de filtros** e selecionado um grupo de filtros, este campo assume como padrão a tabela associada ao grupo de filtros selecionado.
Condição	Defina as condições que conectam este runbook ao incidente ou tarefa. Se você selecionou **Usar grupo de filtros** e selecionou um grupo de filtros, o. **Condição** os campos não são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A guia Detalhes do artigo de conhecimento e uma série de botões são exibidos.
4. Para exibir os detalhes do runbook, clique em **Detalhes da base de conhecimento** guia.
5. Para ver o artigo de conhecimento como ele apareceria para o usuário, clique em **Exibir artigo** .
6. Para edite os detalhes do artigo de conhecimento clique em **Editar artigo** .

Crie regras para validar ataques de phishing relatados pelo usuário

Quando seus funcionários recebem e-mails que parecem ser ataques de phishing, eles podem denunciá-los a você usando um endereço de e-mail de phishing. O e-mail suspeito é validado usando regras definidas pela sua organização.

Antes de Iniciar

Antes que as regras de correspondência de e-mail possam ser usadas para identificar possíveis ataques de phishing, defina um endereço de e-mail para o qual os e-mails encaminhados de seus funcionários serão enviados para processamento. Você tem as seguintes opções para definir este endereço de e-mail (supondo que o domínio de e-mail da sua empresa seja acme.com):

- Defina um endereço de e-mail, como **e phishing@service-now.com** . . **phishing** O marcador é compatível com SMTP para habilitar a filtragem e sua instância pode receber e-mails enviados para ele.
- Defina um endereço de e-mail, como **phishing@acme.com** (Sua caixa de correio do Exchange), que, por sua vez, a encaminha para **e phishing@service-now.com** (sua caixa de correio da instância definida por meio de uma regra de encaminhamento de e-mail).

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Quando um funcionário encontra um e-mail suspeito, ele deve encaminhá-lo como um anexo para o seu endereço de e-mail de phishing. Se o e-mail anexado corresponder a uma regra que define uma ameaça, um incidente de segurança será criado.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Processamento de E-mails** > **Phishing relatado pelo usuário**.
2. Clique em **Nova**.
3. Preencha os campos, conforme necessário.

Formulário Regras de correspondência de e-mail

Campo	Descrição
Nome	Nome desta regra de correspondência de e-mail. Por exemplo, Usuário relatado como phishing.
Condições	Use o construtor de condições validar se um e-mail enviado para o endereço de e-mail de phishing da sua empresa é um ataque de phishing. Veja o exemplo a seguir.

4. Clique em **Enviar**.

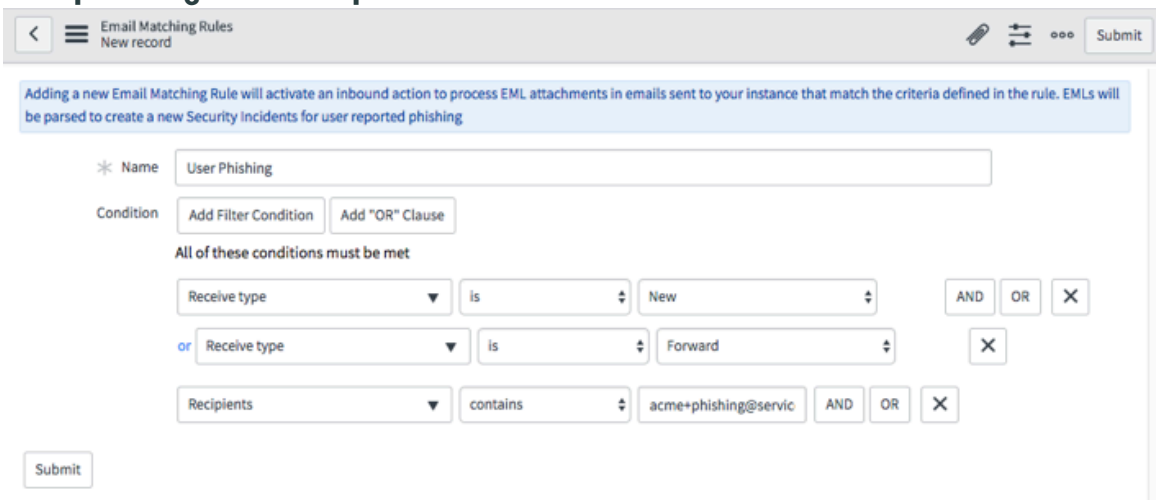
Example:

Este exemplo mostra uma regra correspondente para lidar com phishing relatado pelo usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de regra de correspondência de e-mail



Configure o Espaço do analista de segurança

Configure a interface do usuário do registro de incidente no Espaço do analista de segurança para especificar os campos que você deseja exibir.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Especifique os campos a serem exibidos no registro de incidente e a ordem em que os campos devem aparecer no formulário Incidente de segurança e no formulário Tarefa de resposta. Você também pode definir um limite no número de campos que deseja exibir.

Nota: Você pode criar regras para determinar qual exibição deve ser usada para um formulário específico. Várias exibições estão incluídas com o sistema de base, incluindo as exibições Padrão e Nova IU DO SIR. Várias regras de exibição também são enviadas com o sistema de base, incluindo a regra Tarefa de resposta Todos os outros. Esta regra impõe a exibição padrão no formulário Tarefa de resposta quando a condição especificada na regra de exibição é atendida. . Espaço do analista de segurança Usa a nova exibição de IU do SIR. Se os campos de formulário forem exibidos no Espaço do analista de segurança não corresponda aos campos de formulário no ambiente clássico, uma regra de exibição provavelmente é imposta. Para usar o. **Nova IU DO SIR** exibição para o formulário, você deve desabilitar a regra de exibição. Consulte Controla quando o sistema exibe uma exibição para obter detalhes.

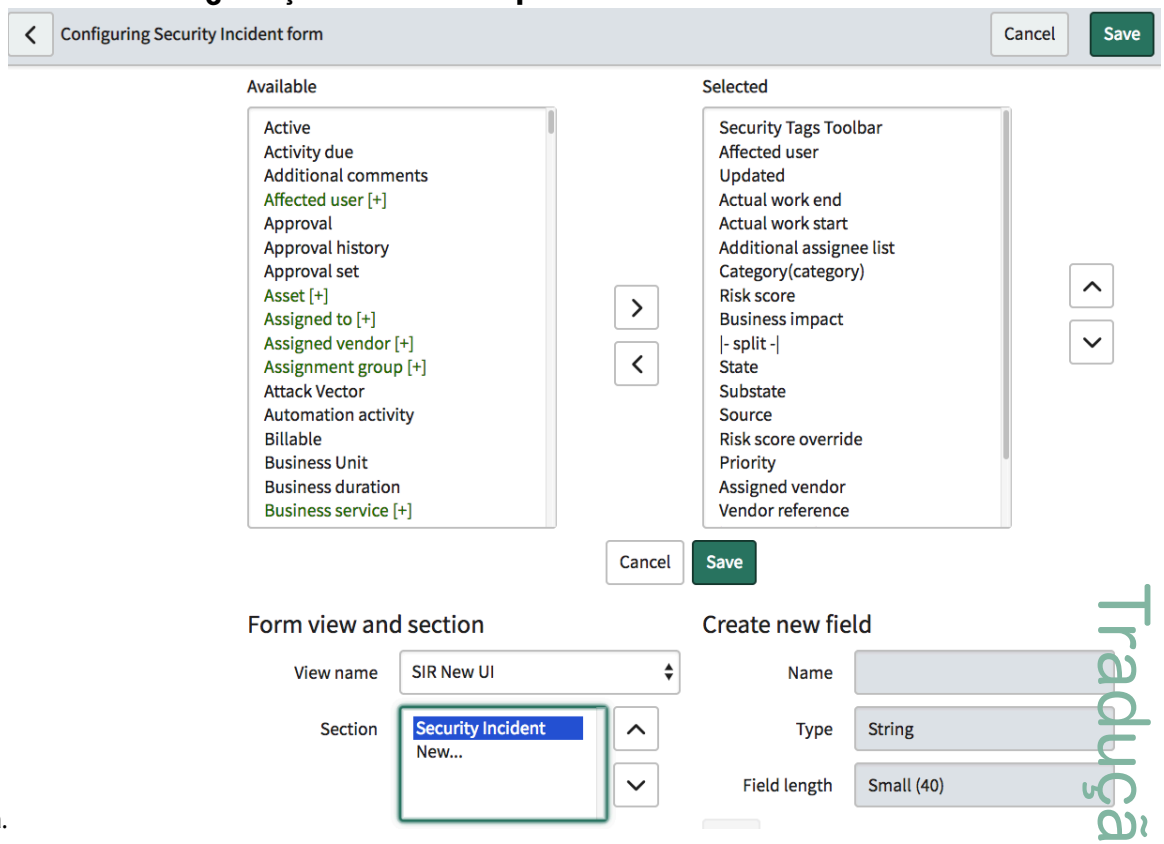
Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**).
2. Para abrir o registro de incidente de segurança, clique em um link de incidente de segurança.
3. Para navegar até a página do formulário Configuração de incidente de segurança, clique em ícone de menu e selecione **Configurar** > **Layout do formulário**.
4. Em **Nome da exibição** , selecione **Nova IU DO SIR** .
5. Em **Seção** selecione a seção apropriada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isso pode ser **Incidente de segurança** ou **Tarefa de resposta do incidente de segurança**.



6. Selecione os campos e a ordem em que você deseja que eles apareçam na faixa Incidente na nova IU.
7. Clique em **Salvar**.

Nota:

- Determinados campos estão ocultos por padrão nas faixas Incidente e Tarefa de resposta. Altere os campos que estão ocultos ou exibidos modificando o. `sn_app_secops_ui.form.excluded_fields.incident` e. `sn_app_secops_ui.form.excluded_fields.response_task` propriedades conforme descrito em Propriedades do Espaço do analista de segurança.
- Especifique o número de campos que podem ser exibidos nas faixas Incidente e Tarefa de resposta e na primeira linha da faixa Incidente definindo estas propriedades:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

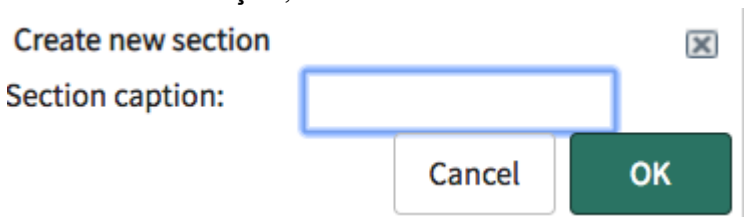
8. Para configurar os estilos dos círculos pontilhados que aparecem ao lado de um valor de campo no registro de incidente, por exemplo, navegue até **IU do Sistema** > **Estilos de Campo** e modificam ou criam um novo registro de estilo para a tabela específica e o nome do campo.
   A propriedade background-color no campo Estilo do registro de estilo determina a cor do círculo pontilhado.
9. Para exibir a faixa de incidente atualizada, clique em **Incidentes de segurança** > **Incidentes (Nova IU)** Para navegar até o registro de incidente no Espaço do analista de segurança E atualize a página para exibir a faixa do incidente atualizada.
10. Para configurar a faixa Tarefa de resposta no registro de incidente, navegue até **Incidentes de segurança** > **Tarefas de resposta** > **Mostrar todas as tarefas** e repita as etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Se você estiver criando uma nova tabela de tarefas que se estende da tabela Tarefa de resposta de incidente de segurança de base, você também deverá adicionar a nova exibição de IU DO SIR à tabela.

    a. Em **Nome da exibição** , selecione **Novo** .



    b. Insira **Nova IU DO SIR** (Diferencia maiúsculas de minúsculas) na janela Criar nova exibição e clique em **OK** .

Resultado

O incidente de segurança e os banners de tarefa de resposta são atualizados em Espaço do analista de segurança(Gerencie ameaças à segurança usando Espaço do analista de segurança).

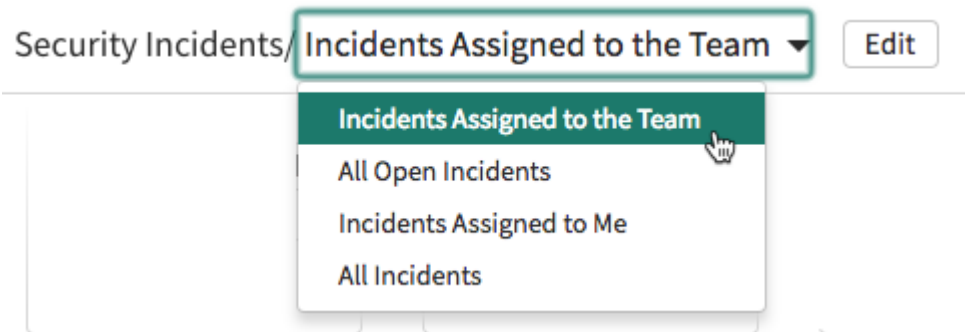
Configurar filtros primário e secundário para Espaço do analista de segurança

. Espaço do analista de segurança o sistema de base inclui um conjunto de filtros primários para restringir a lista de incidentes de segurança para análise (para incidentes de segurança atribuídos a você, todos os incidentes em aberto e assim por diante) e um conjunto de filtros rápidos (ou secundários) para restringir ainda mais a lista (por novos incidentes, incidentes em aberto, somente incidentes críticos e assim por diante).

Antes de Iniciar

Você pode usar o ambiente Clássico para definir filtros primários e secundários adicionais.

Como você define filtros a serem usados no Espaço do analista de segurança, você pode atribuir marcadores para indicar se eles podem ser usados como filtros primários ou secundários. Os filtros primários são mostrados na parte superior da lista de incidentes de segurança.



Clique em **Editar** Ao lado da opção Filtros rápidos para selecionar filtros secundários (ou rápidos).



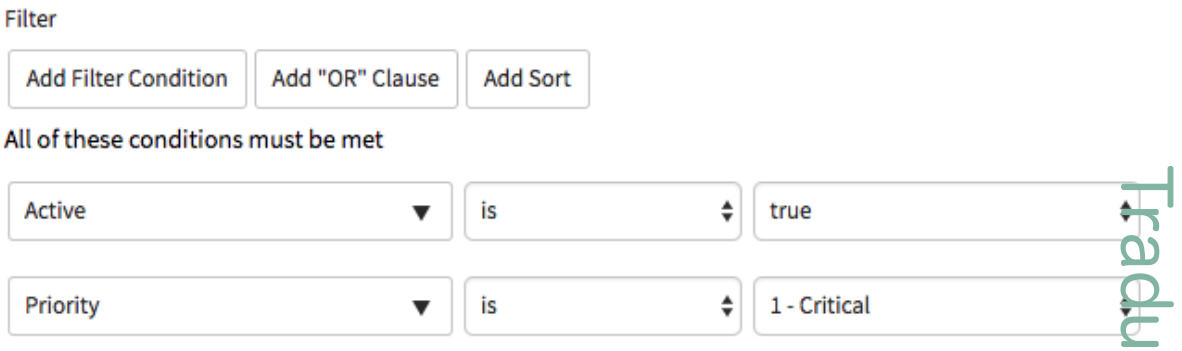
Função necessária: admin ou sn_sec_cmn.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Definição do Sistema** > **Filtros**.
2. Clique em **Novo** e conclua as etapas a seguir.
   a. Insira um **Título** .
   b. Selecione **Incidente de segurança [sn_si_incident]** em **Tabela** lista de seleção.
   c. Adicione suas condições de filtro.
   Por exemplo, o. **Incidentes em aberto com Prioridade Crítica** usa estas condições.



   d. Clique em **Enviar**.
3. . **Marcadores** a coluna não está visível na lista de filtros, clique no ícone de engrenagem e personalize a exibição para adicioná-la.
4. Localize o filtro que você criou e adicione um dos seguintes marcadores para indicar como o filtro deve aparecer no Espaço do analista de segurança.
   - **SN_SI_PRIMARY** : Se este marcador for selecionado, o filtro poderá ser selecionado na caixa de listagem de filtro primário em Espaço do analista de segurança.
   - **SN_SI_PRIMARY_OOB** : Se este marcador for selecionado, o filtro aparecerá em **Selecionado** lado da caixa de listagem do filtro primário por padrão.
   - **SN_SI_Secondary** : Se este marcador for selecionado, o filtro poderá ser selecionado na caixa de listagem de filtro secundário (rápido).
   - **SN_SI_SECONDARY_OOB** : Se este marcador for selecionado, o filtro aparecerá em **Selecionado** lado da caixa de listagem do filtro primário por padrão.

Tópicos relacionados

Criar e editar filtros

Propriedades do Espaço do analista de segurança

Essas propriedades do sistema são usadas para configurar o Espaço do analista de segurança.

Existem dois tipos de propriedades:

- Propriedades que normalmente não são modificadas, como sys_ids e chaves de produto.
- Propriedades modificadas conforme necessário, como intervalos de pesquisa longos e configurações da interface do usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As propriedades do Espaço do analista de segurança estão localizadas neste local: **Incidente de segurança** > **Configuração do Espaço do analista** > **Propriedades do Espaço do analista**.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
Campos ocultos por padrão na faixa da tarefa de resposta. sn_app_secops_ui.form.excluded_fields.response_task	• **Tipo**: cadeia de caracteres • **Valor padrão** : ◦ número ◦ Descrição resumida ◦ comentários ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity
Campos ocultos por padrão na faixa do incidente. sn_app_secops_ui.form.excluded_fields.incident	• **Tipo**: cadeia de caracteres • **Valor padrão** : ◦ número ◦ Descrição resumida ◦ comentários ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity ◦ security_tags
O estilo de cor de fundo é aplicado aos campos listados aqui. sn_app_secops_ui.form.color_coded_fields	• **Tipo**: cadeia de caracteres • **Valor padrão** : ◦ criticidade dos negócios ◦ impacto ◦ prioridade ◦ risk_score ◦ severidade
Se verdadeiro, as tabelas estendidas da tabela de tarefa de resposta base sn_si_task também terão acesso aos	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
modelos de e-mail criados para a tabela de tarefa de resposta de base. sn_app_secops_ui.extend.base.response_task.email_templates	
Define a largura de cada campo de resumo em cada faixa de tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Tipo**: inteiro • **Valor padrão**: 10
Define a largura de cada campo de resumo em cada faixa de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Tipo**: inteiro • **Valor padrão** : 15
Define um limite no número de campos de resumo permitidos na faixa do incidente. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Tipo**: inteiro • **Valor padrão** : 12
Define um limite no número de campos de resumo permitidos na faixa da tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Tipo**: inteiro • **Valor padrão** : 12
Define um limite no número de campos de resumo permitidos na primeira linha da faixa do incidente. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Tipo**: inteiro • **Valor padrão**: 3
Lista separada por vírgulas de campos que podem ter fotos do usuário. sn_app_secops_ui.form.user_fields	• **Tipo**: cadeia de caracteres • **Valor padrão** : ◦ affected_user ◦ Solicitante ◦ sys_updated_by ◦ sys_created_by ◦ opened_by ◦ closed_by ◦ submited_by

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
Define a largura de cada campo de resumo em cada exibição de verificação de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Tipo**: inteiro • **Valor padrão** : 13,5
Lista separada por vírgulas de campos que exibem a hora. sn_app_secops_ui.form.time_fields	• **Tipo**: cadeia de caracteres • **Valor padrão** : ◦ opened_at ◦ sys_created_on ◦ sys_updated_on
Controla a frequência (em milissegundos) em que os resultados da pesquisa de vistas são atualizados. sn_app_secops_ui.poller_interval.search_action	• **Tipo**: inteiro • **Valor padrão** : 30000 **Mínimo** : 15000
Controla a frequência (em milissegundos) em que a contagem ou os dados de consulta são atualizados. sn_app_secops_ui.poller_interval.related_list	• **Tipo**: inteiro • **Valor padrão** : 30000 **Mínimo** : 15000
Controla a frequência (em milissegundos) em que os dados do resultado são atualizados (para o playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Tipo**: inteiro • **Valor padrão** : 30000 **Mínimo** : 15000
ID da integração de operações de segurança - Isolar fluxo de trabalho do host. sn_app_secops_ui.workflow.id.isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão** d72041f1ff203200c68c84648e94fa5e
ID da integração de operações de segurança - Fluxo de trabalho da lista de observação. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão** 35800c0eff343200c68c84648e94fa85
ID da integração de operações de segurança - Bloquear fluxo de trabalho de solicitação.	• **Tipo**: cadeia de caracteres • **Valor padrão** 11a6a5270b9032008f9108e3c5673a24

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
sn_app_secops_ui.workflow.id.block_request	
ID da função de usuário sn_si_analyst. sn_app_secops_ui.roles.id.sn_si.write	• **Tipo**: cadeia de caracteres • **Valor padrão** : 66878663ff123ff123100158bfffffffff8d
ID da função de usuário sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Tipo**: cadeia de caracteres • **Valor padrão** : ae878663ff123100158bfffffffff8e
ID da função de usuário sn_si_admin. sn_app_secops_ui.roles.id.sn_si.admin	• **Tipo**: cadeia de caracteres • **Valor padrão** 22878663ff123ff123100158bfffffffff8d
ID do Microsoft Exchange - Executar pesquisa de e-mail e fluxo de trabalho Excluir. sn_app_secops_ui.email.phishing.manual.workflow	• **Tipo**: cadeia de caracteres • **Valor padrão** : ed9f289cc310220031fbdccdf3d3aeb4
ID da ação personalizada Adicionar à lista de proibições na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Tipo**: cadeia de caracteres • **Valor padrão** : DENY_e9bd0ac50b632200263a089b37673a0b
ID da ação personalizada Adicionar à lista de permissões na guia Explorar no Espaço do analista de segurança sn_app_secops_ui.explore.action.direct.id.allow_list	• **Tipo**: cadeia de caracteres • **Valor padrão** ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
ID da ação de IU Executar pesquisa de ameaças. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão** : da5ff4420b540300263a089b37673ae7
ID do recurso de integração da Pesquisa de ameaças. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão** : 39344d4f0b273200263a089b37673ab1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da ação personalizada de aprimoramento de observável na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão** : Obs_ENRICHMENT_54e2f5d60b5003009f66e94685673a
ID da capacidade de integração do Observável Enrich. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão** : 9ad183640b1003009f66e94685673af4
ID da ação de IU Publicar na lista de observação. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão** 8ee94002ff743200c68c84648e94faf9
ID da ação de IU de solicitação de bloqueio. sn_app_secops_ui.explore.action.id.block_request	• **Tipo**: cadeia de caracteres • **Valor padrão** 7158f6e40b2032008f9108e3c5673adf
ID da ação de IU Executar pesquisa de vistas. sn_app_secops_ui.explore.action.id.sightings_search	• **Tipo**: cadeia de caracteres • **Valor padrão** : 43f91a6f0b032200b97c67d985673a2c
ID da ação de IU Criar incidente de segurança secundário. sn_app_secops_ui.explore.action.id.create_child_incident	• **Tipo**: cadeia de caracteres • **Valor padrão** 5a6882645363530099d5ddeeff7b1272
ID da ação de IU Adicionar anotação de segurança. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Tipo**: cadeia de caracteres • **Valor padrão** 1e3a3e723b5332005a9149a4d2efc4eb
ID da ação personalizada de aprimoramento de IC na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão** IC_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
ID da ação de IU Isolar do host. sn_app_secops_ui.explore.action.id.isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão** d6244e0af203200c68c84648e94fad3

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da ação de IU Adicionar vários observáveis. sn_app_secops_ui.explore.action.id.multiple_observable	• **Tipo**: cadeia de caracteres • **Valor padrão** : 138de478d78322007a6de294de6103aa
Chave do produto do ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Tipo**: cadeia de caracteres • **Valor padrão** ServiceNow_ServiceNow_5Devs2_August_2018__MTUzM

Configuração adicional do Espaço do analista de segurança

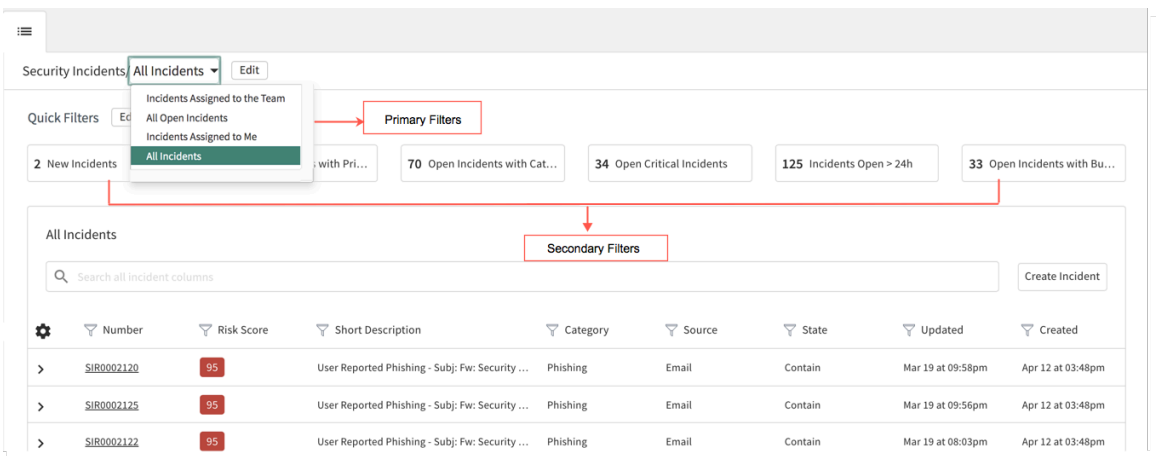
Configure o. Espaço do analista de segurança E definem filtros, ações de IU e listas relacionadas.

- Configuração do filtro da página principal
- Habilitar ações de IU
- Ações de IU do formulário
- Configuração da Lista relacionada
- Ações de IU da lista relacionada
- Propriedades do sistema de configuração de formulário
- Habilitar playbooks para seleção de analista

Configuração do filtro da página principal

Você pode adicionar novos filtros ou modificar filtros existentes que aparecem em Espaço do analista de segurança.

. Espaço do analista de segurança o tem filtros primários e secundários que permitem filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Para obter mais informações, consulte Gerencie ameaças à segurança usando Espaço do analista de segurança.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um novo filtro

1. Navegar até **Incidentes de segurança** > **Configuração do Espaço do analista (Nova IU)** > **Configuração do filtro da página principal**.
2. Clique em **Nova**.
3. Insira um título para o filtro, especifique a condição do filtro e clique em **Enviar** para retornar à página anterior.

   Você verá o filtro recém-adicionado listado na página.
4. Adicione um marcador para este filtro para indicar se este é um filtro primário ou secundário. Os seguintes marcadores estão disponíveis:
   - SN_SI_PRIMARY
   - SN_SI_Secondary

Edite filtros existentes

Você também pode fazer o seguinte:

- Modificar filtros existentes: Clique no Título de um filtro existente. Modifique o título e a condição do filtro e clique em **Atualização** .
- Modificar marcadores: Selecione um filtro e clique na coluna Marcador na Configuração do filtro da página principal. Você pode excluir o marcador existente ou adicionar um novo marcador para o filtro.

Habilitar ações de IU

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança.

Nota: Para modificar as ações de IU, faça login como um usuário com as seguintes funções:

- iu_action_admin
- iu_page_admin
- web_service_admin

Há dois tipos de ações de IU que podem ser configuradas para Espaço do analista de segurança:

- Ação de IU baseada em diálogo
- Ação de IU do lado do servidor

Ação de IU baseada em diálogo

Para habilitar ações de IU baseadas em diálogo no Espaço do analista de segurança, Faça as seguintes mudanças nas páginas de IU associadas às respectivas ações de IU padrão.

1. **Seção HTML** : Modifique a seção HTML para incluir o. `reagir` marcador de entrada. . `reagir` O valor do marcador de entrada é usado na seção de script do cliente para identificar se a Página de IU foi iniciada a partir do Espaço do analista de segurança. Um exemplo é mostrado abaixo:

```
<input id="react" name="react" type="hidden"
value="${JS,HTML:sysparm_react}" />
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Client script** Lógica adicional precisa ser gravada no client script quando `reagir` o sinalizador é verdadeiro. Isso é necessário para lidar com **Enviar** e. **Cancelar** eventos de botão mostrados como parte da janela de diálogo.
   a. O manipulador de eventos onCancel () precisa expedir o evento "SIR_WORKBENCH_POPUP_CANCEL" do Espaço do analista de segurança
   b. O manipulador de eventos onSubmit () precisa expedir o evento "SIR_WORKBENCH_POPUP_SUBMIT" do Espaço do analista de segurança
3. A execução do script de processamento é ignorada do Espaço do analista de segurança O contexto como a ação "onSubmit" foi modificado para retornar falso quando `reagir` o valor do marcador de entrada é verdadeiro. A lógica do script de processamento precisa ser manipulada por meio de um script chamável do cliente (invocado por meio da API GlideAjax) ou do endpoint do recurso REST.

Consulte as seguintes páginas de IU de amostra para obter mais detalhes:

- Exemplo de ação de IU da lista relacionada: Publicar na lista de observação (nome da página de IU: Publish_to_watchlist)
- Exemplo de ação de IU do formulário: Criar problema (nome da página de IU: Create_prb_change_inc)

Ação de IU do lado do servidor

Para habilitar ações de IU do lado do servidor, você deve fazer o seguinte:

A lógica do script de ação de IU padrão deve ser tratada como parte de um recurso REST com script.

Para obter mais detalhes, consulte os exemplos de ações de IU do formulário a seguir:

- Criar indisponibilidade
- Cancelar

Ações de IU do formulário

Você pode configurar as ações de IU que são exibidas no Espaço do analista de segurança.

Pré-requisitos:

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.

Para configurar uma ação de IU de formulário para Espaço do analista de segurança, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do Espaço do analista (Nova IU)** > **Ações de IU do formulário**.
2. Insira os seguintes detalhes:

Nome do Campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Isso pode ser:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
	○ Ação baseada em diálogo: Este tipo de ação é usado quando a interação do usuário ou as entradas são necessárias para executar a lógica de negócios específica. ○ Ação do lado do servidor: Esta ação executa a lógica de negócios necessária sem nenhuma entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.
Aplicação	O nome do escopo da aplicação (IU de resposta do incidente de segurança) no qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página da interface do usuário	Selecione a página de IU associada à ação.
Título da caixa de diálogo	Insira um título para a ação da caixa de diálogo.
Largura e altura da caixa de diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna `sysparm_sys_id` parâmetro somente. Você pode substituir isso especificando parâmetros diferentes aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, insira os seguintes detalhes:	
Recurso REST com script	Selecione o recurso REST de script que define a ação. **Nota:** . **ANALISTA DE IU DO SIR** A ACL deve ser adicionada ao recurso REST.

3. Clique em **Enviar**.
4. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
5. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Você pode ver a nova ação de IU na parte superior da página.

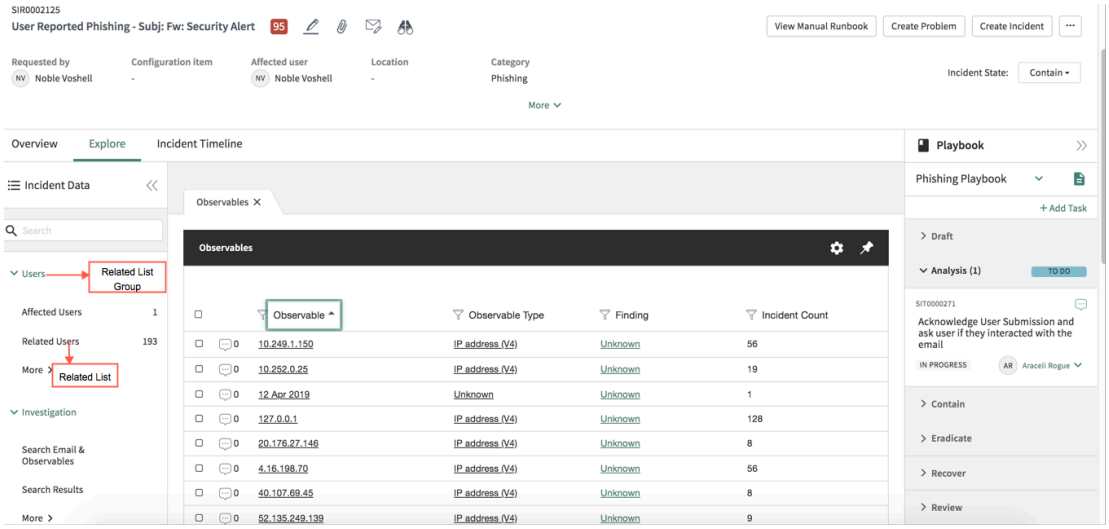
Para modificar uma ação de IU de formulário existente, clique no Nome da ação para navegar até a página Ações de IU de formulário. Você pode modificar o Nome da ação, o Tipo e o restante dos campos com base no tipo selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração da Lista relacionada

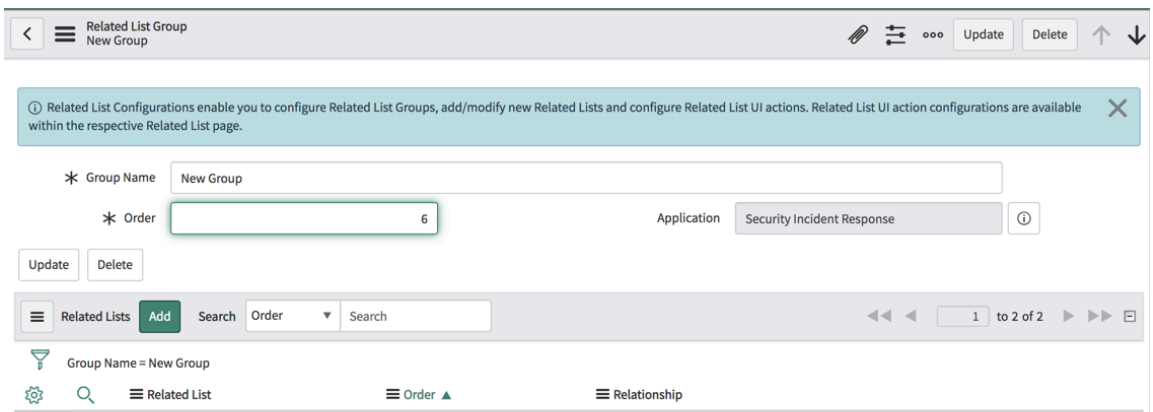
Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem em Espaço do analista de segurança.



Adicione um grupo de lista relacionada

Para adicionar um Grupo de listas relacionadas, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do Espaço do analista (Nova IU)** > **Configurações da lista relacionada**.
2. Clique em **Novo** Para adicionar um novo grupo de lista relacionada. Insira o Nome do grupo e a ordem em que ele deve aparecer na página Incidentes (Nova IU).
3. Clique em **Enviar**. O grupo recém-adicionado aparece na página Grupos de lista relacionada.



Adicione uma Lista relacionada

Para adicionar uma nova Lista relacionada, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Clique em um link Grupo de lista relacionada.
2. Na seção Listas relacionadas, clique em **Adicionar** para adicionar uma nova lista relacionada.

   Se você não vir **Adicionar** Botão, verifique se você está no mesmo escopo da aplicação que o Grupo de listas relacionadas.
3. Selecione a Lista relacionada a ser incluída no grupo.

   Nota: Se você não vir uma lista relacionada específica, faça o seguinte:

   a. Navegar até **IU do Sistema** > **Listas relacionadas** E pesquisam listas relacionadas presentes em `sn_si_incident` tabela.

   b. Clique em `sn_si_incident` tabela associada ao **Nova IU DO SIR** exibir.

   c. Na seção Entradas da lista relacionada, clique em **Novo** Para adicionar a Lista relacionada ao **Nova IU DO SIR** exibir.
4. Especifique a ordem em que ele deve aparecer e clique em **Enviar** .

   A Lista relacionada que você adicionou aparecerá em Espaço do analista de segurança.

Para modificar um grupo de lista relacionada existente, clique no Nome do grupo para navegar até a página Grupo de lista relacionada. Você pode modificar o Nome do grupo, o Pedido e adicionar ou excluir listas relacionadas do grupo.

Ações de IU da lista relacionada

Você pode adicionar novas ações de IU às listas relacionadas que aparecem em Espaço do analista de segurança.

Pré-requisitos:

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.

Para adicionar uma nova ação de IU da Lista relacionada, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do Espaço do analista (Nova IU)** > **Configurações da lista relacionada**.
2. Clique no Nome do grupo. A página de configuração do Grupo de listas relacionado é exibida.
3. Clique na Lista relacionada à qual você deseja adicionar uma ação de IU.
4. Clique em **Adicionar** Na seção Ações de IU da lista relacionada.
5. Insira os seguintes detalhes:

Nome do Campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Isso pode ser:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
	○ Ação baseada em diálogo: Este tipo de ação é usado quando a interação do usuário ou as entradas são necessárias para executar a lógica de negócios específica. ○ Ação do lado do servidor: Esta ação executa a lógica de negócios necessária sem nenhuma entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.
Aplicação	O nome do escopo da aplicação (IU de resposta do incidente de segurança) no qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página da interface do usuário	Selecione a página de IU associada à ação.
Título da caixa de diálogo	Insira um título para a ação da caixa de diálogo.
Largura e altura da caixa de diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna `sysparm_incident_id` , `sysparm_record_table` e `sysparm_related_sys_ids` parâmetros somente. Você pode substituí-los especificando parâmetros diferentes aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, especifique o seguinte:	
Recurso REST com script	Selecione o recurso REST de script que define a ação. **Nota:** . **ANALISTA DE IU DO SIR** A ACL deve ser adicionada ao recurso REST.

6. Clique em **Enviar**.
7. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
8. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Inicie a respectiva Lista relacionada para exibir a nova ação de IU.

Propriedades do sistema de configuração de formulário

Essas propriedades do sistema definem os intervalos de atualização do formulário para as tarefas do playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

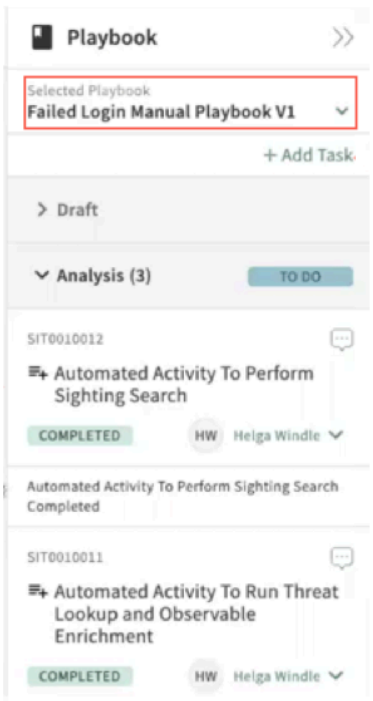
Para configurar essas propriedades, navegue até **Configuração do Espaço do analista (Nova IU)** > **Propriedades do Espaço do analista**.

Propriedade	Valor padrão	Descrição
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	O tempo de intervalo usado pelo componente do playbook para atualizar suas tarefas de resposta para cada tempo de intervalo configurado.
sn_app_secops_ui.poller_interval_count.playbook_tasks	9 vezes	O número de vezes que o componente do playbook pesquisa tarefas de resposta.
sn_app_secops_ui.poller_interval.related_lists	30000 ms	Este intervalo de tempo é usado pelo componente Explorar para atualizar suas contagens de lista relacionada para cada tempo de intervalo configurado.

Habilitar playbooks para seleção de analista

Adicione novos playbooks à lista de seleção de playbooks.

Você pode selecionar um playbook apropriado para investigar incidentes de segurança no Espaço do analista de segurança(Gerencie ameaças à segurança usando Espaço do analista de segurança). A opção de seleção de playbook oferece suporte somente aos playbooks projetados usando o Flow Designer.



Depois de criar um playbook usando o Flow Designer, siga estas etapas para incluí-lo na lista de seleção do Playbook selecionado:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegue até *sys_hub_flow* tabela.
2. PESQUISE o novo playbook que você criou usando o Flow Designer.
3. Adicione **sir_playbook** Marque os playbooks que você deseja incluir na lista de seleção do Playbook selecionado.

Nota: Se você tiver playbooks antigos que não foram migrados de fluxos de trabalho para o Flow Designer, eles não serão exibidos na lista. Mas, se um playbook criado usando fluxos de trabalho for atribuído a um incidente de segurança por uma condição de gatilho ou por seleção manual (usando **Executar Orquestração** no ambiente clássico), este playbook é iniciado quando você abre o incidente de segurança no Espaço do analista de segurança.

Solução de problemas de resposta a incidentes de segurança

Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas à Resposta a incidentes de segurança.

Problemas de regras de controle de acesso

As regras de controle de acesso permitem o acesso ao recurso especificado se todas as três condições a seguir forem atendidas:

- O usuário tem uma das funções especificadas em **Função** ou a lista está vazia.
- Condições no **Condição** o campo avaliar como verdadeiro ou as condições estão vazias.
- O script em **Script** o campo (avançado) é avaliado como verdadeiro ou define a variável **resposta** verdadeiro, ou está vazio.

Para obter mais informações sobre regras de controle de acesso, consulte Explorar listas de controle de acesso

Importante: . **Substituições do administrador** A opção está desmarcada para uma tabela de incidentes de segurança e, se o administrador puder acessar a tabela de incidentes de segurança, consulte KB1444673

Resposta a incidentes de segurança Soluções para Análise da plataforma e relatórios

As Soluções para Análise da plataforma e relatórios contêm painéis pré-configurados. Os painéis apresentam métricas importantes para analisar seu Resposta a incidentes de segurança processo, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Análise da plataforma uso de visualizações de dados Performance Analytics *indicador*dados para mostrar dados ao longo do tempo, ajudando você a analisar seus processos de negócios e identificar áreas de melhoria. Com o Soluções para Análise da plataforma e relatórios, você pode obter valor do Performance Analytics para seu aplicativo com o mínimo de configuração. Você sempre pode criar seus próprios objetos.

. Resposta a incidentes de segurança Performance Analytics A solução está disponível no ServiceNow Store. Para obter informações sobre como baixar e instalar este aplicativo, consulte Operações de segurança e ServiceNow Store .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para avaliar a funcionalidade, você pode ativar as soluções de Performance Analytics e a análise no formulário em instâncias que não tenham o Performance Analytics licenciado. No entanto, você tem as seguintes limitações:

- Você não pode criar novos indicadores.
- Você não pode coletar dados com mais de 180 dias.

Para obter a funcionalidade completa, licencie o Performance Analytics. Para obter mais informações, consulte Ativar assinatura da Análise de desempenho .

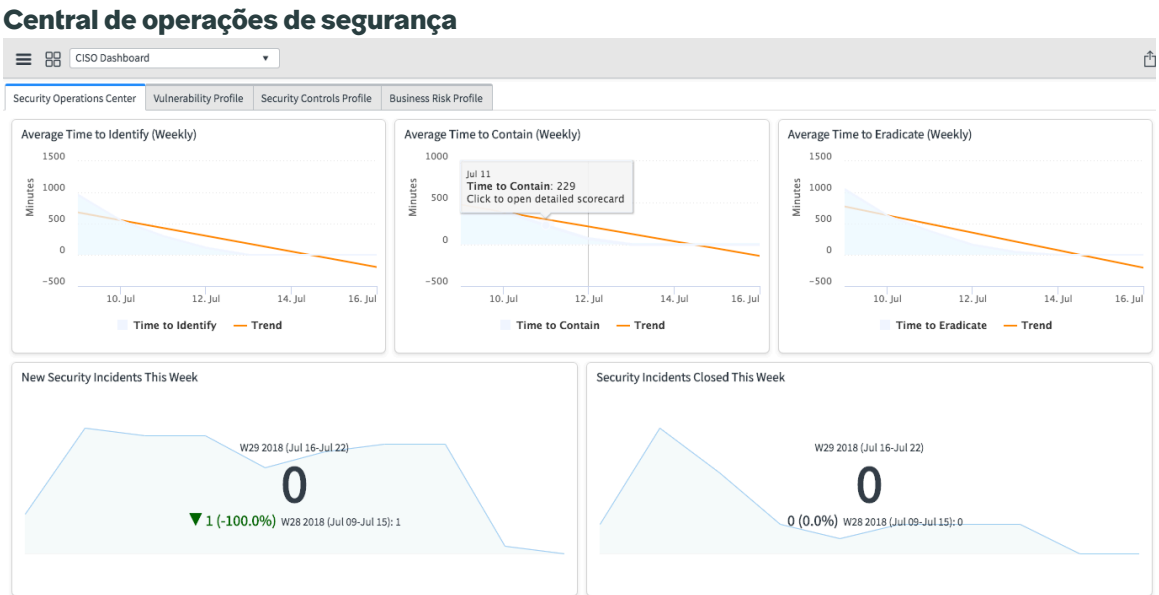
Importante: Por padrão, o limite de coleta de dados para *(com.snc.pa.dc.max_records)* A propriedade no Performance Analytics é definida como 5 000 registros. Mas você pode aumentar esse limite de acordo com seus requisitos, como 50 000 registros. No entanto, aumentar esse limite pode afetar o desempenho durante a coleta de dados ou ao executar operações na tabela Snapshot. Para saber mais sobre as propriedades do Performance Analytics, consulte Propriedades de Performance Analytics .

Tópicos relacionados

Ative sua assinatura do Performance Analytics

Painel do CISO

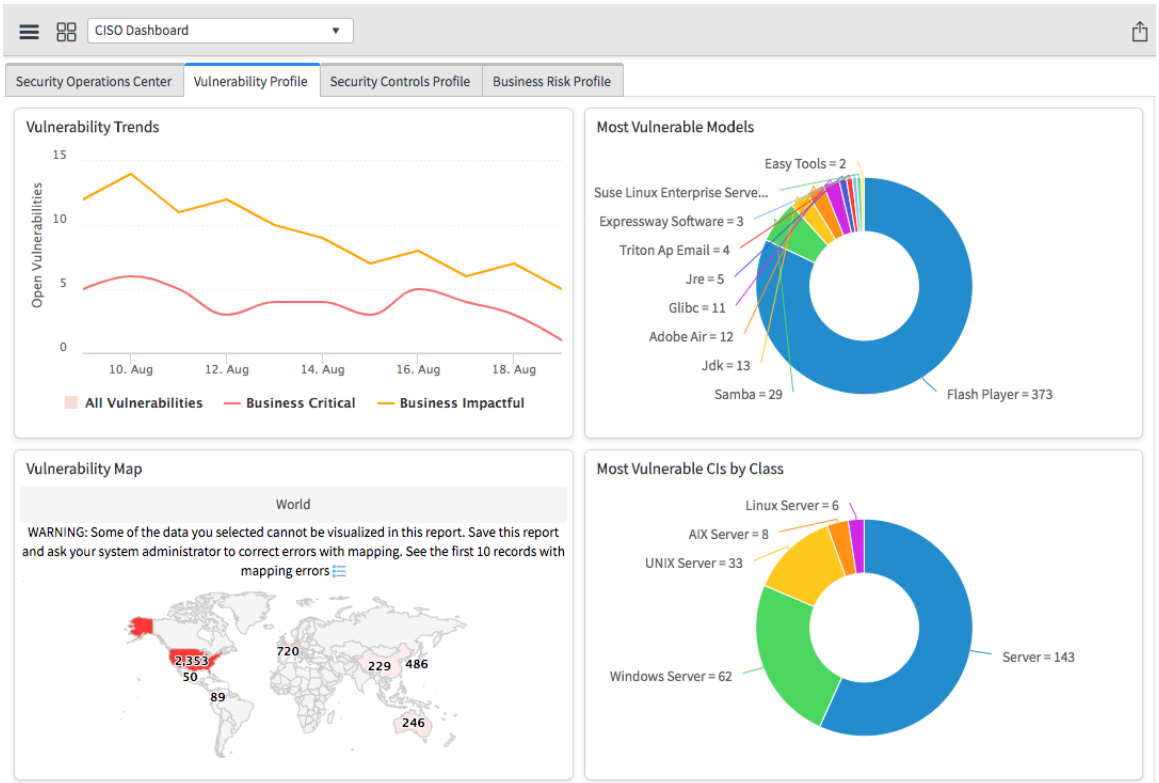
Este painel revela a postura de segurança geral da sua organização, incluindo vulnerabilidades de segurança e incidentes.



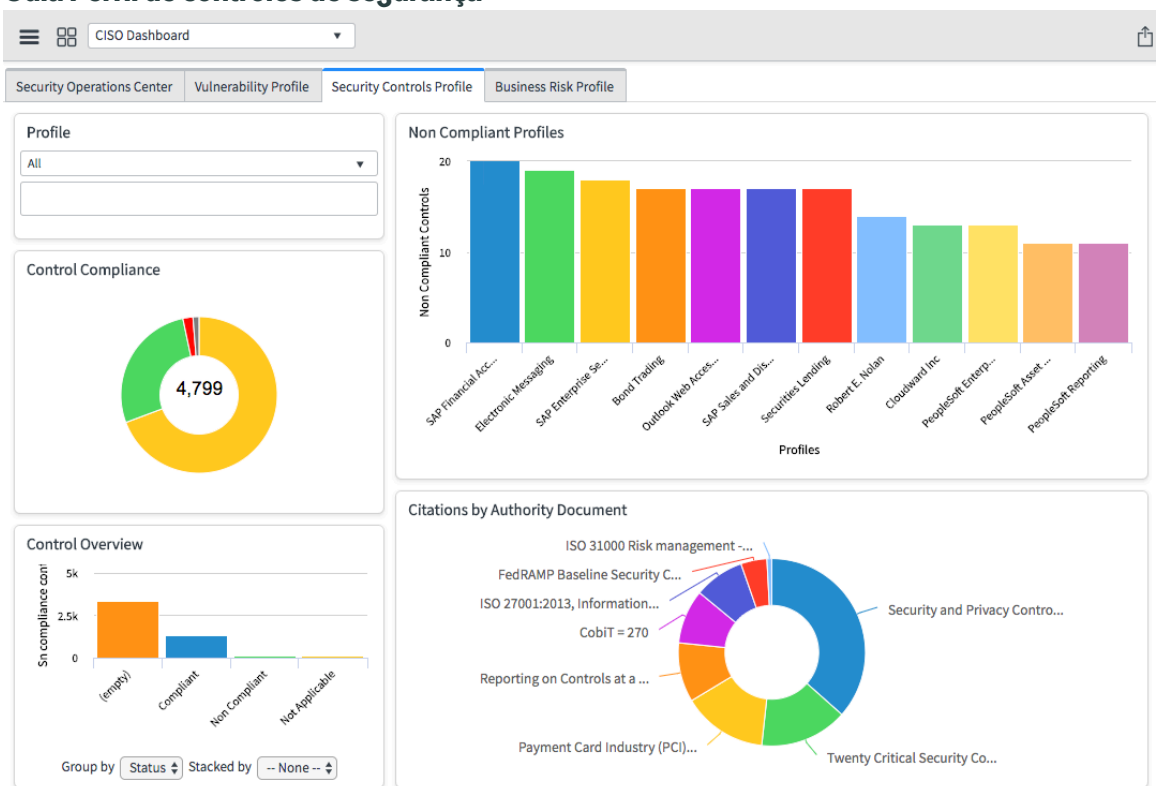
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Perfil de vulnerabilidade



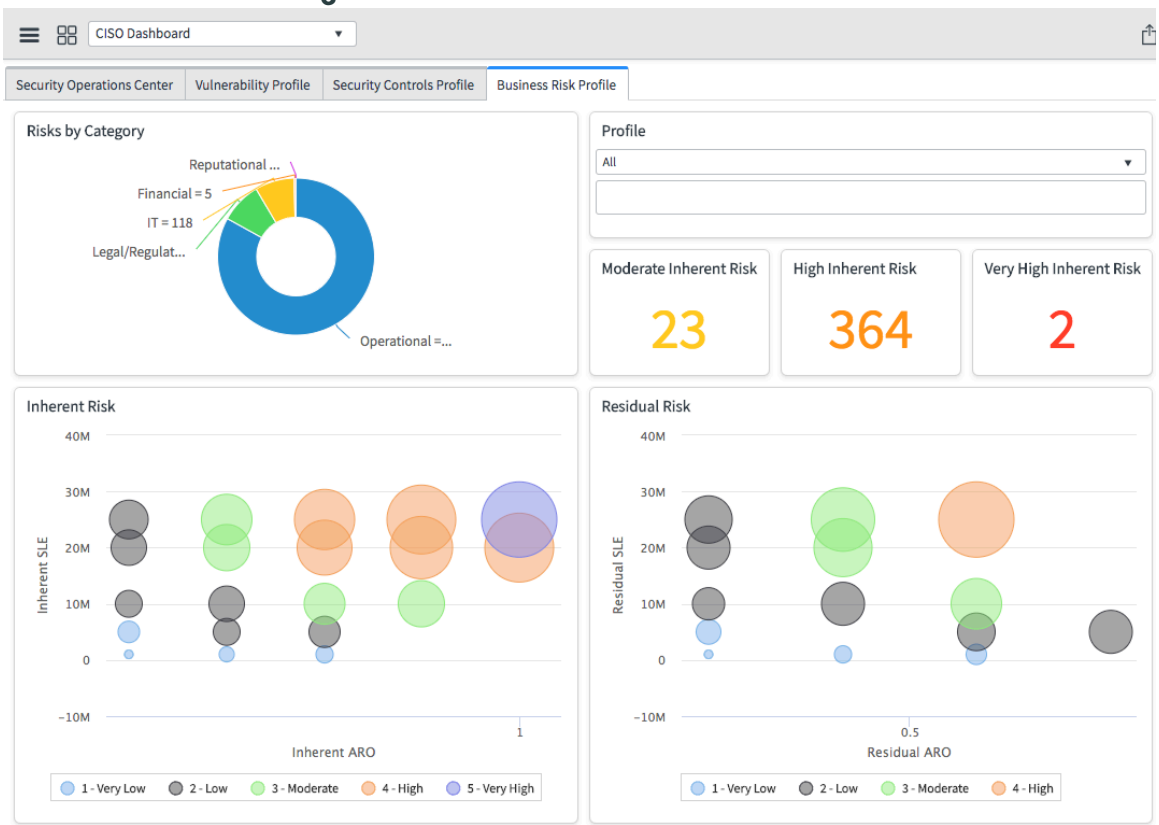
Guia Perfil de controles de segurança



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Perfil de risco de negócio



Funções e usuário finais

Usuário final e objetivo	Função necessária
CISO: Precisa de visibilidade clara sobre a postura de segurança atual da organização em geral	sn_si.ciso

Indicadores do painel do CISO

O painel do CISO apresenta os seguintes principais indicadores de desempenho:

Tempo médio de identificação

Média de 7 dias do tempo em minutos necessário para identificar um incidente de segurança, calculado diariamente.

Tempo médio de contenção

Média de 7 dias do tempo em minutos necessário para conter um incidente de segurança, calculado diariamente.

Tempo médio para eliminar

Média de 7 dias do tempo em minutos necessário para erradicar um incidente de segurança, calculado diariamente. O tempo médio de contenção e o tempo médio de erradicação são baseados no indicador de SI - Tempo médio de duração dividido por estado de incidente de segurança.

Novos incidentes de segurança nesta semana

A soma semanal da pontuação do indicador de número diário de novos incidentes de segurança.

Incidentes de segurança encerrados (semanalmente)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A soma de execução de 7 dias do indicador do número diário de incidentes de segurança encerrados.

Novos incidentes de segurança por prioridade

Detalhamento diário do indicador de número de novos incidentes de segurança por prioridade.

Volume de incidentes de segurança novos versus encerrados (semanalmente)

A série temporal da soma de execução de 7 dias do indicador Número de novos incidentes mapeado em relação à série temporal da soma de execução de 7 dias do indicador Número de incidentes encerrados.

Mapa térmico do incidente de segurança

Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Mapa em árvore de incidentes de segurança

Um mapa de árvore interativo onde você pode selecionar para ver:

- Incidentes de segurança por serviço de negócios, divididos por criticidade de negócios
- Incidentes de segurança divididos por categoria ou subcategoria de incidente
- Incidentes de segurança por grupo de atribuição ou por designado
- "Estatísticas de vítima" do incidente de segurança por recurso afetado ou usuário afetado

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Criticalidade dos negócios
- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Código de fechamento de incidentes de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança
- SI - Serviço de negócios
- Vulnerabilidade

Visualizações de dados

O painel inclui as seguintes visualizações:

Título	Tipo	Descrição
Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado	Mapa térmico 	Exibe modelos com os itens mais vulneráveis.
Risco por categoria	Donut 	Lista a idade dos itens vulneráveis reabertos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
Documento de citações por autoridade	Donut	Número de vulnerabilidades ativas
Incidentes de segurança com designado que não está ativo	Mapa térmico	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros CVE (Common Vulnerability Enumeration, enumeração de vulnerabilidades comuns)), da maior para a menor.
Incidentes de segurança não atualizados por mais de 30 dias por grupo de atribuição e estado	Mapa térmico	Exibe fornecedores com os itens mais vulneráveis.
Mapa de vulnerabilidades	Mapa	Um mapa-múndi mostrando vulnerabilidades por local
Modelos mais vulneráveis	Donut	As aplicações que contêm a maioria das vulnerabilidades
ICs mais vulneráveis por classe	Donut	ICs por tipo de servidor
Serviços com vulnerabilidades críticas significativas	Lista	
Perfis fora de conformidade	Barra	Controles fora de conformidade por perfil
Visão geral de controle	Barra	Número de controles em conformidade e fora de conformidade
Exceções às políticas	Lista	Exceções de política com prioridade, proprietário e descrição resumida
Risco por categoria	Donut	O número de riscos em cada categoria de risco
Risco inerente	Bolha	SLE inerente versus ARO inerente
Risco residual	Bolha	SLE residual versus ARO residual
Riscos Moderados, Alto e Muito Alto	Pontuações	Os números de riscos moderados, altos e muito altos, respetivamente
Risco por perfil	Barra Empilhada	Contagem de risco em que você pode selecionar o que agrupar e o que empilhar

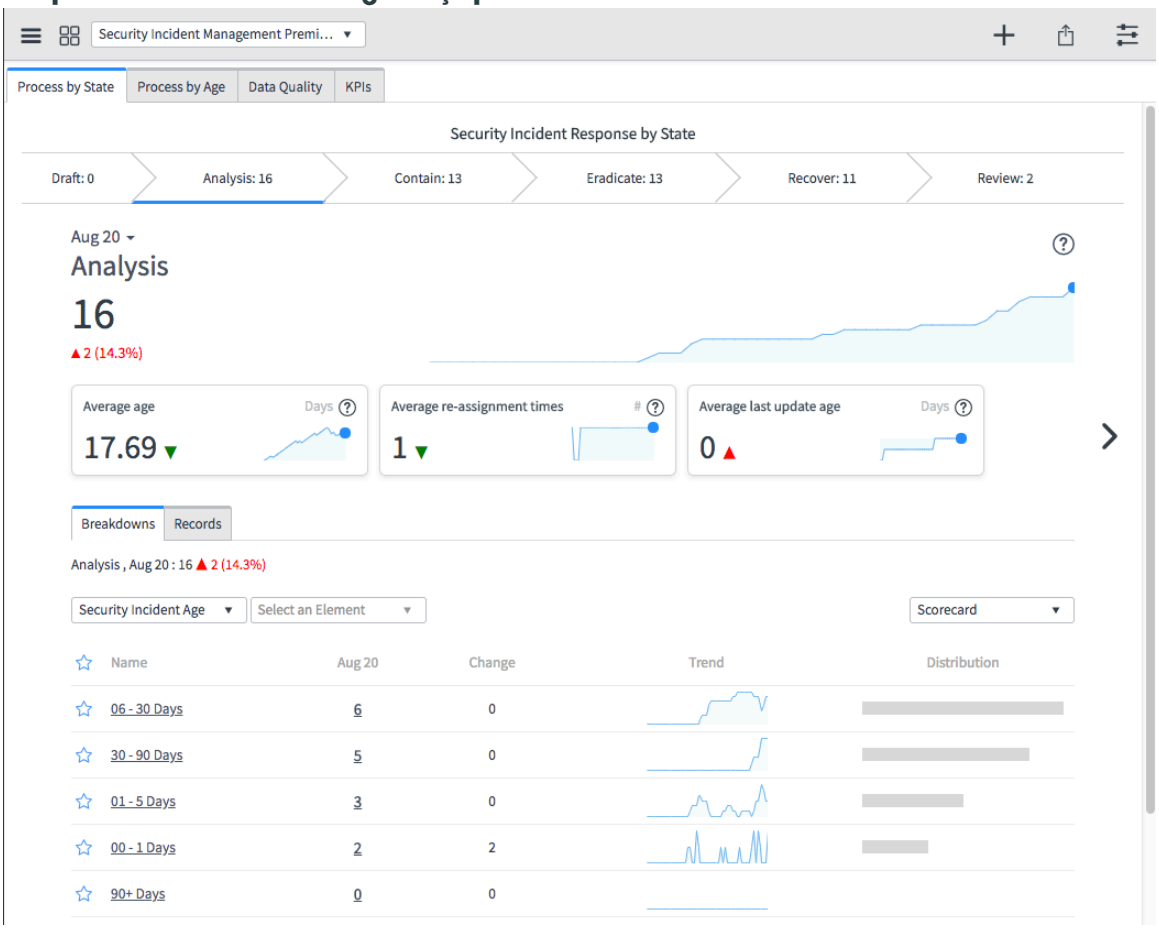
Painel Premium da Gestão de incidentes de segurança

Este painel usa avançado Análise da plataforma visualizações para ajudar os gerentes de segurança a rastrear o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação. A versão licenciada de Performance Analytics portanto, é necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

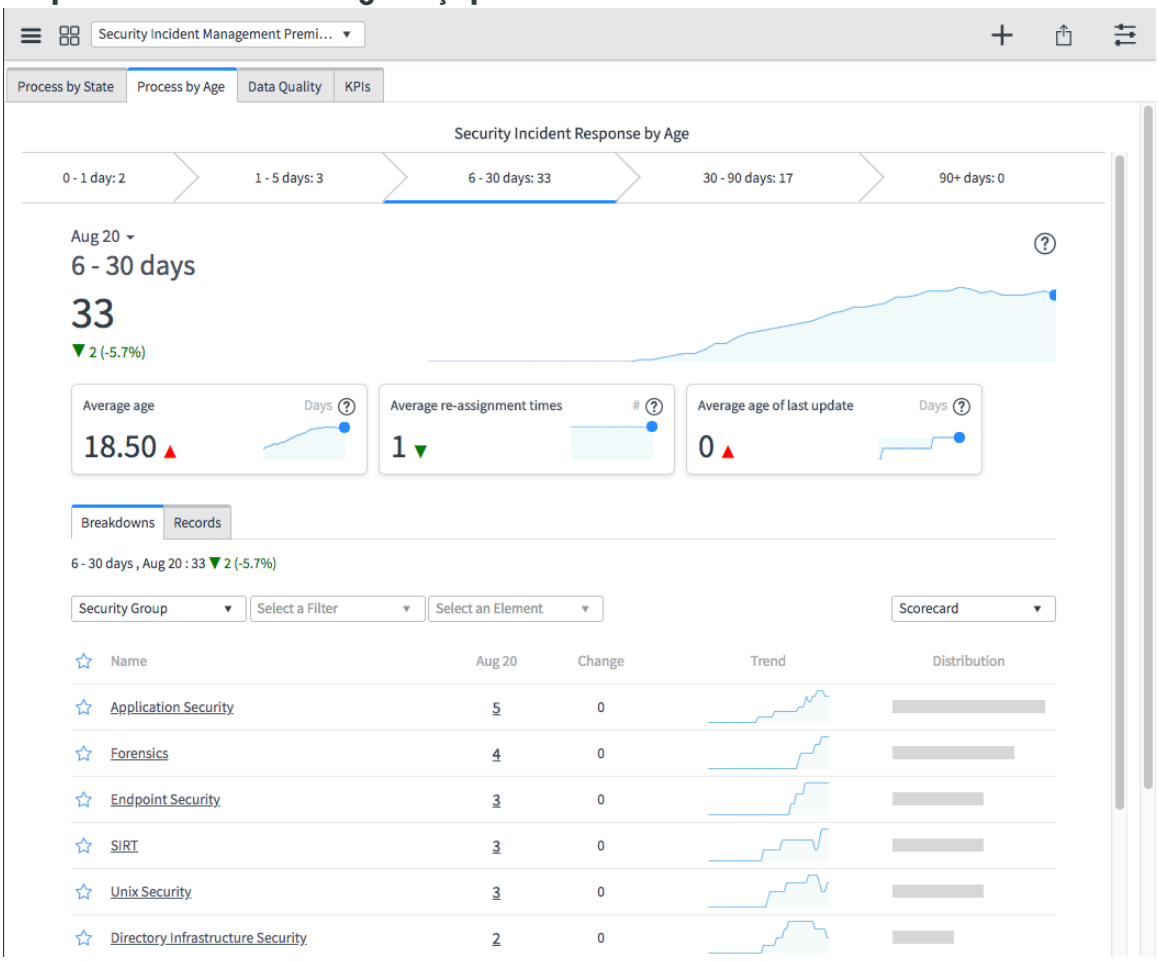
Resposta do incidente de segurança por estado



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança por idade



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: Precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador de resposta de segurança: Precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados de resposta a incidentes de segurança ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam abordados primeiro.
Analistas de resposta de segurança: Precisam priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionados a seus incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores Premium da Gestão de incidentes de segurança

As guias Processo por estado e Processo por idade contêm widgets de workbench com os seguintes indicadores:

Idade média

A idade média do indicador de incidentes de segurança em aberto usa a fórmula [[Soma da idade dos incidentes de segurança em aberto]] / [[Número de incidentes de segurança em aberto]] / 24 para fornecer um resultado em dias.

Tempos médios de reatribuição

O indicador Média de reatribuição de incidentes de segurança em aberto usa a fórmula Reatribuições de incidentes de segurança em aberto/Número de incidentes de segurança em aberto .

Idade média da última atualização

A idade média da última atualização do indicador de incidentes de segurança em aberto usa a fórmula Soma da idade da última atualização de incidentes de segurança em aberto/ Número de incidentes de segurança em aberto/24 para fornecer um resultado em dias.

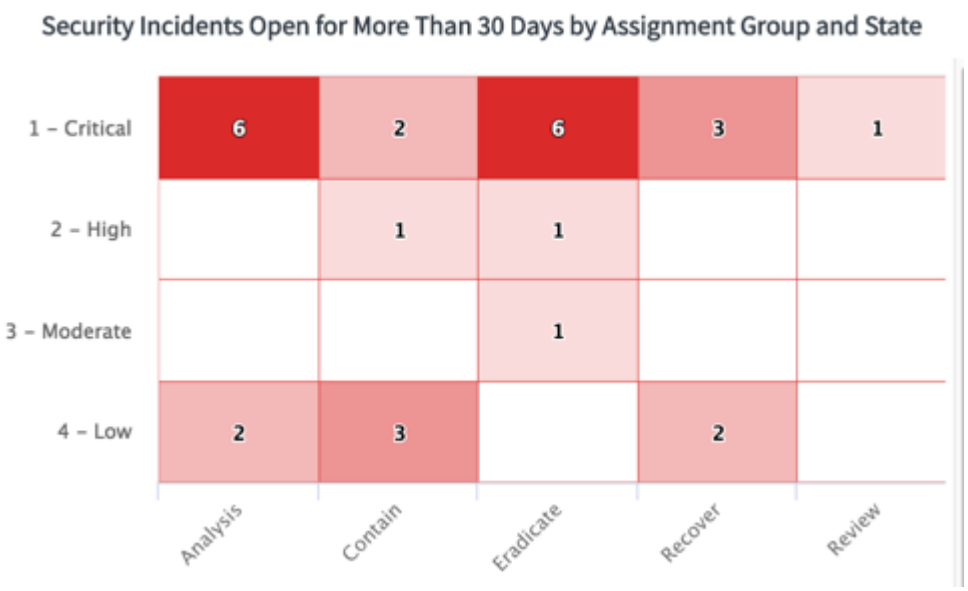
Percentuais não atualizados em 5 dias

O indicador % de incidentes de segurança em aberto não atualizados nos últimos 5 dias usa a fórmula [[Número de incidentes de segurança em aberto não atualizados nos últimos 5 dias]] / [[Número de incidentes de segurança em aberto]]) * 100 .

A guia Qualidade de dados tem filtros interativos para a Categoria do incidente de segurança e os níveis de risco, prioridade e gravidade. Esses filtros são aplicados simultaneamente aos seguintes indicadores:

Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado

O número de incidentes de segurança em aberto filtrados para uma idade de 30 dias e divididos por Grupo de atribuição e Estado.



Incidentes de segurança com designado que não está ativo

O número de incidentes de segurança em aberto sem designado ou um designado que não está ativo.

Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador Número de incidentes de segurança em aberto não atualizados nos últimos 30 dias, dividido por Grupo de atribuição e Estado.

A guia KPI tem os seguintes indicadores adicionais:

- Percentual de novos incidentes de segurança críticos
- Idade média dos incidentes de segurança em aberto
- Tempo médio de encerramento de incidentes de segurança
- Percentual de incidentes de segurança que foram reatribuídos
- Percentual de incidentes de segurança encerrados na primeira atribuição
- percentual de incidentes de segurança encerrados por autoatendimento
- percentual de incidentes de segurança não resolvidos
- Tempo médio de encerramento de tarefas de incidente de segurança

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

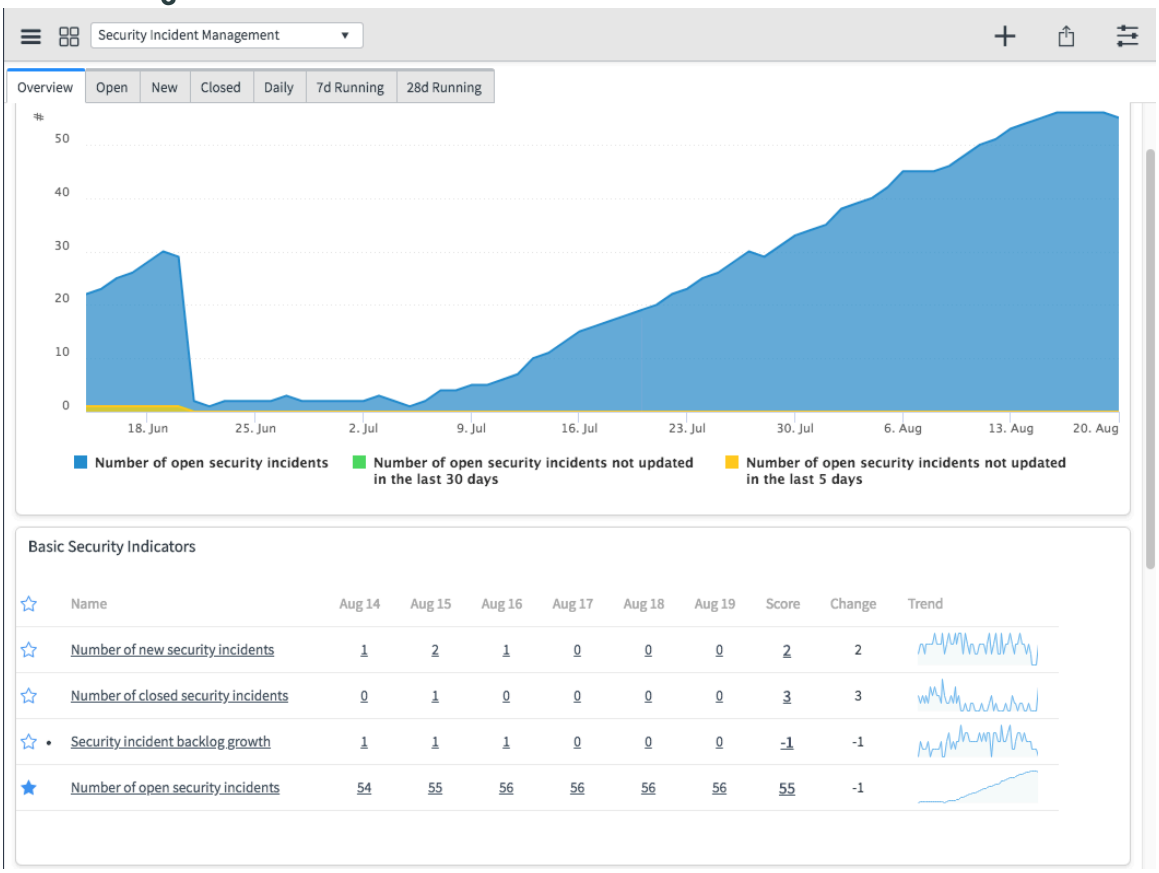
Painel da Gestão de incidentes de segurança

Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento de incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

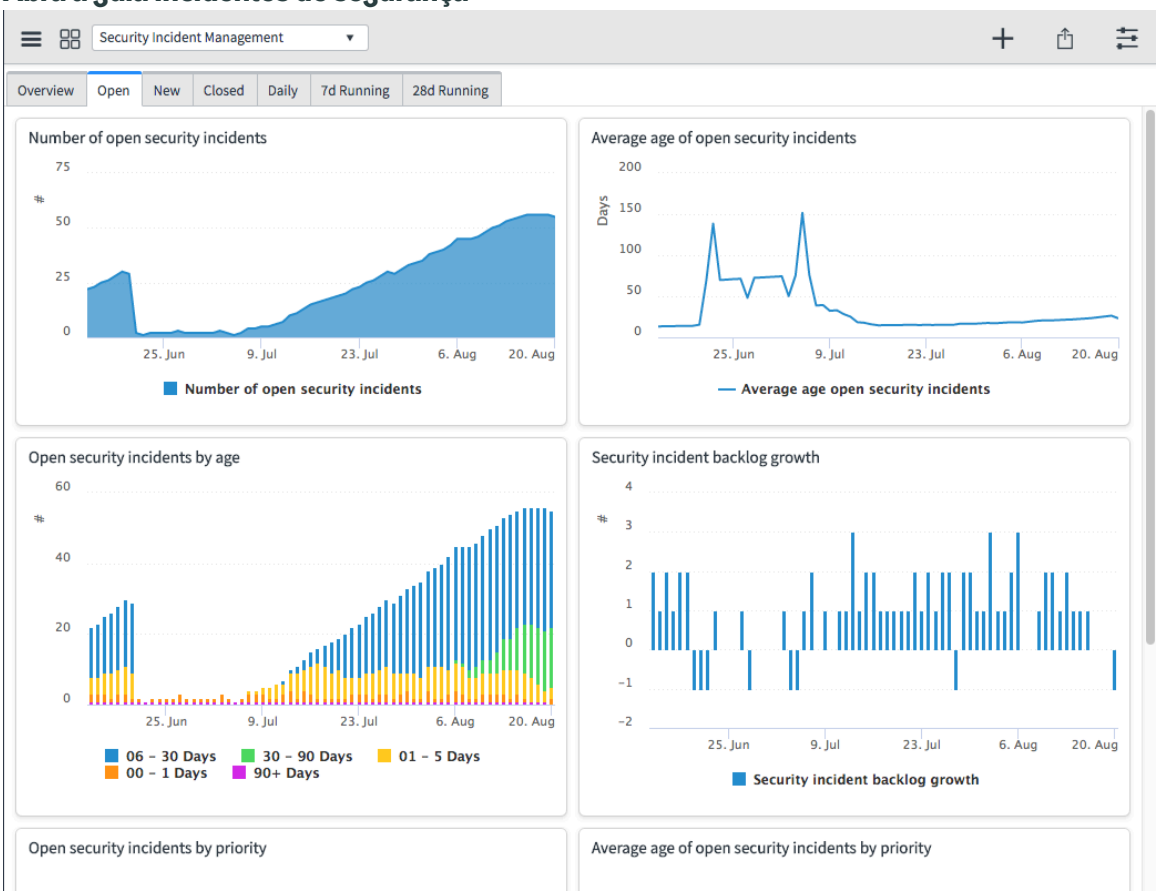
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia "Visão geral"



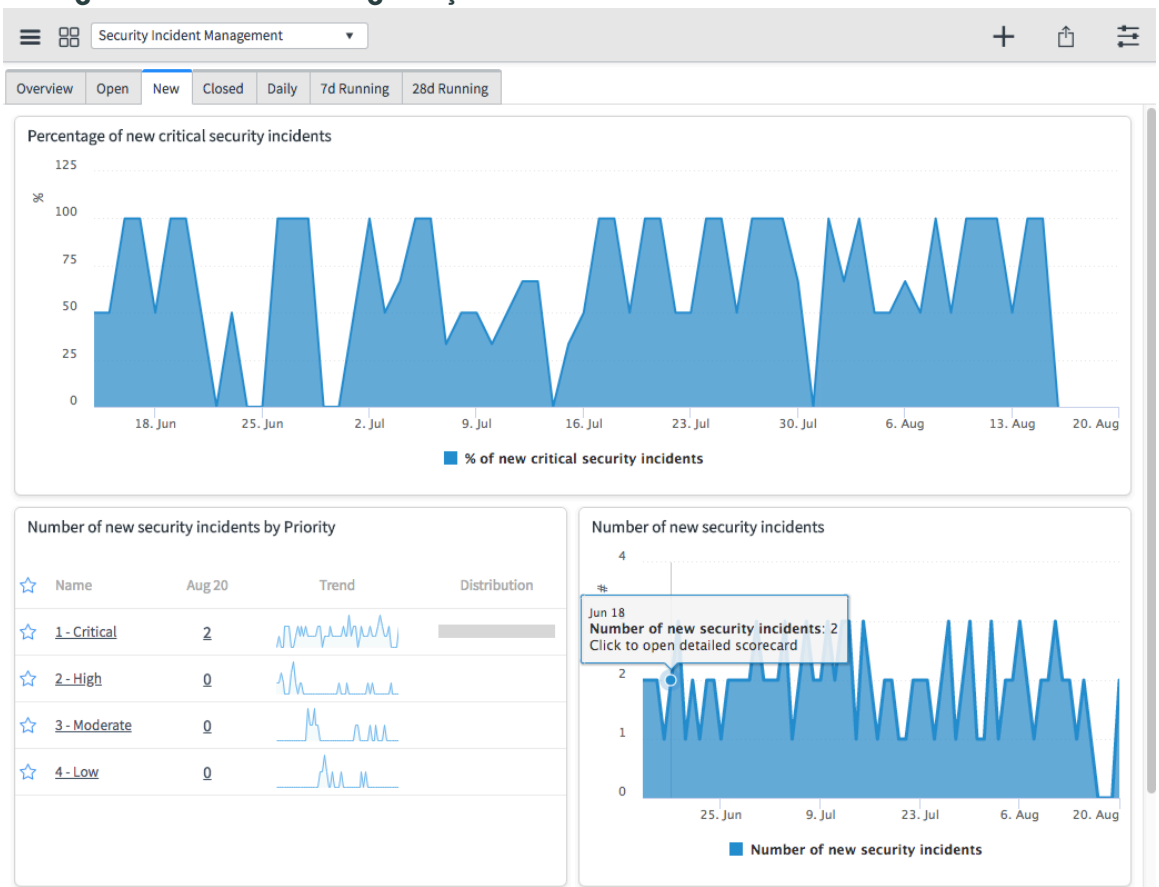
Abra a guia Incidentes de segurança



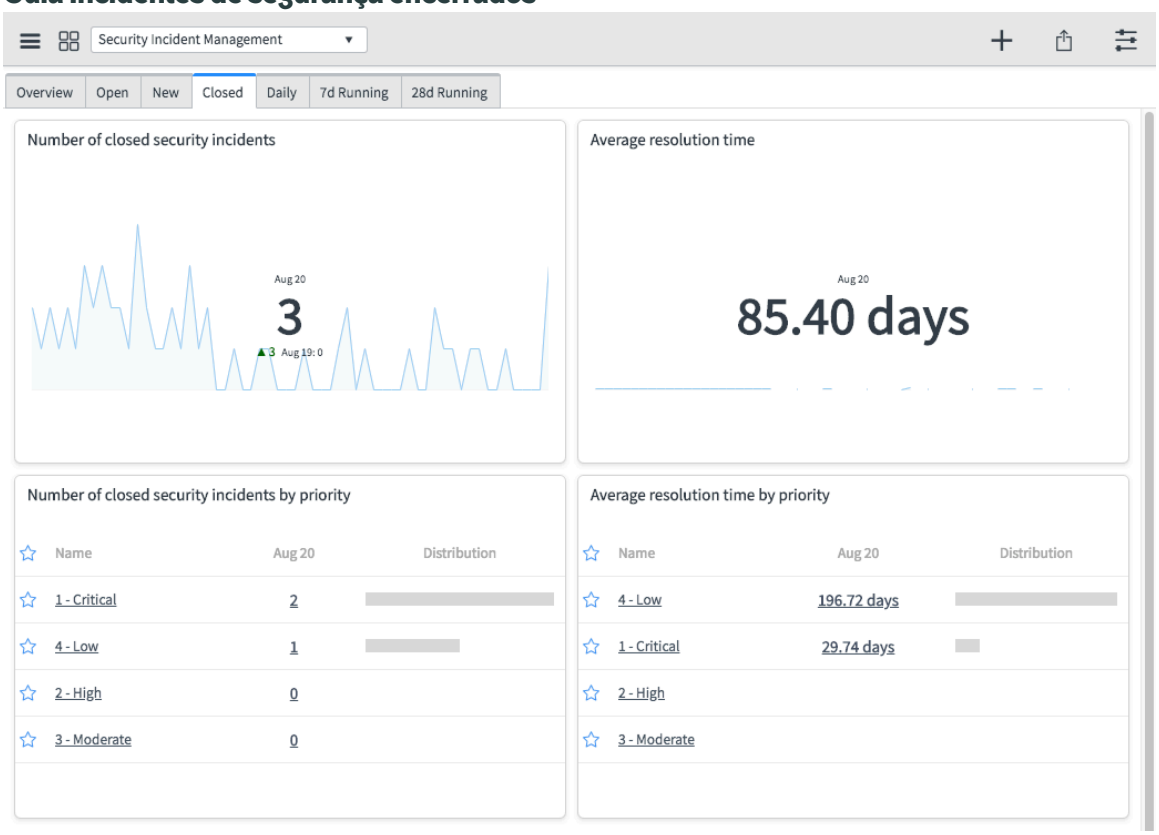
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nova guia de incidente de segurança



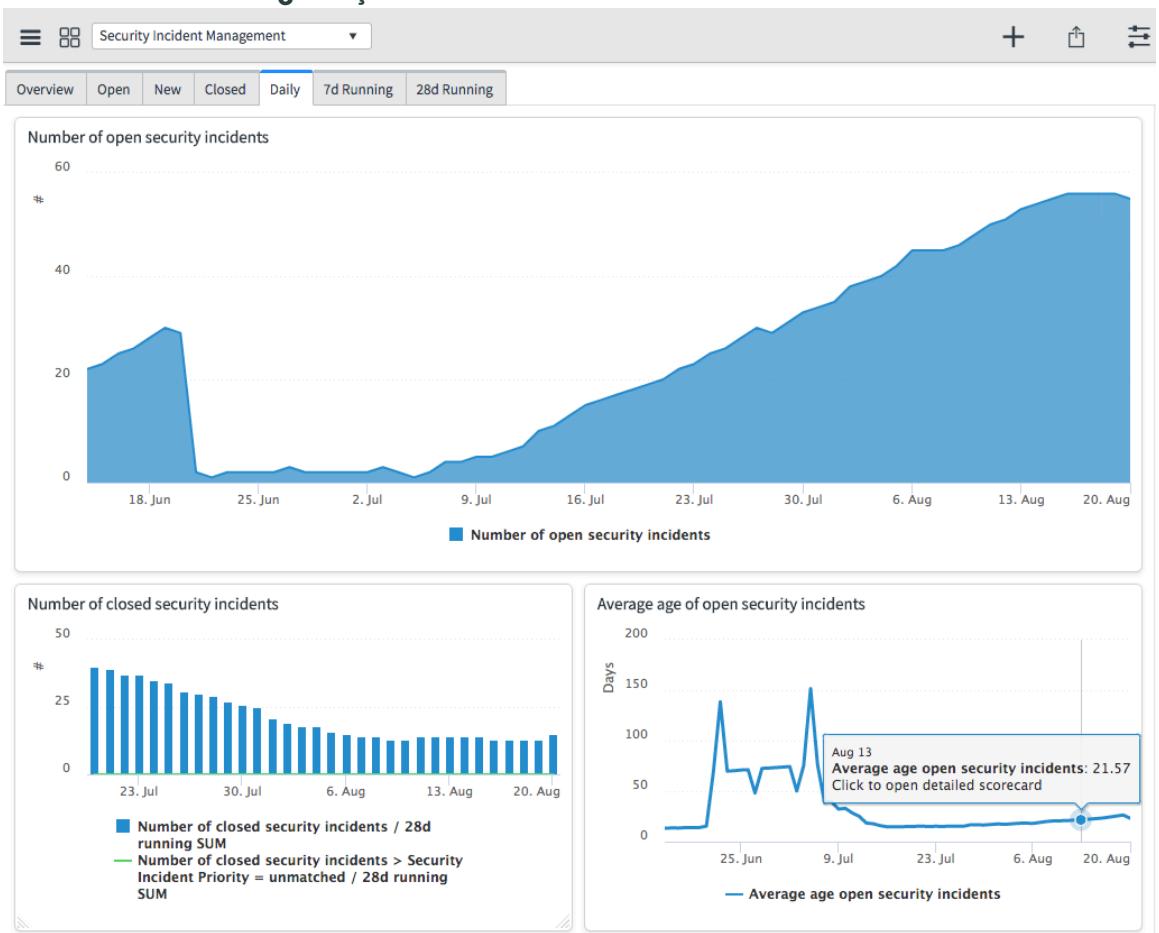
Guia Incidentes de segurança encerrados



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Incidentes de segurança diários



. **7d em execução** e. **28D em execução** as guias seguem o formato do **Diariamente** guia.

Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: Precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador de resposta de segurança: Precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados de resposta a incidentes de segurança ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam abordados primeiro.
Analistas de resposta de segurança: Precisam priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário final e objetivo	Função necessária	Benefícios
		indisponibilidades relacionados a seus incidentes.

Indicadores da Gestão de incidentes de segurança

O painel da Gestão de incidentes de segurança apresenta os seguintes principais indicadores de desempenho:

Novos incidentes de segurança

Um gráfico do número de novos incidentes de segurança.

Incidentes de segurança em aberto

Um gráfico em que você pode comparar o número de incidentes de segurança em aberto, o número de incidentes de segurança em aberto não atualizados nos últimos 30 dias e o número de incidentes de segurança em aberto não atualizados nos últimos 5 dias.

Indicadores básicos de segurança

Pontuações dos últimos 6 dias dos indicadores Número de novos incidentes de segurança, Número de incidentes de segurança encerrados, crescimento do backlog de incidentes de segurança e Número de incidentes de segurança em aberto.

Novos incidentes de segurança por prioridade

O número de novos incidentes de segurança divididos por prioridade.

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

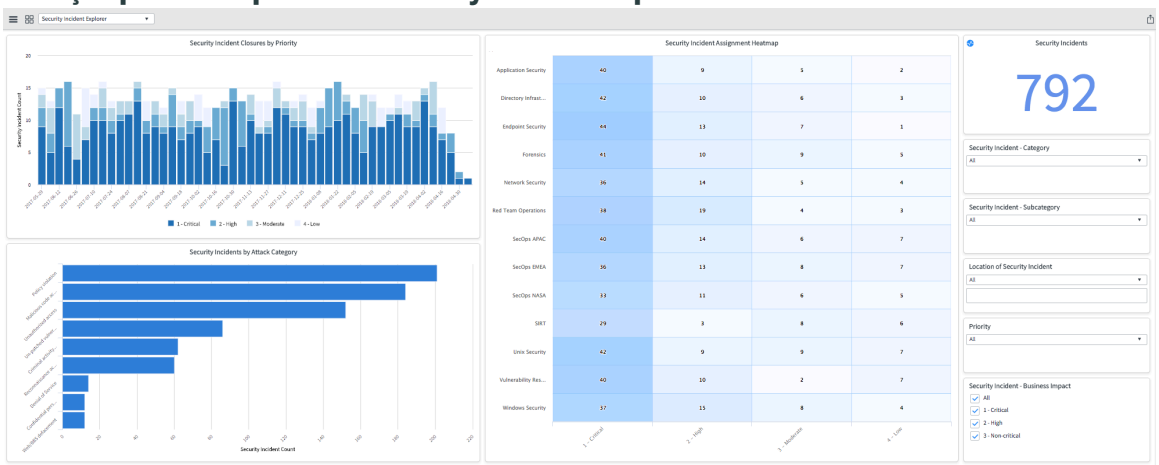
Painel do Security Incident Explorer

Com este painel, os gerentes de segurança podem exibir os incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que os gerentes obtenham rapidamente informações sobre a frequência em que os ataques estão ocorrendo e quais serviços de negócios são afetados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição parcial do painel do Security Incident Explorer



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: Precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador de resposta de segurança: Precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados de resposta a incidentes de segurança ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam abordados primeiro.
Os analistas de resposta de segurança precisam priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionados a seus incidentes.

Indicadores do Explorador de incidentes de segurança

O painel do Gerenciador de incidentes de segurança apresenta os seguintes principais indicadores de desempenho:

Incidentes de segurança

O volume total de incidentes de segurança em aberto e pendentes.

Encerramentos de incidente de segurança por prioridade

O número de incidentes de segurança encerrados divididos por prioridade.

Incidentes de segurança por categoria de ataque

O número de incidentes de segurança em aberto divididos por categoria.

Mapa térmico de atribuição de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um detalhamento em dois níveis do número de incidentes de segurança em aberto por grupo de atribuição e prioridade.

Mapa térmico do incidente de segurança

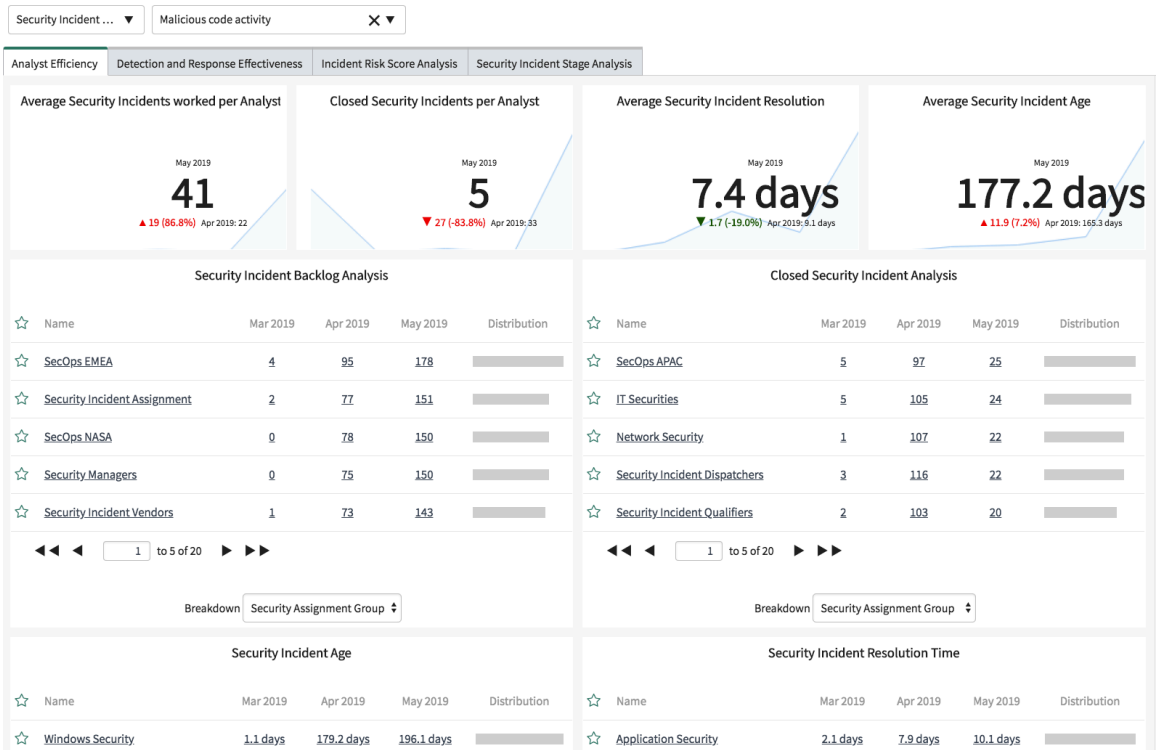
Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Painel de Eficiência de operações de segurança

Os gerentes do Centro de operações de segurança (SOC) podem exibir métricas gerais de eficiência e medir o desempenho individual dos membros da equipe do SOC na organização.

O gerente do SOC pode usar o painel do Performance Analytics para melhorar a eficiência e desenvolver uma imagem do desempenho do SOC em áreas gerais e específicas ao longo do tempo.

Guia Eficiência do analista

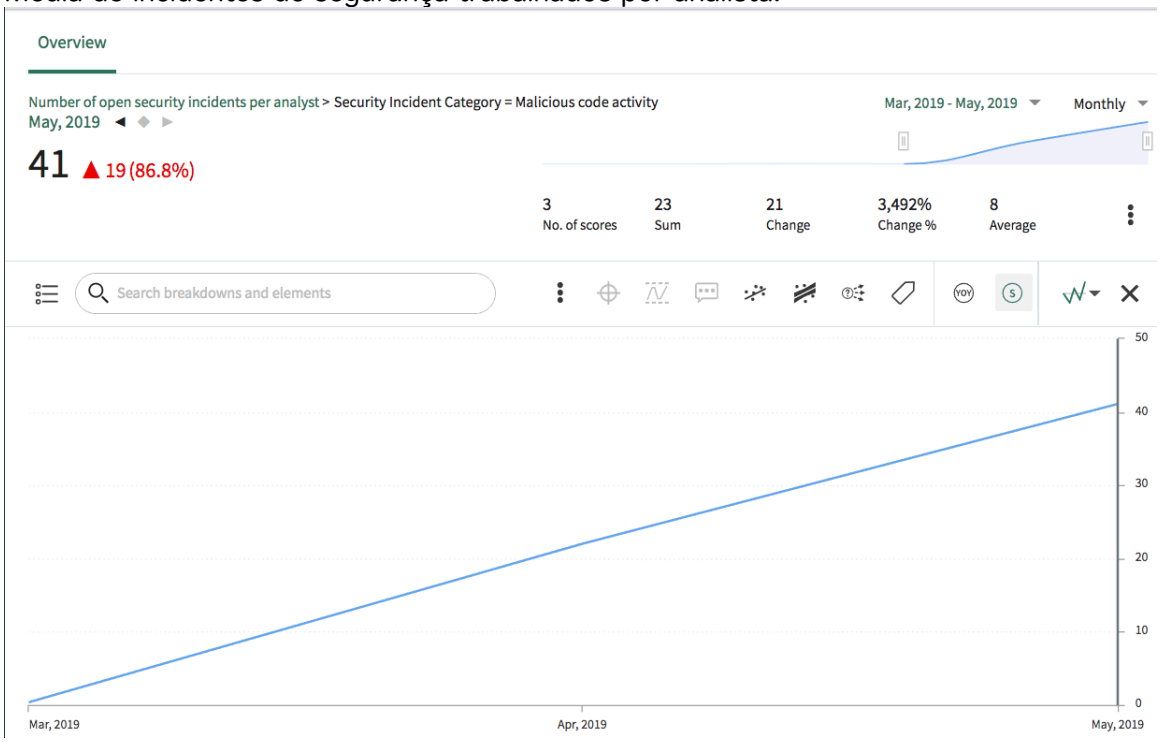


Clique em qualquer um dos indicadores para detalhar para obter mais detalhes. Por exemplo, clique no indicador na seção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Média de incidentes de segurança trabalhados por analista.



O gráfico mostra que o número de incidentes de segurança em aberto aumentou de 0 em março para mais de 40 em maio. Observe os dados exibidos no cabeçalho:

- Indicador de tendência: Mostra a mudança no número de incidentes em aberto no último período para o qual os dados foram coletados. Este gráfico mostra dados do período de março de 2019 a maio de 2019 e o número de incidentes em aberto aumentou 19 no mês de maio. A eficiência do analista será melhor se o número de incidentes em aberto diminuir ao longo de um período.
- Nº de pontuações: O período durante o qual os dados foram coletados (março a maio de 2019).
- Soma: O número de novos incidentes em aberto para o período entre março e maio.
- Mudança: O número de novos incidentes em aberto entre março e abril.
- Média: O número médio de incidentes em aberto por analista para o período selecionado.

Guia Eficiência do analista

Indicador	Descrição
Média de incidentes de segurança trabalhados por analista	Número médio de incidentes de segurança em aberto por analista para o período especificado. A fórmula usada é [[Número de incidentes de segurança em aberto / Média por mês]]/[[Número de agentes de segurança]]
Incidentes de segurança encerrados por analista	O número total de incidentes encerrados por cada analista na categoria selecionada no período especificado. A fórmula usada é [Número de incidentes de segurança encerrados > Categoria de incidente de segurança: SOMA DE <category_name> / por mês]]/[[Número de agentes de segurança / Média por mês]]
Resolução média de incidentes de segurança	O tempo médio gasto por cada analista para fechar incidentes de segurança no período especificado. A fórmula usada para mostrar o resultado em dias é [[Soma da duração dos incidentes de segurança encerrados >

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

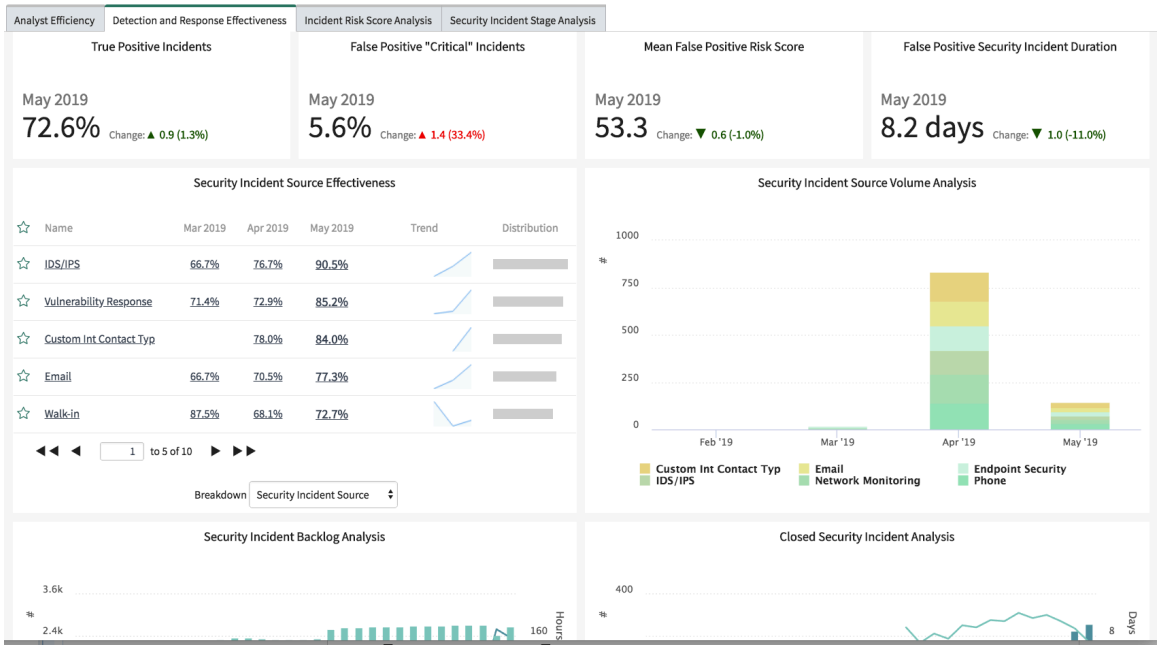
Guia Eficiência do analista

Indicador	Descrição
	Categoria de incidente de segurança: <category_name> / Média por mês]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança: <category_name> / Média por mês]] / 24
Idade média do incidente de segurança	O número médio de dias durante os quais os incidentes de segurança permanecem abertos para cada analista. A fórmula usada para mostrar o resultado em dias é [[Soma da idade dos incidentes de segurança em aberto > Categoria de incidente de segurança: <category_name> / Média por mês]]/ [[Número de incidentes de segurança em aberto > Categoria de incidente de segurança: <category_name> / Média por mês]]] / 24
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado. Selecione uma opção na lista de detalhamento para exibir o backlog de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados.
Análise de incidente de segurança encerrada	O número total de incidentes de segurança encerrados no período especificado. Selecione uma opção na lista de detalhamento para exibir a contagem de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança que foram encerrados entre dois meses selecionados.
Idade do incidente de segurança	O número médio de dias dos incidentes de segurança que permanecem em aberto no período especificado. Selecione uma opção na lista de detalhamento para exibir a idade do incidente de segurança de cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é ([[Soma da idade dos incidentes de segurança em aberto > Categoria de incidente de segurança: <category_name> > Grupo de atribuição de segurança: <group_name> / Média por mês]]/ [[Número de incidentes de segurança em aberto > Categoria de incidente de segurança: <category_name> > Grupo de atribuição de segurança: <group_name> / Média por mês]]) / 24
Tempo de resolução do incidente de segurança	O número médio de dias necessários para resolver incidentes de segurança durante o período especificado. Selecione uma opção na lista de detalhamento para exibir o tempo de resolução do incidente de segurança de cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é ([[Soma da duração dos incidentes de segurança encerrados > Categoria de incidente de segurança: Atividade de código mal-intencionado > Segurança atribuída a John Ashby / Média por mês]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança: Atividade de código mal-intencionado > Segurança atribuída a John Ashby / Média por mês]] / 24

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detecção e eficácia da resposta



Detecção e eficácia da resposta

Indicador	Descrição
Incidentes positivos verdadeiros	Percentual de incidentes de segurança verdadeiros positivos na categoria selecionada para o período especificado. A fórmula usada é (1-([[Número de incidentes de segurança falso-positivos > Categoria de incidente de segurança: Atividade de código mal-intencionado / SOMA por mês]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança: Atividade de código mal-intencionado / SOMA por mês]]) * 100
Incidentes críticos falso-positivos	Percentual de incidentes de segurança críticos falso-positivos na categoria selecionada para o período especificado. A fórmula usada é [[Número de incidentes de segurança falso-positivos > Pontuação de risco de incidente de segurança Risco crítico > Categoria de incidente de segurança atividade de código mal-intencionado / SOMA mensal] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança atividade de código mal-intencionado / SOMA mensal]] * 100 **Nota:** Qualquer incidente de segurança em que Código encerrado: Vulnerabilidade inválida ou falso-positivo é tratado como um incidente falso-positivo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detecção e eficácia da resposta

Indicador	Descrição
Pontuação de risco falso-positivo média	Pontuação média de risco mensal de incidentes de segurança encerrados que foram identificados como incidentes falso-positivos. Uma pontuação de risco mais baixa indica que os analistas de segurança gastaram menos tempo analisando incidentes falso-positivos. A fórmula usada é [[Número de incidentes de segurança falso-positivos > Pontuação de risco de incidente de segurança Risco crítico > Categoria de incidente de segurança atividade de código mal-intencionado / SOMA mensal] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança atividade de código mal-intencionado / SOMA mensal]] * 100
Duração do incidente de segurança falso-positivo	Número médio de dias que os analistas de segurança gastaram na investigação de incidentes falso-positivos. A fórmula usada é [[Soma da duração de incidentes de segurança falso-positivos]] / [[Número de incidentes de segurança falso-positivos]] / 24
Eficácia da origem do incidente de segurança	Percentual de incidentes de segurança verdadeiros positivos identificados por uma origem específica para o período especificado. A origem pode ser e-mail, atividade de rede, suporte ao cliente e assim por diante. Esses dados ajudam a medir a eficácia da origem do incidente de segurança. A fórmula usada é (1-([[Número de incidentes de segurança falso-positivos > Categoria de incidente de segurança: Atividade de código mal-intencionado > Origem do incidente de segurança: IDS/IPS / SOMA mensal]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança atividade de código mal-intencionado > Origem do incidente de segurança: IDS/IPS / SOMA mensal]) * 100
Análise de volume de origem do incidente de segurança	Número de incidentes de segurança encerrados para o mês atual para cada origem de incidente de segurança. Você também pode comparar o número de incidentes de segurança para cada tipo de origem entre dois meses selecionados.
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado e o número médio de dias em que os incidentes permanecem em aberto. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados. A fórmula usada para calcular o período médio de

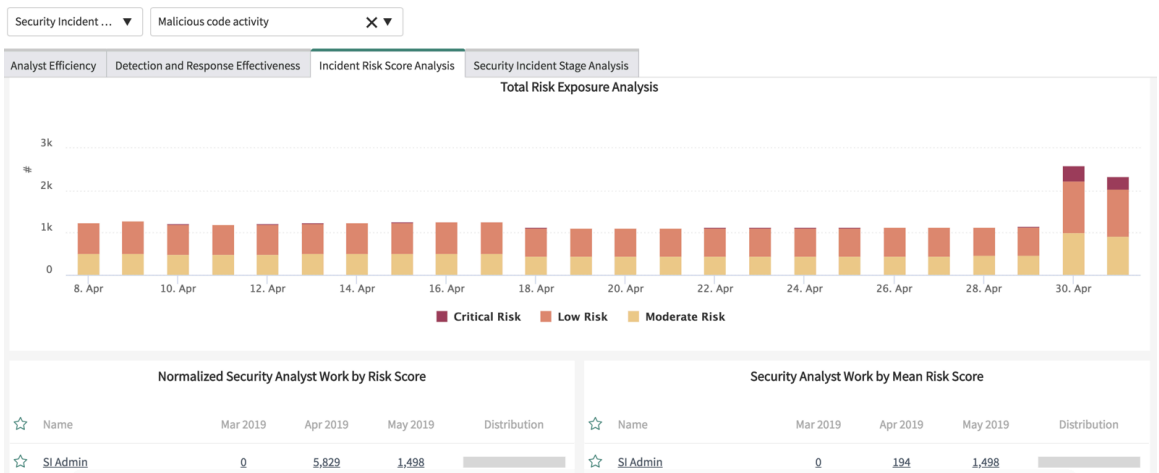
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detecção e eficácia da resposta

Indicador	Descrição
	backlog é ([[Soma da idade dos incidentes de segurança em aberto > Categoria de incidente de segurança: Atividade de código mal-intencionado]]/ [[Número de incidentes de segurança em aberto > Categoria de incidente de segurança: Atividade de código mal-intencionado]]) / 24
Análise de incidente de segurança encerrada	O número total de incidentes de segurança encerrados no período especificado e o tempo médio de resolução desses incidentes. A fórmula usada para calcular o tempo médio de resolução é ([[Soma da duração dos incidentes de segurança encerrados > Categoria do incidente de segurança: Atividade de código mal-intencionado]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança: Atividade de código mal-intencionado]]) / 24

Guia Análise de pontuação de risco do incidente



Guia Análise de pontuação de risco do incidente

Indicador	Descrição
Análise de exposição ao risco total	Número total de incidentes em aberto em cada categoria de risco (baixo, moderado e crítico) no período especificado. Você também pode comparar o número de incidentes nas diferentes categorias de risco entre dois meses.
Trabalho de analista de segurança normalizado por pontuação de risco	A pontuação total de risco de cada analista de segurança para o período especificado. Isso é calculado com base no número de incidentes de segurança positivos verdadeiros que o analista de segurança encerrou. A fórmula usada é [[Soma da pontuação de risco de incidentes de

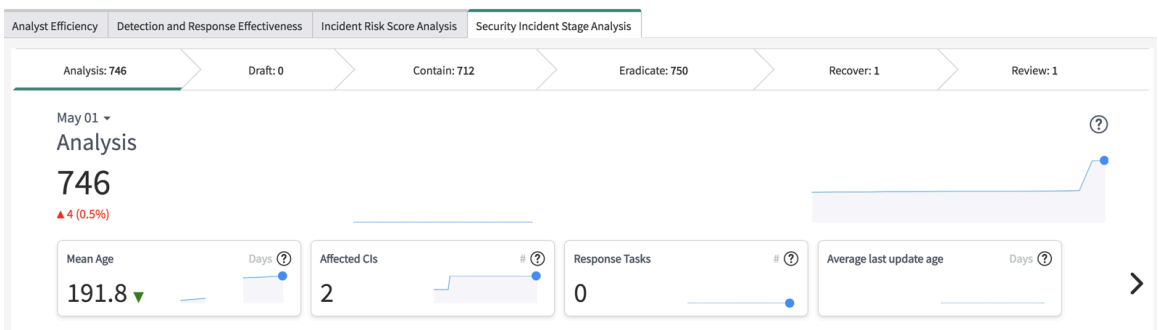
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Análise de pontuação de risco do incidente

Indicador	Descrição
	segurança encerrados > Categoria de incidente de segurança Atividade de código mal-intencionado > Segurança atribuída a administrador de segurança / SOMA por mês] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos > Categoria de incidente de segurança Atividade de código mal-intencionado > Segurança atribuída a Administrador de segurança / SOMA por mês]]
O analista de segurança trabalha por pontuação de risco média	A pontuação média de risco de cada analista de segurança para o período especificado. A fórmula usada é [[Soma da pontuação de risco de incidentes de segurança encerrados > Categoria de incidente de segurança Atividade de código mal-intencionado > Segurança atribuída a administrador de segurança / média por mês] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos > Categoria de incidente de segurança Atividade de código mal-intencionado > Segurança atribuída a Administrador de segurança / Média por mês]]

Guia Análise da fase do incidente de segurança



Você pode ver o número de incidentes em aberto em um dia específico e o status (análise, rascunho, conter, erradicar, recuperar, ou revisão) desses incidentes. Em cada fase, você pode exibir a idade média, ICs afetados, tarefas de resposta e assim por diante. Clique em um link para exibir detalhes adicionais ou o detalhamento desses incidentes.

Espaço de resposta a incidentes de segurança

. ServiceNow® Espaço de resposta a incidentes de segurançaÉ uma interface reimaginada que fornece uma experiência de usuário de última geração para os analistas de segurança e gerentes de SOC. Os analistas de segurança podem usar isso para gerenciar o ciclo de vida dos incidentes de segurança, desde uma análise inicial até contenção, erradicação e recuperação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para começar com Espaço SIR

Selecione um bloco para começar.

Explorar o espaço



Saiba mais sobre os conceitos e recursos do SIR Workspace

Administradores que usam o espaço



Configurar o Espaço SIR e os recursos

Analistas que usam o Espaço



Saiba como os analistas usam o SIR Workspace

Exibir Painéis SIR



Exibir painéis do Espaço do SIR

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Importante:

- Instalando o. Resposta a incidentes de segurança versão 13.4.5 ou posterior do ServiceNow Store instalará automaticamente o. Espaço de resposta a incidentes de segurança(sn_si_aw) versão 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte Espaço SIR plug-ins e funções seção.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/upgrade do Resposta a incidentes de segurança e não podem ser instaladas independentemente.

Mais recursos

Visite Resposta a incidentes de segurança fórum em Comunidade ServiceNow.

Explorando Espaço SIR

Explorar Espaço de resposta a incidentes de segurança Para entender como os analistas e gerentes de segurança executam suas operações diárias com uma experiência do usuário aprimorada, faça uma investigação completa de incidentes e obtenha uma visão geral dos incidentes de segurança, tarefas de resposta e SLAs atribuídos ao analista de segurança e à equipe.

Esta seção descreve o seguinte:

- Espaço SIR plug-ins e funções necessárias.
- Chave Espaço SIR recursos.

Espaço SIR plug-ins e funções

A seguir estão as aplicações necessárias para trabalhar com Espaço de resposta a incidentes de segurança plug-in (sn_si_aw).

Aplicações

Instalando o. Resposta a incidentes de segurança a aplicação versão 13.4.5 ou posterior instala automaticamente o. Espaço de resposta a incidentes de segurança e os seguintes apps.

- PAD Commons da Gestão de casos de segurança empresarial PAD [sn_escm_pad_cmn]
- Espaço comum de operações de segurança [sn_escm_ws_cmn]
- Componente do cartão de IU de incidente de segurança [sn_sirw_evam]
- Spoke de operações de segurança [sn_sec_spoke]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

- Instalando o. Resposta a incidentes de segurança versão 13.4.5 ou posterior do ServiceNow Store instalará automaticamente o. Espaço de resposta a incidentes de segurança(sn_si_aw) versão 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte Espaço SIR plug-ins e funções seção.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/upgrade do Resposta a incidentes de segurança e não podem ser instaladas independentemente.

PAD Commons da Gestão de casos de segurança empresarial Requer o plug-in Playbook Experience [playbook_experience].

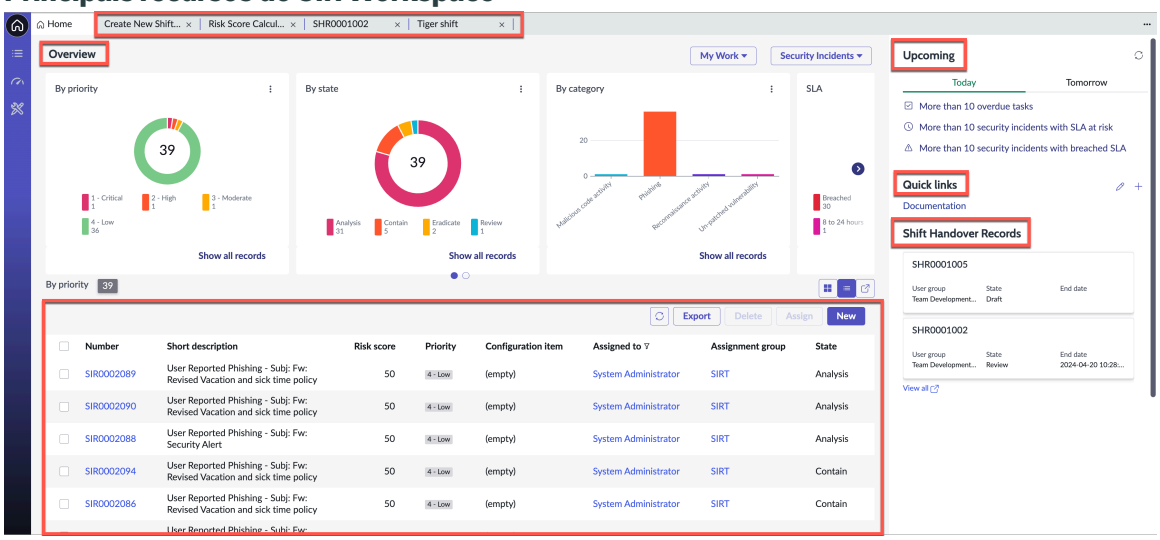
Para obter informações sobre Resposta a incidentes de segurança funções, tabelas, propriedades e trabalhos agendados, consulte Componentes instalados com Resposta a incidentes de segurança

Recursos do Espaço SIR

. Espaço de resposta a incidentes de segurança consiste nos seguintes recursos principais.

- Seção de Visão geral
- Seção A seguir
- Seção Links rápidos
- Seção Registros de entrega do turno
- Exibição em lista
- Interface de várias guias que oferece suporte à abertura de vários incidentes de segurança

Principais recursos do SIR Workspace



Espaço SIR visão geral da interface

. Espaço SIR A página Visão geral consiste nos detalhes Incidentes de segurança e Tarefas de resposta que estão sob os analistas de segurança e sua equipe.

Cada filtro é agrupado por prioridade, categoria, estado e ANS, que estão nas filas dos analistas de segurança e na fila da equipe de analistas de segurança.

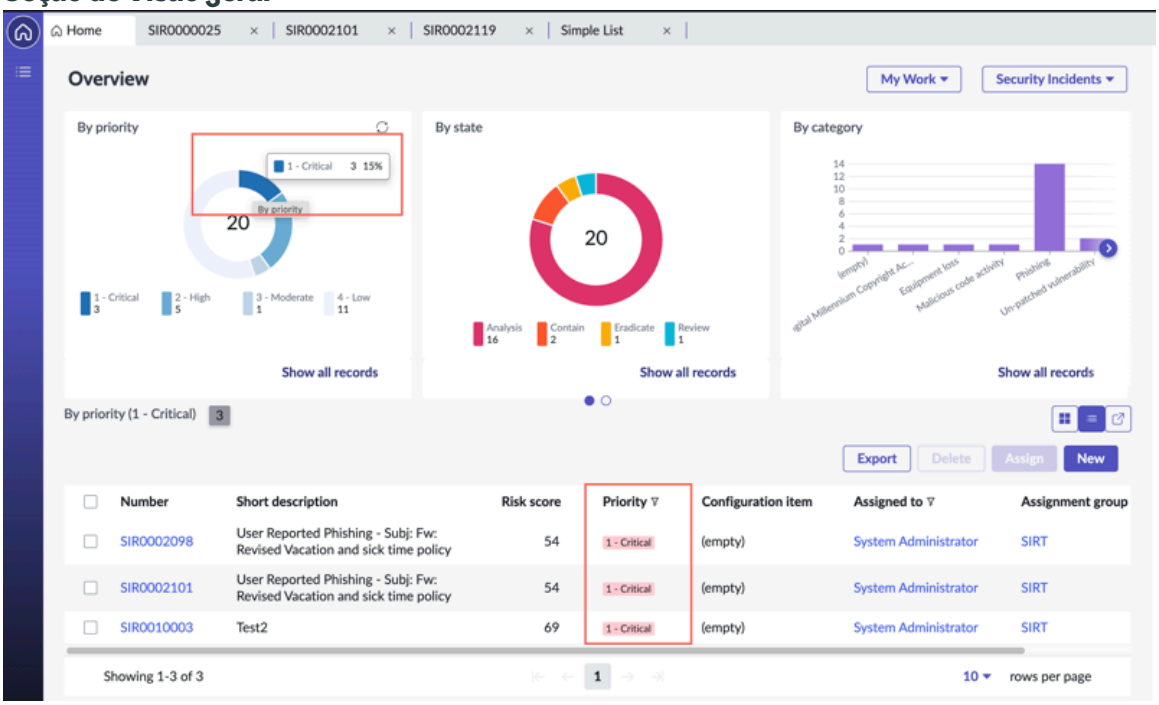
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando filtros são aplicados nos widgets, a metade inferior da página de visão geral é preenchida com os incidentes de segurança correspondentes ou tarefas de resposta apresentadas como cartões ou itens de lista. O analista pode alternar entre a exibição de cartão ou a exibição de lista conforme desejado.

Por exemplo, em **Prioridade** se você quiser selecionar todos os incidentes críticos ou tarefas de resposta, clique em **Crítico** o segmento (exemplo de captura de tela abaixo) do widget e os incidentes ou tarefas de resposta que são críticos são exibidos na exibição de lista ou cartão.

Seção de Visão geral

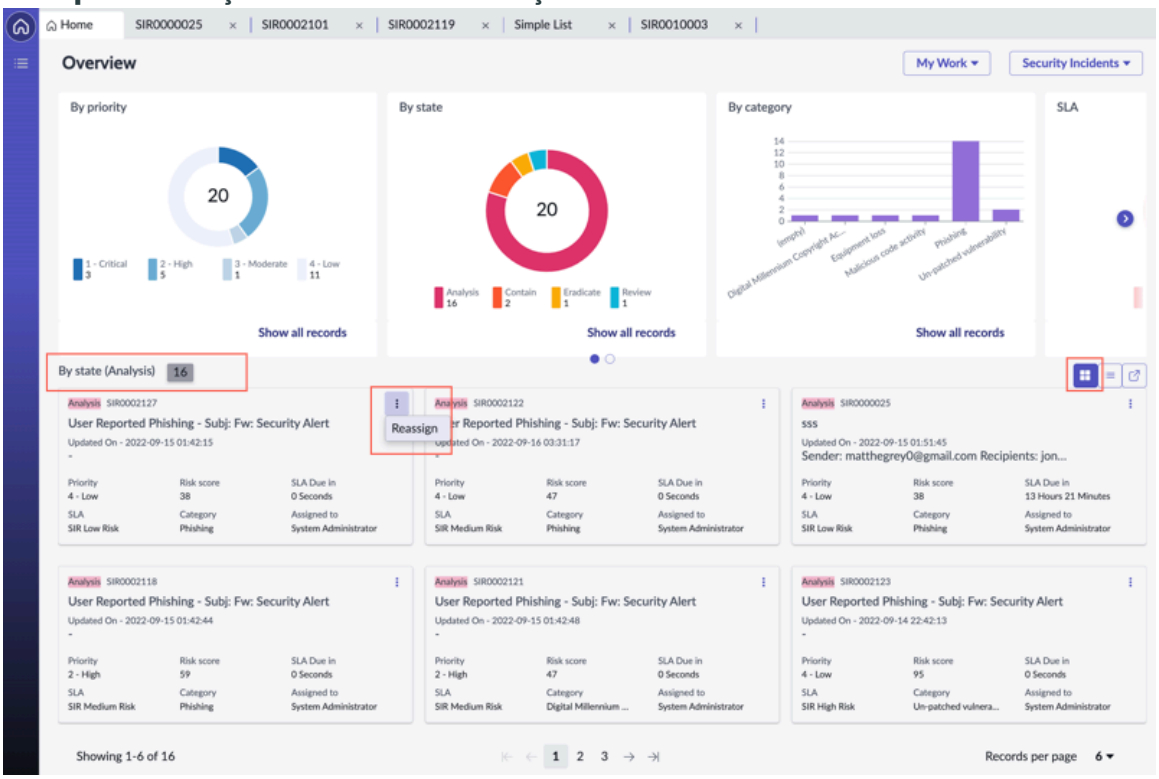


Você pode atribuir ou reatribuir os incidentes de segurança ou tarefas de resposta diretamente nesta exibição clicando no ícone de reticência e selecionando **Atribuir** (opção na exibição de cartão) ou diretamente o. **Atribuir** botão (opção na exibição de lista) para atribuir um incidente.

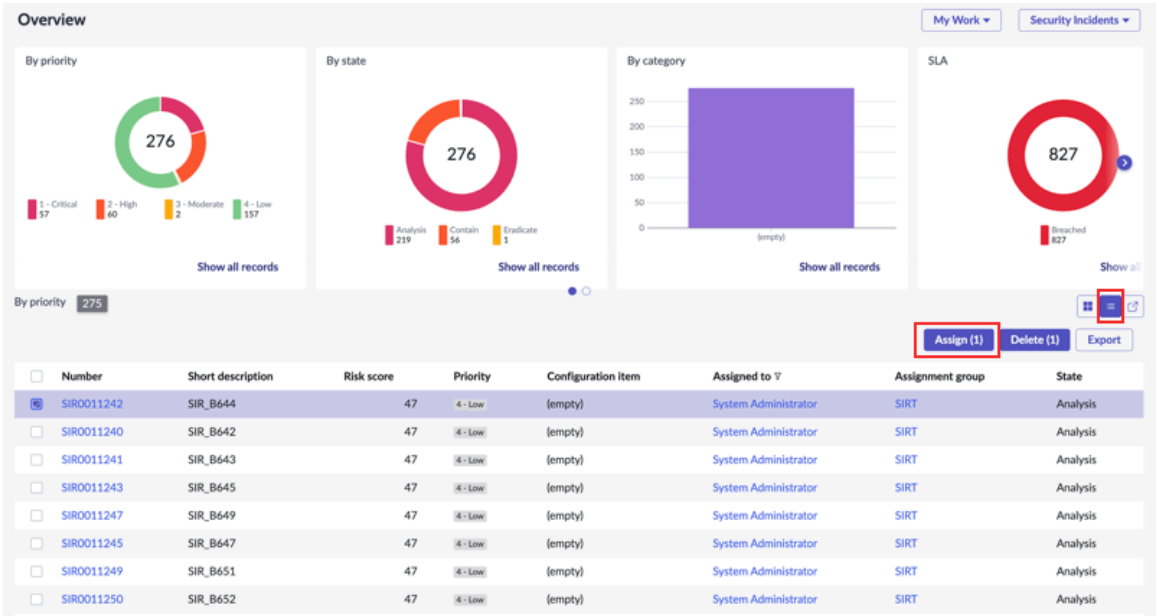
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de exibição de cartão e reatribuição



Atribuir incidente

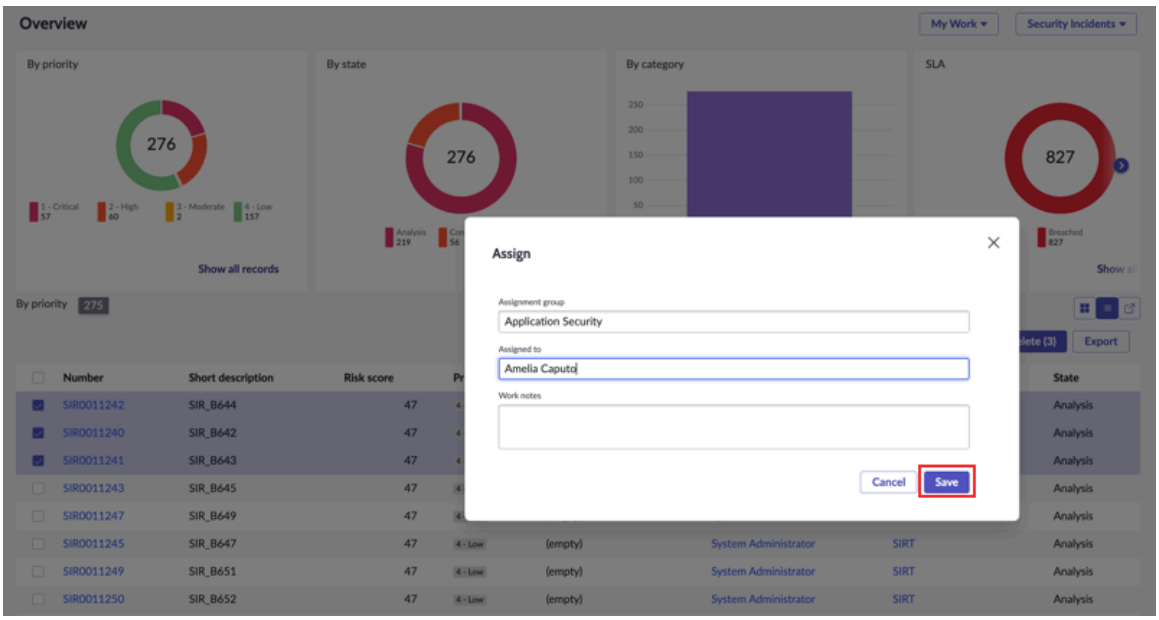


Este é um exemplo da exibição de lista. O usuário também pode atribuir incidentes na exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuir incidente



Adicionar Ou modifique os detalhes do designado, como Grupo de atribuição e Atribuído a, adicione anotações de trabalho, se necessário.

Nota: Você pode atribuir um ou mais incidentes de segurança ou tarefas de resposta aos grupos de atribuição. O número selecionado é exibido no **Atribuir** botão.

O usuário pode excluir incidentes de segurança desta exibição. Clique em **Excluir** para excluir o incidente de segurança, o registro será excluído da exibição de lista.

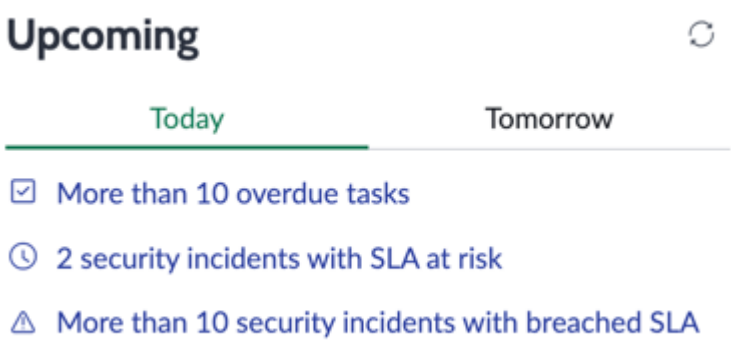
O usuário também pode exportar o conteúdo da lista. Clique em **Exportação** botão para exportar a lista no formato desejado.

Seção A seguir

Esta seção exibe as próximas tarefas, como incidentes de segurança e tarefas de resposta que vencem no mesmo dia e no dia seguinte.

A lista de incidentes de segurança e tarefas de resposta exibida é baseada no campo Data de vencimento e na definição de ANS definidos para esses registros.

Se esta seção contiver mais de um incidente de segurança ou tarefa de resposta, o incidente ou os registros abrirão todos esses registros em uma nova guia.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir tarefas futuras

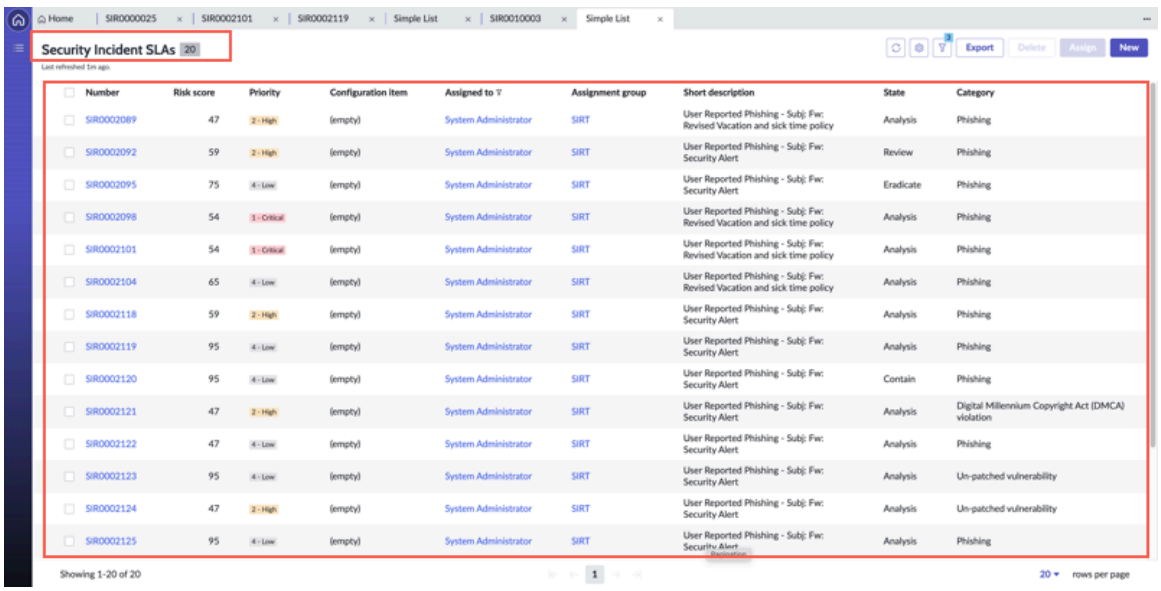
O analista de segurança pode exibir as próximas tarefas relacionadas aos incidentes de segurança e às tarefas de resposta que estão vencidas, atrasadas ou violadas o ANS definido.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Por vir**.
2. Clique em **Hoje** para exibir as tarefas que vencem no mesmo dia.
3. Selecione **Amanhã** para exibir as tarefas atrasadas para o dia seguinte.
   A seção Próximos lista os incidentes de segurança ou as tarefas de resposta que estão atrasadas com base na data de vencimento e que violaram a definição do ANS.
4. Clique em **Atualizar** ícone para atualizar a lista de próximas seções.
   Por exemplo, se você clicar no link, **Mais de 10 incidentes de segurança com ANS violado** Em seguida, a lista de incidentes de ANS violados é exibida em uma nova guia no espaço.



Nota: Você pode executar as operações Novo, Atribuir, Exportar e Excluir de qualquer exibição de lista.

Seção de links rápidos

Links rápidos funcionam como links de favoritos. Você pode adicionar URLs externos e acessá-los rapidamente de dentro do espaço.

Trabalhar com links rápidos

Adicione links rápidos para facilitar a referência.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

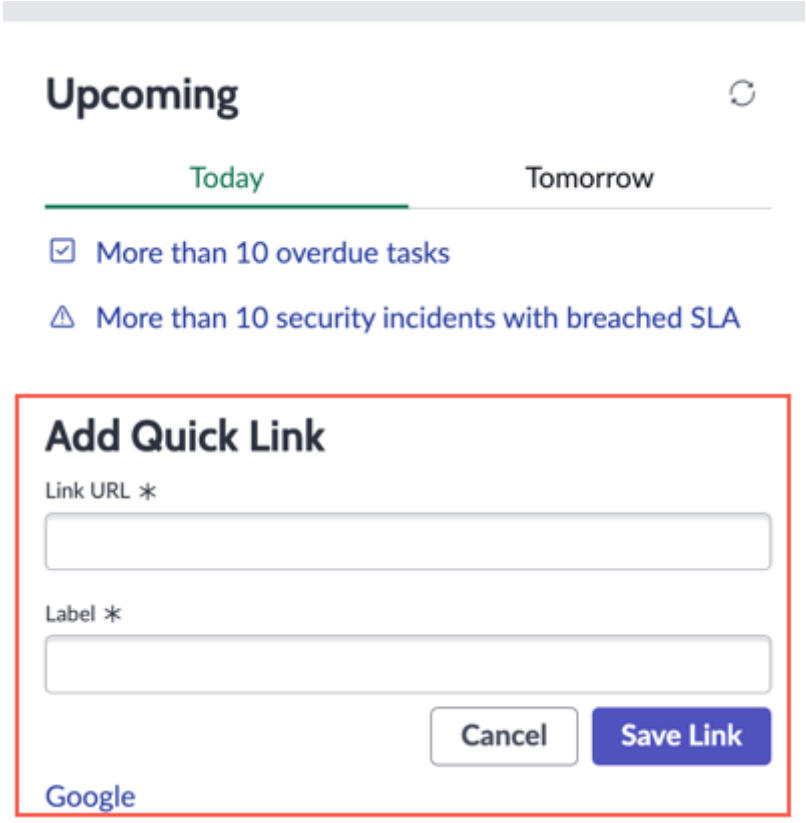
Você pode adicionar e modificar links rápidos úteis e marcar esses links que ajudam na resolução do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Links rápidos**.
2. Clique em **Adicionar link rápido** ícone para adicionar os links.
3. Insira o link para o URL e o Rótulo.
4. Clique em **Salvar link** .



O novo link é adicionado abaixo da seção de links rápidos.

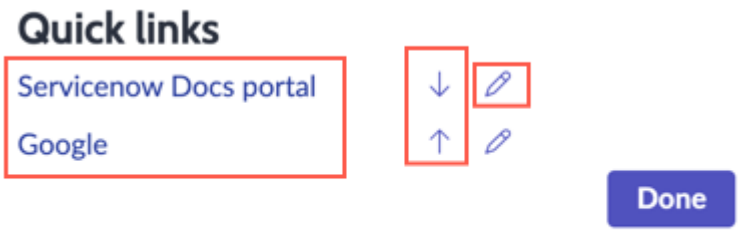
5. **Para modificar ou excluir os links:**

   a. Clique em **Editar link** ícone.

   b. Modifique o link desejado ou o texto de exibição que é o rótulo da URL.

   c. Clique em **Salvar**.

   d. Clique em **Concluído**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Utilize as setas para cima e para baixo para mover a posição dos elos.

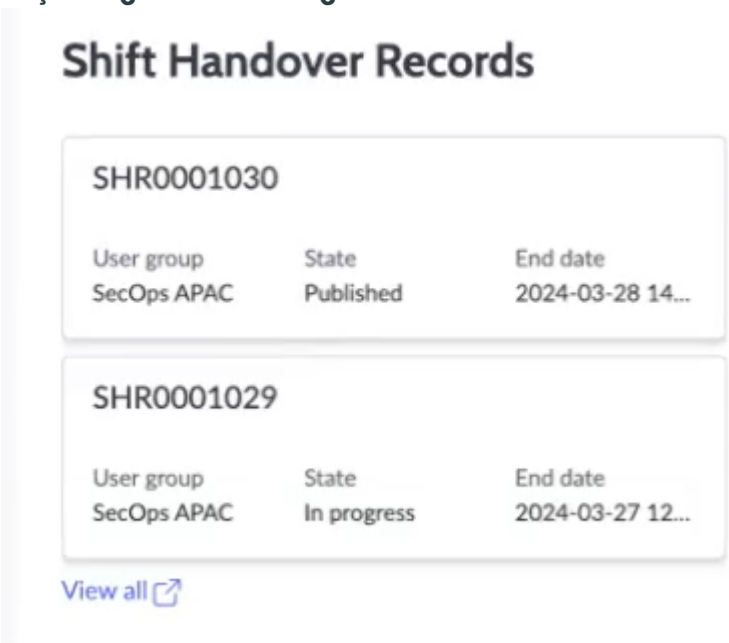
f. Clique em **Excluir** para excluir os links marcados durante a edição.

Seção Registros de entrega do turno

A seção exibe a lista de registros de entrega de turno no Espaço de resposta a incidentes de segurança.

A seção Registros de entrega de turno no Espaço de resposta a incidentes de segurança exibe os dois últimos registros de entrega de turno com base nos campos Data de término, Estado e Grupo de usuários definidos para esses registros. Para exibir todos os registros de entrega de turno, selecione **Exibir tudo** .

Seção Registros de entrega do turno



Exibição de lista em Espaço SIR

A exibição de lista consiste nos incidentes de segurança, tarefas de resposta, e-mails de phishing e avaliações.

A exibição de lista tem filtros pré-aplicados, como Atribuído a mim, Atribuído à equipe, Não atribuído, Todos em aberto, Todos, e assim por diante.

Usando essas categorias de lista e listas filtradas, os analistas podem encontrar rapidamente os registros de Incidentes de segurança e Tarefas de resposta necessários nos quais precisam trabalhar.

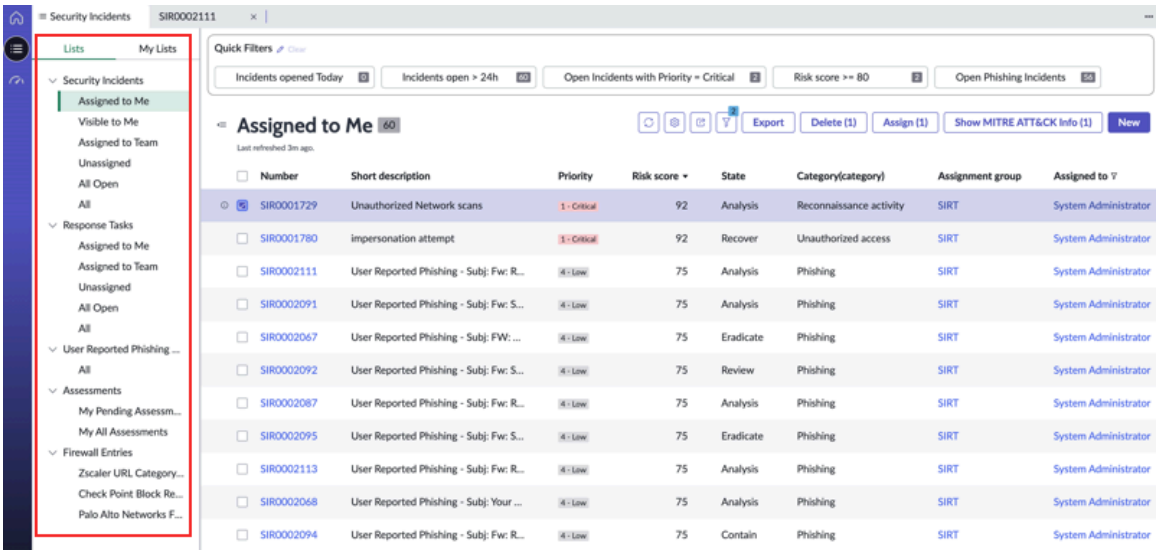
Para acessar a exibição de lista, você precisa clicar no ícone de lista ( ). Quando você clica em um registro em uma exibição de lista, o registro é aberto em uma nova guia.

Tipos de listas

A seguir, você tem um exemplo de exibição das listas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O painel de lista contém as seguintes seções:

Listas

Item de lista	Descrição	Capacidade
Incidentes de segurança	Exiba a lista de incidentes de segurança e navegue até o incidente desejado para começar a trabalhar neles. As seguintes listas estão disponíveis: • **Visível para mim** Incidentes de segurança visíveis para o usuário conectado. • **Atribuído a mim** Incidentes de segurança atribuídos ao analista. • **Atribuído à equipe** Incidentes de segurança atribuídos a todas as equipes às quais os analistas pertencem. • **Não atribuído** : Lista de incidentes de segurança não atribuídos. • **Todos abertos** : Lista de todos os incidentes de segurança em aberto. • **Todos** : Lista de todos os incidentes de segurança.	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidente. • O analista pode selecionar um ou mais incidentes de segurança e atribuir esses incidentes aos outros usuários. • O analista pode excluir os incidentes de segurança. • O analista pode criar um novo incidente de segurança. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando em **Filtros rápidos** em vez de usar o avanço **Filtro** opção. Usando os filtros rápidos, você pode filtrar rapidamente a lista de incidentes de segurança que precisam de atenção imediata. Para obter mais informações, consulte Trabalhar com filtros rápidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
		• Os analistas podem atualizar a lista de incidentes. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF.
Registros de transferência de turno	Exiba a lista de registros de entrega de turno. As seguintes listas estão disponíveis: • **Atribuído à equipe** Registros de entrega de turno atribuídos a todas as equipes/grupos de usuários aos quais os analistas pertencem. • **Todos** : Lista de todos os incidentes de segurança.	A entrega de turno oferece suporte às três funções a seguir: • Administrador: Função de responsável pelo turno • Analista de segurança: Função de analista de turno • Gerente de segurança: Função de responsável pelo turno, mas não tem acesso ao grupo de usuários ao qual o registro de entrega de turno está atribuído. • Os usuários com a função Proprietário/analista de turno que fazem parte do grupo de usuários no turno ativo podem adicionar ou modificar conteúdo nos registros de entrega de turno no estado de rascunho. • Os usuários que não têm a função de responsável/analista de turno ou não fazem parte do grupo de usuários no turno ativo só podem exibir o conteúdo nos registros de entrega de turno.
Tarefas de resposta	Exiba a lista de tarefas de resposta e navegue até a tarefa de resposta desejada para começar a trabalhar nelas. A exibição de lista contém:	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Atribuído a mim** Tarefas de resposta atribuídas ao analista. • **Atribuído à equipe** Tarefas de resposta atribuídas às equipes aos quais os analistas pertencem. • **Não atribuído** : Lista de tarefas de resposta não atribuídas. • **Todos abertos** : Lista de todas as tarefas de resposta em aberto. • **Todos** : Lista de todas as tarefas de resposta.	• O analista pode selecionar uma ou mais tarefas de resposta e atribuir essas tarefas a outros usuários. • O analista pode criar uma nova tarefa de resposta. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando em **Filtros rápidos** em vez de usar o avanço **Filtro** opção. Usando os filtros rápidos, você pode filtrar rapidamente a lista de tarefas de resposta que precisam de atenção imediata. • Os analistas podem atualizar a lista de tarefas de resposta. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF. Para obter mais informações, consulte Exportar incidentes de segurança ou tarefas de resposta.
E-mails de Phishing	Exiba a lista de todos os e-mails de phishing. A exibição de lista será classificada com base na última atualização.	• Relatar e-mail de phishing. Para obter mais informações, consulte Relatar E-mail de Phishing sobre como denunciar um e-mail de phishing. • Excluir e-mails de phishing. • Exporte a exibição da lista de e-mails de phishing para os formatos Excel, CSV, JSON e PDF.
Avaliações	Exiba a lista de avaliações necessárias para executar a revisão pós-incidente.	Fazer avaliações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Minhas avaliações pendentes** : Lista de avaliações pendentes. • **Todas as minhas avaliações** : Lista de todas as avaliações.	

Personalize uma lista

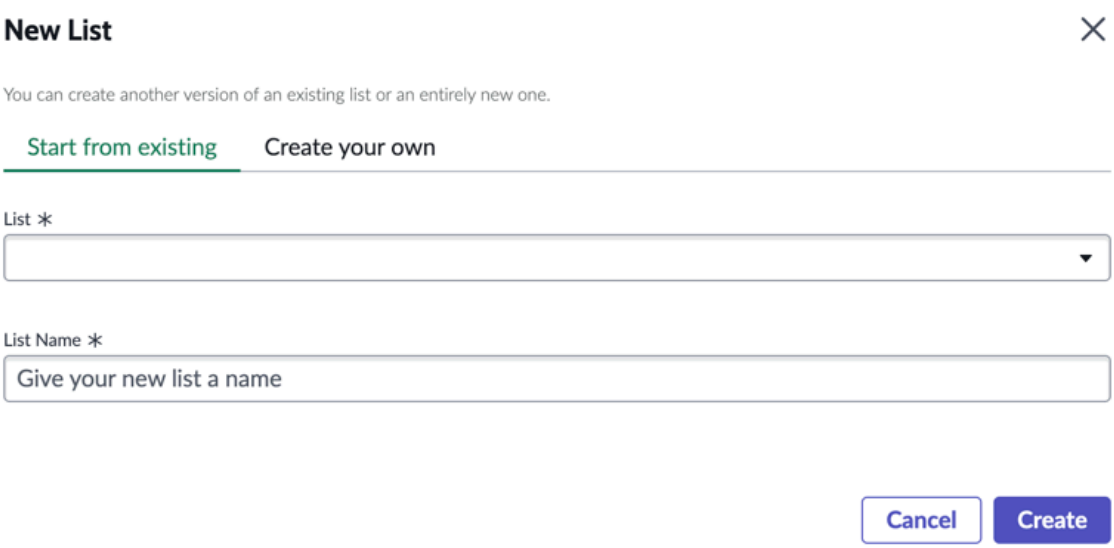
Os analistas ou gerentes de segurança podem personalizar os incidentes de segurança ou as tarefas de resposta ou a exibição de lista personalizada de e-mails de phishing com base em suas preferências individuais.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique em **Exibição de lista** .
3. Clique **Minhas listas**.
4. Clique em **Adicionar nova lista** , disponível na parte inferior de **Minhas listas** exibir.



Os analistas de segurança podem criar outra versão de uma lista existente ou uma lista personalizada totalmente nova.

5. **Para criar a partir de uma exibição de lista existente:**

   a. Clique em **Começar a partir de existente** link.

   b. Selecione **Lista** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

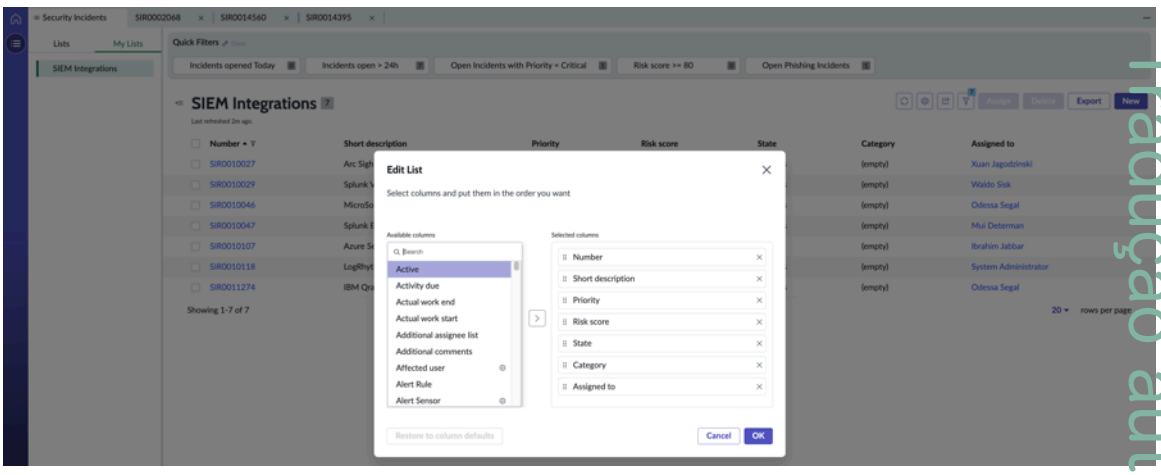
Nota: Qualquer que seja a lista selecionada na lista suspensa, o nome da lista será a cópia da sua Lista principal. Por exemplo, se você selecionar **Atribuído a mim** Na seção Incidentes de segurança, o nome da lista será **Cópia Atribuída a Mim** da seção incidentes de segurança.

c. Selecione as colunas a serem personalizadas e adicione filtros.
Crie um filtro adicionando condições que contenham um campo, operador e valor(es).

d. Clique em **Criar**.

Nota: Para personalizar sua própria exibição de lista, você pode adicionar colunas personalizadas, filtros, definir condições e classificar pela ordem conforme necessário.

e. Depois que uma exibição de lista personalizada for criada, clique no ícone de engrenagem e personalize as colunas da lista escolhendo **Editar colunas** opção para editar as colunas e colocá-las na ordem que preferir.



Você também pode:

- **Renomear** a exibição de lista personalizada.
- **Excluir** a exibição de lista personalizada.
- Salve a exibição de lista personalizada conforme desejado usando **Salvar como** opção.
- **Redefinir largura** da exibição de lista.

Nota: Você também pode executar diretamente essas operações usando os outros botões Ações de lista, como atribuir, excluir e exportar a exibição de lista fornecida.

6. Para criar sua própria lista:

a. Clique em **Crie o seu próprio** link.

b. Forneça um **Nome da lista** .

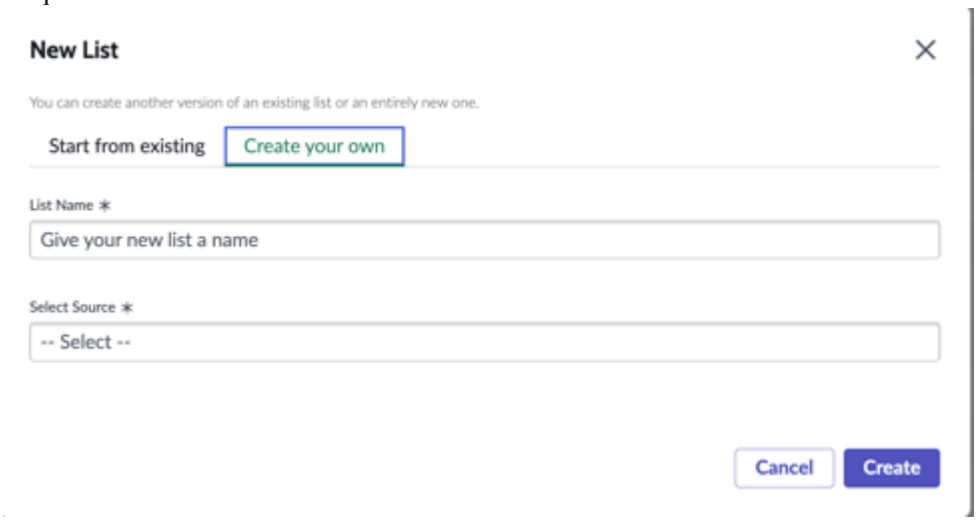
c. Selecione **Origem** e. **Colunas** .

d. Adicionar filtros.
Crie um filtro adicionando condições e forneça a ordem em que a lista deve ser exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Clique em **Criar**.



Uma nova lista é criada conforme definido e personalizada por você abaixo de **Minhas listas** seção.

Nota: você pode **Reordenar** sua exibição personalizada movendo suas posições.

Atribuir incidentes de segurança

Atribuir incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

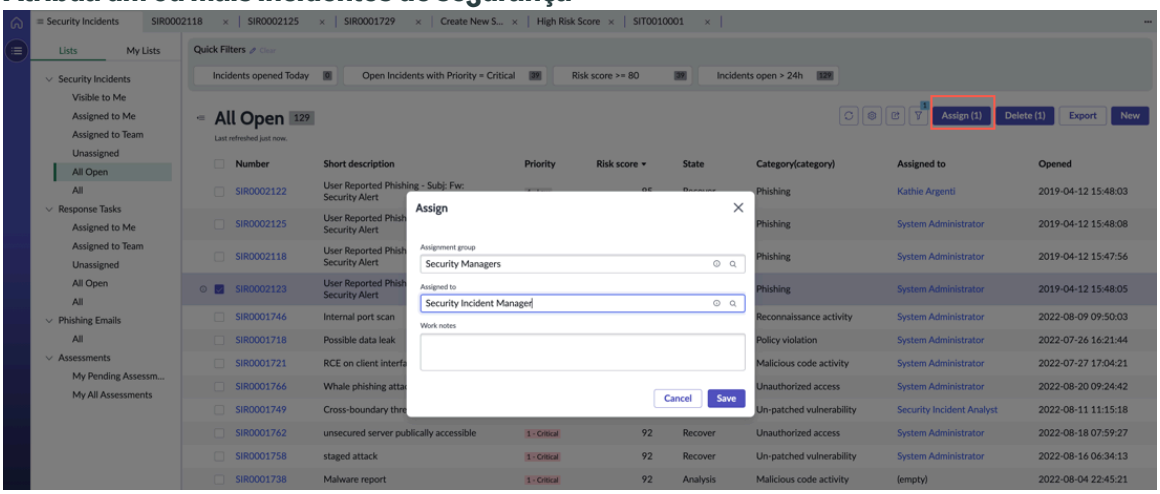
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique na lista (ícone).
3. Clique em **Listas** .
4. Por exemplo, acesse **Incidentes de segurança** > **Todos em aberto**.
5. Selecione um ou mais incidentes de segurança.
6. Clique em **Atribuir** .
7. Preencha os detalhes, como Grupo de atribuição, Atribuído a e adicione anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Salvar**.

Atribua um ou mais incidentes de segurança



Encerrar múltiplos incidentes de segurança

Feche vários incidentes de segurança ao mesmo tempo, para evitar a necessidade de fechar incidentes relacionados individualmente , como incidentes criados com uma causa raiz comum ou falso-positivo incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione L ícone ist ( ).
3. Selecione **Listas** .
4. Selecionar **Incidentes de segurança** > **Todos em aberto**.
5. Selecione um ou mais incidentes de segurança para fechar e selecione **Fechar** .
   Os incidentes de segurança são encerrados em massa janela exibido links para listas de acesso dos incidentes de segurança selecionados para serem encerrados.
   - Se pelo menos um incidente de segurança selecionado tiver atividades pendentes, como tarefas ativas, playbooks, SIs secundários, avaliações ou fluxos ativos, . **Incidentes de segurança com tarefas ativas, playbooks, SIs secundários, avaliações e fluxos ativos** é exibido.
   - Se pelo menos um incidente de segurança selecionado para fechamento não tiver atividades de fechamento pendentes, o **Incidentes de segurança prontos para serem encerrados** . d é exibido ed .
6. **Opcional:** Revise os incidentes de segurança com atividades pendentes .

   Nota: Se você não fechar manualmente nenhuma atividade pendente, elas serão encerradas automaticamente se você prosseguir com o fechamento em massa.

   a. Feche todas as tarefas, playbooks, SIs secundários, avaliações e fluxos ativos ativos.
   b. Selecione **Leve-me de volta** para retornar ao Feche em massa a janela de incidentes de segurança .
7. Selecione **Avançar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione o aplicável **Código de fechamento** .
9. Insira **Fechar anotações** .
10. Selecione **Fechamento em massa** .
    A atividade de fechamento do incidente é executada em . plano de fundo.

Atribuir tarefas de resposta

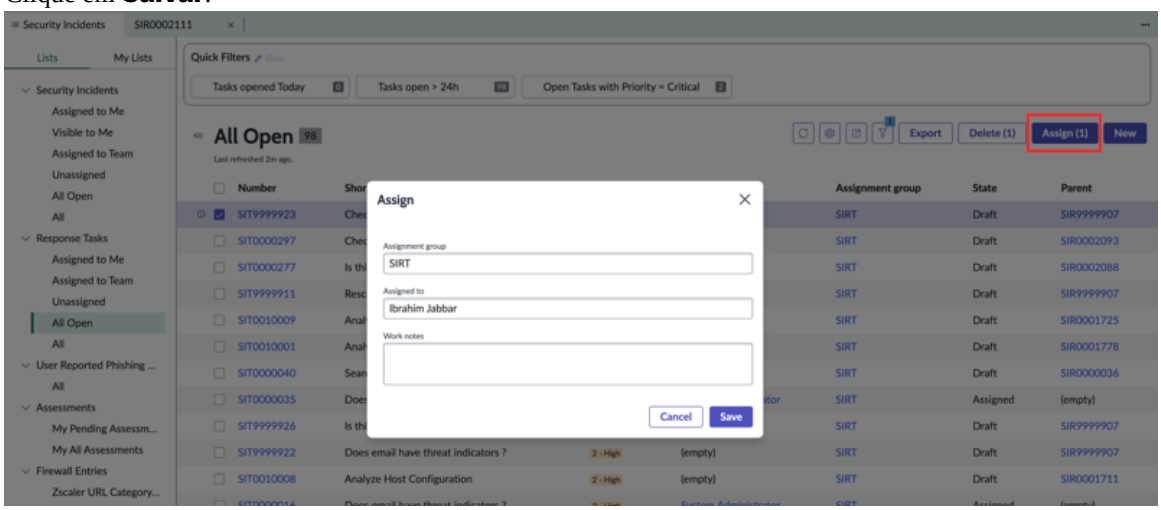
Atribuir tarefas de resposta para um problema de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique na lista (ícone).
3. Clique em **Listas** .
   Por exemplo, acesse **Tarefas de resposta** > **Todos em aberto**.
4. Selecione uma ou mais tarefas de resposta.
5. Clique em **Atribuir** .
6. Preencha os detalhes, como Grupo de atribuição, Atribuído a e adicione anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.
7. Clique em **Salvar**.



Relatar E-mail de Phishing

Relate e-mails de phishing na exibição de listas.

Antes de Iniciar

Função necessária: sn_si.analyst

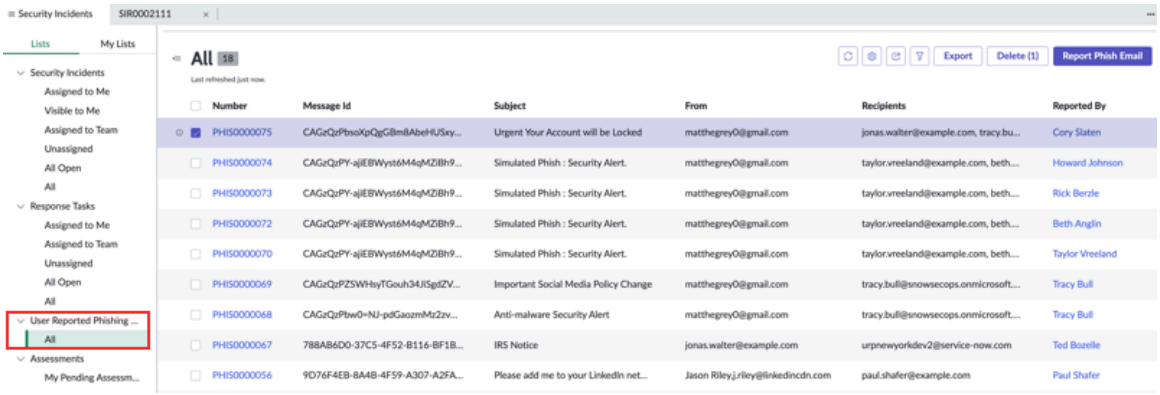
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique na lista (ícone).
3. Ir para **E-mails de phishing relatados por usuário** > **Tudo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A lista de e-mails de phishing relatados pelo usuário é exibida.



4. Clique em **Relatar e-mail de phishing** botão.
   Denunciar um e-mail de phishing carregando-o.
5. Clique em **Adicionar arquivo** para adicionar anexos.
6. Clique em **Upload** (Carregar).

> **Nota:** Denunciar um e-mail de phishing carregando os anexos. Você pode carregar apenas um e-mail de phishing de uma vez e deve estar no formato .eml.

7. Clique em **Enviar**.
   O e-mail de phishing para registrar um incidente de segurança é criado.

Trabalhar com filtros rápidos

Filtros rápidos são filtros de fácil acesso que estão disponíveis nas listas de incidentes de segurança e tarefas de resposta.

Antes de Iniciar
Função necessária: sn_si.admin

. Espaço SIR fornece o recurso de filtros rápidos que permite filtrar a lista de incidentes de segurança ou tarefas de resposta com facilidade.

Você pode usar filtros rápidos para configurar novos filtros ou modificar filtros existentes que aparecem nessas listas. O sistema de base fornece os seguintes filtros rápidos para cada incidente de segurança:

- **Incidentes em aberto hoje**
- **Incidentes em aberto > 24 horas**
- **Incidentes em aberto com prioridade: Crítico**
- **Risco > 80**
- **Incidentes de phishing em aberto**

O sistema de base fornece os seguintes filtros rápidos para cada tarefa de resposta:

- **Tarefas em aberto > 24h**
- **Tarefas em aberto com prioridade igual a Crítica**

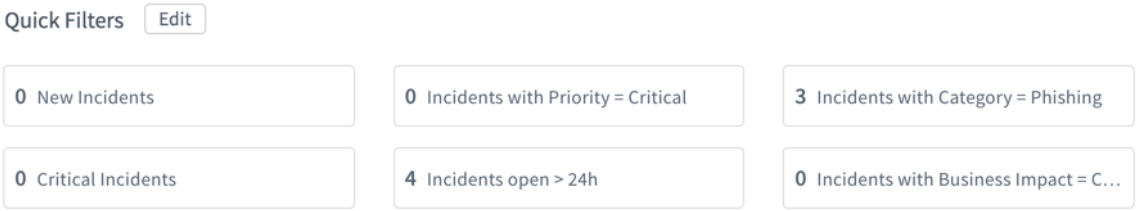
> **Nota:** Um administrador pode configurar a lista necessária de filtros rápidos de acordo com a necessidade da organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Definição do Sistema** > **Tabelas**.
2. Pesquisar **Filtros rápidos** (sn_si_aw_quick_filters).

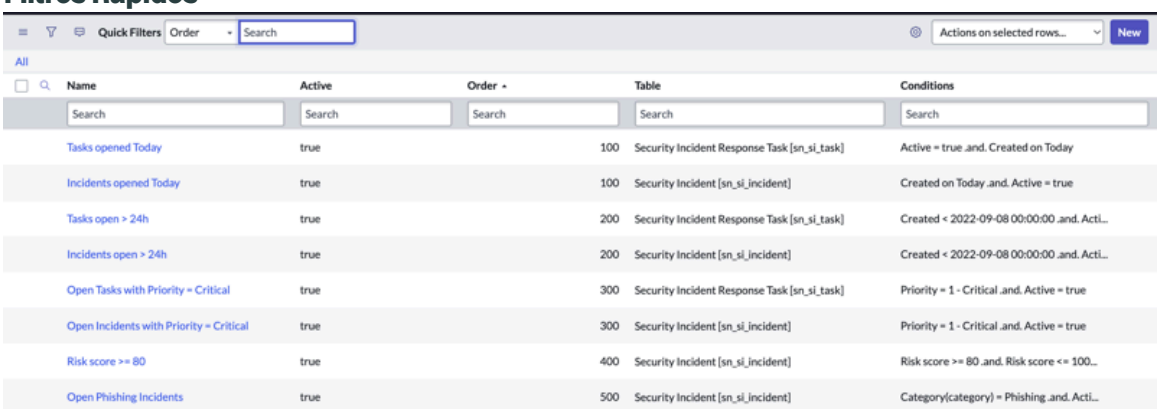


3. Ir para **Links relacionados** > **Mostrar lista** seção.
. **Filtros rápidos** a página de lista é exibida. OOTB, a seguir está a lista de filtros rápidos enviados com a aplicação.

Nome	Tabela	Valor
Tarefas abertas hoje	Tarefa de incidente de segurança [sn_si_task]	Verdadeiro(a)
Incidentes abertos hoje	Incidente de segurança [sn_si_incident]	Verdadeiro(a)
Tarefas em aberto > 24h	Tarefa de resposta de incidente de segurança [sn_si_task]	Verdadeiro(a)
Incidentes em aberto > 24h	Incidente de segurança [sn_si_incident]	Verdadeiro(a)
Tarefas em aberto com prioridade igual a Crítica	Tarefa de resposta de incidente de segurança [sn_si_incident]	Verdadeiro(a)
Incidentes em aberto com Prioridade Crítica	Incidente de segurança [sn_si_incident]	Verdadeiro(a)
Pontuação de risco > 80	Incidente de segurança [sn_si_incident]	Verdadeiro(a)
Incidentes de phishing em aberto	Incidente de segurança [sn_si_incident]	Verdadeiro(a)

Nota: O administrador de segurança pode prosseguir e configurar esses filtros rápidos. De acordo com a necessidade de negócios, o administrador pode modificar o valor existente para falso e criar um novo filtro rápido.

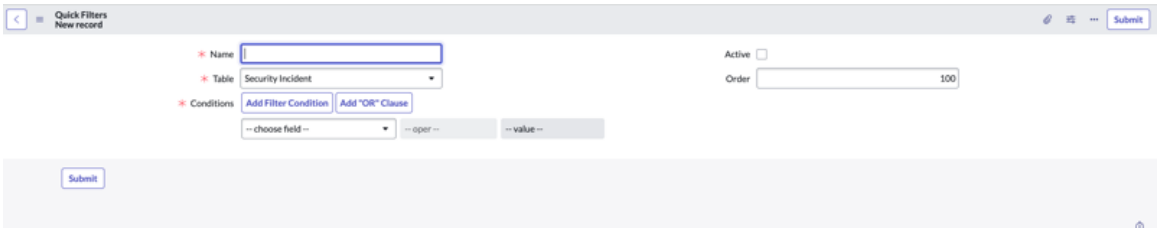
Filtros Rápidos



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

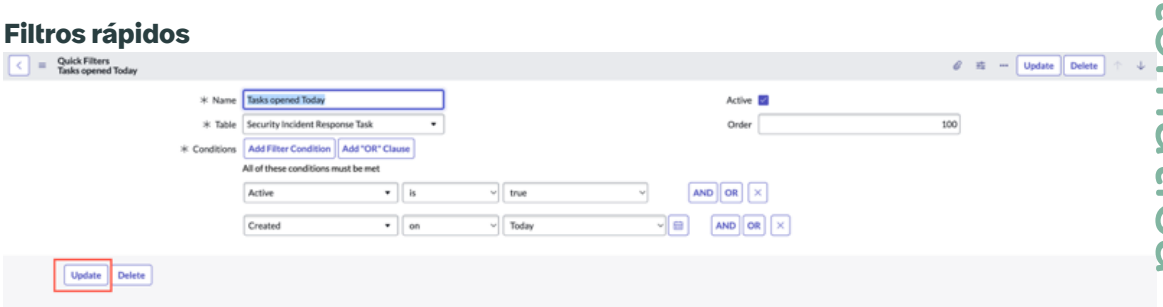
4. Clique em **Novo** para criar um novo filtro.
5. Insira um nome para o filtro, selecione a Tabela e especifique a condição do filtro.
6. Clique em **Enviar** para retornar à página da lista anterior.
   Você verá o filtro recém-adicionado listado na página.



Nota:

- O filtro rápido será aplicável somente se **Ativo** a caixa de seleção está marcada.
- No espaço, qualquer usuário conectado pode personalizar os filtros rápidos ativos que estão disponíveis na aplicação. Os usuários podem ocultar ou exibir os filtros rápidos recém-criados. Este recurso é baseado na preferência do usuário.
- Se um usuário modificou as preferências de filtros rápidos e um novo filtro rápido for criado depois disso, se o filtro rápido estiver definido como ativo, ele não será aplicado à preferência do usuário. O usuário precisa mudar manualmente as preferências na exibição personalizada.

7. Selecione qualquer registro de filtro existente para modificar os filtros rápidos existentes.
8. Modifique o nome e a condição do filtro.
9. Clique em **Atualizar**.



Adicione ou modifique filtros rápidos

Adicione ou modifique filtros rápidos para incidentes de segurança ou tarefas de resposta na exibição de lista.

Antes de Iniciar

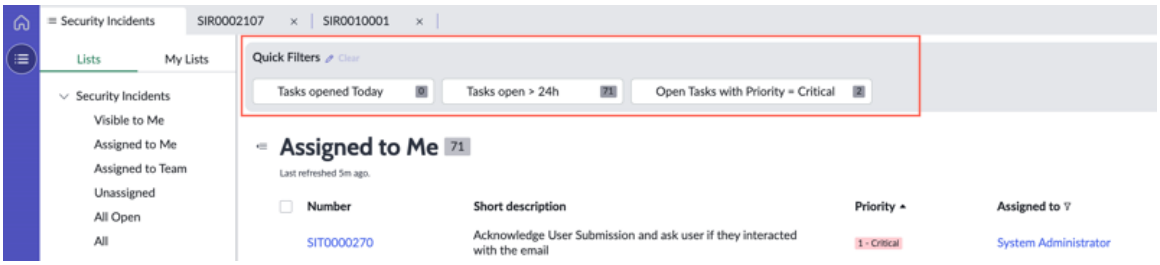
Função necessária: sn_si.basic

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique na lista (ícone).
3. Por exemplo, acesse **Listas** > **Incidentes de segurança** > **Filtros Rápidos** seção.

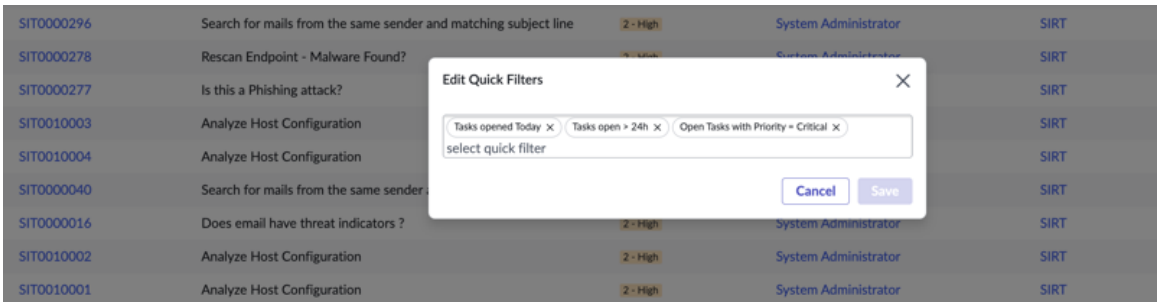
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Editar** ícone para fazer as mudanças.

> **Nota:** A mudança que você fizer persistirá e, quando o usuário retornar a esta página na próxima vez, a preferência persistente será exibida.



5. Clique em **Salvar**.

Exportar incidentes de segurança ou tarefas de resposta

Exporte os incidentes de segurança ou as tarefas de resposta da exibição de lista.

Antes de Iniciar

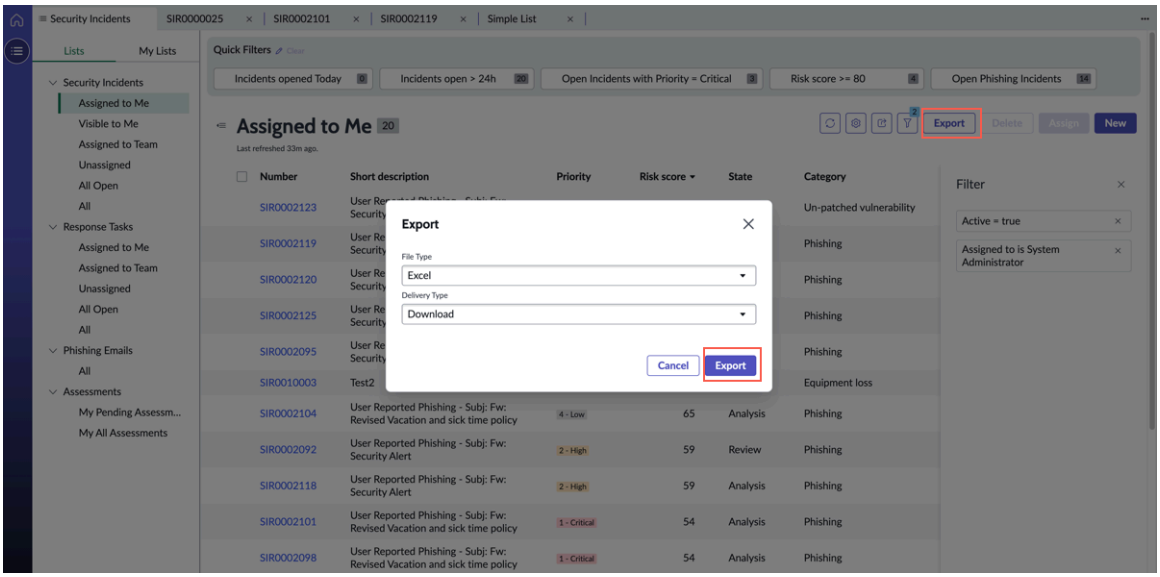
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique na lista ícone.
3. Clique em **Listas** .
4. Ir para **Incidentes de segurança ou tarefas de resposta** > **Todos em aberto**.
5. Exiba a lista e clique em **Exportação** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Tipo de arquivo** e. **Tipo de entrega** .
   Por exemplo, **Excel** e qualquer um **Download** ou **E-mail** a lista.
7. Clique em **Exportar**.
   O arquivo será baixado ou enviado por e-mail de acordo com a opção escolhida.

Gerenciar registros de entrega de turno

Use a exibição da lista de registros de Entrega de turno para criar, editar, copiar ou excluir registros de Entrega de turno. Cada registro de entrega de turno está associado a um Modelo de relatório de entrega de turno.

Antes de Iniciar

Função necessária:

- sn_escm_sh.shift_analyst: Requisito mínimo para acessar os registros de entrega de turno.
- sn_escm_sh.shift_owner: Crie, edite e exclua registros de log de entrega nos grupos de usuários dos quais o responsável pelo turno faz parte. Esta função herda a função sn_escm_sh.shift_analyst.
- sn_escm_sh.shift_analyst: Exibe todos os registros de log de Entrega de turno, mas pode contribuir somente com registros de Entrega de turno em andamento atribuídos ao grupo de Analistas de turno.
- sn_si.analyst - Herda a função sn_escm_sh.shift_analyst.
- sn_si.admin - Herda a função sn_escm_sh.shift_admin.
- sn_escm_sh.shift_admin - Herda a função sn_escm_sh.shift_owner

Importante: Para saber como configurar o Modelo de entrega de turno como administrador, consulte Configurar modelos de entrega de turno.

Por Que e Quando Desempenhar Esta Tarefa

O responsável pelo turno e a respectiva equipe ou grupo de usuários criam os registros de log de entrega do turno. O responsável pelo turno deve escolher o modelo de entrega de turno e o grupo de usuários que trabalharão no relatório de entrega de turno. Após a conclusão do relatório de entrega de turno, ele será compartilhado com o próximo responsável pelo turno ativo e a equipe.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontos principais do modelo de entrega de turno:

- Se algum outro analista da equipe de turno ativa já tiver atualizado o relatório antes de você e se as mudanças estiverem sendo processadas, talvez você veja uma mensagem de erro informando que há atualizações de conteúdo pendentes. Você deve aguardar 30 segundos e selecionar **Mude para o estado "Revisão"** novamente. Você pode ver o relatório consolidado no painel direito atualizado com o conteúdo atualizado de outros analistas.
- Se o responsável pelo turno modificou o conteúdo em uma seção no estado Revisão, o mesmo conteúdo será refletido para o analista quando o registro voltar para o estado Em andamento.
- O responsável pelo turno deve estar atento ao editar o conteúdo no estado Revisão e executar ações como mesclar duas linhas, mesclar duas seções, remover uma seção, pois isso afetará o relatório de Entrega de turno dos outros analistas.
- Depois de publicar o relatório de Entrega de turno, o responsável pelo turno pode modificar o conteúdo, mas não pode mudar o estado do registro.
- Quando alguém está modificando o conteúdo e durante esse tempo, se o estado do registro for alterado de Em andamento para Revisão, as mudanças de conteúdo não salvas serão descartadas.
- O administrador de turno terá acesso de gravação a todos os registros de log de entrega de turno, independentemente dos grupos de usuários.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione a Lista de incidentes de segurança  ícone.
3. Em **Listas** , selecione **Registros de entrega do turno** .
4. Selecione **Todos os registros** Para exibir a lista de todos os registros de Entrega de turno.
5. Selecione **Atribuído à equipe** Para exibir a lista de registros de entrega de turno atribuídos a todas as equipes/grupos de usuários aos quais os analistas pertencem.
6. Para criar um novo registro de Entrega de turno, selecione **Novo** .
7. No formulário, preencha os campos.

Registros de entrega de turno

Campo	Descrição
Número	Número exclusivo gerado automaticamente para um registro de Entrega de turno.
Modelo	O modelo de entrega de turno a ser usado. Por exemplo, Modelo de turno de amostra.
Descrição	Descrição do registro de entrega de turno.
Grupo de usuários	O grupo/equipe de usuários para o registro de entrega de turno a ser atribuído. Por exemplo, Revisores de código de desenvolvimento de equipe.
Estado	O estado atual do registro de Entrega de turno. Por padrão, o estado inicial é Rascunho

Tradução automática

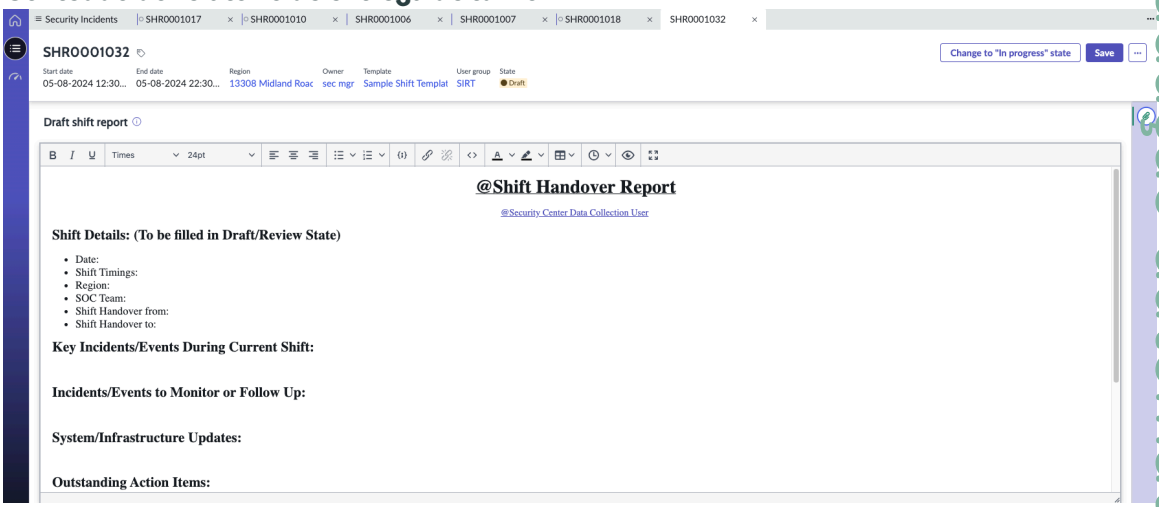
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O Estado não pode ser alterado durante a criação de um registro.
Nome do turno	O nome do turno que contém os detalhes de início e término do turno. Por exemplo, Turno do dia dos EUA.

8. Selecione **Criar**.
   Um novo registro de Entrega de turno é criado com base no modelo selecionado e adicionado à exibição de lista.
9. Abra o novo registro de Entrega de turno para atualizar o status e os detalhes dos incidentes de segurança no relatório de Entrega de turno.
   Por padrão, o registro de Entrega de turno está no **Rascunho** estado.

   Nota: Somente o responsável pelo turno pode modificar o conteúdo.

   Conteúdo do relatório de entrega de turno



10. No editor de relatório Rascunho de turno, use as seções do modelo de relatório de entrega de turno para atualizar os detalhes dos incidentes de segurança e usuários.

    Você pode formatar seu relatório com todas as opções no editor, como fontes, cores, marcadores, links, e anexos.

    Nota: O responsável pelo turno e o analista de turno podem modificar o conteúdo.

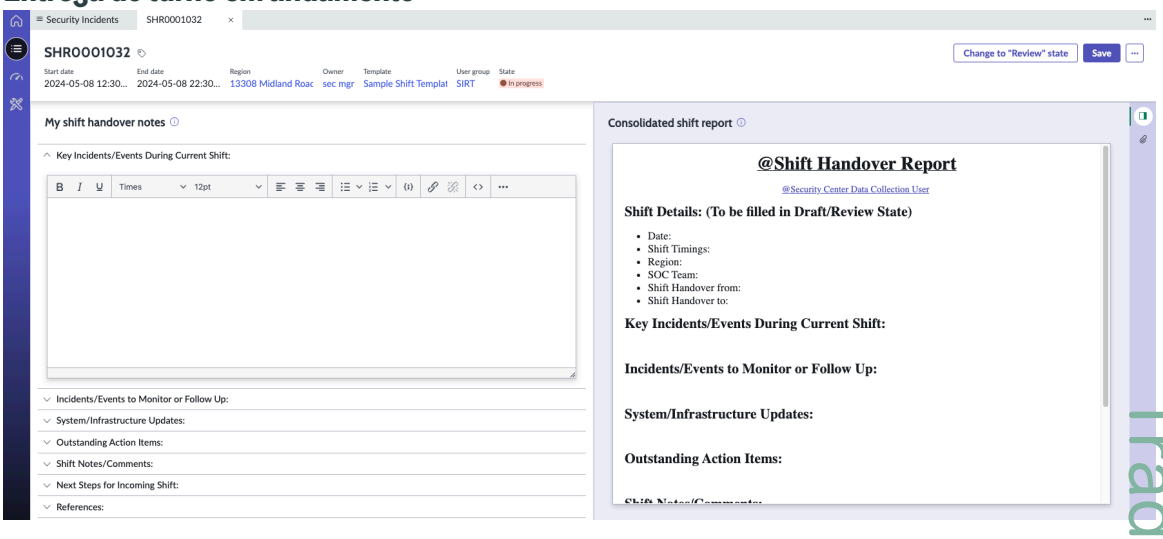
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Depois de fazer as mudanças necessárias no relatório de Entrega de turno, selecione **Salvar** .

b. Selecione **Mude para o estado "Em andamento"** Ação para mover o registro de Entrega de turno para o estado Em andamento.

Entrega do turno em andamento

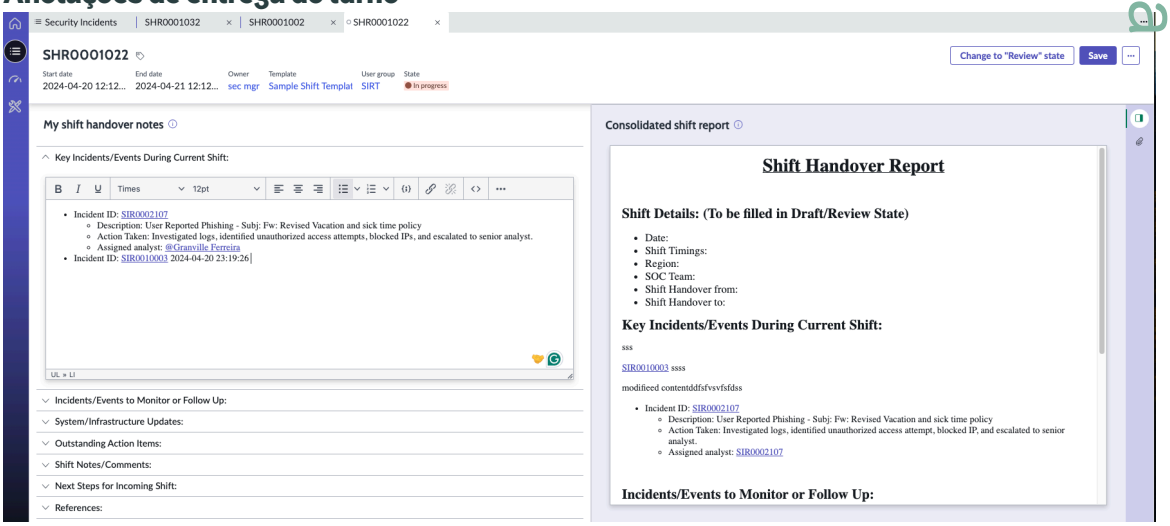


11. No editor de anotações de entrega do meu turno, atualize os detalhes necessários para todas as seções, como incidente de segurança e detalhes do usuário.

Nota: O responsável pelo turno e o analista de turno podem modificar o conteúdo.

a. Para mencionar um registro específico no editor, use **/** e escolha **Selecione um registro** e selecione um registro na lista de tabelas que aparece.
Por exemplo, se você selecionar **Incidentes de segurança** , em seguida, uma lista de incidentes de segurança será exibida. Selecione um incidente de segurança (**SIR0010025** Na lista e atualize os detalhes de entrega de turno necessários. Você também pode mencionar os campos associados ao incidente de segurança, como Descrição resumida, observação i st usando **/** após o número do incidente de segurança.

Anotações de entrega do turno



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Para mencionar um usuário específico no editor, use **/** e escolha **Selecione um usuário** e selecione um usuário na lista exibida.

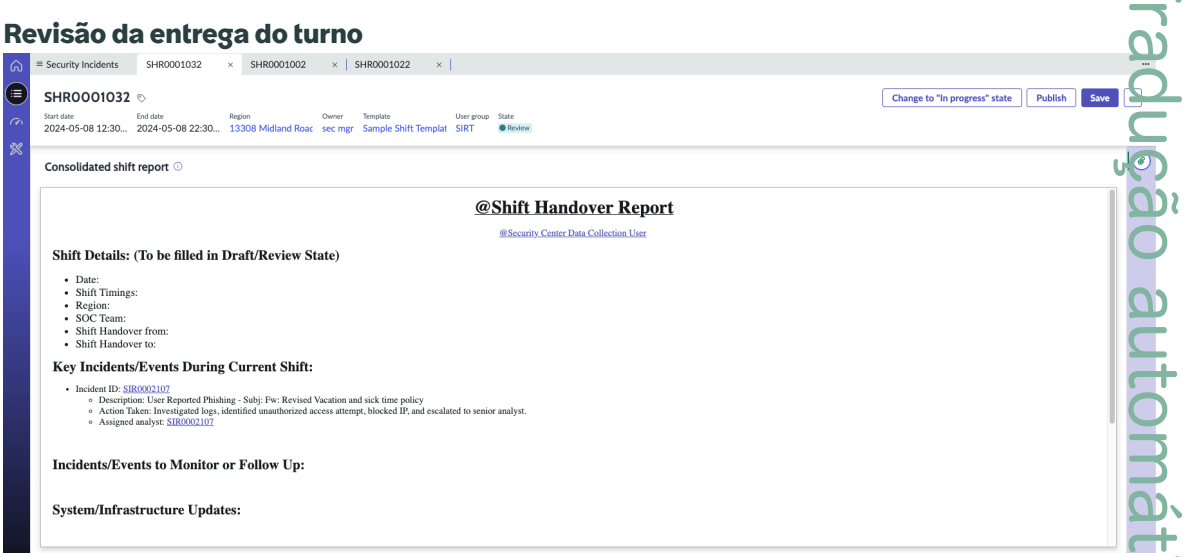
c. Para mencionar a contagem de registros no editor, use **/** e escolha **Contagem de menções** e selecione o registro na lista exibida.

d. Você pode formatar seu relatório com todas as opções no editor, como fontes, cores, marcadores, links, e anexos.

e. Depois de fazer as mudanças necessárias nas anotações de entrega de turno, selecione **Salvar** .

f. Selecione **Mude para o estado "Revisão"** Ação para mover o registro de Entrega de turno para o estado Revisão.

Nota: Se algum outro analista da equipe de turno ativa já tiver atualizado o relatório antes de você e se as mudanças estiverem sendo processadas, você poderá ver uma mensagem de erro. Aguarde alguns segundos e selecione **Mude para o estado "Revisão"** novamente.



12. No relatório de turno consolidado, revise o relatório de Entrega de turno e faça as mudanças necessárias.

Nota: Somente o responsável pelo turno pode modificar o conteúdo.

a. Depois de fazer as mudanças necessárias nas anotações de entrega de turno, selecione **Salvar** .

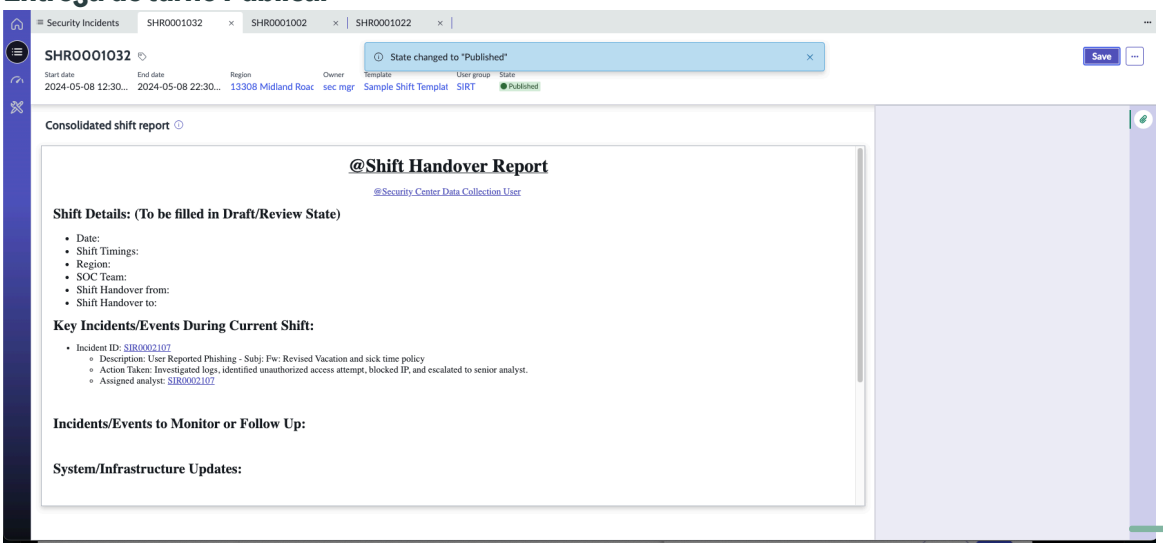
b. Se o relatório de Entrega de turno exigir mais atualizações dos analistas, você poderá selecionar **Mude para o estado "Em andamento"** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Selecione **Publicar** Ação para publicar o relatório de entrega de turno.

Entrega de turno Publicar



13. Selecione **Salvar** Para salvar o relatório de Entrega de turno.
Depois de salvar, você pode ver uma visualização do relatório de entrega de turno com suas atualizações mais recentes no painel de visualização.

Nota: Embora você possa visualizar as atualizações feitas no relatório de Entrega de turno imediatamente, os outros analistas podem levar alguns segundos para ver as mudanças.

14. Como responsável pelo turno, você também pode executar as seguintes ações na exibição de lista Entrega de turno.

a. Para editar um registro de Entrega de turno existente, selecione o registro e selecione **Editar** ação.
Você pode modificar somente a Hora de início, Hora de término, Descrição e Região.

b. Para criar uma cópia de um registro de Entrega de turno, selecione o registro e selecione **Criar cópia** ação.

c. Para excluir um registro de Entrega de turno existente, selecione o registro e selecione **Excluir** ação.

Configuração da Espaço SIR

Esta seção descreve as configurações necessárias para trabalhar com o. Espaço de resposta a incidentes de segurança.

Configure a exibição dos registros SIR

Esta seção descreve como as listas relacionadas são agrupadas e apresentadas na guia Registros relacionados DO SIR para facilitar a navegação.

Os usuários do espaço também podem pesquisar a lista relacionada por nome. Para obter mais informações sobre como configurar listas relacionadas, consulte Espaço SIR Registros relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar investigação de tempo de design de SI

Use esta seção para configurar a página Investigação de tempo de design de incidente de segurança para adicionar vários pontos de entrada e seus registros associados ao Espaço de resposta a incidentes de segurança.

Função necessária: sn_si.admin.

Os detalhes a seguir detalham as etapas envolvidas na configuração da página Investigação no Espaço de resposta a incidentes de segurança.

- Criando exibição para tabelas de informações associadas
- Adição de uma lista de pontos de entrada
- Exibição de mapeamento da lista Associar informações à lista de pontos de entrada
- Configure cada lista associada na exibição para lidar com a renderização de dados em tempo de execução

Tópicos relacionados

Explorar tela de investigação

Criando exibição para tabelas de informações associadas

A tela Investigação aproveita as exibições de lista relacionada criadas no incidente de segurança para configurar as listas associadas.

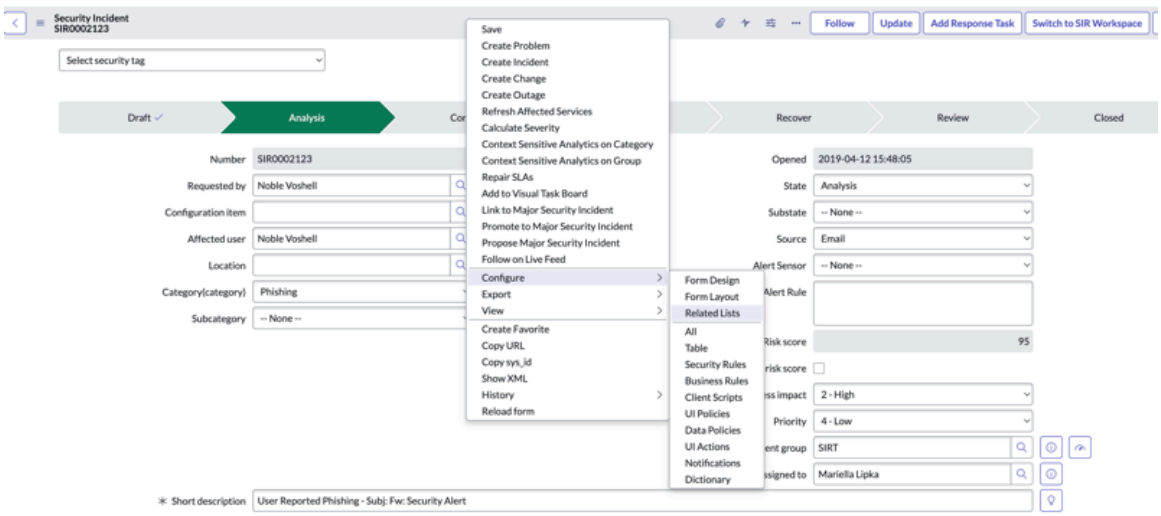
Antes de Iniciar

Função necessária: sn_si.admin

A seguir está um procedimento para criar uma exibição e adicionar listas relacionadas a ela.

Procedimento

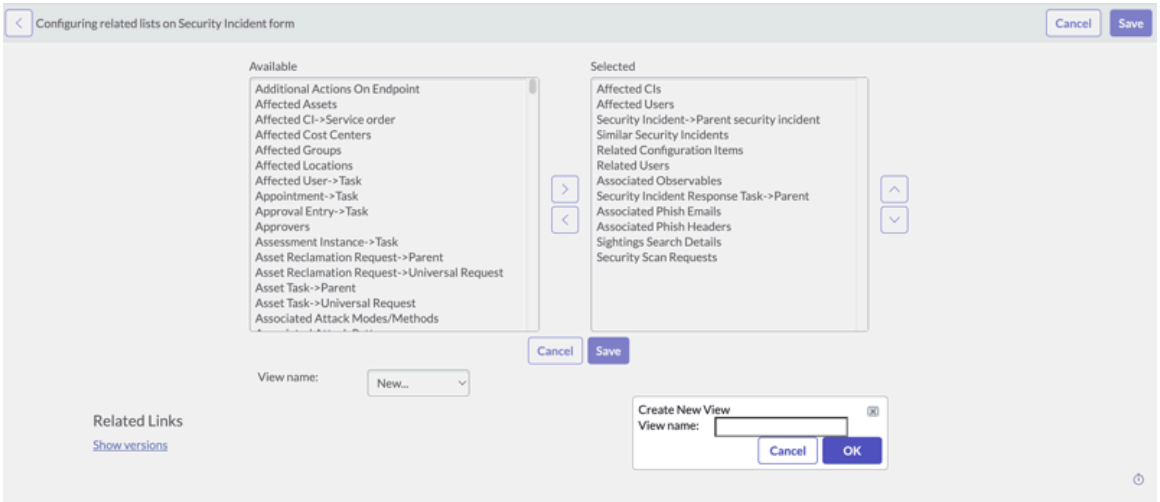
1. Navegue até **Incidente de segurança** lista.
2. Abra qualquer incidente de segurança na IU clássica.
3. No menu de contexto do formulário, navegue até **Configurar** > **Listas relacionadas**.
   A janela de bucket de lama é exibida.



4. Vá para **Nome da exibição** lista suspensa e clique em **Novo** para criar uma nova exibição.
   Você deve adicionar um nome à exibição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Adicione as listas relacionadas desejadas ao bucket direito na exibição recém-criada e salve a exibição. Esta exibição será usada para renderizar as informações associadas na guia Investigação.

Adição de uma lista de pontos de entrada

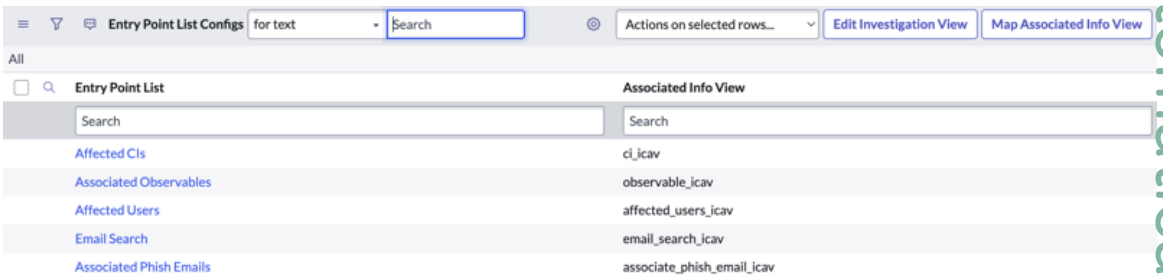
Configure a nova lista de pontos de entrada para adicioná-la à página Investigação.

Antes de Iniciar

Função necessária: administrador

Procedimento

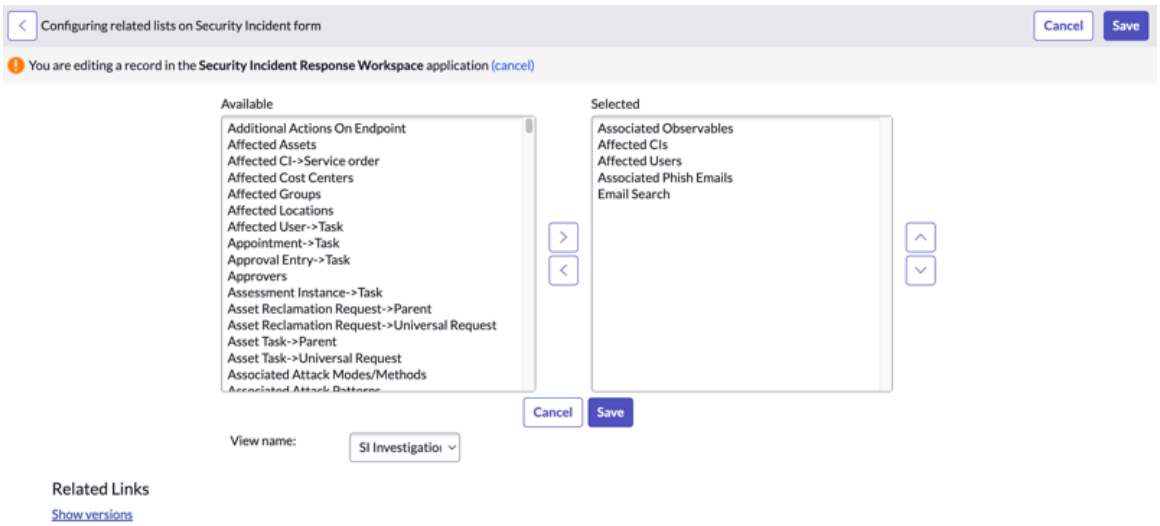
1. Navegar até **sn_si_aw_entry_point_config.list**.
   . **Listas de pontos de entrada** a página é exibida.



2. Clique em **Editar Exibição de investigação** botão para adicionar uma lista de pontos de entrada à tela de investigação.
   . **Configurar listas relacionadas no formulário Incidente de segurança** é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Adicione ou remova a lista de pontos de entrada da exibição de bucket de slush.
4. Clique em **Salvar**.

> **Nota:** A exibição correspondente à tela de investigação que contém as listas de pontos de entrada é chamada **Exibição de investigação de SI** e isso é selecionado por padrão quando você navega até **Editar Exibição de investigação** página.
>
> A ordem na qual as listas de pontos de entrada são exibidas na tela de investigação é determinada pela ordem na exibição selecionada do bucket de slush.

Exibição de mapeamento da lista Associar informações à lista de pontos de entrada

Mapeie a exibição de informações associada para a lista de pontos de entrada recém-adicionada usando a ação Mapear Exibição de informações associada.

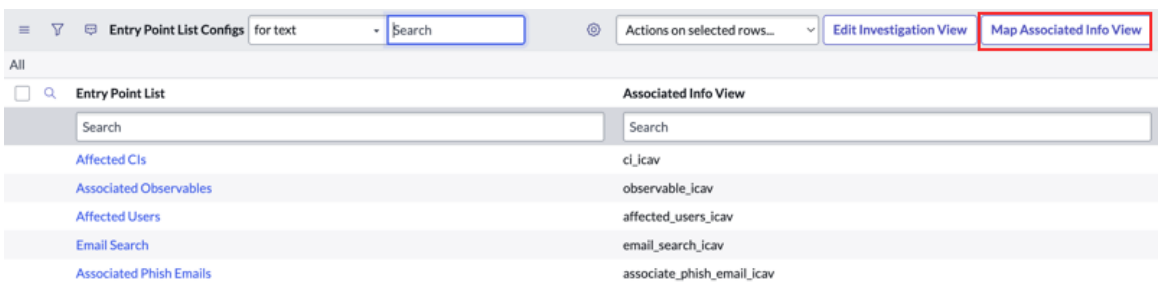
Antes de Iniciar

> **Nota:** Esta etapa é necessária para que a lista de pontos de entrada fique visível na página Investigação. Mesmo que você não queira que nenhuma lista de informações associada seja mostrada em um ponto de entrada, ainda será necessário criar uma exibição fictícia e mapeá-la.

Função necessária: administrador

Procedimento

1. Clique em **Exibição de informações associadas do mapa** botão no **Configurações do ponto de entrada** página.

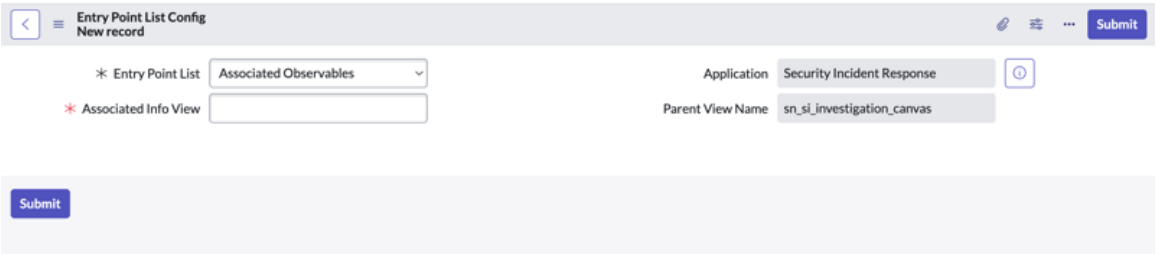


2. Selecione a lista de pontos de entrada recém-adicionados em **Lista de pontos de entrada** lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Insira o nome da exibição que contém as listas relacionadas de informações associadas no **Exibição de informações associadas** campo.
   Para obter informações sobre como criar uma exibição para as listas relacionadas de informações associadas, consulte Criando exibição para tabelas de informações associadas.



4. **Salvar** o formulário.
5. Se necessário, você pode adicionar ou remover mais listas associadas usando **Editar exibição de informações associadas** .
   Você também pode configurar o layout da lista de pontos de entrada usando **Editar layout da lista de pontos de entrada** ação. Adicione ou remova colunas do bucket de slush conforme desejado e salve o formulário.

Configure cada lista associada na exibição para lidar com a renderização de dados em tempo de execução

Configure cada lista associada na exibição para lidar com a renderização de dados em tempo de execução.

Antes de Iniciar

Nota: Esta etapa é obrigatória para cada lista associada configurada na exibição de informações associada. Caso contrário, a lista associada não estará disponível na página Investigação.

Cada uma das listas associadas adicionada (ao mapear uma exibição de informações associada para uma lista de pontos de entrada) Exibição de mapeamento da lista Associar informações à lista de pontos de entrada(ou da exibição diretamente) precisa de uma configuração adicional para filtrar os dados em relação à seleção de registro em tempo de execução e à seleção de filtros.

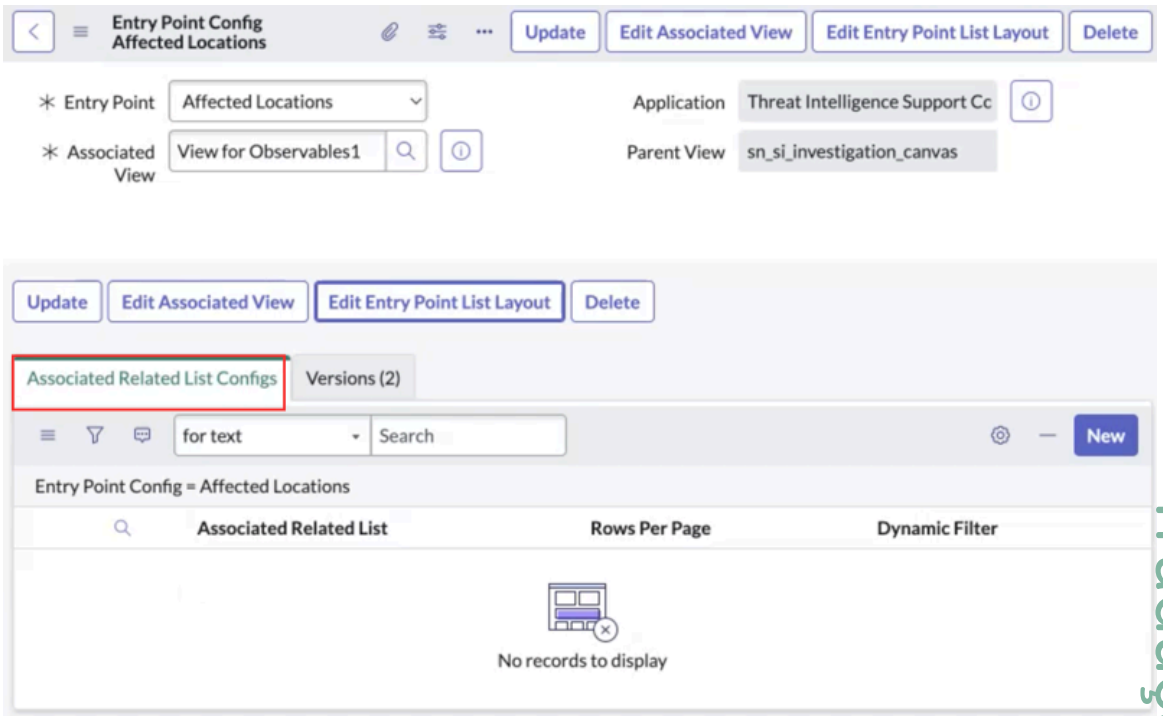
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

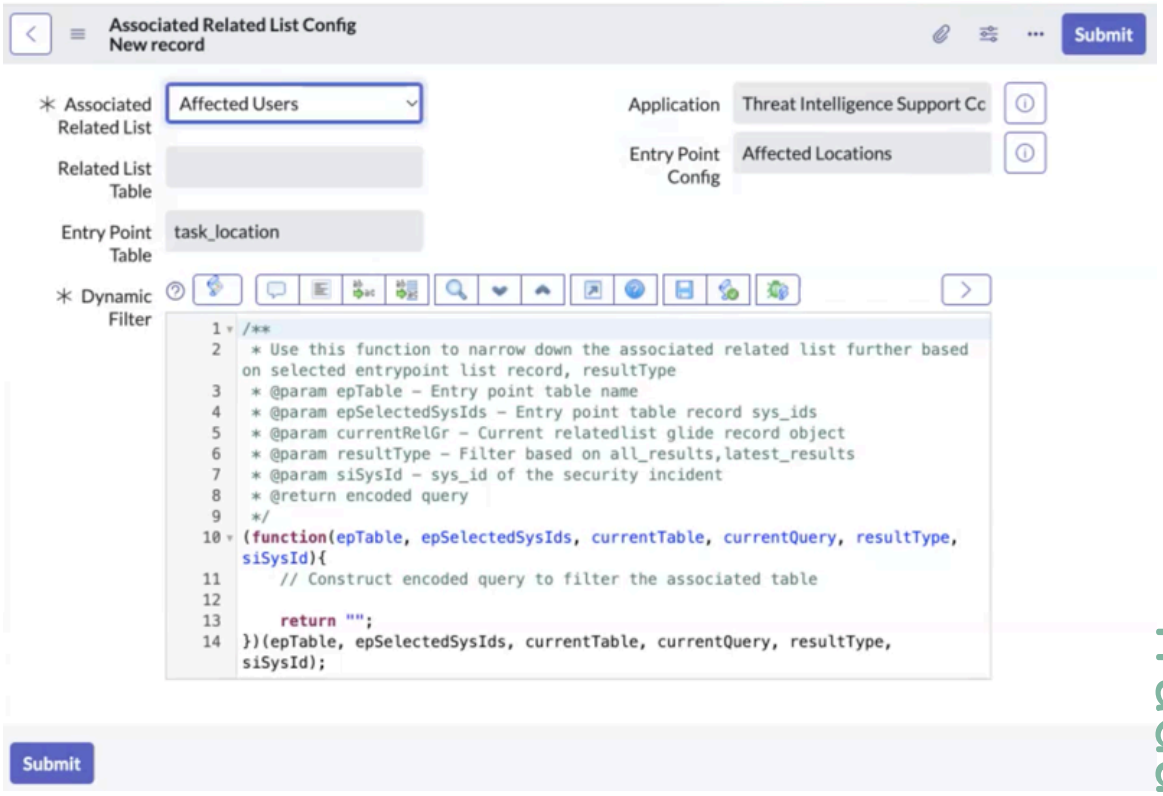
1. Clique em **Novo** em **Configurações de lista associadas** .



2. Selecione **Lista associada** valor do campo.
3. Use **Filtro dinâmico** coluna para filtrar ainda mais a lista associada com base nos registros da lista de ponto de entrada selecionados e no tipo de resultado (resultados mais recentes de cada implementação de fornecedor, todos os resultados).
   Consulte os exemplos existentes que são enviados dentro do produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Além disso, você pode configurar o layout de lista associado usando **Editar Layout de Lista Associado** ação.
   Na janela de bucket de lama, adicione ou remova colunas conforme necessário.

Espaço SIR Registros relacionados

Esta seção consiste nos itens das listas relacionadas que são agrupados em seções, como observáveis associados e itens de configuração.

Os grupos relacionados a seguir listam os grupos que estão disponíveis como parte do sistema de base. Você pode modificar esses grupos ou criar grupos na aplicação e suas respectivas ações.

Você pode modificar esses grupos ou criar novos grupos. Para obter mais informações, consulte Configurar Lista relacionada de incidentes de segurança sobre como configurar e agrupar a lista relacionada para incidentes de segurança e tarefas de resposta. Cada lista relacionada é totalmente funcional em Espaço SIR.

Lista relacionada	Item agrupado
Impacto nos negócios	• Itens de configuração • Usuários afetados • Itens de Configuração Relacionados • Usuários relacionados • Serviços afetados

Tradução automática

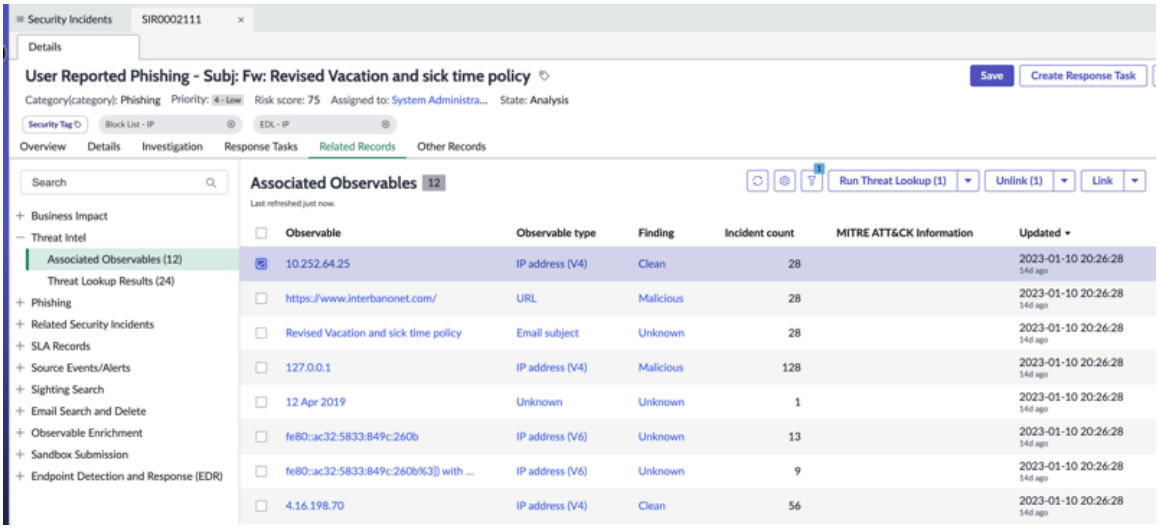
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
Inteligência sobre ameaça	• Observáveis Associados • Resultados da Pesquisa de ameaças
Phishing	• E-mails de Phishing Associados • Cabeçalhos de phishing associados
Incidentes de segurança relacionados	• Incidente primário de segurança • Incidente secundário de segurança • Incidente de segurança semelhante
Registro de ANS	ANS de tarefas
Eventos/alertas de origem	Eventos ou alertas de origem são a lista relacionada habilitada para integração SIEM, como E-mail de origem, LogRhythm Drill Down Logs, LogRhythm Events, Ofensão agregada do IBM QRadar e assim por diante. **Nota:** Esta lista depende completamente da integração que você tem em sua instância. Para exibir a lista relacionada de integração SIEM relevante, você deve instalar a versão mais recente.
Pesquisa de Vistas	• Resultados da pesquisa de detecções • Detalhes de Pesquisa de detecções • Detecção
Aprimoramento de Observável	• Resultados de enriquecimento observável • Eventos de MISP associados • Resultados de enriquecimento de MISP
Detecção e resposta de endpoint (EDR	• Detalhes do host • Processos em execução • Serviços em execução • Usuários Conectados • Estatísticas de Rede • Obter arquivo • Isolar Entradas de Host

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
	• Ações adicionais no endpoint • Detalhes do Microsoft Defender para máquinas relacionadas a endpoint



Nota: Em geral, você poderá criar novos registros, vincular ou desvincular registros existentes ou novos registros em relação ao grupo de lista relacionada, conforme aplicável.

Tópicos relacionados

Configurar Lista relacionada de incidentes de segurança

Configurar Lista relacionada de incidentes de segurança

Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem em Espaço SIR.

Antes de Iniciar

A lista relacionada de incidentes de segurança é agrupada e exibida como itens da lista relacionada ao grupo no **Registros relacionados** no espaço.

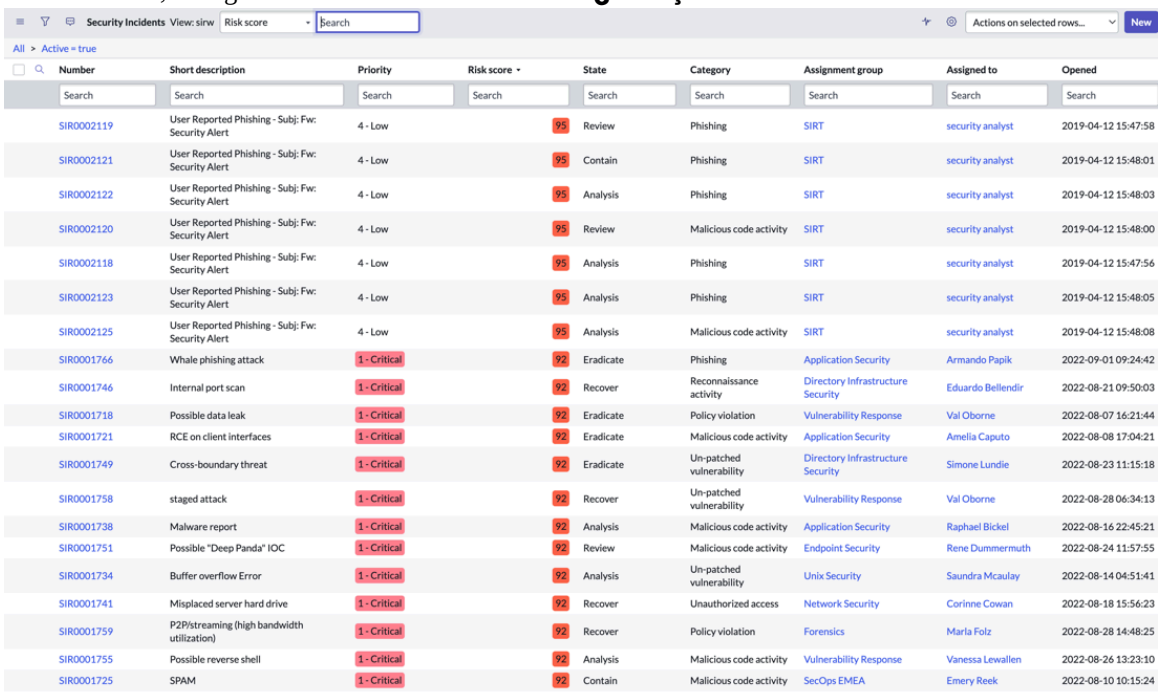
Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na IU clássica, navegue até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.

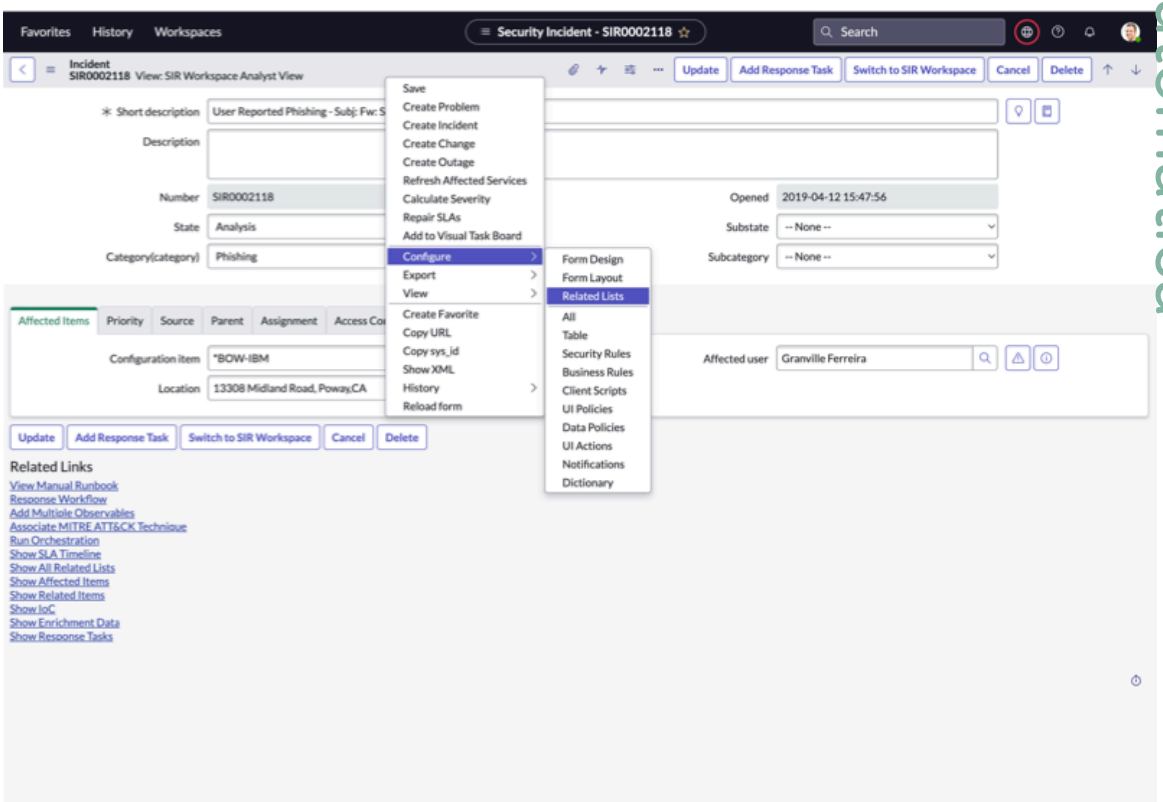


Security Incidents View: sirw | Risk score | Search | Actions on selected rows... | New

All > Active = true

Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Selecione qualquer registro de incidente.
3. Clique com o botão direito do mouse no menu de contexto do incidente.
4. Ir para **Configurar** > **Lista relacionada**.



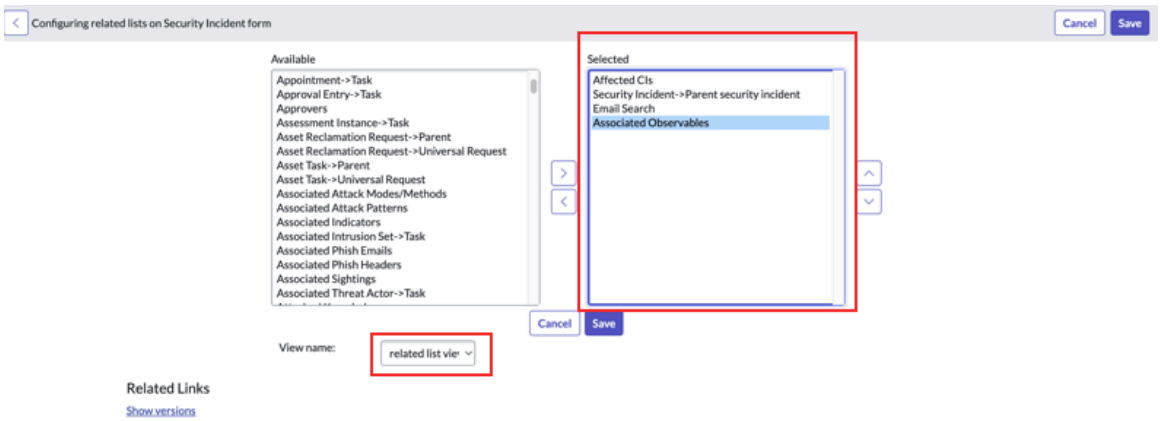
. **Configurar listas relacionadas no formulário Incidente de segurança** é exibido.

5. Vá para **Nome da exibição** e selecione **Novo** .

Tradução automática

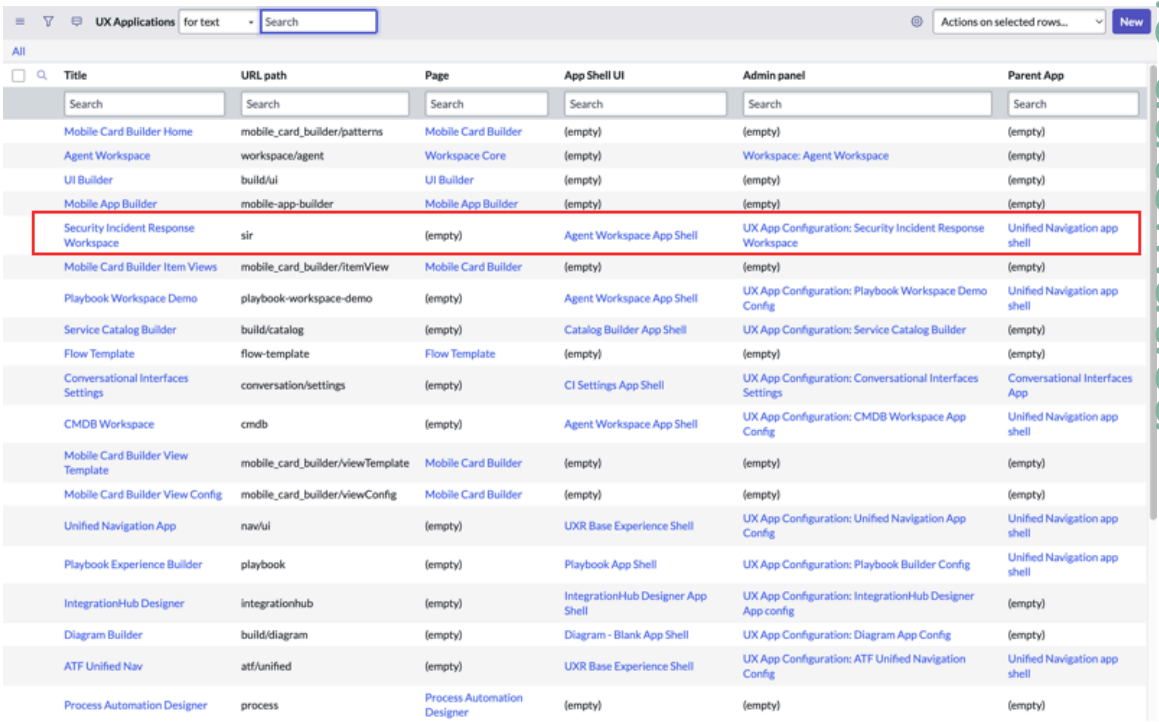
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Insira um nome para a exibição.
7. Selecione a exibição recém-criada.
   Depois de selecionar a exibição, escolha os campos de lista relacionada obrigatórios no bucket de slush.



Nota: Se você quiser modificar algo, selecione a exibição e remova ou adicione os itens.

8. Clique em **Salvar**.
9. Na navegação à esquerda, navegue até **Tudo** > **Estrutura do Now Experience** > **Experiências**.
10. Selecione **Espaço de resposta a incidentes de segurança** .

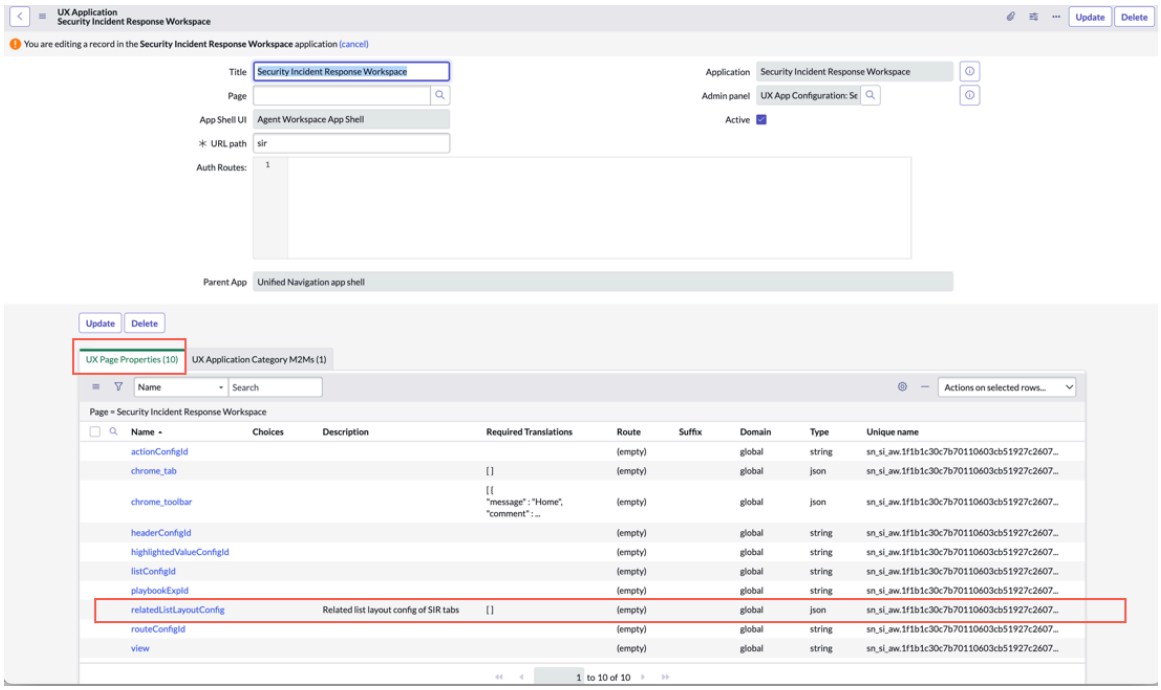


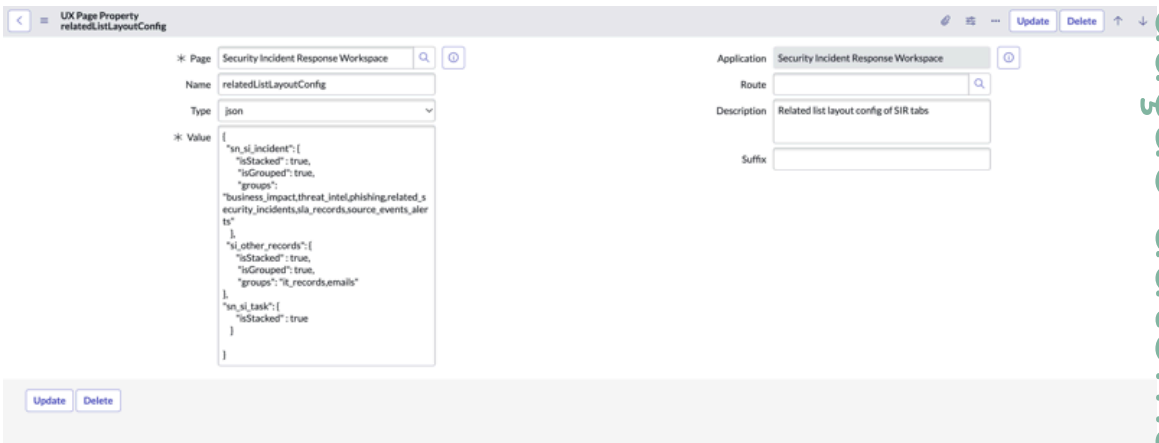
. **Espaço de resposta a incidentes de segurança da aplicação UX** a página é exibida.

11. Vá para **Propriedades da página de UX** e selecione **RelatedListLayoutConfig** opção na exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

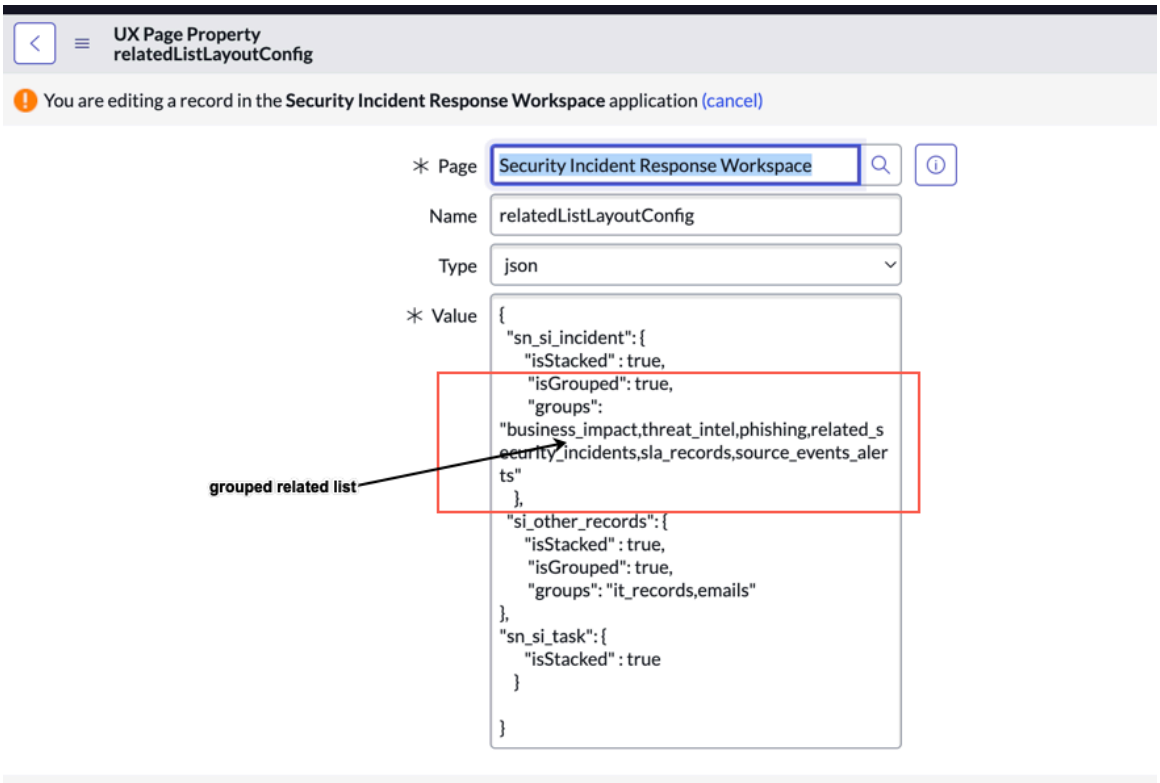




12. Adicione o nome de exibição recém-criado separado por uma vírgula a uma lista de valores já existente em **Valor** caixa de texto abaixo de **sn_si_incident.visualizaçõesUsedForGrouping** campo.
Por exemplo, se você criou um novo nome de exibição como, **Impacto nos negócios** em seguida, em **Valor** caixa de texto em que você deve especificá-la **business_impact** (que é separado por sublinhado no nome da exibição e separado por uma vírgula após um valor existente) no campo sn_si_incident:groups.

Tradução automática

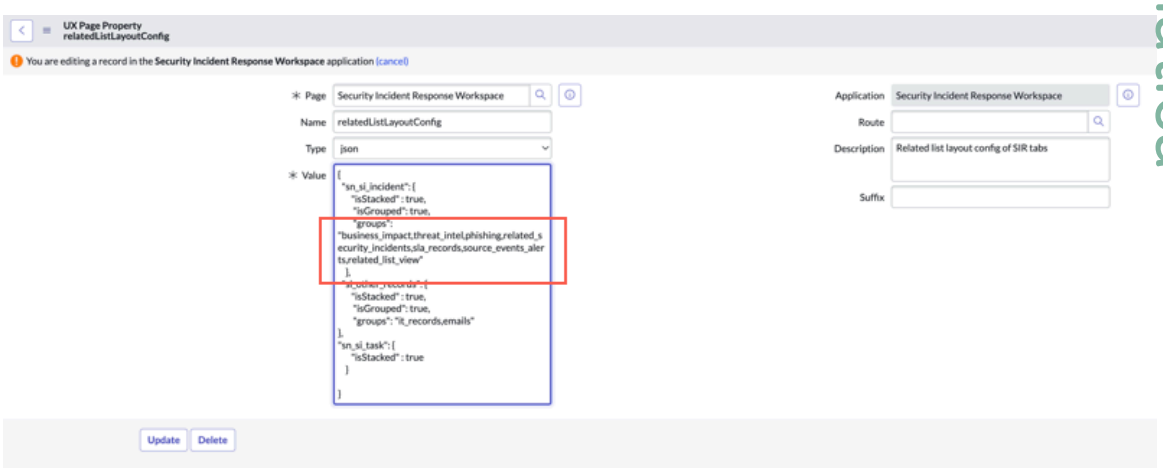
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Se você adicionar o novo nome de exibição em **sn_si_incident.visualizaçõesUsedForGrouping** em seguida, a entrada será criada no **Registros relacionados** do espaço.

Se você atualizar a entrada do nome da exibição em **si_other_records.visualizaçõesUtilizado para Agrupamento** em seguida, o grupo de lista relacionada será adicionado em **Outros registros** do espaço.

Abaixo está um exemplo de exibição que mostra as exibições recém-criadas adicionadas.



Nota: **RequiredRolesForGrouping** contém nomes de registro sys_user_role separados por vírgulas. O usuário do Espaço SIR deve ter pelo menos uma dessas funções para usar as listas relacionadas agrupadas. Quando um usuário não tiver nenhuma dessas funções, a exibição de listas relacionadas configurada para a função de usuário atual usando a configuração de regra de exibição será representada verticalmente sem agrupamento. Esta propriedade é ignorada quando **Isagrupado** a propriedade está definida como falsa. Se esta propriedade estiver vazia, qualquer usuário poderá acessar as listas relacionadas agrupadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

13. Clique em **Salvar**.
14. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
15. Selecione qualquer incidente de segurança específico.
16. Vá para **Registros relacionados** do espaço.
    As listas relacionadas agrupadas são exibidas.

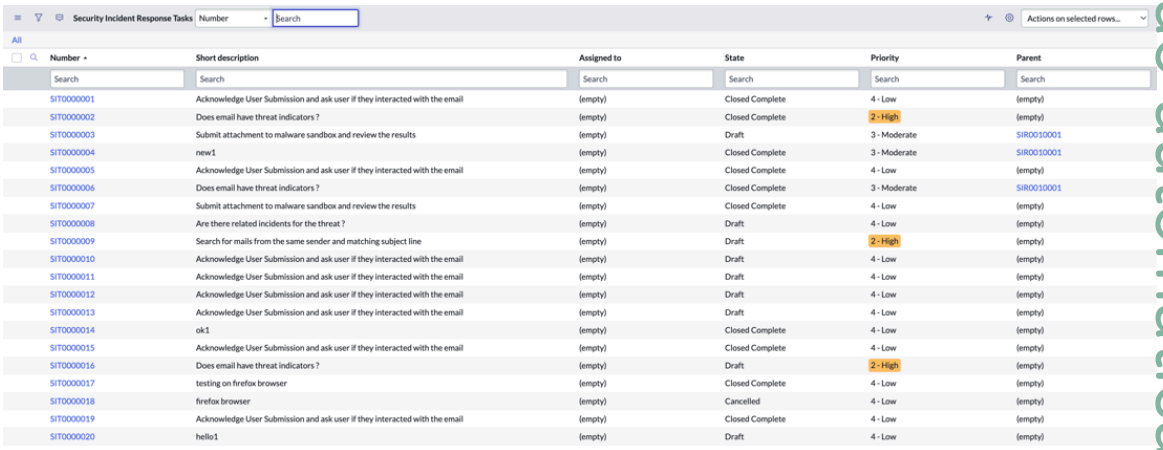
Configurar Lista relacionada de tarefa de resposta

Use esta seção para configurar as novas listas relacionadas de tarefas de resposta que aparecem na aplicação Resposta de incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A lista relacionada de tarefas de resposta não é agrupada, mas exibida como itens de lista relacionados individuais, pois há algumas listas padrão. Exiba os itens relacionados às tarefas de resposta do **Tarefas de resposta** do registro de incidente de segurança do espaço.

Procedimento
1. Navegar até **Tudo** > **Incidente de segurança** > **Tarefas de resposta** > **Mostrar todas as tarefas**.

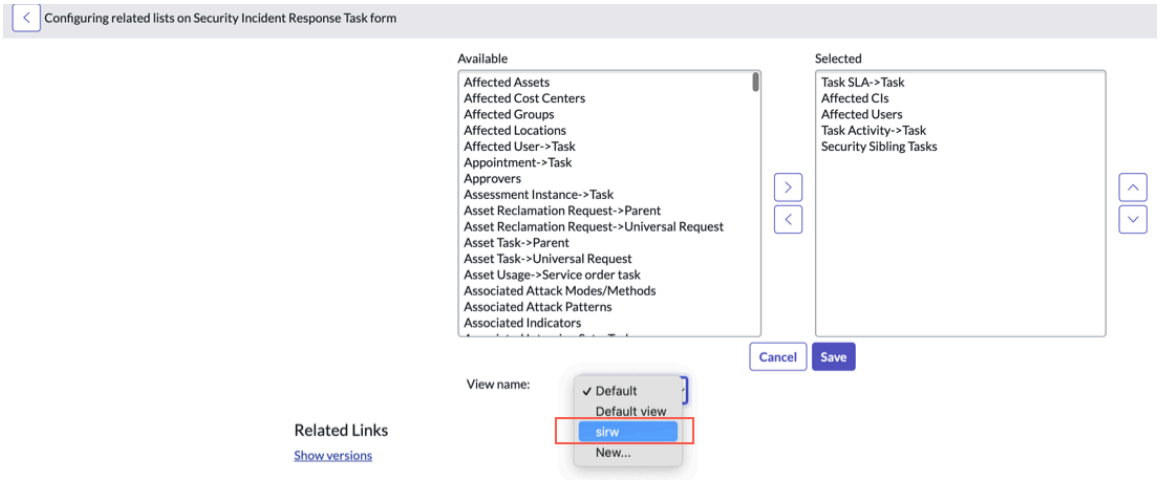


Number	Short description	Assigned to	State	Priority	Parent
SIT0000001	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000002	Does email have threat indicators ?	(empty)	Closed Complete	2 - High	(empty)
SIT0000003	Submit attachment to malware sandbox and review the results	(empty)	Draft	3 - Moderate	SIR0010001
SIT0000004	new1	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000005	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000006	Does email have threat indicators ?	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000007	Submit attachment to malware sandbox and review the results	(empty)	Closed Complete	4 - Low	(empty)
SIT0000008	Are there related incidents for the threat ?	(empty)	Draft	4 - Low	(empty)
SIT0000009	Search for mails from the same sender and matching subject line	(empty)	Draft	2 - High	(empty)
SIT0000010	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000011	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000012	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000013	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000014	ok1	(empty)	Closed Complete	4 - Low	(empty)
SIT0000015	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000016	Does email have threat indicators ?	(empty)	Draft	2 - High	(empty)
SIT0000017	testing on firefox browser	(empty)	Closed Complete	4 - Low	(empty)
SIT0000018	firefox browser	(empty)	Cancelled	4 - Low	(empty)
SIT0000019	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000020	hello1	(empty)	Draft	4 - Low	(empty)

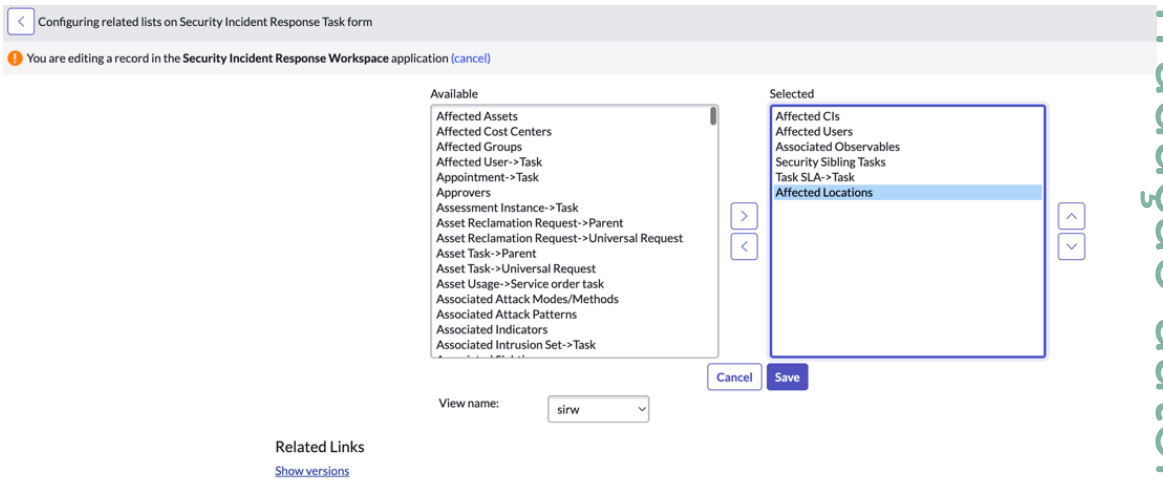
2. Selecione qualquer registro de tarefa de resposta.
3. Clique com o botão direito do mouse no menu de contexto da tarefa de resposta do incidente de segurança.
4. Navegar até **Configurar** > **Lista relacionada**.
   . **Configurar listas relacionadas no formulário Tarefa de resposta de segurança** é exibido.
5. Vá para **Nome da exibição** e selecione **sirw** exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione os campos de lista relacionada desejados no bucket de slush.
   Por exemplo, Locais afetados.

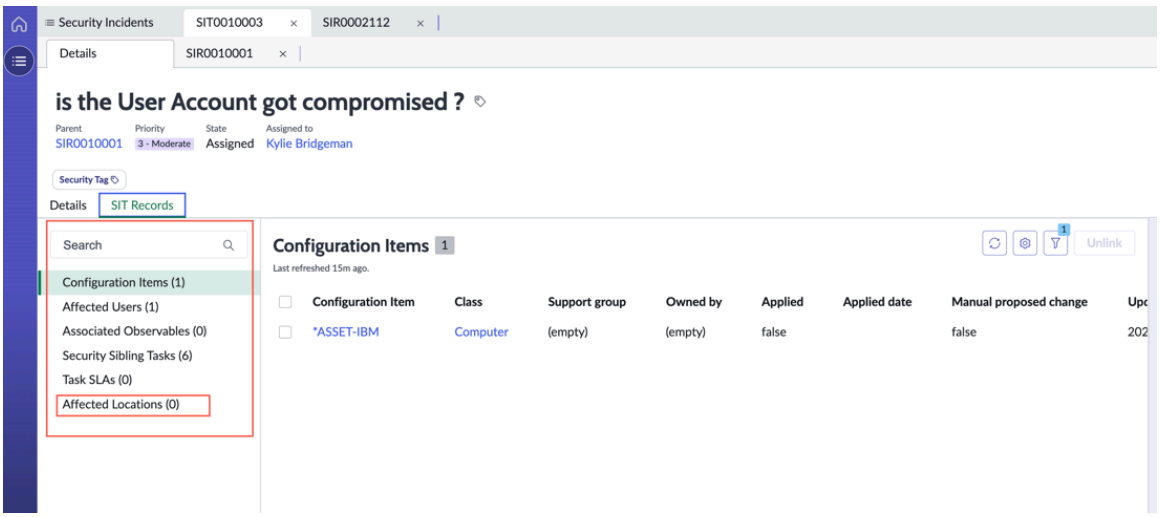


7. Clique em **Salvar**.
8. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Tarefas de resposta** > **Registros DO SIT**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas relacionadas configuradas (por exemplo, Locais afetados conforme selecionado) são listadas na lista de registros DO SIT.



Defina as novas regras da calculadora de pontuação de risco

Use a nova Calculadora de pontuação de risco para definir e calcular a pontuação de risco de incidentes de segurança com base nos critérios definidos pelo usuário, que fornecem uma pontuação de inteligência transparente de incidentes de segurança. A pontuação de risco é calculada automaticamente para os registros de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin.

Ative a nova Calculadora de pontuação de risco definindo `sn_si_aw.activate_new_risk_score_calculator` propriedade do sistema como verdadeira.

Por Que e Quando Desempenhar Esta Tarefa

Defina uma pontuação de risco para os registros de incidentes de segurança gerados com base nos parâmetros definidos pelo usuário. O sistema de base é provisionado com uma regra de pontuação de risco, que pode ser personalizada e habilitada de acordo.

Nota:

- Por padrão, a nova regra da calculadora de pontuação de risco está inativa e você precisa habilitar a regra para ver a pontuação de risco dos incidentes de segurança.
- Para calcular a pontuação de risco para tabelas relacionadas adicionais diferentes das disponíveis no sistema de base, consulte Calculadora de pontuação de risco para tabelas relacionadas adicionais.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Administração**.
2. Navegar até **Mecanismo de regras** > **Regra da calculadora de pontuação de risco**.
   A página Regra da calculadora de pontuação de risco é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Como parte do sistema de base, você recebe um modelo de regra de pontuação de risco predefinido para exibir, editar ou modificar a pontuação de risco. No entanto, você não pode criar ou excluir o modelo de regra de pontuação de risco predefinido.
- As mudanças feitas serão aplicadas a todos os novos incidentes de segurança ou atualizações aos existentes. Para redefinir pontuações históricas, use **Recalcular pontuação** ação.

3. Selecione **Calculadora de pontuação de risco** regra.
4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do valor da pontuação de risco. Por exemplo, Calculadora de pontuação de risco.
Ponderação geral (aplicável ao construtor de critérios)	Ponderação deste campo na regra de risco. Este campo não é editável e exibe a ponderação geral calculada pelo sistema com base no peso correspondente aos critérios habilitados. O peso geral deve ser sempre 100%.
Descrição	Descrição do registro de pontuação de risco. Por exemplo, calcula a pontuação de risco com base na soma ponderada das pontuações de critérios predefinidos.
Critérios de pontuação	Indica os critérios de pontuação para um incidente de segurança. Você pode definir o risco **Critérios de pontuação** usando as seguintes opções: ○ **Construtor de critérios** : Use esta opção para adicionar, editar ou remover e habilitar e desabilitar critérios que contribuem para o cálculo da pontuação de risco e verificar se a ponderação agregada total é de 100%. ○ **Usar script (Avançado)** : O recurso de script é um recurso avançado para criar um script personalizado que deve retornar a pontuação de risco, que é um valor inteiro que varia de 0 a 100.

5. Para definir **Critérios de pontuação** usando o. **Construtor de critérios** execute as seguintes etapas:

Nota: Você pode editar ou modificar os critérios existentes ou adicionar novos critérios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para adicionar novos critérios, selecione **Novos critérios** ação.

b. Selecione **Tabela** para o qual você deseja definir os critérios.

Nota:

- Se a tabela selecionada for um incidente de segurança, a condição será aplicada ao registro de incidente de segurança para o qual a pontuação de risco é calculada. Se a tabela selecionada não for um incidente de segurança, a condição será aplicada somente se os registros estiverem relacionados ao incidente de segurança para o qual a pontuação de risco é calculada.
- Um tipo agregado adicional é adicionado para definir as pontuações com base no número de relações associadas aos incidentes de segurança.

c. Selecione **Tipo** critérios para a tabela selecionada.
O valor Tipo pode ser **Campo** ou **Agregado** com base na tabela escolhida.

d. Selecione **Campo** critérios para a tabela selecionada.
Se você selecionou o valor Tipo como **Campo** , Em seguida, os Critérios de campo exibem os valores de campo relacionados à tabela. Se você selecionou o valor Tipo como **Agregado** , Em seguida, os Critérios de campo exibem os valores agregados relacionados à tabela.

Nota: O tipo de agregado oferece suporte somente ao valor de Contagem.

Por exemplo, se você selecionar os Critérios de tabela como **Incidente de segurança** , Em seguida, os Critérios de tipo serão exibidos somente **Campo** opção. Os Critérios de campo exibem todos os Valores de campo relacionados à tabela, que podem ser Severidade, Ativo e assim por diante da mesma forma, se você selecionar os Critérios de tabela como **Usuários afetados** , Em seguida, os Critérios de tipo exibem ambos **Campo** e. **Agregado** opção. Se você selecionar o Tipo como Agregado, os Critérios de campo exibirão os valores agregados relacionados à tabela, que é **Contagem** .

e. Insira **Ponderação** dos critérios entre 0-100.
A ponderação geral de todos os critérios deve ser de 100%.

f. Insira o nome e uma descrição resumida dos critérios.

g. Selecione **Habilitar critérios de pontuação** caixa de seleção para habilitar os critérios de pontuação.

h. Defina **Condições** e definir a pontuação para as condições.

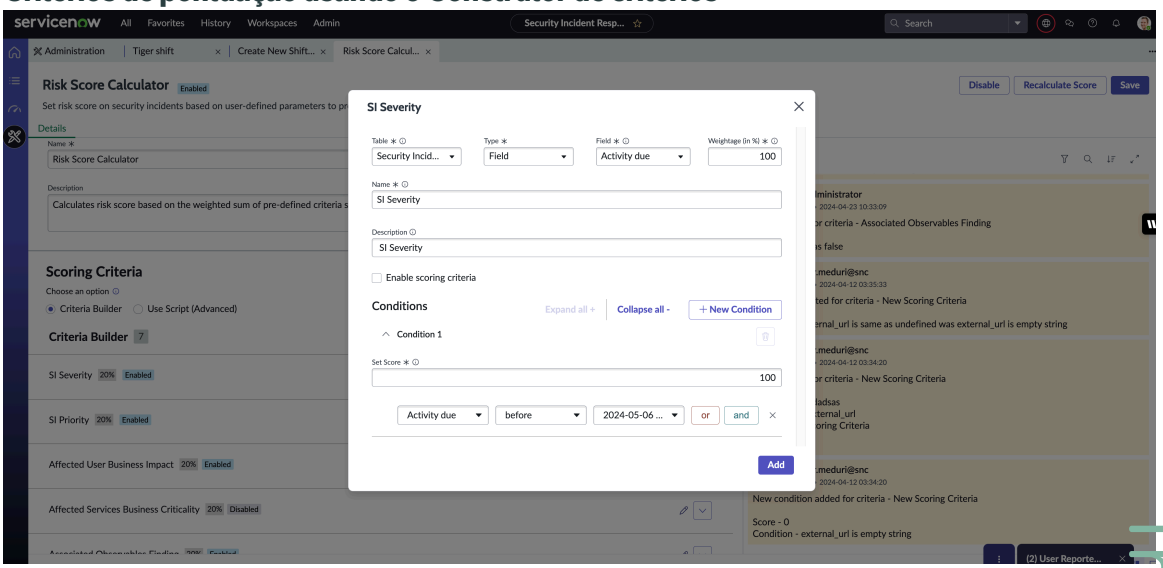
i. Você também pode adicionar novas condições usando **Nova condição** e exclua as condições existentes usando **Excluir critérios** ícone.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

j. Selecione **Adicionar** para adicionar os critérios configurados.

Critérios de pontuação usando o Construtor de critérios



6. Selecione **Recalcular pontuação** opção para recalcular a pontuação de risco.

Por exemplo, se houver mudanças na regra de pontuação de risco. Nesse caso, você deve reaplicar a regra de pontuação aos incidentes de segurança com a pontuação de risco já calculada no passado. Use **Recalcular pontuação** ação para acionar o trabalho de recálculo.

7. Selecione **Confirmar** .

Nota: Quando você acionar esta ação, o processo será executado em segundo plano e levará alguns minutos para ser concluído. Você não poderá fazer mudanças até que ela seja concluída.

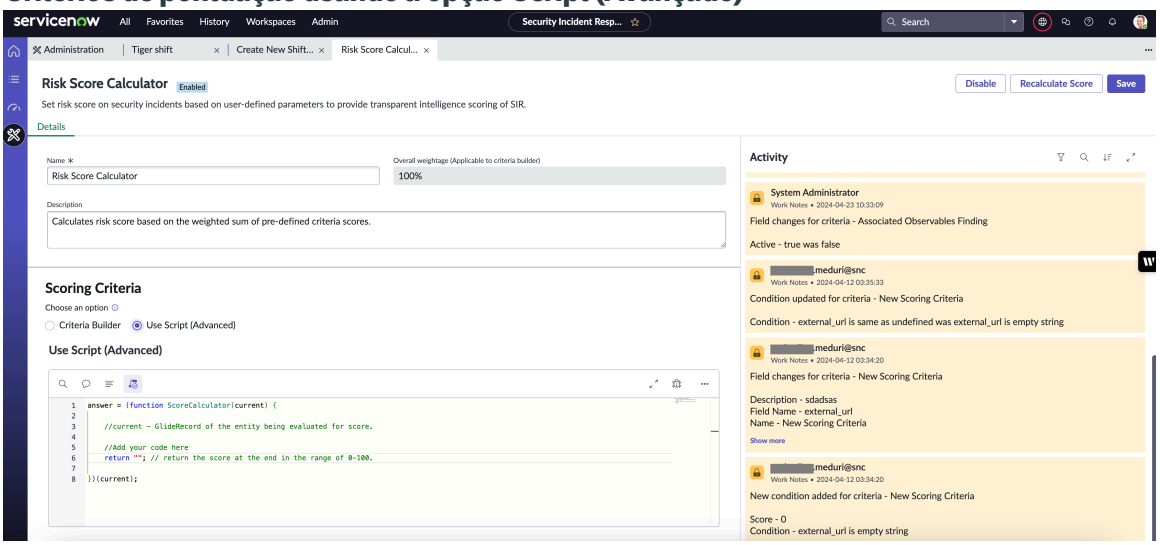
8. Para definir **Critérios de pontuação** usando **Usar script (Avançado)** execute as seguintes etapas:

a. Use este script predefinido para criar um script personalizado que deve retornar a pontuação de risco, que é um valor inteiro que varia de 0 a 100.
O campo de script avançado é preenchido automaticamente com uma função, que usa os parâmetros **atual** e esta função deve retornar a pontuação de risco, que é um valor inteiro que varia de 0 a 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios de pontuação usando a opção Script (Avançado)



Aqui, o parâmetro atual é o objeto GlideRecord da entidade (incidente de segurança) para a qual a pontuação de risco está sendo calculada. Para os incidentes de segurança, corresponde ao GlideRecord da tabela sn_si_incident.

9. Para desabilitar a Calculadora de pontuação de risco, selecione **Desabilitar** .
10. Selecione **Save** (Salvar).

Calculadora de pontuação de risco para tabelas relacionadas adicionais

A Calculadora de pontuação de risco é provisionada com uma regra de pontuação de risco como parte do sistema de base para calcular a pontuação de risco de incidentes de segurança com base em critérios definidos pelo usuário. No entanto, você pode personalizar e incluir tabelas relacionadas adicionais para calcular a pontuação de risco.

Antes de Iniciar

Função necessária: sn_si.admin.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**.
2. Selecione qualquer registro de incidente de segurança.
3. Selecione **Ações adicionais** opção ao lado do número do incidente de segurança.
4. Ir para **Configurar** > **Listas relacionadas**.
5. Vá para o Nome da exibição e selecione **Calculadora de pontuação de risco** .
   Depois de selecionar a exibição, escolha a lista relacionada necessária que você deseja adicionar do bucket de slush. Por exemplo, avistamentos associados.
6. Selecione **Save** (Salvar).
   Você adicionou com sucesso as novas listas ou tabelas relacionadas para as quais deseja calcular a pontuação de risco.

> **Importante:** Para calcular a pontuação de risco dos incidentes de segurança que têm novos critérios com as listas relacionadas recém-criadas, você precisa definir regras de negócio na tabela base da lista relacionada.

7. Navegar até **Tudo** > **Definição do Sistema** > **Regras de negócio**.

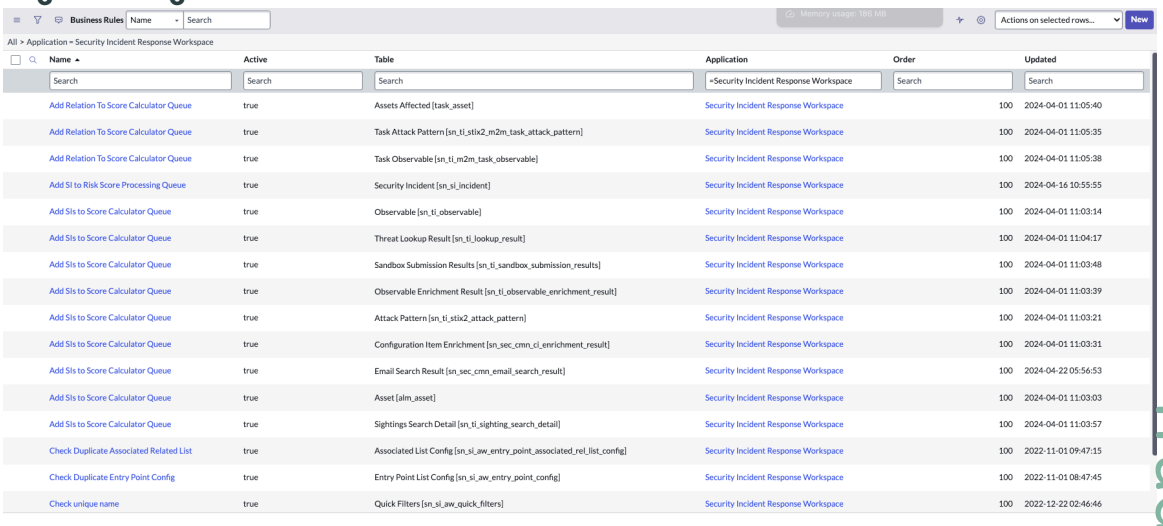
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar as duas regras de negócios a seguir como referência para criar suas próprias regras de negócios:

- Adicionar incidentes de segurança (SIS) à fila da calculadora de pontuação
- Adicionar relação à fila da calculadora de pontuação (isso se aplica a tabelas m2m)

Regras de negócio



All > Application = Security Incident Response Workspace

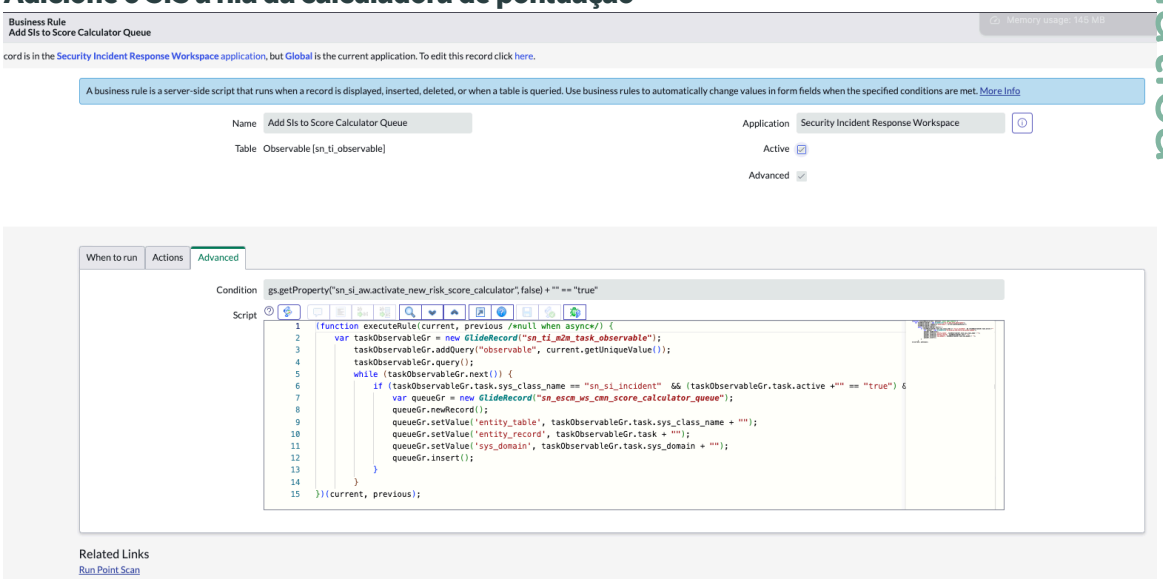
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. Por exemplo, para que os critérios de observáveis associados funcionem, definimos duas regras de negócio.

O primeiro é **Adicione o SIS à fila da calculadora de pontuação** regra de negócio.

Por exemplo, um novo incidente de segurança é criado e associado a um observável (Observáveis[sn_ti_observable]). Após a pesquisa de ameaças, o observável é considerado mal-intencionado. Em seguida, você precisa adicionar todos os incidentes de segurança associados a este observável mal-intencionado à fila para recalcular a pontuação de risco dos incidentes de segurança.

Adicione o SIS à fila da calculadora de pontuação



Business Rule
Add SIs to Score Calculator Queue

cord is in the Security Incident Response Workspace application, but Global is the current application. To edit this record click here.

A business rule is a server-side script that runs when a record is displayed, inserted, deleted, or when a table is queried. Use business rules to automatically change values in form fields when the specified conditions are met. More Info

Name: Add SIs to Score Calculator Queue
Table: Observable [sn_ti_observable]
Application: Security Incident Response Workspace
Active
Advanced

When to run | Actions | Advanced

Condition: gs.getProperty("sn_si_aw.activate_new_risk_score_calculator", false) + "" == "true"

Script:

```
(function executeRule(current, previous /*null when async*/) {
    var taskObservableGr = new GlideRecord("sn_ti_m2m_task_observable");
        taskObservableGr.addQuery("observable", current.getUniqueValue());
        taskObservableGr.query();
        while (taskObservableGr.next()) {
            if (taskObservableGr.task.sys_class_name == "sn_si_incident"  && (taskObservableGr.task.active +"" == "true") &
                var queueGr = new GlideRecord("sn_escm_ws_cmn_score_calculator_queue");
                queueGr.newRecord();
                queueGr.setValue('entity_table', taskObservableGr.task.sys_class_name + "");
                queueGr.setValue('entity_record', taskObservableGr.task + "");
                queueGr.setValue('sys_domain', taskObservableGr.task.sys_domain + "");
                queueGr.insert();
            }
        }
})(current, previous);
```

Related Links
Run Point Scan

O segundo é o. **Adicionar relação à fila da calculadora de pontuação** regra de negócio.

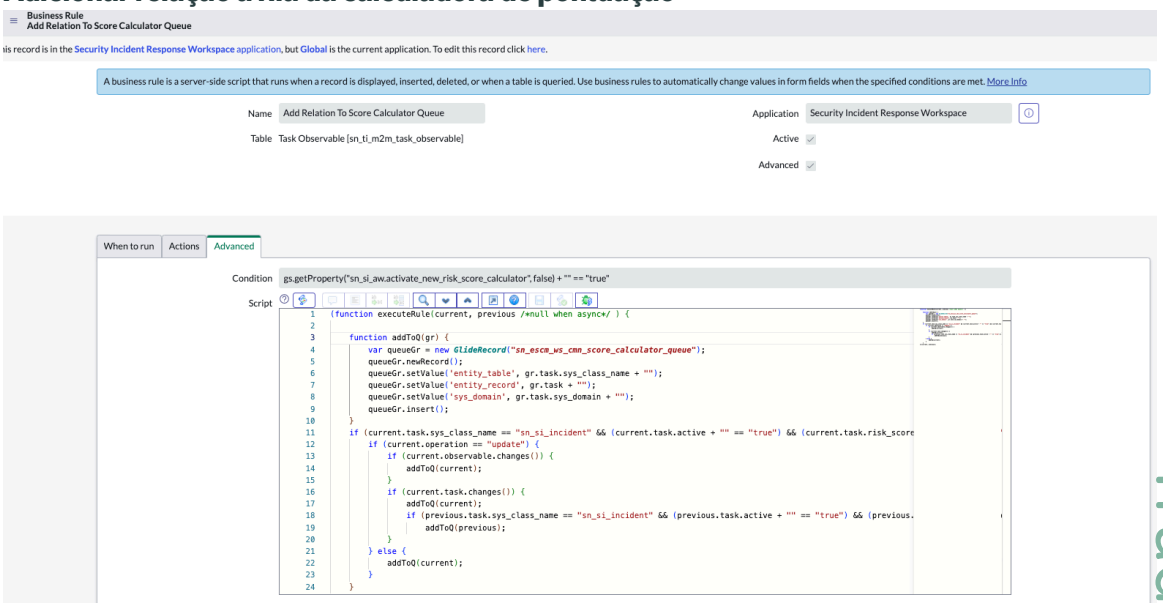
Por exemplo, um novo incidente de segurança é criado ou excluído e associado a um observável (Observáveis de tarefa[sn_ti_m2m_task_observable]). Portanto, há uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mudança na associação do incidente de segurança. Em seguida, você precisa adicionar esse incidente de segurança à fila para recalcular a pontuação de risco do incidente de segurança.

Adicionar relação à fila da calculadora de pontuação



Configurar a entrega de turno

Defina as configurações de entrega de turno para fornecer informações completas do turno para os próximos analistas de turno.

Configurar modelos de entrega de turno

O administrador pode definir e configurar diferentes modelos de entrega de turno para que o responsável pelo turno crie registros de entrega de turno e os entregue à próxima equipe de turno.

Antes de Iniciar

Função necessária:

- sn_escm_sh.shift_admin
- sn_si.admin herda a função sn_escm_sh.shift_admin

Por Que e Quando Desempenhar Esta Tarefa

Para configurar um modelo de Entrega de turno, o administrador cria um novo modelo de Entrega de turno ou abre um modelo existente no sistema de base com o nome **Modelo de turno de amostra** e modifica os detalhes e as seções de acordo com seus requisitos.

O responsável pelo turno pode usar o modelo configurado para criar registros de log de entrega de turno e, em seguida, o relatório de entrega de turno é compartilhado com o próximo responsável pelo turno ativo e a equipe.

Nota: Somente os modelos de entrega de turno ativos ficam visíveis para o responsável pelo turno criar registros de log de entrega.

Procedimento

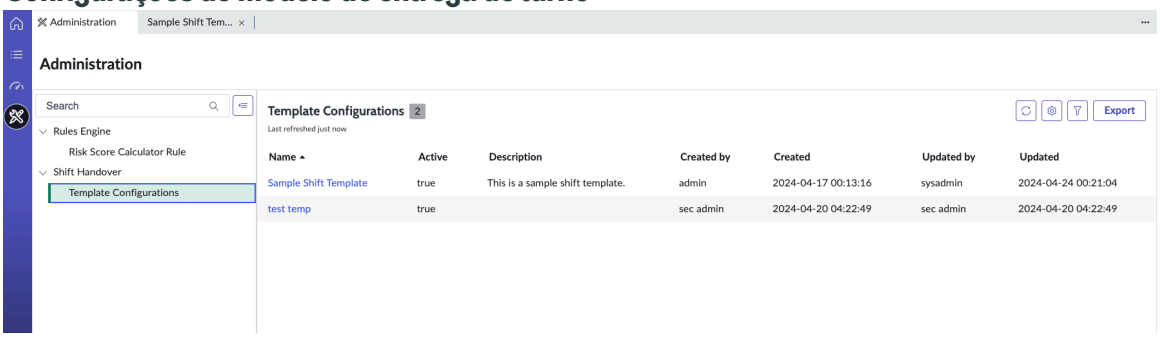
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Administração**.
2. Navegar até **Transferência de turno** > **Configurações do modelo**.
   A página Configurações do modelo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Como parte do sistema de base, você recebe uma configuração predefinida do modelo de entrega de turno para exibir, editar ou modificar o modelo de entrega de turno. No entanto, você não pode criar ou excluir a configuração predefinida do modelo de Entrega de turno.

Configurações do modelo de entrega de turno



3. Para criar um novo modelo de entrega de turno, selecione **Novo** .
4. No formulário Detalhes, preencha os campos.

Crie um novo modelo de entrega de turno

Campo	Descrição
Nome	Nome do modelo de entrega de turno. Por exemplo, Modelo SIR.
Aplicação	Nome da aplicação para a qual você está criando o modelo de Entrega de turno. Por exemplo, Espaço de resposta a incidentes de segurança.
Ativo	Opção para indicar se o modelo de entrega de turno está ativo. Habilite esta opção para ativar o modelo de Entrega de turno.
Descrição	Descrição do modelo de entrega de turno.
Configuração da menção de registro	Use este campo para configurar os detalhes da menção do registro do Editor de Rich Text (RTE). A entrada é uma matriz de objetos JSON com os seguintes campos: ○ `SourceTable` Nome da tabela de origem. ○ `rótulo` Nome do rótulo a ser exibido. ○ `FilterCondition` Consulta codificada para filtragem. Você pode adicionar várias consultas para a mesma tabela para recuperar os valores dinamicamente. Esses valores são atualizados quando o registro de entrega do turno é publicado ou com base na data de início ou/e na data de término do turno. Por exemplo, contagem de registros de incidentes de segurança por prioridade, contagem de registros de incidentes de segurança por estado. Você pode usar os argumentos "start_date" e "end_date" na consulta para especificar um intervalo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de datas. Por exemplo, `"FilterCondition": "Ative "sys_created_on>"` ○ *campos* : Selecione os campos para consultar o padrão. Configuração de amostra que você pode copiar e colar no campo Configuração de Menção de registro. `[ { "sourceTable": "incident", "label": "Incidents active", "filterCondition": "active=true", "fields": [ "number" ] } { "sourceTable": "incident", "label": "Active incidents created after selected date", "filterCondition": "active=true^sys_created_on>=${start_date}", "fields": [ "number" ] } ]` Para copiar a configuração de amostra, use **Copiar para a área de transferência** Ação no painel Assistência contextual. Em seguida, você pode fazer modificações adicionais com base em seus requisitos.

Modelo	Crie um modelo de entrega de turno usando seções. Certifique-se de que haja pelo menos uma seção para que os analistas possam contribuir com os registros de log de entrega de turno com base no modelo.
	O modelo pode ter texto estático, imagens e assim por diante, nas seções apropriadas. Você pode copiar e colar imagens diretamente no campo Modelo. Você pode criar seções no modelo usando o seguinte código:
	`${section:Section Label}`
	Exemplo:
	`${section:Key Incidents/Events During Current Shift} ${section:Incidents/Events to Monitor or Follow Up} ${section:System/Infrastructure Updates} ${section:Next Steps for Incoming Shift} ${section:References}`

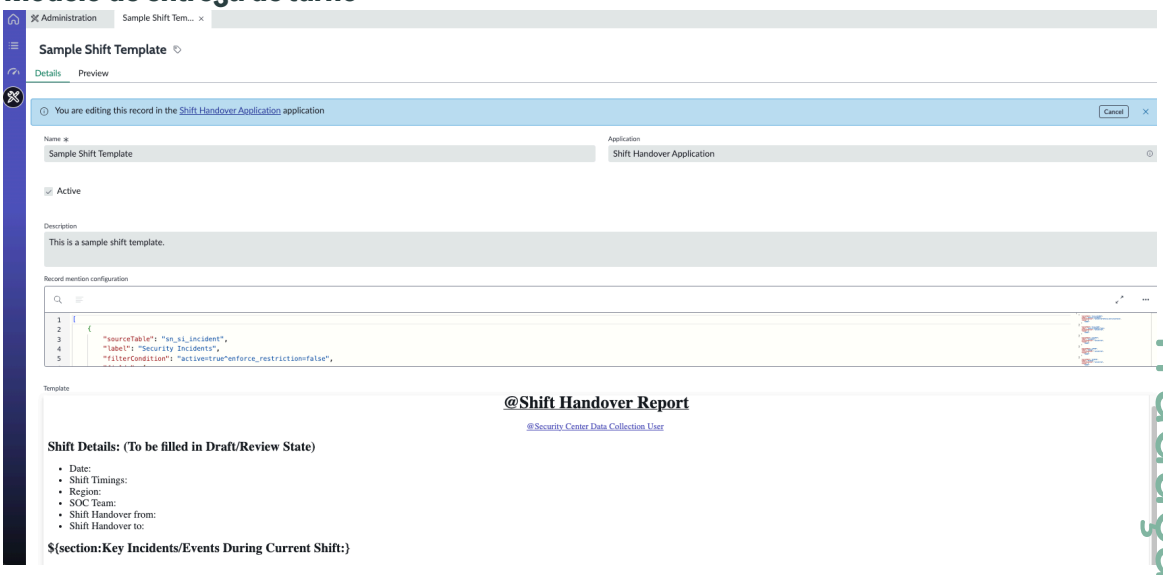
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para obter mais informações, consulte **Assistência contextual** no painel direito.

5. Para usar e modificar um modelo de entrega de turno existente, selecione **Modelo de turno de amostra** .

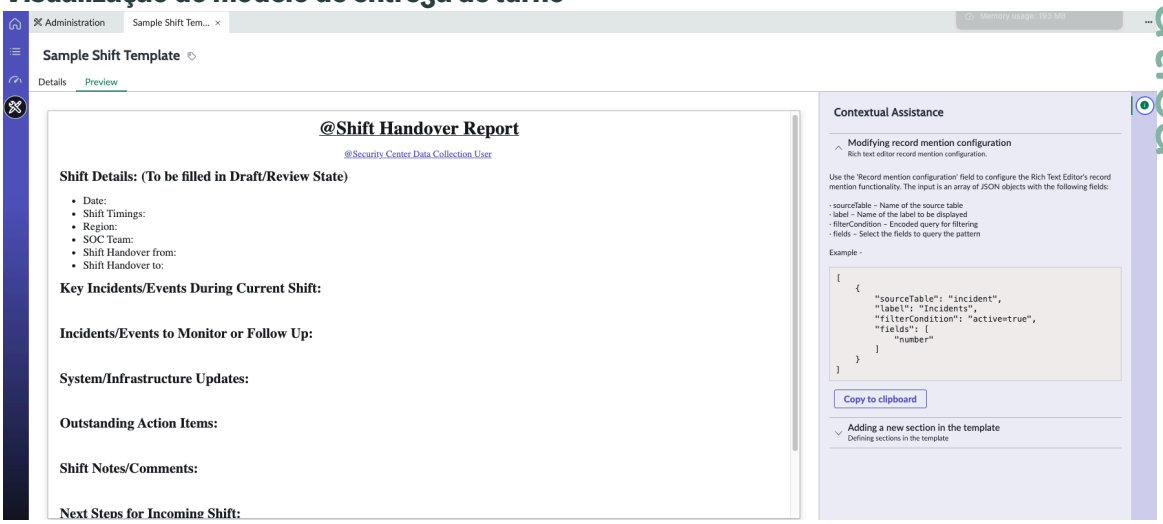
Modelo de entrega de turno



6. Atualize o modelo de entrega de turno de acordo com seus requisitos.
7. Selecione **Visualização** Para exibir a visualização do tempo de execução do modelo de Entrega de turno.

   O relatório gera uma visualização com base na configuração do modelo de Entrega de turno.

Visualização do modelo de entrega de turno



8. Selecione **Salvar** Para salvar o modelo de Entrega de turno.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Para saber como gerenciar registros de entrega de turno na exibição de lista e executar ações como criar, editar, copiar ou excluir registros de entrega de turno, consulte Gerenciar registros de entrega de turno.

Criar . hifts por Espaço de resposta a incidentes de segurança

Criar turnos por meio de Espaço de resposta a incidentes de segurança . usar ao configurar . deslocamento . andover r ecords.

Antes de Iniciar

Função necessária:

- sn_escm_sh.shift_admin
- sn_si.admin herda a função sn_escm_sh.shift_admin

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Administração**.
2. Navegar até **Transferência de turno** > **Configurações do horário de turno**.
   A página Configuração de tempo do turno exibe todos os turnos existentes.
3. Selecione **Novo**.
4. Insira um nome em . **Turno** campo .
5. Fornecer horas de início e término do turno em . **Hora de início** e. **Hora de término** campos .

   Nota: A hora de início e a hora de término estão em . do usuário atual configurado fuso horário .

6. Selecione **Save** (Salvar).

Resposta a incidentes de segurança c onferência c todos integração

. Resposta a incidentes de segurança A integração de Chamada em conferência permite gerenciar e iniciar chamada em conferência e bate-papo para analistas, gerentes e usuários afetados.

Com Resposta a incidentes de segurança recurso de chamada em conferência, você pode colaborar com clientes e agentes de pares para resolver incidentes de segurança em uma chamada. Você também pode colaborar usando um bate-papo em grupo.

Você pode iniciar chamadas em conferência usando canais de comunicação de terceiros, como Microsoft Teams, Cisco Webex ou Zoom Meetings. Para colaborar usando o bate-papo, use o bate-papo da barra lateral da aplicação SIR.

Principais recursos

. Resposta a incidentes de segurança a colaboração de chamadas fornece os seguintes recursos principais:

- Os gerentes/analistas DO SIR podem iniciar uma chamada em conferência do Microsoft Teams, Cisco Webex ou Zoom diretamente do incidente de segurança.
- Gerentes/analistas de SIR podem iniciar um bate-papo diretamente da aplicação SIR.
- Convide participantes adicionais para a chamada ou bate-papo.
- Exibir gravações de chamadas e detalhes de bate-papo.
- Envie convites aos participantes por e-mails e bate-papo do Microsoft Teams.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar usuários e grupos de chamadas em conferência

O administrador pode definir as configurações de chamada em conferência para exibir uma lista predefinida de usuários e grupos a serem adicionados a uma chamada.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Espaços** > **Espaços de resposta a incidentes de segurança** > **Administração**.
2. Selecione **Chamada em conferência** e, em seguida **Configuração de chamada** .
3. Na página Configurações de chamada, selecione **Configuração de chamada em conferência** .
   A página de configuração é exibida para configurar a lista predefinida de usuários e grupos.
4. No formulário Detalhes, preencha os campos.

Campo	Descrição
Nome	Nome da configuração da chamada em conferência.
Preencher usuários automaticamente	Opção para preencher automaticamente os usuários configurados para uma chamada em conferência. Selecionar esta opção adiciona os usuários e grupos configurados a uma chamada em conferência. **Nota:** Também é possível adicionar ou remover usuários/grupos ao iniciar uma chamada.
Mostrar usuários afetados	Opção para exibir os usuários afetados para adicionar a uma chamada.
Mostrar usuários do grupo de atribuição	Opção para exibir os usuários do grupo de atribuição para adicionar a uma chamada.
Grupos padrão	Opção para adicionar grupos padrão para adicionar a uma chamada.
Usuários padrão	Opção para adicionar usuários padrão para adicionar a uma chamada.

5. Selecione **Salvar** para salvar a configuração da chamada em conferência.

Integrar O SIR a canais de comunicação de terceiros

A integração de Chamada em conferência DO SIR com canais de comunicação de terceiros, como Microsoft Teams, Zoom e Cisco Webex, permite gerenciar e iniciar uma chamada diretamente de um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

- Inicie e encerre chamadas em conferência diretamente de qualquer incidente de segurança.
- Adicionar ou remover participantes em uma chamada em conferência.
- Rastreie e relate os detalhes da reunião, como a duração da reunião e os participantes, para análise posterior.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins do Hub de integração em sua instância da ServiceNow.

- Notify (com.snc.notify). Para obter mais informações, consulteConfiguração da Notify
- Componentes de IU do Notify para espaços configuráveis
- Para integrar o Microsoft Teams como um canal de comunicação:
  - Plug-in Spoke do Microsoft Teams Communications (sn_msteams_com_spk).
  - Plug-in Mapeamento de usuário do Azure Active Directory (sn_now_azure).
- Para integrar o Zoom como um canal de comunicação:
  - Spoke do Zoom (sn_zoom_spoke)
  - Notify Zoom (sn_notify_zoom)
- Para integrar o Cisco Webex como um canal de comunicação:
  - Notify Cisco Webex Connector (sn_notify_webex)
  - Cisco Webex Teams spoke (sn_cisco_teams_spk)

Para obter mais informações, consulte Solicitação IntegrationHub .

Configuração

Execute a seguinte configuração para os canais de comunicação que você deseja usar:

- Para configurar a integração do Cisco Webex da Chamada em conferência usando o canal de comunicação Notify, consulte Configuração do Notify Cisco Webex Connector .
- Para configurar a integração do Zoom de chamada em conferência usando o canal de comunicação Notify, consulte Configuração do conector Notify para Zoom no Notify .
- Para configurar a integração de Chamada em conferência do Microsoft Teams usando o aplicativo pré-configurado, consulte Integre o aplicativo pré-publicado do Conector Notify ao Microsoft Teams .
- Para configurar a integração de Chamada em conferência do Microsoft Teams usando o aplicativo autoconfigurado, consulte Integrat ing Aplicativo autoconfigurado do Conector do Notify com Microsoft Teams .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure modelos de relatório em Resposta a incidentes de segurança

Você pode criar modelos de relatório que podem ser usados para gerar um resumo de incidente ou um resumo executivo para análise e compartilhamento.

Usar Resposta a incidentes de segurança Recurso de Modelos de relatório para criar modelos de relatório para gerar relatórios que fornecem um resumo de nível de analista ou executivo de um incidente. Você pode formatar e configurar o relatório com base em seus requisitos usando vários campos de incidente.

A tabela a seguir explica os modelos de relatório provisionados no sistema de base.

Modelos de relatório na Resposta a incidentes de segurança

Nome	Descrição
Emissão de relatórios de status do analista	Fornece informações completas de um incidente de segurança para um analista.
Resumo executivo	Fornece uma visão geral do status de um incidente de segurança para a gestão.

Nota: Por padrão, esses relatórios estão no estado de rascunho e no modo somente leitura. Você precisa reutilizar esses modelos padrão para criar e publicar modelos de relatório.

Crie um modelo de relatório em Resposta a incidentes de segurança

Crie um novo modelo de relatório para o resumo do analista ou um resumo executivo para um incidente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Espaços** > **Espaços de resposta a incidentes de segurança** > **Administração**.
2. Selecione **Relatórios** e, em seguida **Modelos de relatório** .
   A página Modelos de relatório é exibida com todos os modelos disponíveis no sistema de base.
3. Selecione **Novo**.
   Exibe o. **Detalhes** página do modelo.
4. Insira o nome e a descrição do modelo.
5. Selecione **Save** (Salvar).
6. Selecione **Conteúdo** guia.
   Exibe a página de conteúdo do modelo com um relatório em branco.
7. Selecione **Expandir** e insira os campos desejados no corpo do modelo.
   - **Campos SIR comuns** : A lista de campos mais usados para um incidente.
   - **Todos os campos SIR** : Todos os campos relacionados a um incidente. Por exemplo, quando você está gerando um relatório de incidente e deseja adicionar um campo chamado Descrição resumida, selecione esse campo em Todos os campos SIR. O campo Descrição resumida é adicionado como uma variável no modelo de relatório. Quando você gera um relatório para o analista, a descrição resumida do incidente é exibida no relatório.
   - **Registros relacionados** : Os registros relacionados de um incidente específico. Por exemplo, se você quiser adicionar observáveis associados ao relatório, poderá adicioná-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

lo ao seu modelo de relatório. Esses registros relacionados são exibidos no formato de tabela

- **Scripts** : Para adicionar a data e a hora do relatório, você pode adicionar o script de data e hora atual ao seu modelo de relatório. Esta ação adicionará a data e hora de criação do relatório no relatório.

8. Selecione **Salvar conteúdo** para salvar o conteúdo do seu modelo de relatório.
9. Selecione **Visualização** para visualizar o formato do relatório.

   Depois de adicionar todos os campos obrigatórios ao seu modelo de relatório, você precisa publicar seu modelo de relatório.

10. Selecione **Publicar** para publicar o modelo.

    Uma mensagem de confirmação será exibida se você deseja publicar o modelo de relatório.

11. **Opcional:** Selecione **Mais ações** e selecione **Excluir** para excluir o modelo de relatório.

Propriedades do sistema para relatórios

As propriedades do sistema para Resposta a incidentes de segurança os relatórios são explicados abaixo.

Propriedades do sistema para relatórios

Propriedade	Descrição	Valor
sn_si.sn_si_incident.load_all_records	Carrega todos os registros das listas no relatório criado a partir de um modelo. “verdadeiro” carrega todos os registros e “falso” carrega o número específico de registros definidos pela propriedade sn_si.sn_si_incident.reporting_list_records_count.	Falso(a)
sn_si.sn_si_incident.max_list_columns_allowed	Insira o número de colunas que podem ser adicionadas ao renderizar listas em pdfs de relatório. As colunas serão usadas desde o início da exibição até o limite permitido.	5
sn_si.sn_si_incident.report_default_style_object	Use esta propriedade para controlar o CSS de campos de formulário livre, painel esquerdo, listas de relatório.	(Objeto JSON)
sn_si.sn_si_incident.reporting_list_records_count	Carrega um número específico de registros no editor de relatórios.	200
sn_si_reporting_email_template_sn_si_incident	SYS ID do modelo de cliente de e-mail para a tabela SIR (sn_si_incident) que será usada no relatório compartilhado.	9ce97ae643461210416896ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	Cabeçalho do campo	sn_si_incident_report_field_header,sn_si_incident_rep

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema para relatórios

Propriedade	Descrição	Valor
sn_si.sn_si_incident.defang_record_list_urls	Controle se os URLs da lista são corrigidos ou não.	Falso(a)
sn_si.sn_si_incident.reporting_dot_walk_tables	Lista de tabelas disponíveis para referência com pontos em relatórios.	(Objeto JSON)

Duplique um modelo de relatório em Resposta a incidentes de segurança

Duplique um modelo de relatório para editar ou reutilizar um modelo existente para criar um novo modelo.

Antes de Iniciar

Nota: Você precisa criar uma cópia dos modelos Resumo executivo e Relatório de status do analista para reutilizá-los.

Para reutilizar o Resumo executivo e o Relatório de status do analista, você precisa criar uma cópia deles e, em seguida

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Espaços** > **Espaços de resposta a incidentes de segurança** > **Administração**.
2. Selecione **Relatórios** e, em seguida **Modelos de relatório** .
   A página Modelos de relatório é exibida com todos os modelos disponíveis no sistema de base.
3. Selecione o modelo.
4. Selecione **Duplicado** .

Resultado

O conteúdo do modelo selecionado é duplicado e a cópia do modelo selecionado está disponível na lista de modelos. O modelo duplicado está no estado Rascunho. Você pode personalizar o conteúdo e renomear o modelo conforme necessário.

O que Fazer Depois

Edite um modelo de relatório em Resposta a incidentes de segurança

Edite um modelo de relatório em Resposta a incidentes de segurança

Edite um modelo de relatório para reutilizar um modelo existente e criar um novo modelo.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaços de resposta a incidentes de segurança** > **Administração**.
2. Selecione **Relatórios** e, em seguida **Modelos de relatório** .
   A página Modelos de relatório é exibida com todos os modelos disponíveis no sistema de base.
3. Selecione o modelo.
   Exibe o. **Detalhes** do modelo no modo de edição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Atualize o nome e a descrição do modelo.
5. Selecione **Save** (Salvar).
6. Selecione **Conteúdo** guia.
   Exibe a página de conteúdo do modelo com um relatório em branco.
7. Selecione **Expandir** e insira/remova os campos desejados.
   - **Campos SIR comuns** : A lista de campos mais usados para um incidente.
   - **Todos os campos SIR** : Todos os campos relacionados a um incidente. Por exemplo, quando você está gerando um relatório de incidente e deseja adicionar um campo chamado Descrição resumida, selecione esse campo em Todos os campos SIR. O campo Descrição resumida é adicionado como uma variável no modelo de relatório. Quando você gera um relatório para o analista, a descrição resumida do incidente é exibida no relatório.
   - **Registros relacionados** : Os registros relacionados de um incidente específico. Por exemplo, se você quiser adicionar observáveis associados ao relatório, poderá adicioná-lo ao seu modelo de relatório. Esses registros relacionados são exibidos no formato de tabela
   - **Scripts** : Para adicionar a data e a hora do relatório, você pode adicionar o script de data e hora atual ao seu modelo de relatório. Esta ação adicionará a data e hora de criação do relatório no relatório.
8. Selecione **Salvar conteúdo** para salvar o conteúdo do seu modelo de relatório.
9. Selecione **Visualização** para visualizar o formato do relatório.

   Depois de adicionar todos os campos obrigatórios ao seu modelo de relatório, você precisa publicar seu modelo de relatório.

10. Selecione **Publicar** para publicar o modelo.

    Uma mensagem de confirmação será exibida se você deseja publicar o modelo de relatório.

Agendamento de plantão em Resposta a incidentes de segurança

Usar Programação de plantão em Resposta a incidentes de segurança para exibir e gerenciar turnos para seus analistas.

Com o recurso Programação de plantão, você pode exibir e gerenciar turnos, aprovar ou rejeitar solicitações de ausência. Você também pode gerenciar preferências de notificação, canais de entrega, regras de gatilho de escalação e políticas de grupo.

Principais recursos para sn_si.manager/rota_manager

- Exibir a programação de plantão, incluindo lacunas e solicitações de folga para seu grupo.
- Aprovar ou rejeitar solicitações de folga.
- Analisar e gerenciar lacunas e conflitos.
- Fornecer, substituir ou excluir cobertura e excluir solicitações de folga.
- Criar um turno e adicionar ou excluir membros a ele.
- Exibir relatórios de escalação, grupo e desempenho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos para sn_si.analyst/oc_read

- Exiba as cronogramas de plantão e confira os demais membros do seu turno.
- Enviar uma solicitação de folga e indicar outro membro do grupo para cobrir seu turno.
- Especificar sua disponibilidade e seus métodos de contato preferenciais.
- Exiba os membros e os detalhes de escalação de um turno.

Documentação para Agendamento de plantão

Para obter informações detalhadas sobre como configurar e usar os recursos de Agendamento de plantão, consulte IT Service Management Agendamento de plantão documentação.

Como usar o Espaço SIR

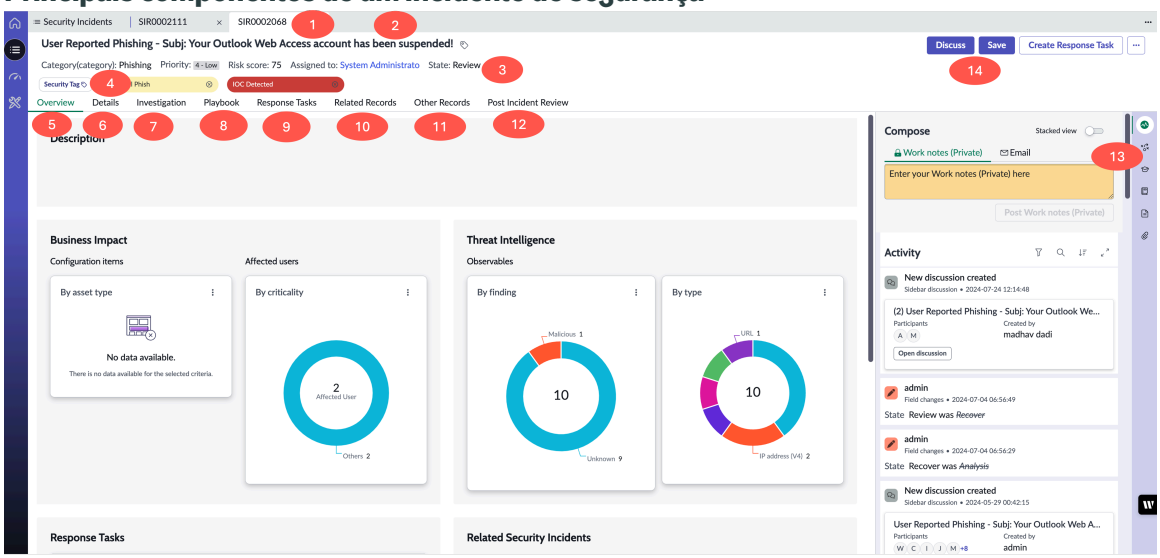
Analistas e gerentes de segurança usam Espaço SIR para executar operações diárias com uma experiência do usuário aprimorada, conclua a investigação de incidentes e obtenha uma visão geral.

Trabalhar com registros de incidentes de segurança

O registro de incidente de segurança consiste no seguinte.

Principais componentes disponíveis em um registro de incidente de segurança:

Principais componentes de um incidente de segurança



Número	Nome	Descrição
1	Número do incidente de segurança	O número do incidente de segurança está disponível em relação ao nome da guia.
2	Descrição resumida	Descrição resumida do incidente de segurança que é exibida acima da faixa do formulário.
3	Faixa do formulário	Esta é a seção somente leitura, que contém os campos principais, como Categoria, Prioridade, Pontuação de risco, Estado e os detalhes de atribuição do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
		Nota: Os marcadores regulares da plataforma também podem ser aplicados aqui.
4	Marcadores de segurança	Exibe os marcadores de segurança associados a um incidente de segurança.
5	Visão geral	Fornece uma visão geral do snapshot do incidente de segurança, como Descrição, Impacto nos negócios, que compreende detalhes do ativo por tipo, usuários afetados por criticidade, itens de inteligência contra ameaças que compreendem observáveis por descoberta e por tipo, Tarefas de resposta, incidentes de segurança relacionados que compreendem incidentes de segurança secundários e incidentes de segurança semelhantes.
6	Detalhes	A guia de detalhes exibe o formulário de incidente de segurança.
7	Investigação	A guia Investigação exibe a experiência de investigação do incidente.
8	Playbook	O Playbook é acionado por meio do Designer de automação de processos (PAD). Se um processo for criado e se uma condição de gatilho estiver definida para acionar o playbook para um incidente de segurança. Em seguida, um playbook será exibido.
9	Tarefas de resposta	As Tarefas de resposta capturam todas as tarefas de resposta associadas a um incidente de segurança.
10	Registros relacionados	A guia Registros relacionados consiste em todas as listas relacionadas da IU clássica nesta seção. As listas relacionadas são agrupadas em várias seções, como impacto nos negócios, informações sobre ameaças e assim por diante, para facilitar a navegação.
11	Outros registros	A guia Outros registros consiste em registros DE TI, como solicitações de mudanças, incidentes e e-mails agrupados e exibidos nesta seção.
12	Guia Revisão pós-incidente	À medida que o incidente de segurança progride para o estado Revisão, a guia Revisão pós-incidente é exibida com as avaliações pós-incidente e os relatórios na guia.
13	Menu contextual	Fornece acesso fácil às ações rápidas e está disponível em todas as guias para que o analista acesse sempre que necessário. O menu contextual fornece navegação fácil para os vários recursos, como: **1.** Fluxo de atividades **2.** Playbook **3.** Assistência de Analista **4.** Runbook

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
		5. Modelos **6.** Anexos
14	Ações de IU do formulário	As várias ações de IU do formulário de incidente de segurança são exibidas no canto superior direito do formulário de incidente. As ações de IU de formulário disponíveis são: • Discutir • Salvar • Criar Tarefa de Resposta • Compor e-mail • Adicionar Playbook • Abrir fluxo ou fluxos de trabalho associados • Incidente em Creta • Criar Problema • Criar solicitação de mudança • Criar indisponibilidade • Calcular Gravidade • Vincular a Incidente grave de segurança • Propor como Incidente grave de segurança • Promover para Incidente grave de segurança • Executar ações adicionais no endpoint • Associar técnica de MITRE ATT&CK • Alternar para a IU Clássica • Adicionar ao Caso de Segurança • Excluir Para obter mais informações, consulte Trabalhar com ações de IU de formulário.

Seção Visão geral do incidente de segurança

A seção Visão geral no espaço apresenta as principais informações associadas ao incidente de segurança.

Os gráficos de rosca são habilitados para detalhamento. Quando um analista seleciona qualquer um dos itens do gráfico, ele o leva até o respectivo registro com uma exibição de lista filtrada de itens nessa guia correspondente. Por exemplo, se **Observáveis mal-intencionados** é selecionado, leva você para os observáveis com uma exibição de lista filtrada de observáveis mal-intencionados no **Registros relacionados** guia.

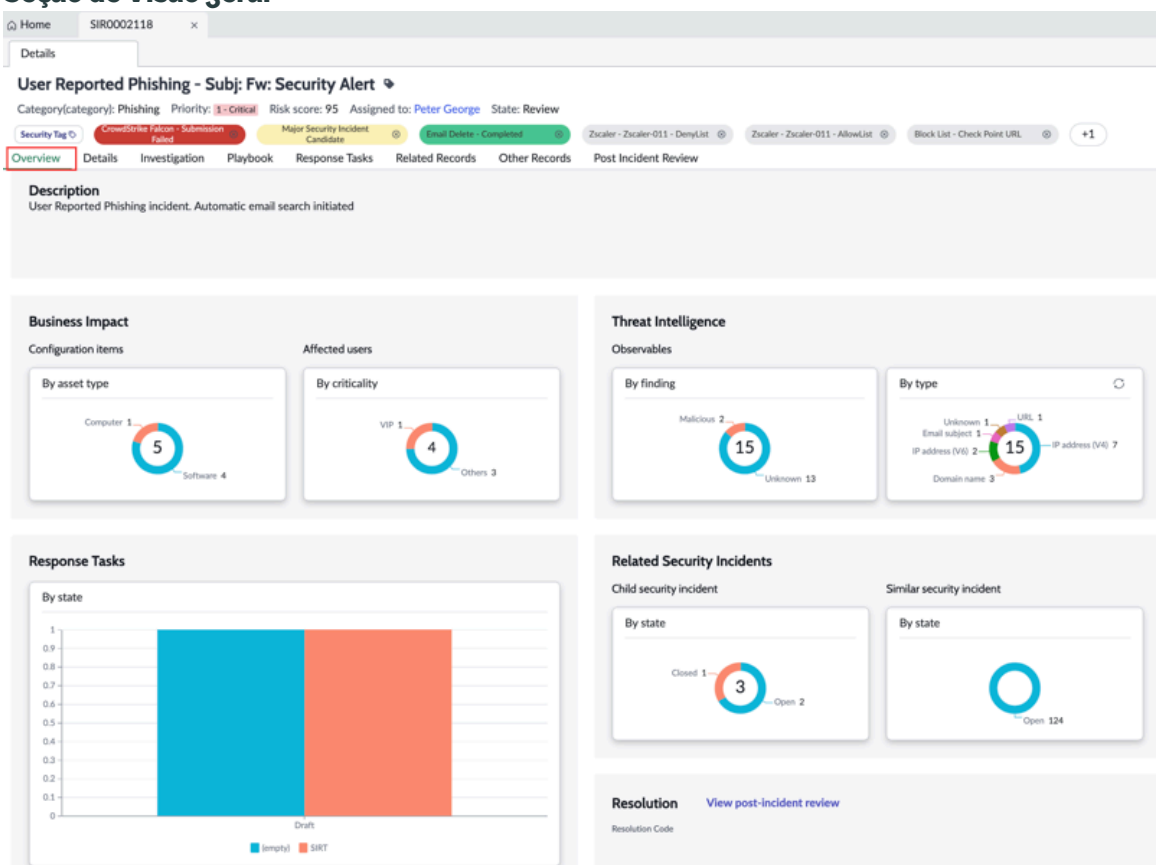
A seção Visão geral exibe o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Descrição do incidente de segurança.
- Detalhes do impacto nos negócios, como itens de configuração por tipo de ativo e usuários afetados por criticidade - sejam usuários VIP ou outros usuários.
- Itens de inteligência contra ameaças, como observáveis, descobrindo se observáveis ou mal-intencionados ou desconhecidos, e por tipo.
- Tarefas de resposta por estado e grupo de atribuição.
- Incidentes de segurança relacionados que incluem incidentes de segurança secundários por estado - abertos ou encerrados, e incidentes de segurança semelhantes por estado - abertos ou encerrados.
- A seção Resolução é exibida quando um incidente passa para o estado Revisão e, em seguida, a seção de resolução é exibida em **Visão geral** seção com capacidade de exibir a revisão pós-incidente.
- Resolução - exibir revisão pós-incidente: Selecione o link para navegar até **revisão pós-incidente** página.
- Depois que o incidente é encerrado, a seção Resolução exibe o código de resolução, as anotações de resolução e Resolvido por (usuário) junto com os detalhes da revisão pós-incidente.
- Iniciais de todos os usuários que estão acessando o mesmo incidente no momento.

Seção de Visão geral



Incidente de segurança Seção de detalhes

Esta seção exibe os campos do formulário de incidente de segurança que são renderizados a partir da IU clássica de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

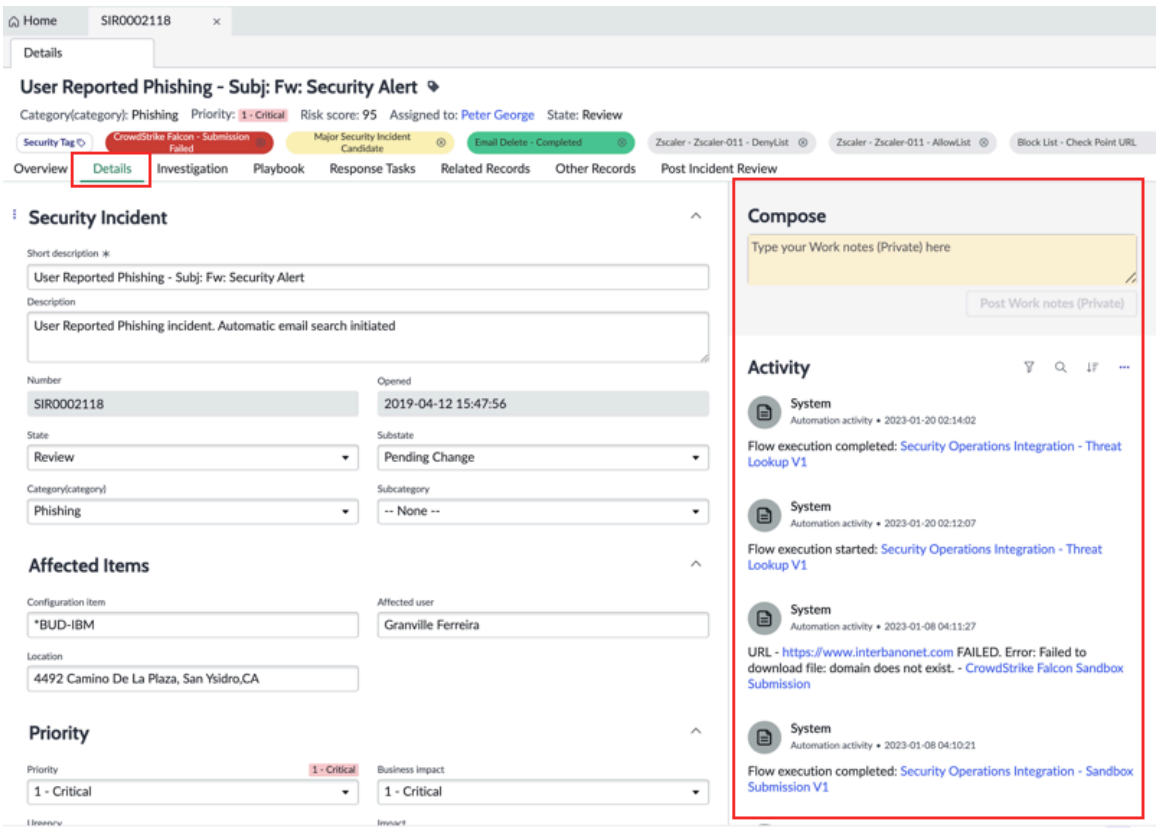
A IU clássica tem uma exibição chamada **SIRW** Exibição criada. Esta exibição é mapeada para **Detalhes** no novo espaço. Todas as personalizações necessárias precisam ser implementadas nesta exibição.

Os campos do formulário são agrupados nas seguintes seções e exibidos na exibição do formulário da guia Detalhes, clique em qualquer uma das seções ou pule para a respectiva seção no formulário:

- Incidente de segurança
- Prioridade
- Origem
- Primário
- Atribuição
- Controles de acesso
- Itens afetados
- Resolução

. **Detalhes** contém **Atividade** seção de fluxo no próprio formulário de detalhes para um acesso rápido aos analistas de segurança para adicionar comentários e publicá-los.

Guia Detalhes e Fluxo de atividades



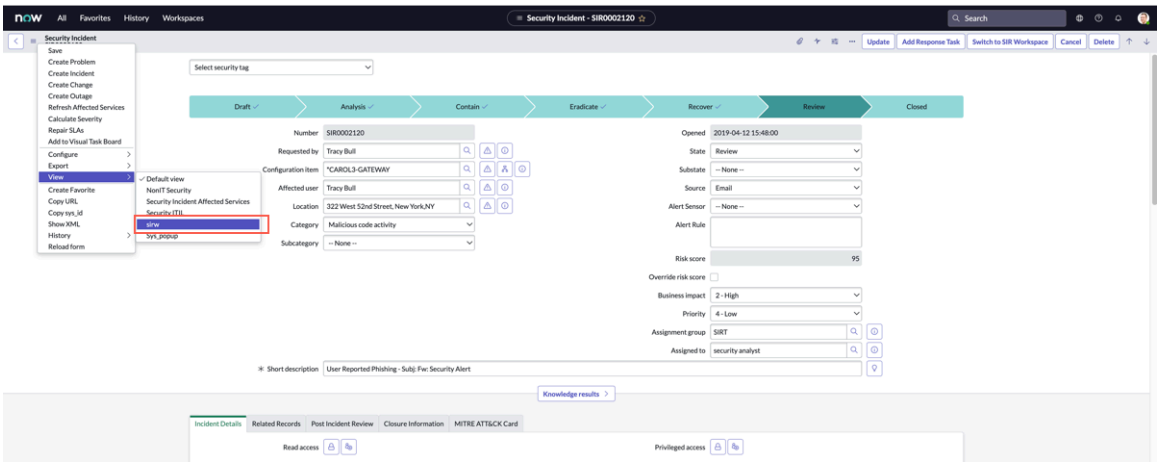
Exibir a exibição do Espaço do analista do SIR:

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Selecione qualquer registro de incidente de segurança.
3. Clique no menu de contexto e selecione **Exibição** > **SIRW**.

Tradução automática

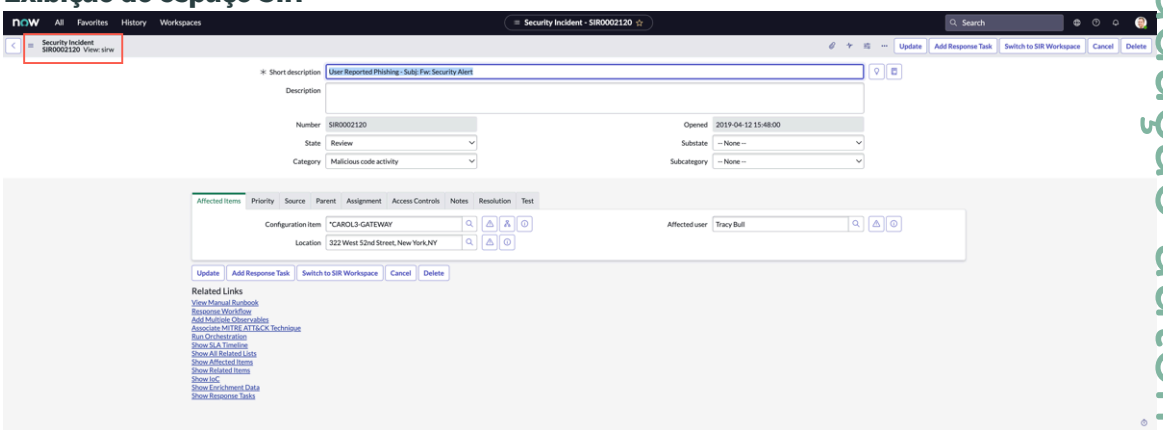
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode personalizar usando **sirw** Exibição do espaço no formulário de IU clássico.



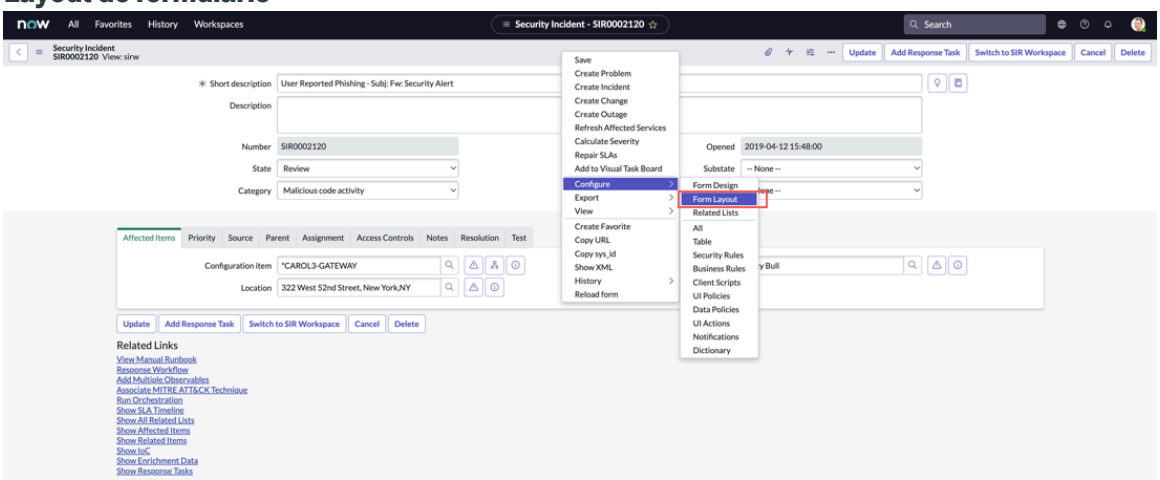
4. A exibição do espaço do incidente de segurança é renderizada conforme mostrado abaixo.

Exibição do espaço SIR



5. No registro de Incidente de segurança, clique com o botão direito do mouse e vá para **Configurar** > **Layout do formulário**.

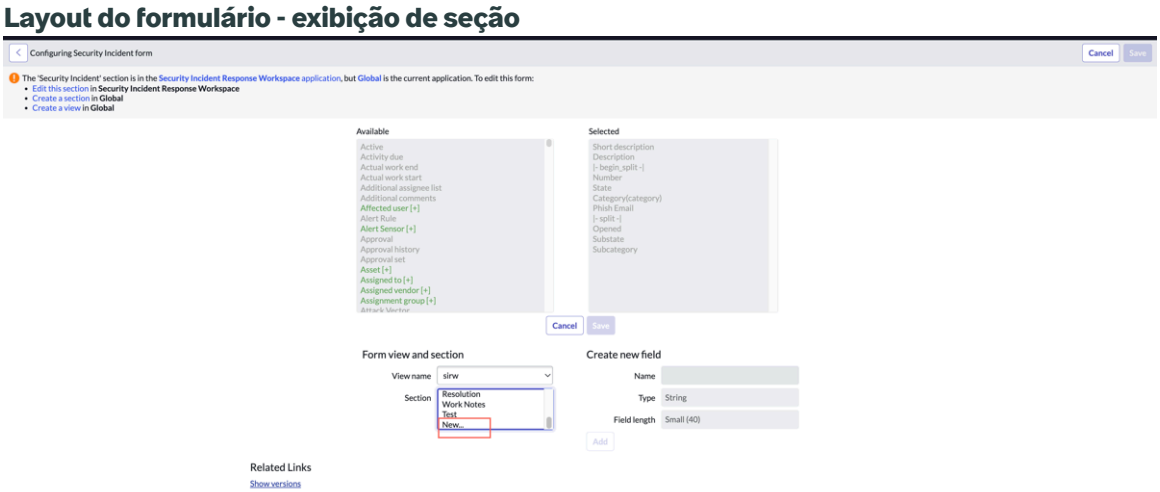
Layout do formulário



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

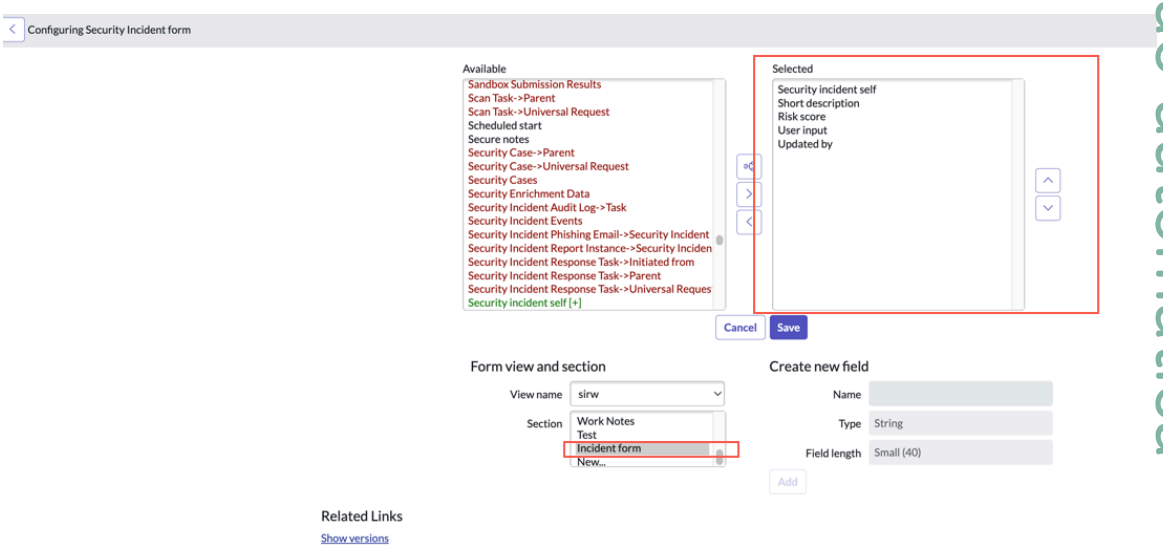
6. Detalhar até **Exibição e seção do formulário** e selecione **Novo** de **Seção** para criar uma nova seção.



7. Forneça o novo nome da seção e clique em **OK** .

   Por exemplo, formulário Incidente.

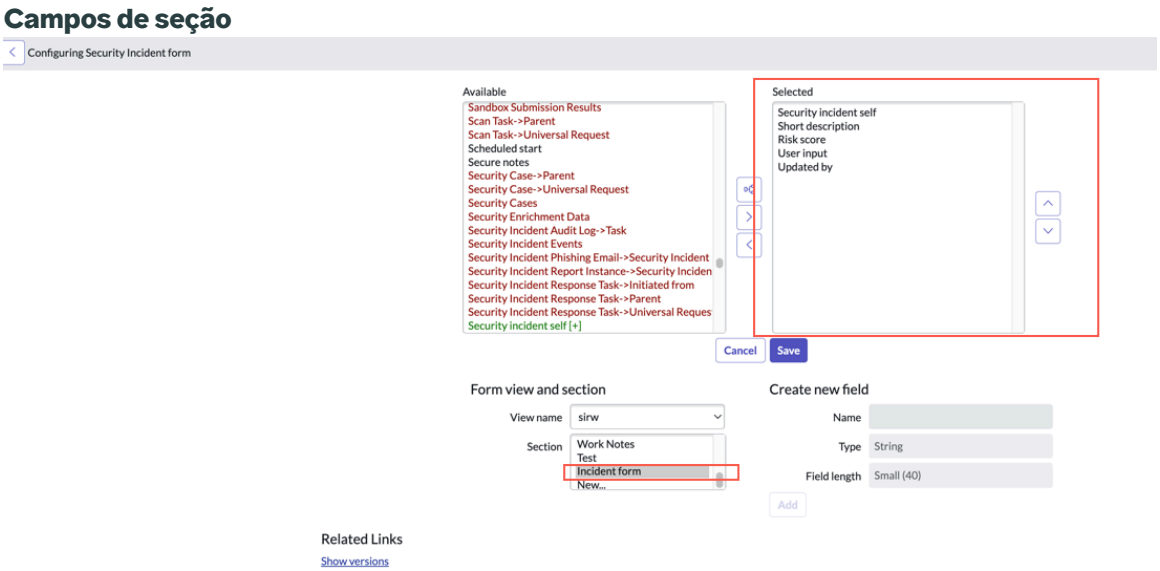
8. A nova seção é criada e adicionada ao **Seção** .



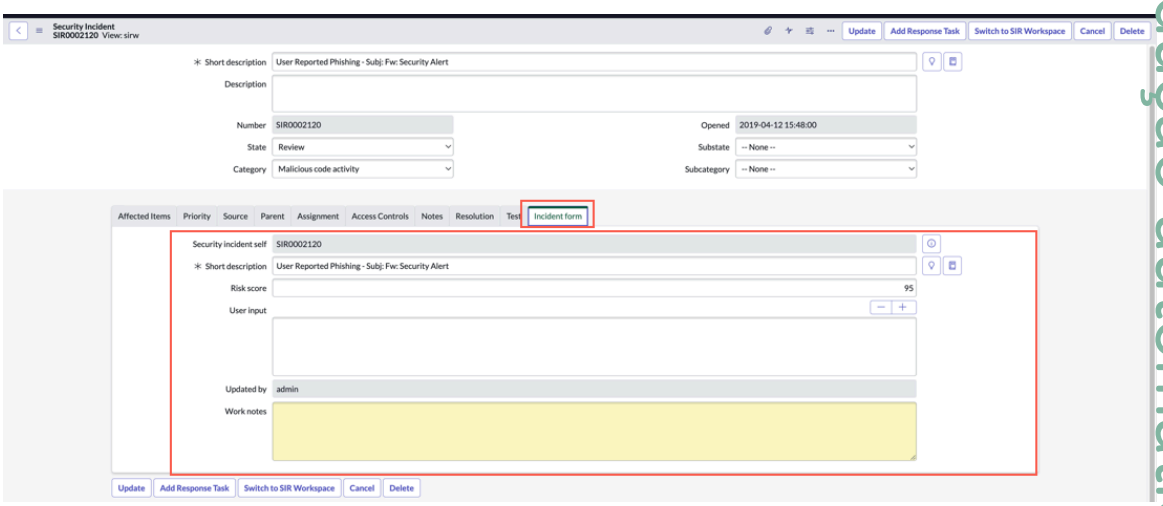
9. Selecione sua nova seção, adicione os campos de seção obrigatórios ao bucket de slush e clique em **Salvar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. A seção recém-adicionada é exibida junto com o layout da seção existente no formulário de incidente de segurança.



11. Clique em **Alterne para o espaço SIR** para ir para o formulário de incidente de segurança e a seção personalizada em **Detalhes** do espaço.

Espaço SIR Orquestração

Espaço de resposta a incidentes de segurança as atividades de orquestração ajudarão os analistas de segurança a exibir a tela de investigação e executar várias ações aplicáveis.

Espaço SIR Tela de investigação

Espaço de resposta a incidentes de segurança Permite que os analistas de segurança exibam as principais informações associadas ao incidente de segurança durante o processo de correção do incidente. As principais informações também incluem as listas relacionadas, como observáveis, resultados da pesquisa de ameaças, pesquisa de detecções, aprimoramento de observáveis e assim por diante.

Na IU clássica, a maioria das ações de orquestração associadas às integrações prontas para uso está disponível nas listas relacionadas. Por exemplo, Executar pesquisa de ameaças, Executar aprimoramento de observável etc. estão presentes na lista relacionada

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de observáveis associados. Da mesma forma Obter detalhes do host, Obter estatísticas de rede e assim por diante, estão disponíveis na lista relacionada Itens de configuração.

Quando um analista de segurança executa essas ações, os resultados são preenchidos em uma lista relacionada diferente. Por exemplo, quando um usuário executa Executar pesquisa de ameaças, os resultados ficam disponíveis na tabela Resultados da pesquisa de ameaças. Às vezes, os resultados estão disponíveis em várias tabelas diferentes. Durante esse processo, os Analistas de segurança têm uma experiência do usuário desarticulada e desorganizada ao co-relacionar as informações de vários lugares.

No novo reimaginado Espaço SIR. **Investigação** A tela (guia) fornece todas as informações necessárias agrupadas logicamente em um só lugar para que o analista execute a investigação.

Explorar tela de investigação

O objetivo primário da tela de investigação é apresentar os dados de incidente de segurança necessários em um local comum.

Em Espaço SIR, a investigação de incidentes de segurança gira principalmente em torno de alguns pontos de entrada principais.

A seguir estão alguns pontos de entrada principais provisionados para os analistas de segurança no sistema de base:

- Observáveis Associados
- Itens de configuração
- Usuários afetados
- E-mails de Phishing Associados
- Pesquisa de E-mail

Você também pode configurar os pontos de entrada acima adicionando, modificando ou removendo os pontos de entrada, conforme aplicável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

Em **Investigação** , a tabela de ponto de entrada atua como a tabela primária. Todas as tabelas que contêm os resultados de uma ação de orquestração realizada na tabela primária são apresentadas como tabela secundária no ponto de entrada.

Por exemplo, para **Observáveis associados** ponto de entrada, **Associar observáveis** Tabela é a tabela primária e outras tabelas, como Resultados da pesquisa de ameaças, Resultados de envio da área restrita e assim por diante, são a tabela secundária.

O analista de segurança pode executar todas as ações de orquestração na tabela Observáveis associados e poderá exibir todas as informações associadas na mesma página, sem a necessidade de navegar em vários lugares.

Nota: Quando um usuário clica nos gráficos interativos no **Visão geral** como observáveis mal-intencionados, o usuário será direcionado para a exibição filtrada de observáveis mal-intencionados na tela de investigação. Como alternativa, o usuário pode iniciar diretamente a investigação navegando até a tela de investigação, que terá todos os dados.

A lista de tabela secundária em um ponto de entrada também é configurável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

A seguir está um exemplo detalhado de um ponto de entrada (observável associado) configurado e provisionado no sistema de base:

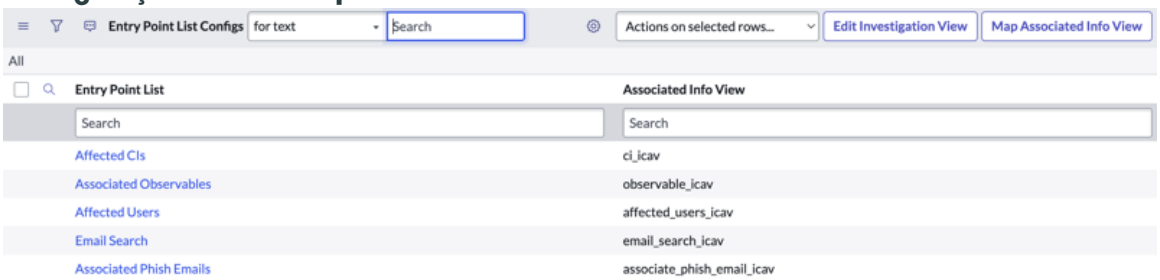
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecione **Observáveis associados** ponto de entrada na lista suspensa.

   Aqui a tabela primária também é **Observável associado** .

Configurações de lista de ponto de entrada



2. Selecione um ou mais observáveis na tabela primária.
3. Execute a capacidade desejada.

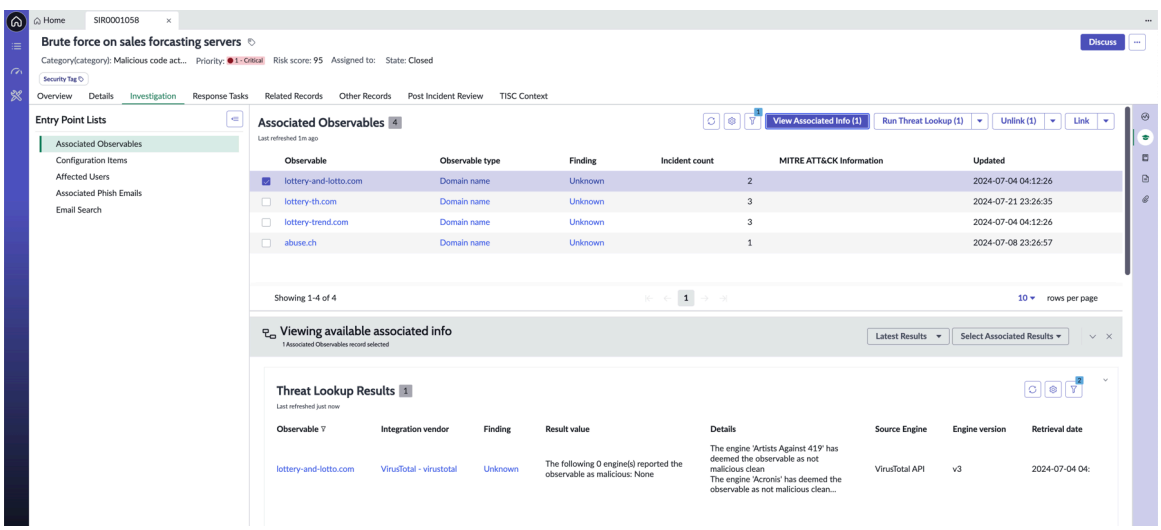
   Por exemplo, selecione **Executar Pesquisa de ameaças** para buscar os resultados da pesquisa de ameaças para um observável selecionado.

   Nota: Quando uma ação observável correspondente é executada, o processo é executado no back-end e os resultados são exibidos abaixo da lista de observáveis.

4. Clique em **Exibir informações associadas** para exibir os resultados dos observáveis. Os resultados são exibidos na mesma página.

   Nota: Você pode exibir os resultados usando filtros por resultados, selecione um deles **Todos os resultados** ou **Resultados mais recentes** qualquer que seja a exibição desejada. Os resultados mais recentes são exibidos por padrão. Se houver várias implementações (de integrações), os resultados mais recentes por implementação serão mostrados.

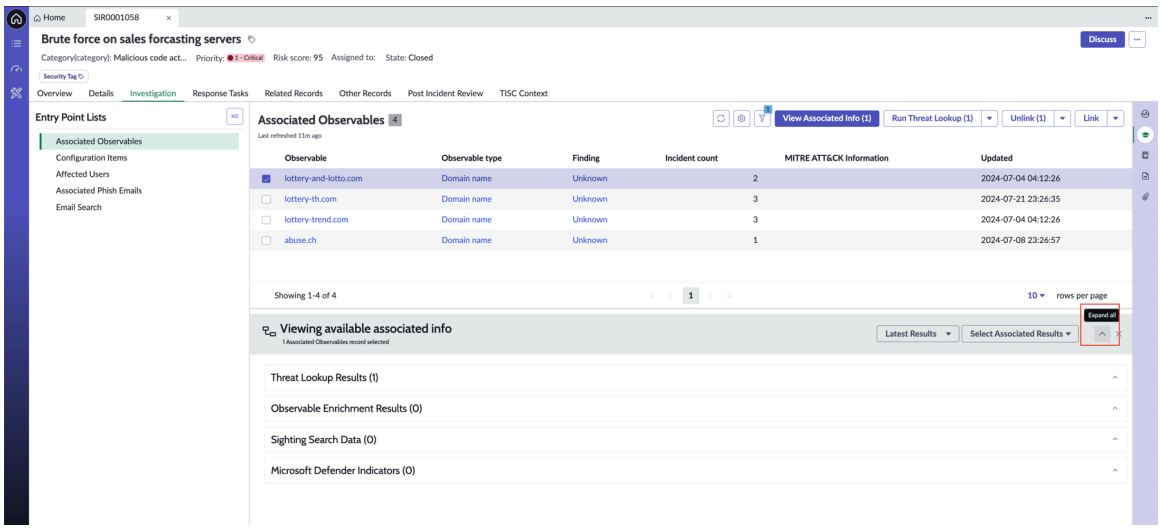
   Além disso, você pode filtrar os resultados **por listas relacionadas associadas** que são os resultados da tabela secundária. Por padrão, todas as listas relacionadas da tabela secundária configuradas são exibidas. Para obter mais informações, consulte Configurar investigação de tempo de design de SI. No entanto, você pode optar por selecionar somente as tabelas secundárias necessárias.



Tradução automática

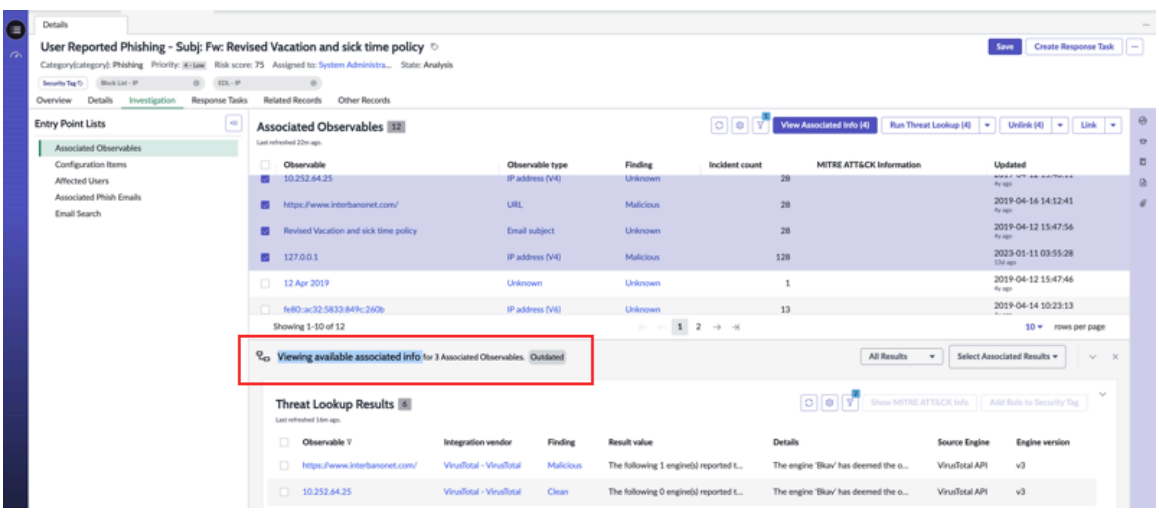
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clicando em **Exibir informações associadas** você pode exibir todos os dados da tabela secundária associada em um só lugar, no entanto, é possível fechar a exibição de listas relacionadas selecionando **Fechar exibição** botão. Depois de fechar a exibição, você só poderá ver a tabela primária de observáveis como anteriormente.
6. Clique em **Expandir tudo** ícone de direção para cima em **Exibindo informações associadas disponíveis** tabela de resultados para expandir todos os dados da tabela secundária de listas relacionadas.



7. Clique em **Recolher tudo** ícone de direção para baixo para recolher todos os dados da tabela secundária de listas relacionadas.

Nota: A faixa na parte superior da seção de informações associada que contém todos os dados da tabela secundária mostra quantas informações relacionadas ao observável estão sendo apresentadas ao usuário. Por exemplo, inicialmente, se você selecionar dois observáveis e clicar em **Exibir informações associadas** , a faixa mostra, **Exibir informações associadas disponíveis para 2 observáveis associados.** . Se você selecionar, por exemplo, outro observável, a faixa dirá que as informações estão desatualizadas (captura de tela abaixo). Você terá que clicar **Exibir informações associadas** novamente para obter os dados mais recentes.



Para além da exibição abrangente acima das informações associadas aos observáveis, se você quiser exibir mais informações sobre um registro na tabela primária, clique no observável e o formulário de registro da tabela primária será aberto em uma guia diferente com uma exibição mais detalhada do registro selecionado. Todos os dados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da tabela secundários associados desse registro selecionado específico também são apresentados em **Informações associadas** seção.

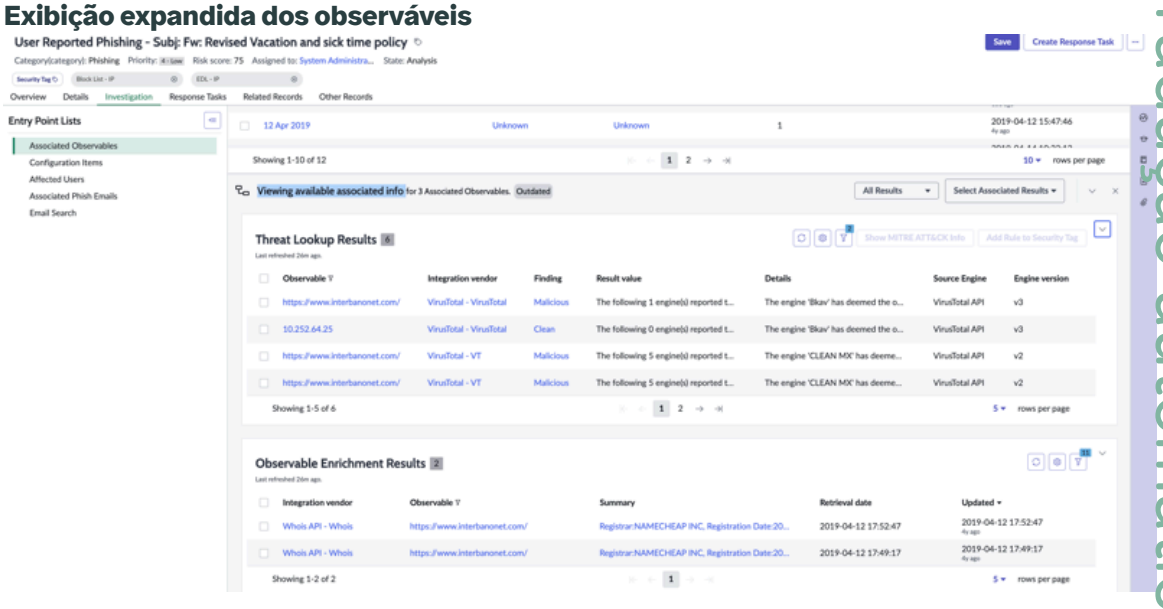
No entanto, a seção de informações associada exibe somente os resultados mais recentes da tabela secundária, conforme visto na tela de investigação, no modo somente leitura. Nenhuma ação é possível nesta exibição. A página do formulário da tabela secundária pode ser aberta em uma nova guia que renderizará a página totalmente funcional com quaisquer ações, se houver.

Você pode alternar entre as diferentes tabelas usando a lista suspensa. Você também pode expandir ou recolher cada formulário na seção de informações associada.

Em **Observável** página de formulário (página de formulário de registro de tabela primária) você pode executar determinadas ações conforme disponíveis. Sempre que executar uma ação, você pode clicar em atualizar na faixa de informações associada para atualizar os dados.

8. Clique em **Expandir tudo** para expandir todas as tabelas secundárias de listas relacionadas. Por padrão, todos os secundários são expandidos.

Exibição expandida dos observáveis



Tópicos relacionados

Configurar investigação de tempo de design de SI

Estrutura de experiência unificada para integrações com tecnologia da Estrutura de capacidade

Na IU clássica, a experiência é desarticulada ao executar atividades de orquestração, como executar a aparência de ameaça, executar a pesquisa de vistas e assim por diante. Cada capacidade tem sua própria experiência ao executá-la. No novo espaço, há uma experiência unificada em todos os recursos.

A experiência unificada é aplicável somente às integrações e atividades de orquestração que se enquadram na estrutura de capacidade. Pode haver ações específicas para a integração, por exemplo, Criar indicadores no Microsoft Defender. Essas ações terão sua própria experiência, conforme exigido pelo caso de uso.

A nova estrutura consiste em telas modais com três etapas, conforme explicado abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. **Implementações** : A primeira etapa envolve a seleção de uma ou mais implementações presentes em relação à capacidade selecionada.

   Por exemplo, quando o analista clica **Executar Pesquisa de ameaças** , O analista poderá selecionar uma ou mais implementações presentes para **Executar recurso de pesquisa de ameaças** .

   Cada implementação terá os detalhes da origem de integração. Consulte a tabela abaixo. Informações adicionais também são apresentadas em relação a cada implementação.

   Informações adicionais podem incluir, por exemplo, informações sobre quaisquer filtros, tipos de observáveis compatíveis etc. As Informações adicionais podem ser configuradas conforme desejado. Para obter mais informações, consulte o procedimento de configuração técnica da estrutura de UX.

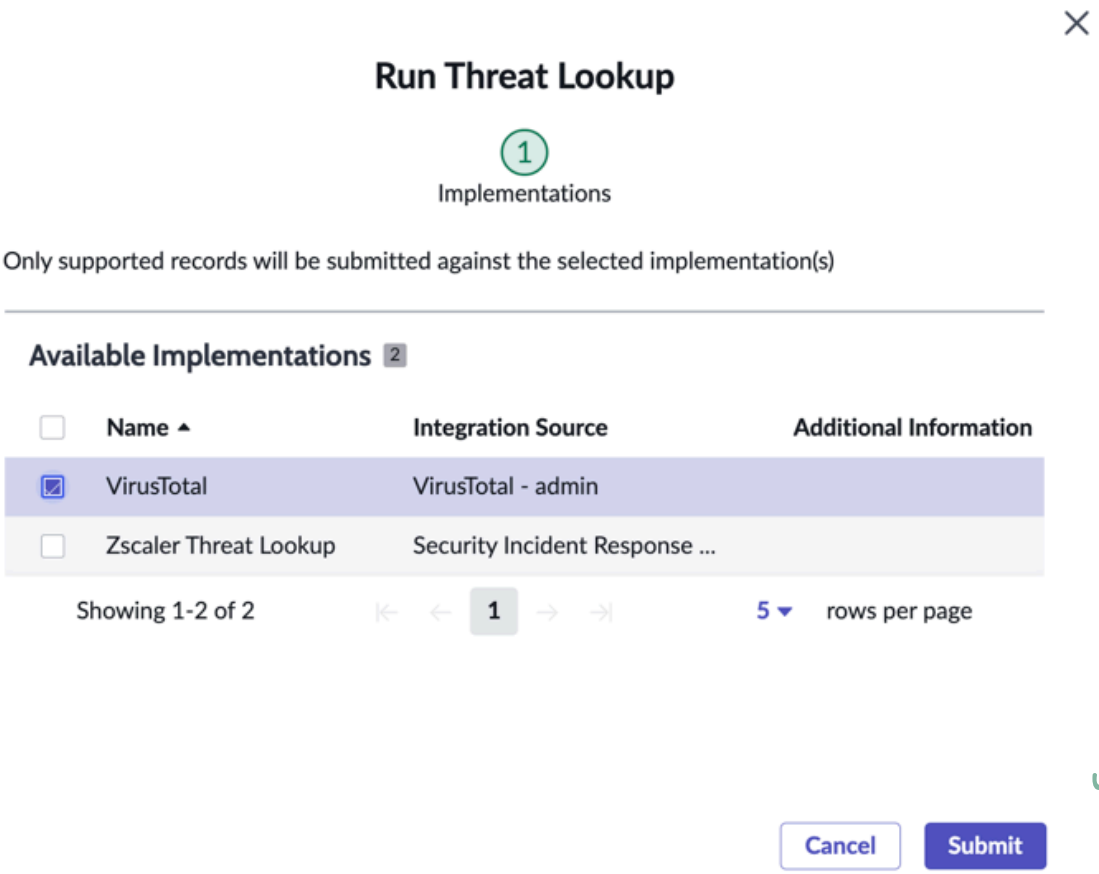
Modal da Estrutura de implementação unificada

Implementação	Descrição
Nome	Nome da implementação.
Origem da Integração	A origem da implementação, como a configuração que está sendo usada.
Informações adicionais	Esta coluna captura as informações estáticas que adicionam mais contexto ao analista de segurança em relação às implementações selecionadas para prosseguir com uma ação. Por exemplo, capacidade de suporte ou informações filtradas. Além disso, se uma implementação oferecer suporte a apenas um determinado tipo de observáveis, como Domínio ou URL, você poderá adicionar essas informações adicionais aqui nesta coluna para fornecer o contexto ao usuário. **Nota:** Basicamente, a estrutura de IU permitiria a seleção de qualquer tipo de implementação e qualquer tipo de observáveis. Durante o envio, as integrações do sistema de base existentes que são enviadas cuidarão da filtragem no back-end e enviarão somente o tipo compatível de observáveis. Os demais registros que não corresponderem à capacidade de suporte serão ignorados. Portanto, uma mensagem de informações de IU é exibida enquanto você seleciona a capacidade: **Somente registros compatíveis serão enviados em relação às implementações selecionadas.**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1: Implementação(ões)

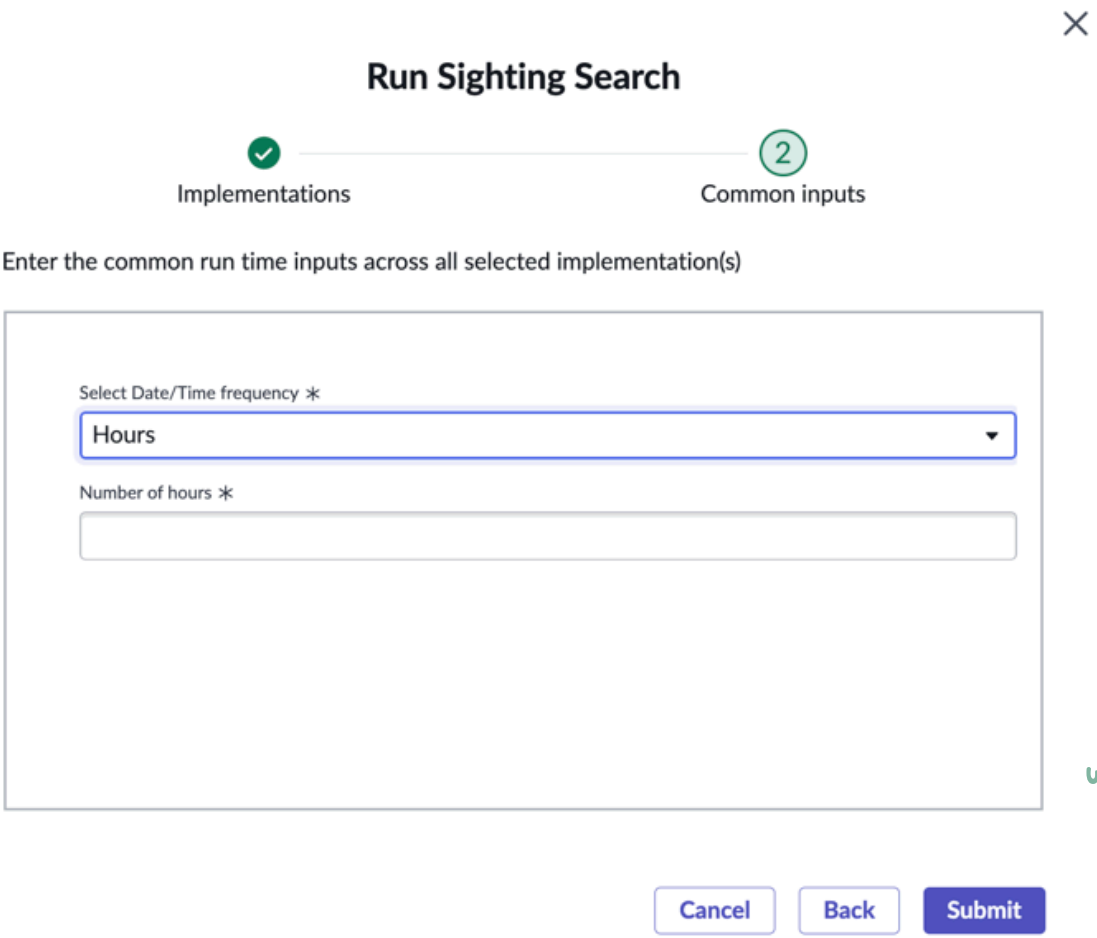


2. **Entradas comuns** : Adicione entradas comuns para as implementações selecionadas ou para todas as implementações aplicáveis selecionadas. Esta é a tela 2 da sua implementação. Somente a partir de agora **Pesquisa de vistas** tem a tela de entradas comuns. Esta implementação é uma combinação da tela 1 (implementações) e da tela 2 (entradas comuns).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1 e tela 2



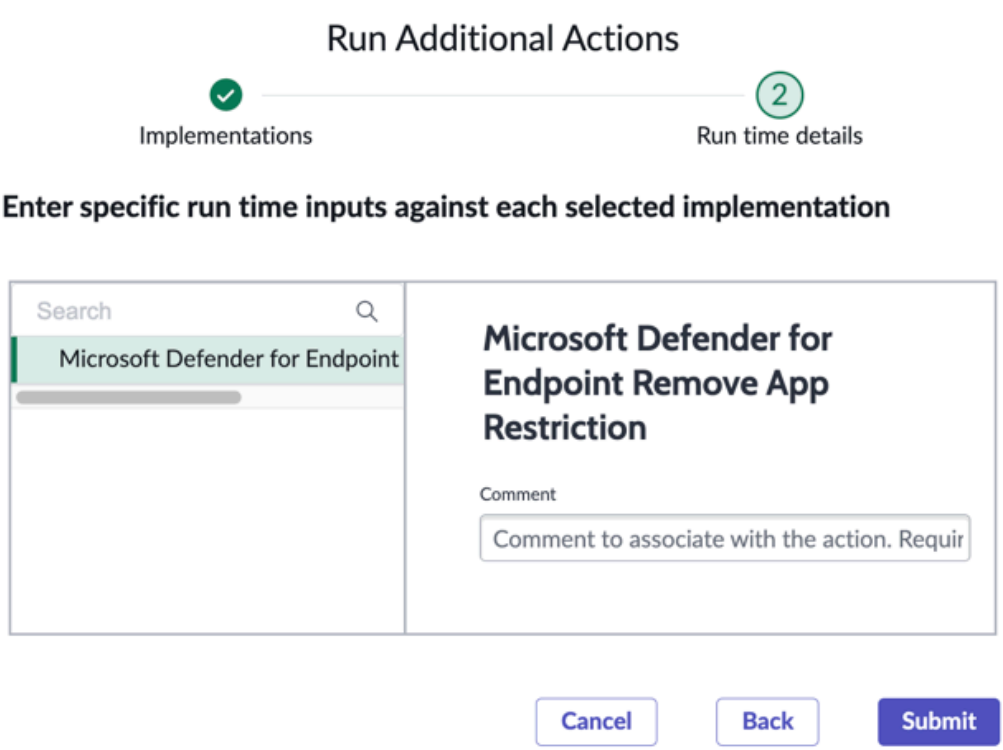
3. **Detalhes do tempo de execução** : Adicione entradas de tempo de execução específicas para as implementações selecionadas que são diferentes entre si. Esta é a tela 3 da sua

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

implementação. Esta implementação é uma combinação da tela 1 (implementações) e da tela 3 (entradas de tempo de execução específicas).

Entradas específicas



Nota: Nem todas as três etapas são sempre necessárias. Dependendo da capacidade e do tipo de entradas necessárias, a etapa de detalhes do tempo de execução e a etapa de entradas comuns estarão visíveis.

Recursos de experiência unificada e telas modais

A tabela a seguir descreve os recursos e as telas aplicáveis.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Executar pesquisa de ameaças	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Executar pesquisa de ameaças. Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou	• Total de vírus • Hybrid Analysis • Integração da Resposta a incidentes de segurança com Zscaler • Phistank • Metadender • Threatcrowd

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• Eu fui penhorado? • Crowd Strike Falcon Intelligence
Executar Aprimoramento do observável	Somente a tela 1 - Selecionar implementações é aplicável Não há entradas comuns ou entradas específicas de implementação aplicáveis para Executar aprimoramento do observável. Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• MISP • Endpoint do Microsoft Defender • Shodan • RiskIQ • WHOIS • Reverter WHOIS
Executar Pesquisa de vistas/ Executar Pesquisa de vistas na web/Executar Pesquisa de vistas por e-mail	Tela 1 – **Selecione Implementações** E tela 2 – **Entradas comuns** aplicáveis. A pesquisa de vistas usa a frequência de data e hora como entradas comuns em várias implementações do Splunk e outras integrações. Esta tela será apresentada ao analista de segurança para capturar frequências de data e hora. Para integrações que não exigem essas entradas, por exemplo, FireEye HX, elas serão ignoradas. Depois de selecionar uma ou mais implementações e fornecer entradas comuns, o analista de segurança poderá enviar a ação.	• Aprimoramento de incidente Splunk • Carbon Black • Pesquisa elástica • FireEye HX • McAfee ESM • MSFT Defender para endpoint • Splunk avistamento • Pesquisa de detecções do Qradar • MISP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Enviar para área restrita	Tela 1 – Selecionar implementações e Tela 3 – Implementações específicas são aplicáveis. Enviar para área restrita usa entradas diferentes para diferentes implementações. Não há entradas comuns para esta capacidade no momento. Por exemplo, quando o analista seleciona Crowdstrike Falcon X Quick Scan, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux e Zscaler, as entradas variam. Crowdstrike Falcon X Quick scan e Zscaler não precisam de entradas de tempo de execução adicionais. Crowdstrike Falcon X Windows 64 usa entradas opcionais de tempo de execução que diferem do Crowdstrike Falcon X Linux. Estes podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas, conforme aplicável.	• Integração do CrowdStrike Falcon X Sandbox • Integração da Resposta a incidentes de segurança com Zscaler
Publicar na lista de observadores	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para **Publicar na Lista de observação** . Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	Host do Crowdstrike Falcon

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Permitir/bloquear solicitação	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para **Solicitação de permissão/bloqueio** . Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• Palo Alto Network NGFW • NGFW do ponto de verificação • Integração da Resposta a incidentes de segurança com Zscaler
Obter detalhes do host	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter detalhes do host. Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• FireEye HX • Endpoint do Microsoft Defender
Obter arquivo	As telas 1 - Selecionar Implementações e Tela 2 - Entradas comuns são aplicáveis. Obter arquivo usa o nome do arquivo, o caminho como entradas comuns. Depois de selecionar uma ou mais implementações e fornecer entradas comuns, o analista de segurança poderá enviar a ação.	FireEye HX

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Obter estatísticas de rede	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter estatísticas de rede. Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• FireEye HX • Netstat
Obter processos em execução	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter processos em execução. Somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• FireEye HX • Carbon Black • Comando do sistema
Obter serviços em execução	Somente a tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter serviços em execução. Somente a tela 1 é apresentada ao analista para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista poderá enviar a ação.	FireEye HX

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Isolar host/Desisolar host	Tela 1 – Selecionar implementações e Tela 3 – Implementações específicas são aplicáveis. Isolar host/Não isolar host usa entradas diferentes para diferentes implementações. Não há entradas comuns para esta capacidade no momento. Por exemplo, quando o analista seleciona FireEye HX e Microsoft Defender para Endpoint, as entradas variam. O FireEye HX não precisa de entradas de tempo de execução. Por outro lado, o Microsoft Defender usa entradas como Tipo de isolamento e Comentários. Estes podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas, conforme aplicável.	• FireEye HX • Endpoint do Microsoft Defender • Carbon Black
Executar ações adicionais	Tela 1 – Selecionar implementações e Tela 3 – Implementações específicas são aplicáveis. Executar ações adicionais O host usa entradas diferentes para diferentes implementações. Não há entradas comuns para esta capacidade no momento. Por exemplo, quando o analista seleciona Script de detalhes investigativos padrão do FireEye HX, Aquisição de triagem do FireEye HX e descarregamento de registro do Crowdstrike Falcon Insight, as entradas variam.	• FireEye HX • Endpoint do Microsoft Defender • Crowdstrike Falcon Insight

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de capacidades e telas aplicáveis

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	O script de detalhes investigativos padrão do FireEye HX e a aquisição de triagem do FireEye HX consideram os comentários como a entrada que pode ser diferente para ambos. O descarregamento de registro do Crowdstrike Falcon Insight usa a subchave como entrada. Estes podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas, conforme aplicável. **Nota:** Atualmente oferece suporte a apenas uma seleção de implementação. Em versões futuras, a seleção múltipla de implementação será compatível.	

Exemplos de experiência unificada

Este exemplo demonstra os recursos da estrutura de experiência unificada.

Exemplo 1: Selecione Implementações: Pesquisa de ameaças

O exemplo abaixo demonstra a(s) implementação(ões).

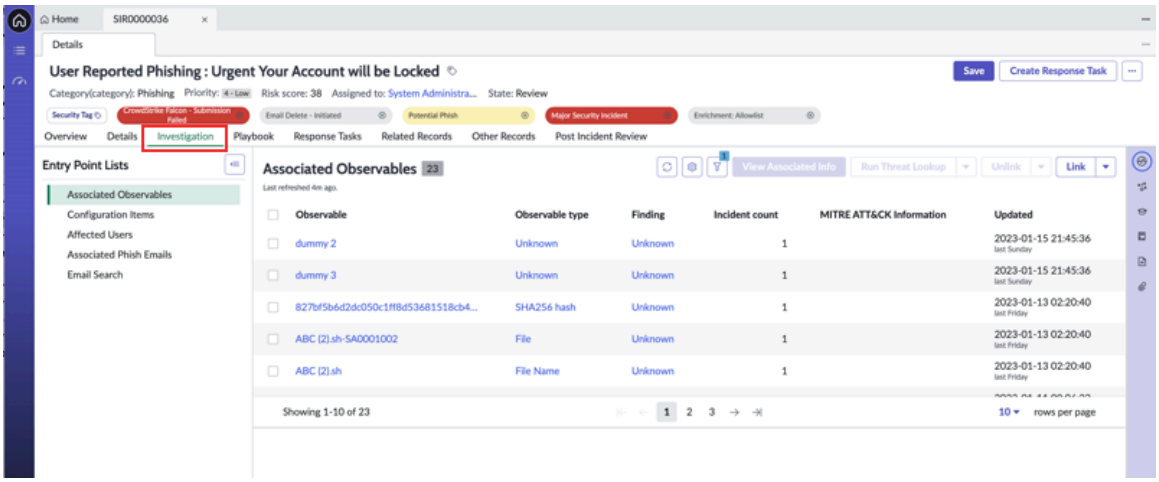
Exemplo 1: Somente tela 1: Pesquisa de ameaças

Você pode executar **Executar Pesquisa de ameaças** ação de capacidades de integração relacionadas usando **Investigação** . Espaço SIR.

1. Em **Investigação** , navegue até **Listas de pontos de entrada** seção exibida no lado esquerdo da página.
2. Selecione qualquer ponto de entrada e execute a ação de capacidade de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você também pode navegar até **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

Pesquisa de ameaças é um dos exemplos que é descrito em detalhes sobre como executar as integrações.

Selecione Implementações

Selecione uma ou mais implementações conforme aplicável.

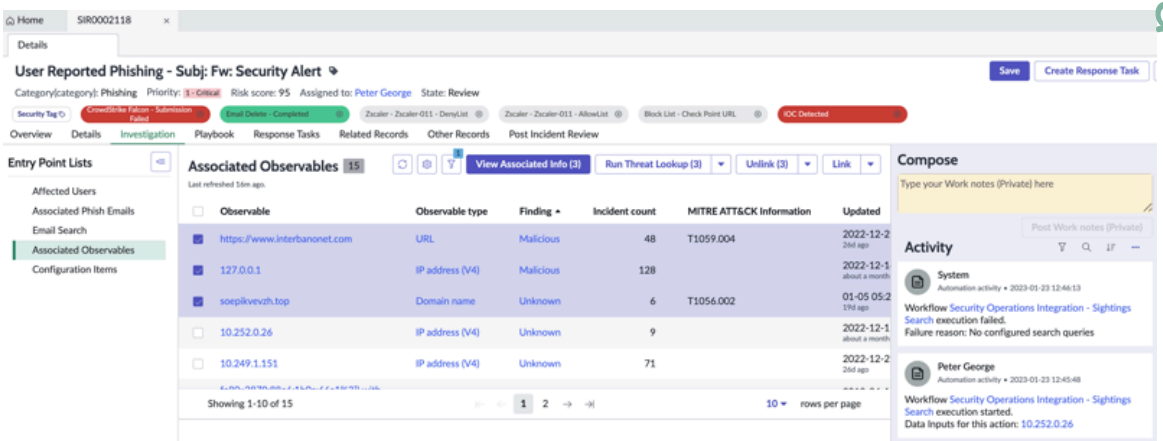
Antes de Iniciar

Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Depois de selecioná-las, somente os registros compatíveis serão enviados para cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para **Investigação** do espaço.
   A guia Investigação com as listas de pontos de entrada é exibida.



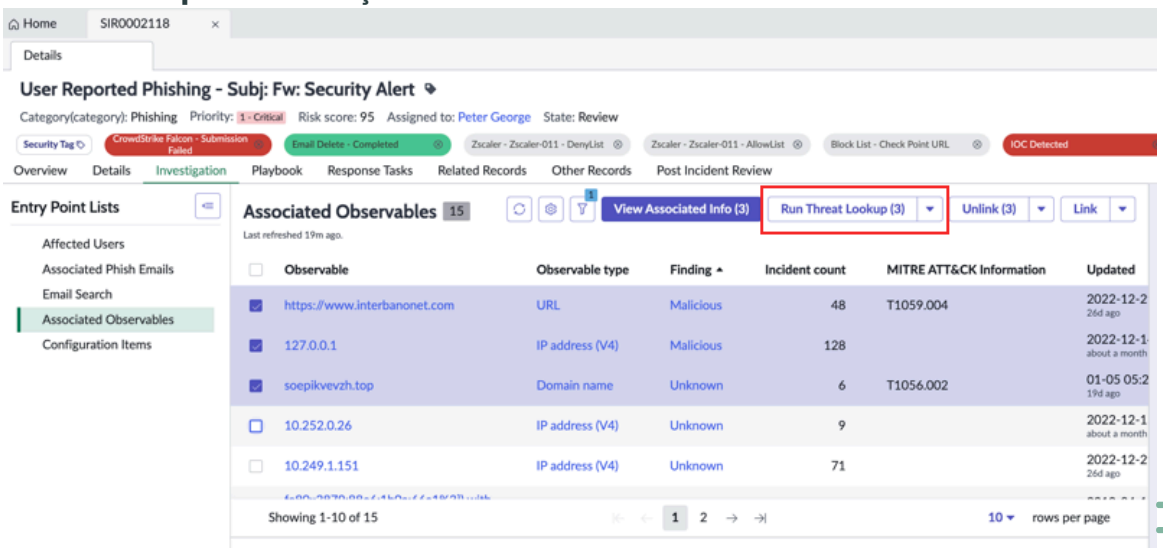
4. Selecione o observável associado nas listas de pontos de entrada.
   Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode selecionar uma implementação para executar uma pesquisa nos observáveis selecionados ou pode executar a pesquisa selecionando Todas as implementações.

Executar Pesquisa de ameaças

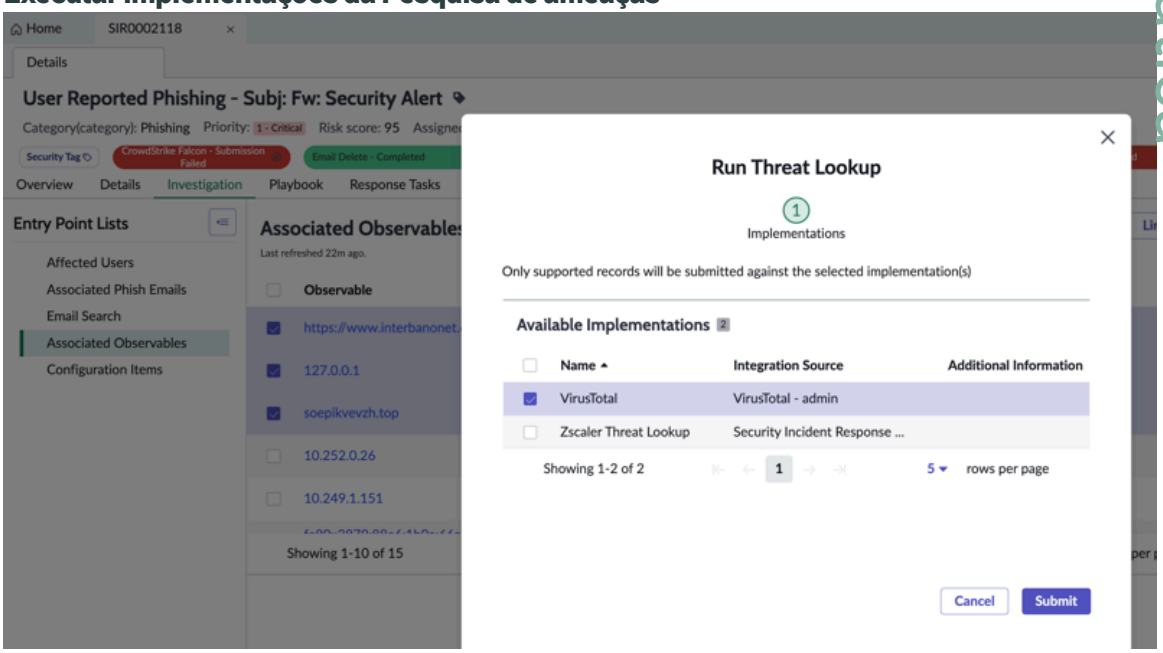


5. Marque qualquer caixa de seleção de observável que você deseja executar a pesquisa de ameaça.
6. Navegue até o menu suspenso Ações de listas relacionadas que é exibido na parte superior da página Listas relacionadas.
7. Selecione **Executar Pesquisa de ameaças** para executar a ação de capacidades de integração relacionadas à intel contra ameaças.

Nota: O recurso Executar pesquisas de ameaças executa pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

. **Executar implementações da Pesquisa de ameaças** a tela modal é exibida.

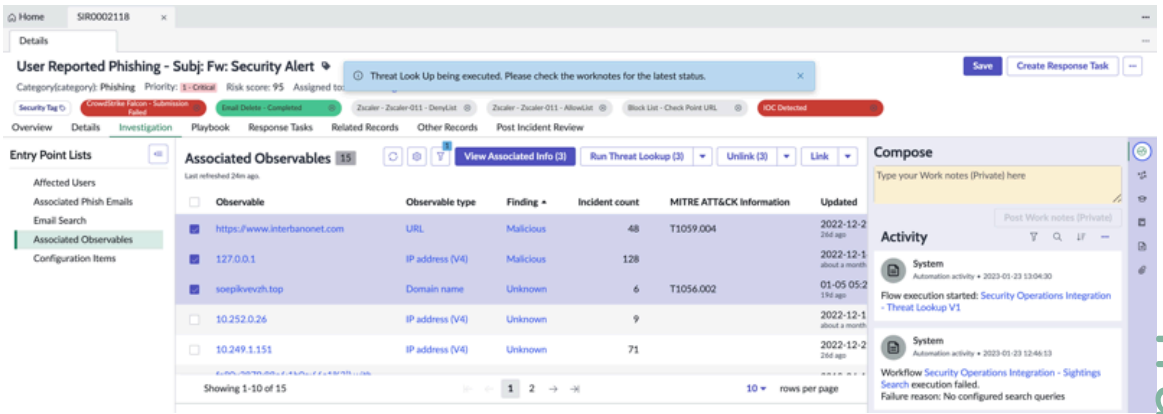
Executar implementações da Pesquisa de ameaças



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione uma ou mais implementações na lista.
9. Clique em **Enviar**.
   Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a pesquisa está sendo executada. Depois que a implementação é processada no back-end, os resultados são exibidos no **Resultados da pesquisa de ameaças** seção de lista relacionada. Além disso, a respectiva atividade de implementação é exibida em **Atividade** seção. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.



Nota: . **informações sobre ameaças** listas relacionadas, como as listas relacionadas de observáveis associados, são exibidas no **Resultados da pesquisa de ameaças** e **Pesquisa de vistas** as listas relacionadas são exibidas no **Resultados da pesquisa de vistas** Seção em Registros relacionados.

Exemplo 2: Entradas comuns: Pesquisa de vistas

O exemplo abaixo demonstra a ação de capacidade de entradas comuns.

Você pode executar **Executar Pesquisa de vistas** ação de capacidades de integração relacionadas usando **Investigação** . Espaço SIR.

1. Em **Investigação** , navegue até **Listas de pontos de entrada** seção exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação de capacidade de integração.

Nota: Você também pode navegar até **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

Adicione entradas comuns a uma implementação

Adicione entradas de tempo de execução comuns que se aplicam a todas as implementações selecionadas, conforme aplicável.

Antes de Iniciar

Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Depois de selecioná-las, somente os registros compatíveis serão enviados para cada implementação selecionada.

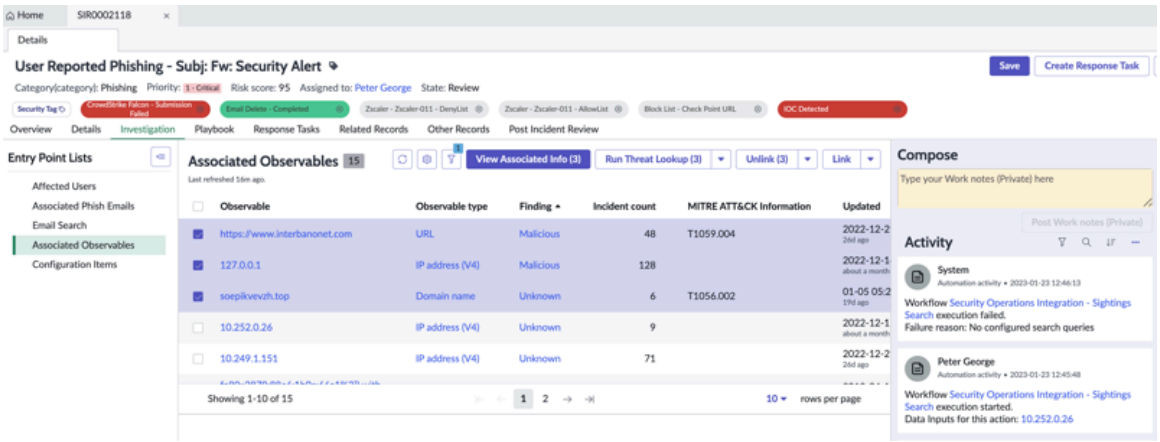
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

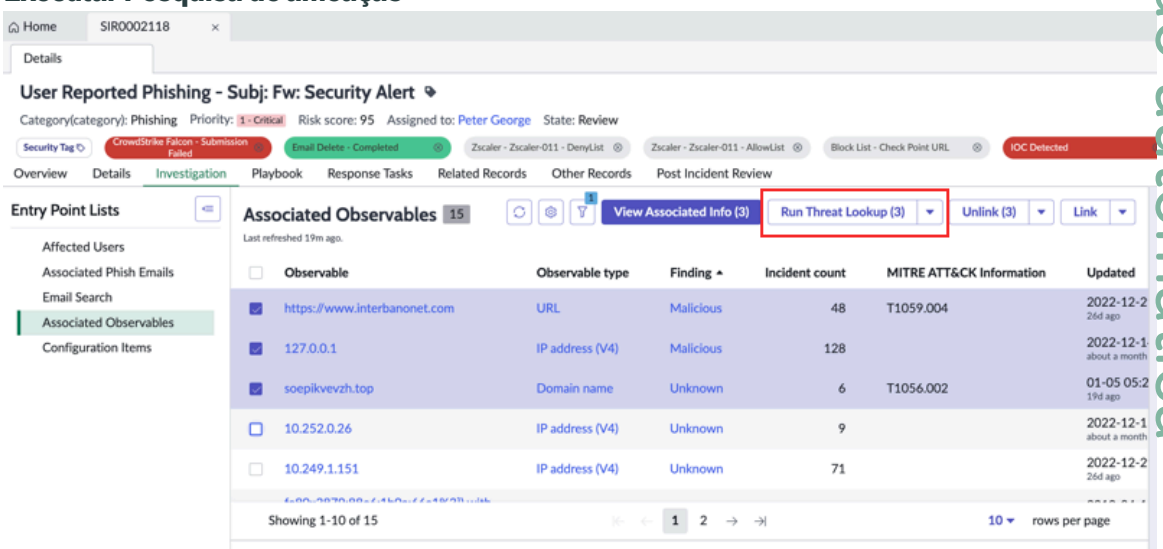
3. Vá para **Investigação** do espaço.
   A guia Investigação com as listas de pontos de entrada é exibida.



4. Selecione o observável associado nas listas de pontos de entrada.
   Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

   Nota: Você pode selecionar uma implementação para executar uma pesquisa de observação para os observáveis selecionados ou selecionando várias implementações.

Executar Pesquisa de ameaças



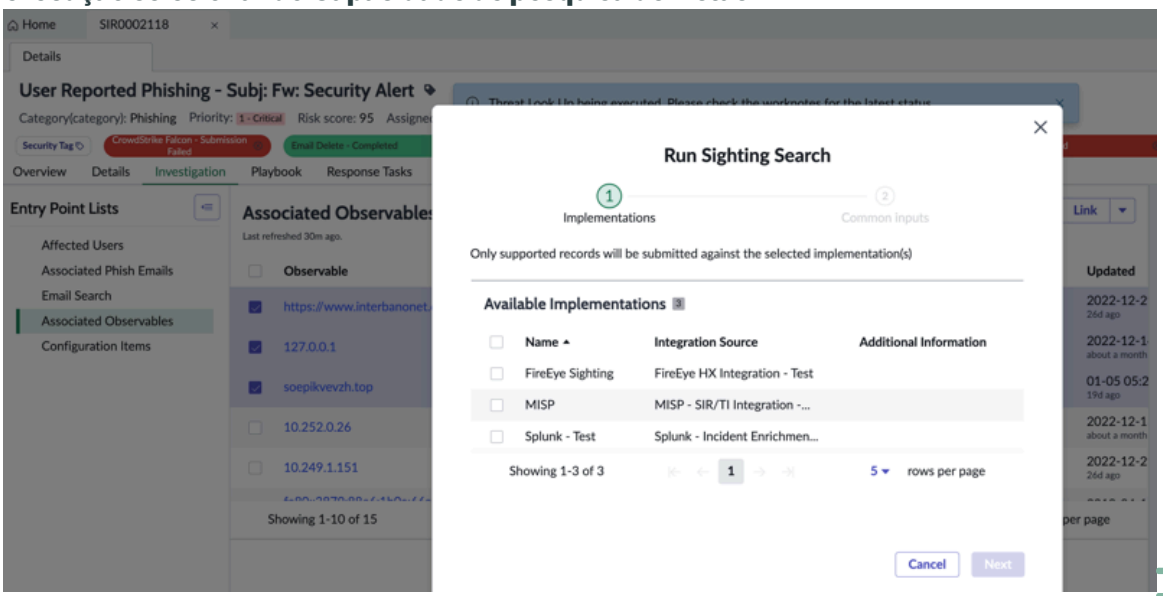
5. Marque qualquer caixa de seleção de observável que você deseja executar a pesquisa de ameaça.

6. Selecione **Executar Pesquisa de vistas** para executar a pesquisa de e-mail.
   A caixa de diálogo do modal Executar implementações de pesquisa de vistas é exibida.

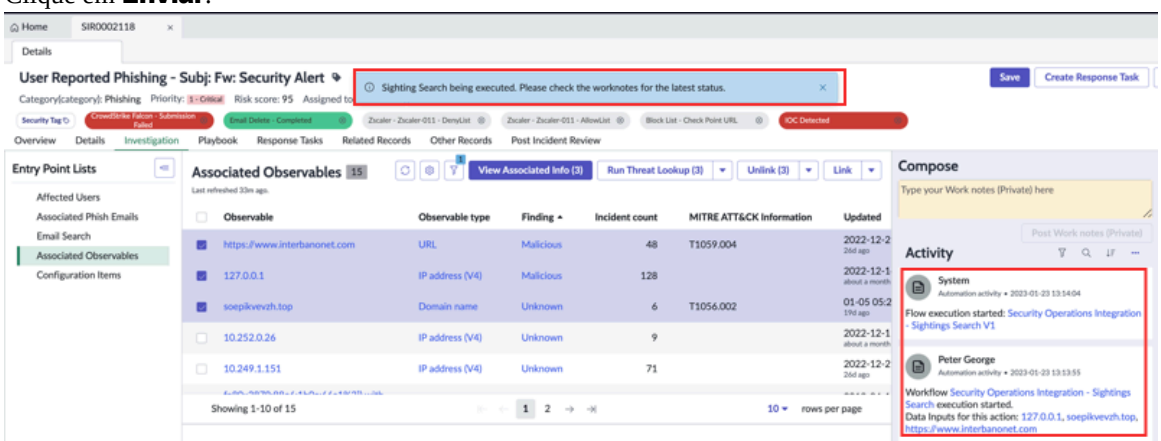
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um exemplo que mostra como adicionar entradas comuns de tempo de execução selecionando Capacidade de pesquisa de vistas



7. Selecione uma ou mais implementações na lista.
8. Clique em **Avançar**.
   Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a pesquisa de vistas está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos no **Pesquisa de vistas** seção de lista relacionada. Além disso, a respectiva atividade de implementação é exibida na seção Atividade. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.
9. Selecione o valor de entrada de tempo de execução comum.
10. Clique em **Enviar**.



Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a pesquisa de vistas está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos no **Resultados da pesquisa de vistas** seção de lista relacionada. Além disso, o respectivo status de processamento da atividade de implementação é exibido em **Atividade** seção.

Exemplo 3: Adicione entradas de detalhes de tempo de execução específicas a uma implementação: Executar ações adicionais

Adicione entradas de detalhes de tempo de execução específicas a uma implementação, Executar ações adicionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode executar **Executar ações adicionais** ação de capacidades de integração relacionadas usando **Investigação** . Espaço SIR.

1. Em **Investigação** , navegue até **Listas de pontos de entrada** seção exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação de capacidade de integração.

Nota: Você também pode navegar até **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

Adicione entradas específicas a uma implementação

Adicione entradas de tempo de execução específicas para cada uma das implementações selecionadas, conforme aplicável.

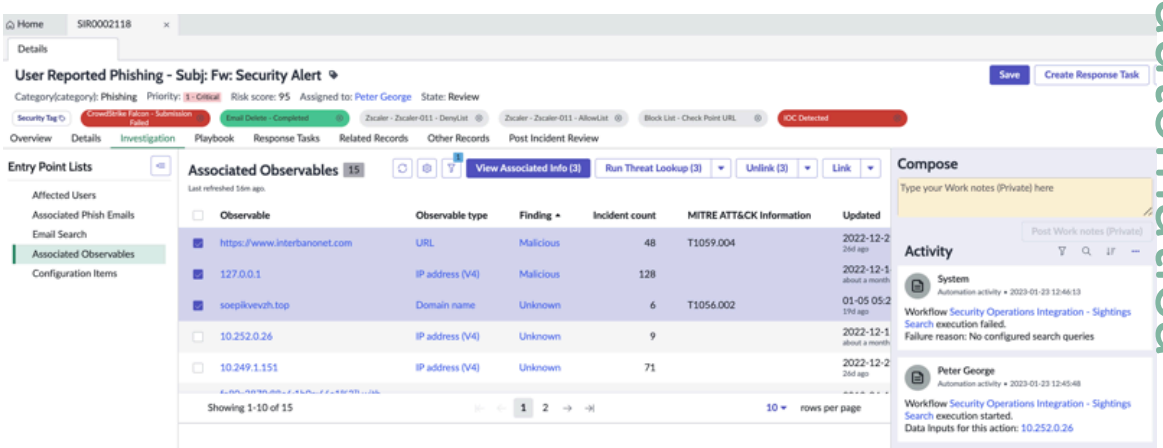
Antes de Iniciar

Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Depois de selecioná-las, somente os registros compatíveis serão enviados para cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para **Investigação** do espaço.
   A guia Investigação com as listas de pontos de entrada é exibida.

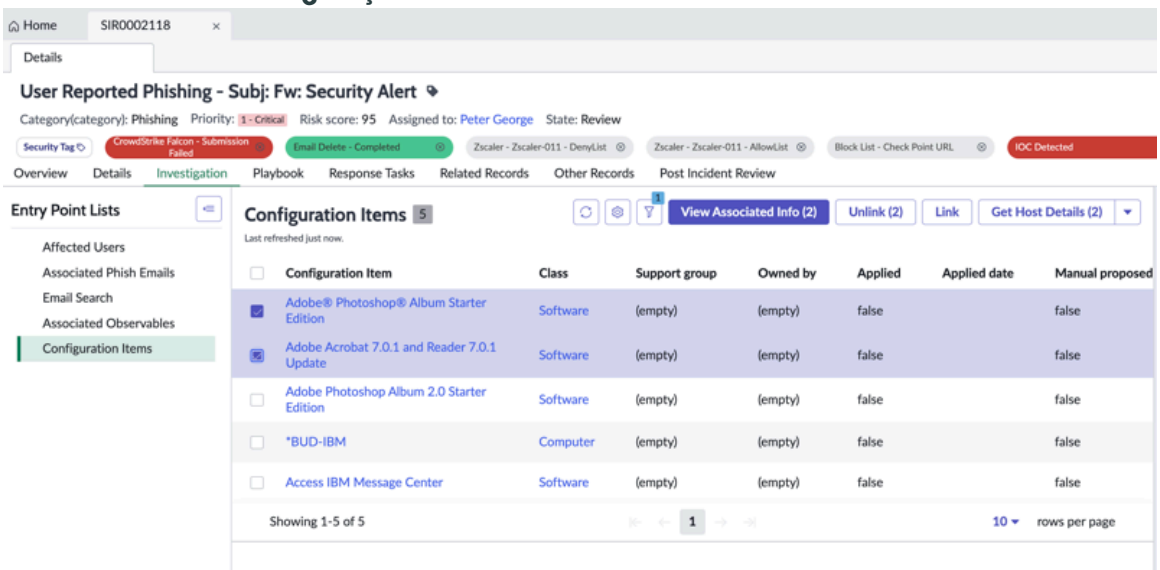


4. Selecione o item de configuração na lista de pontos de entrada.
   Por exemplo, selecione **Item de configuração** lista de pontos de entrada. Os registros de itens de configuração correspondentes são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

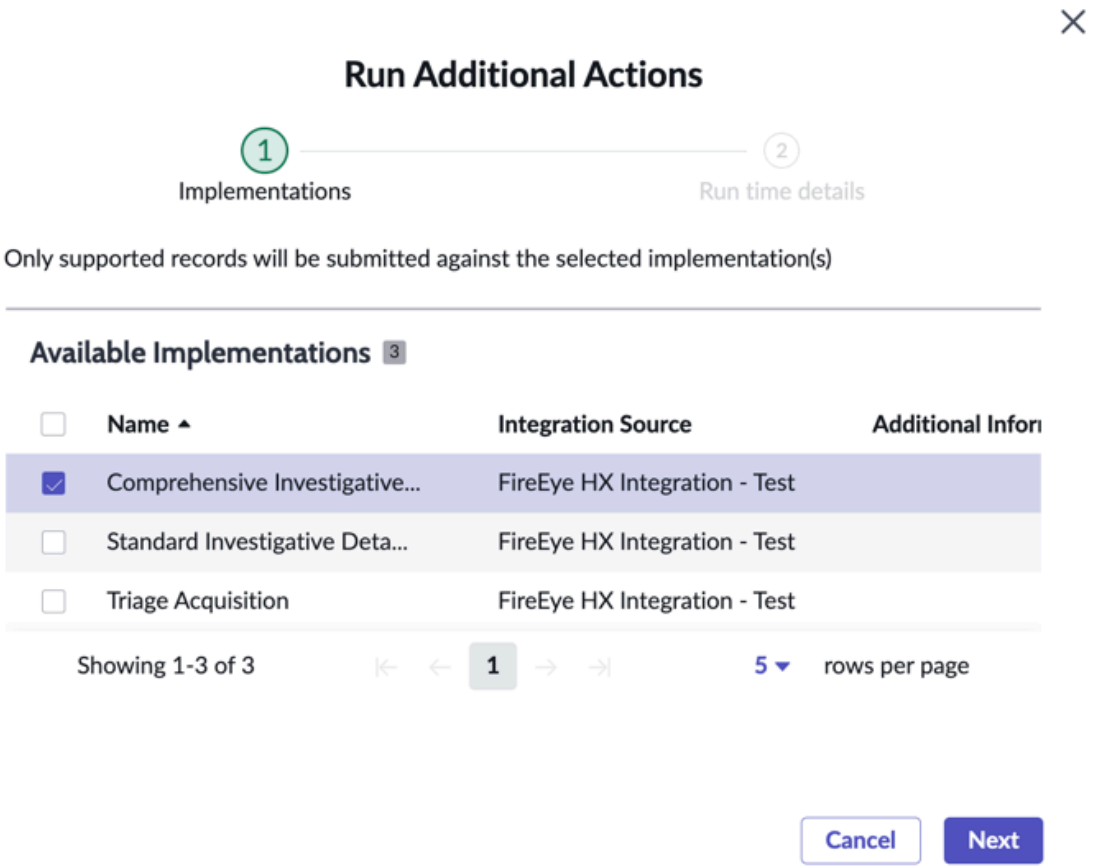
Selecione Item de configuração



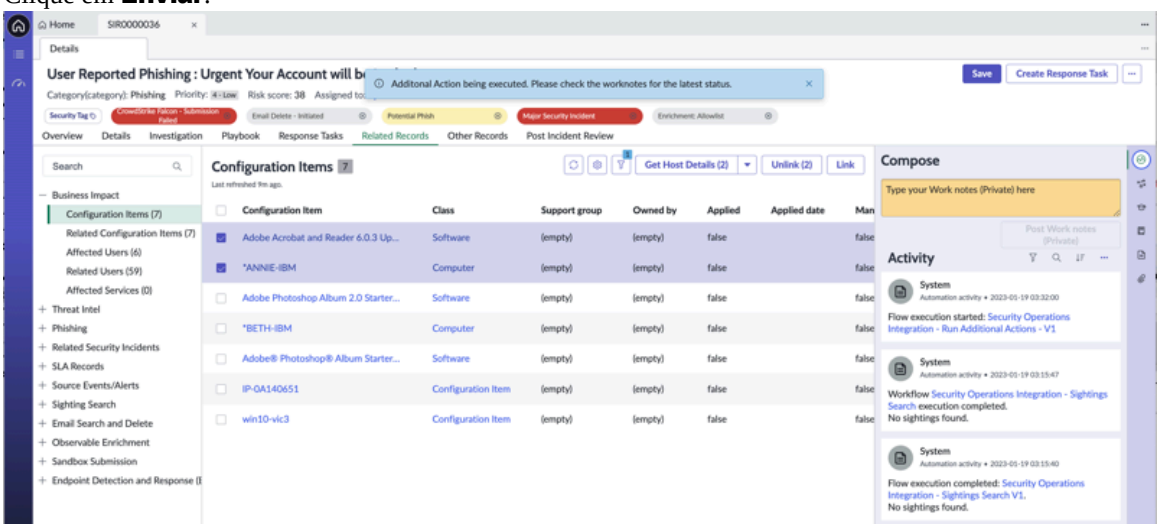
5. Selecione Qualquer **Item de configuração** .
6. Navegue até o menu suspenso Listas relacionadas que é exibido na parte superior da página.
   Para o item de configuração (IC) de incidente de segurança, as listas suspensas contêm a seguinte lista de ações de recursos. As ações de IC listadas coletam os resultados e os armazenam como dados de aprimoramento em um incidente de segurança:
   - Obter arquivo: Este recurso executa a ação para obter arquivos com um valor de hash específico ou um nome de arquivo.
   - Isolar host: Este recurso restringe as conexões do sistema a outros dispositivos.
   - Obter detalhes do host: Este recurso recupera os detalhes do host, os detalhes dos usuários conectados e outros recursos de aprimoramento.
   - Executar ações adicionais: Este recurso executa as ações adicionais além das ações padrão.
   - Obter estatísticas de rede: Este recurso recupera as estatísticas de rede de um recurso afetado.
   - Obter processo em execução: Este recurso recupera uma lista de processos em execução em um item de configuração (IC) de um host.
   - Obter usuários conectados: Este recurso coleta os dados de usuários conectados e os relaciona ao incidente de segurança.
7. Selecione **Executar ações adicionais** para executar a ação de capacidades de integração relacionadas à intel contra ameaças.
   A caixa de diálogo do modal Executar implementações adicionais é exibida.
8. Selecione uma ou mais implementações na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Avançar**.
   Agora, você será movido para a próxima etapa para adicionar os detalhes do tempo de execução.
10. Insira um comentário para associar à ação.
11. Clique em **Enviar**.



Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a Solicitação de ação adicional está sendo executada. Além disso, o respectivo andamento da ação de implementação é exibido em **Atividade** seção.

12. Exiba os resultados da seção de lista relacionada do EDR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

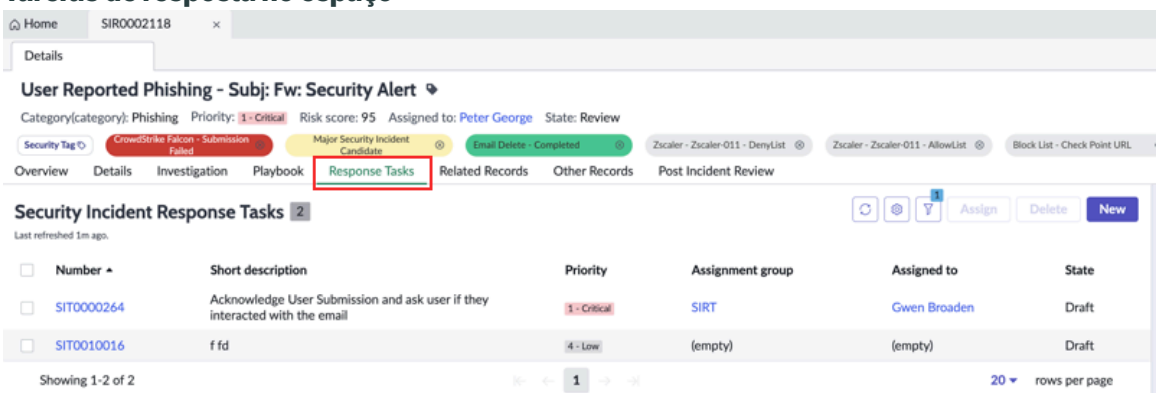
Tarefas de resposta a incidentes de segurança

Todas as tarefas de resposta associadas a um incidente de segurança são exibidas na seção Tarefas de resposta.

O analista será capaz de:

- crie uma nova tarefa de resposta
- atribua tarefas de resposta a si mesmo ou a outras pessoas
- exclua tarefas de resposta

Tarefas de resposta no espaço



Nota: Para fazer edições rápidas nas tarefas de resposta. Selecione a tarefa de resposta e uma lista de tarefas de resposta será exibida, selecione o registro e faça mudanças e salve a tarefa de resposta.

Crie uma tarefa de resposta

Crie tarefas de resposta para rastrear ações separadas a serem executadas para responder ao problema de segurança.

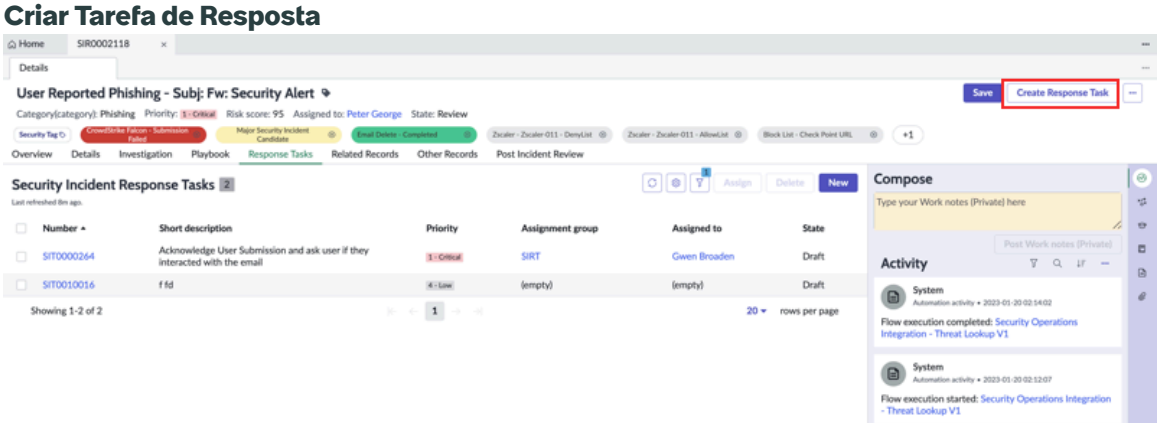
Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique em **Criar tarefa de resposta** Nas Ações de IU.

Criar Tarefa de Resposta



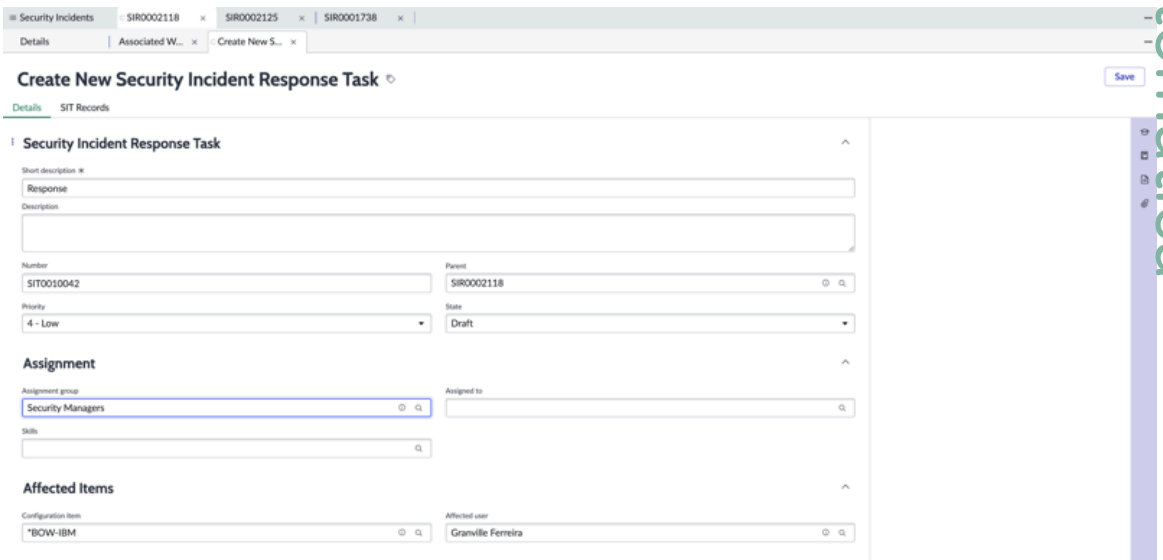
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Incidente de segurança

Campo	Descrição
Descrição resumida	Uma descrição do Resposta a incidentes de segurança tarefa.
Descrição	Uma descrição da tarefa selecionada.
Número	Número exclusivo gerado automaticamente para um incidente de segurança.
Primário	O número do incidente de segurança relacionado.
Prioridade	A prioridade usada para determinar quando esta tarefa é executada.
Estado	O estado atual da tarefa de resposta de segurança. Por padrão, o estado inicial é **Rascunho** .
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuição a	O indivíduo atribuído para executar a tarefa.
Habilidades	A habilidade necessária para executar esta tarefa. PESQUISE na pesquisa e selecione a habilidade necessária.
Itens afetados	Os itens afetados pelo problema de segurança.
Item de configuração	O item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.



4. Clique em **Salvar**.
A nova Tarefa de resposta (SIT) é criada.

Outros registros de resposta a incidentes de segurança

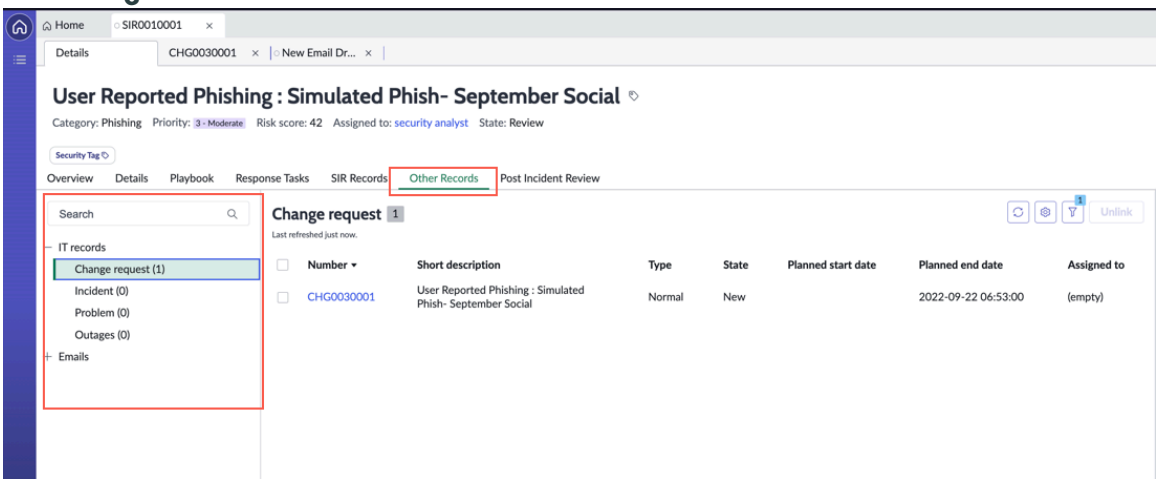
Esta seção exibe os outros registros, como registros relacionados A TI e registros de e-mail. Em Registros DE TI, Incidente, Solicitação de mudança, Problema e Indisponibilidades são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em E-mail, Rascunho, E-mails enviados e E-mails recebidos são exibidos.

Outros registros



Criar um incidente

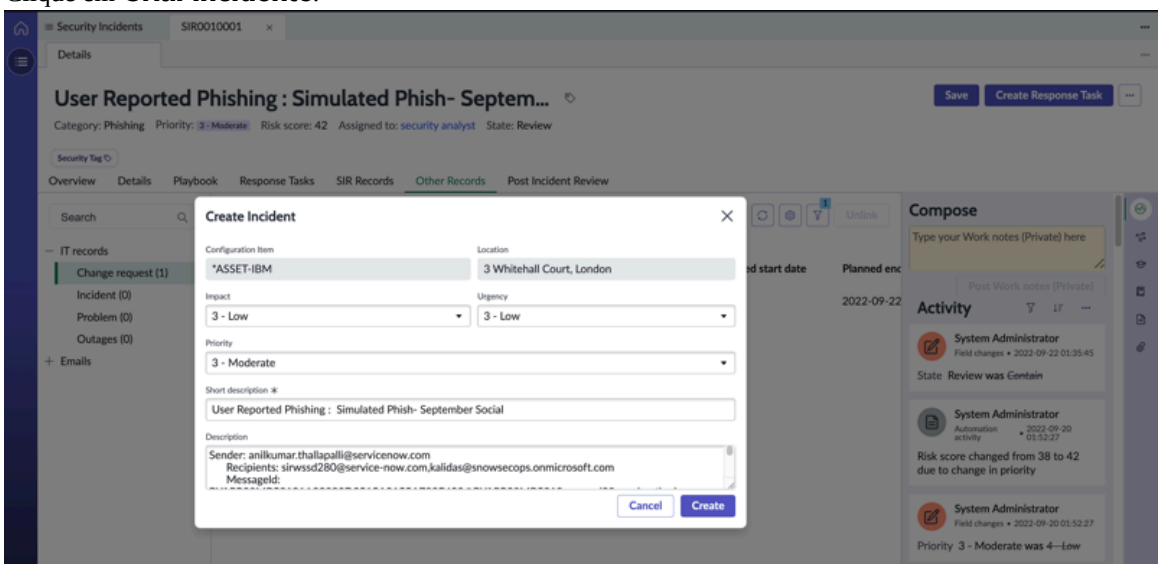
Crie um incidente em um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique em **Criar incidente**.

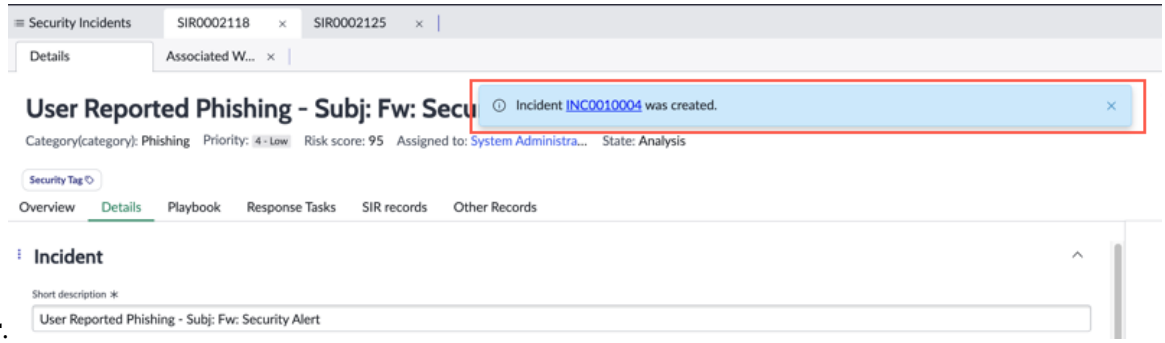


4. Insira os detalhes, como Item de configuração, Impacto, Urgência, Local, Prioridade, e Descrição resumida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Criar**.



6. Um incidente é criado.

Vincular vários incidentes ITSM

Link IT Service Management(ITSM incidentes relacionado a um incidente de segurança.

Antes de Iniciar

Nota: Você também pode criar um ITSM incidente a ser vinculado a um incidente de segurança. Para obter mais informações, consulte Criar um incidente.

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione Lista ícone (ícone.
3. Aberto . registro de incidente.
4. Selecione **Outros registros** guia.
5. Em **Registra** , selecione **Incidente** .

   Nota: Se você alternar para a IU clássica, em **Registros relacionados** . **Incidente** o campo foi removido.

6. Selecione **Link** .
7. . escolha . ITSM incidentes que você deseja vincular ao incidente de segurança selecionado.
8. Selecione **Link** .

Resultado

Selecionado ITSM os incidentes são listados em Registra seção do incidente de segurança selecionado registro .

Como criar tarefa de problema

Crie uma tarefa de problema.

Antes de Iniciar

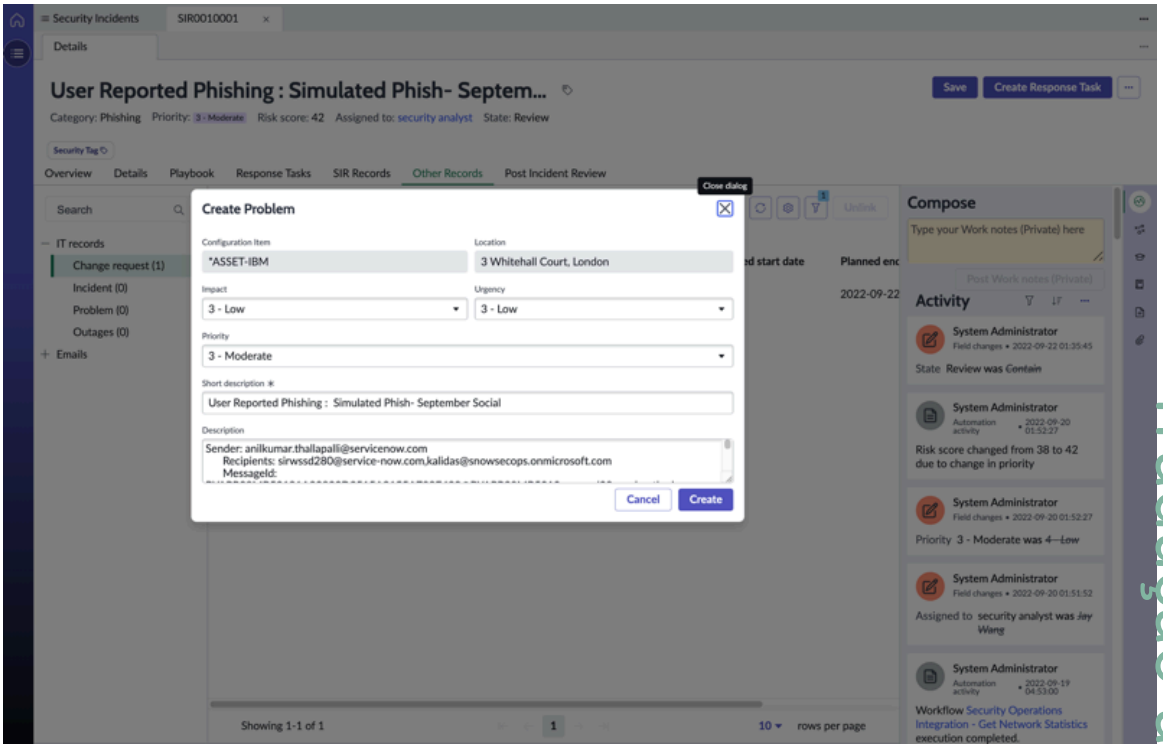
Função necessária: sn_si.analyst

Tradução automática

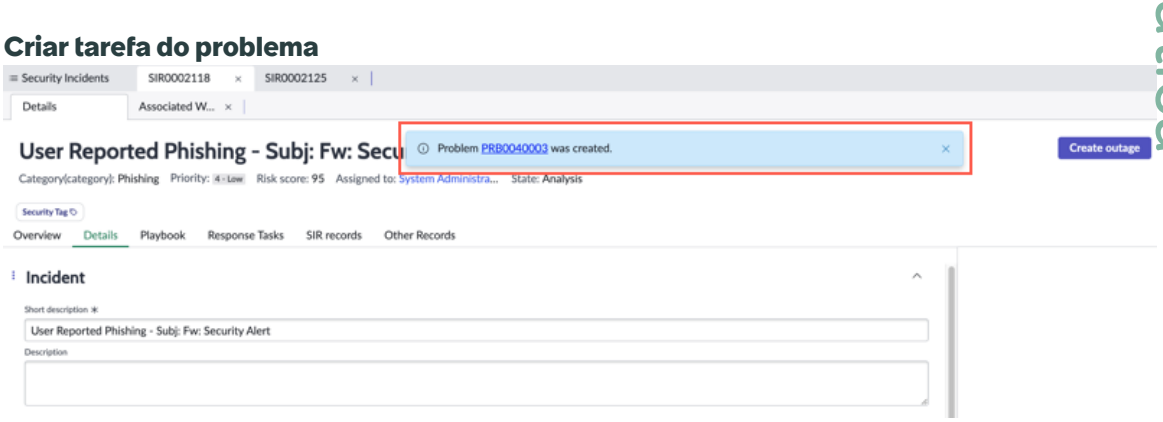
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique em **Criar problema** .



4. Preencha os detalhes, como Item de configuração, Local, Impacto, Urgência, Prioridade, e descrição resumida.
5. Clique em **Criar**.



6. Uma tarefa de problema é criada.

Criar uma solicitação de mudança

Crie uma solicitação de mudança.

Antes de Iniciar

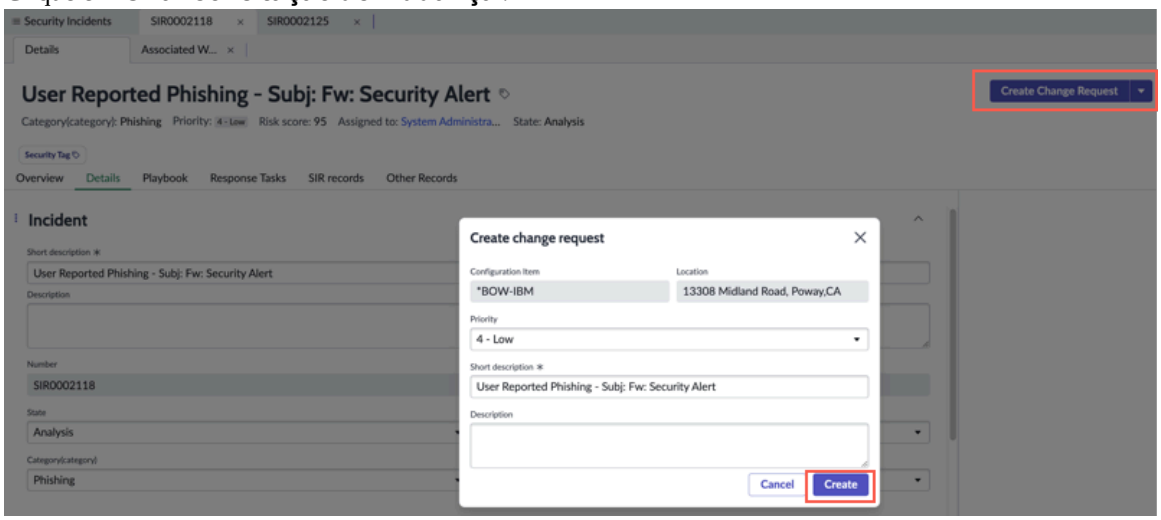
Função necessária: sn_si.analyst.

Tradução automática

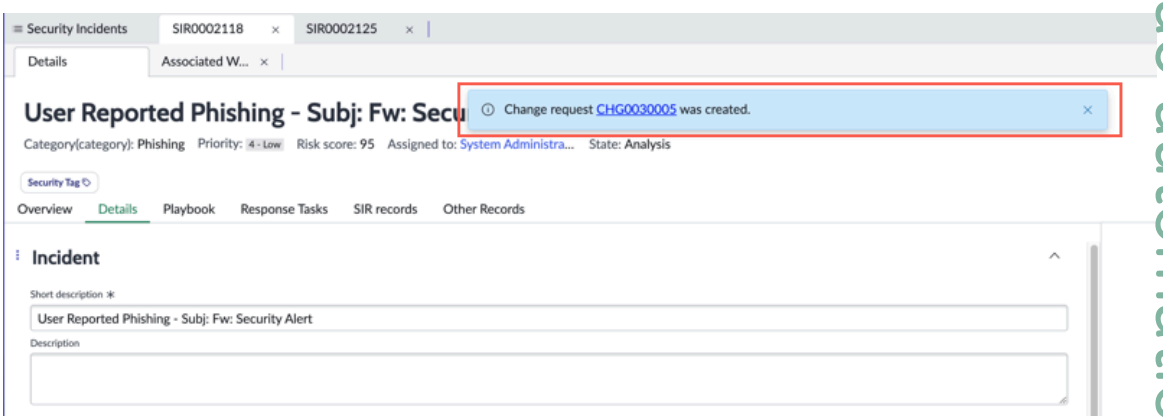
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique em **Criar solicitação de mudança** .



4. Insira os detalhes, como Item de configuração, Local, Prioridade e Descrição resumida.
5. Clique em **Criar**.



6. Uma solicitação de mudança é criada.

Tradução automática

Criar indisponibilidade

Crete uma indisponibilidade de um incidente para rastrear o tempo de inatividade de um item de configuração.

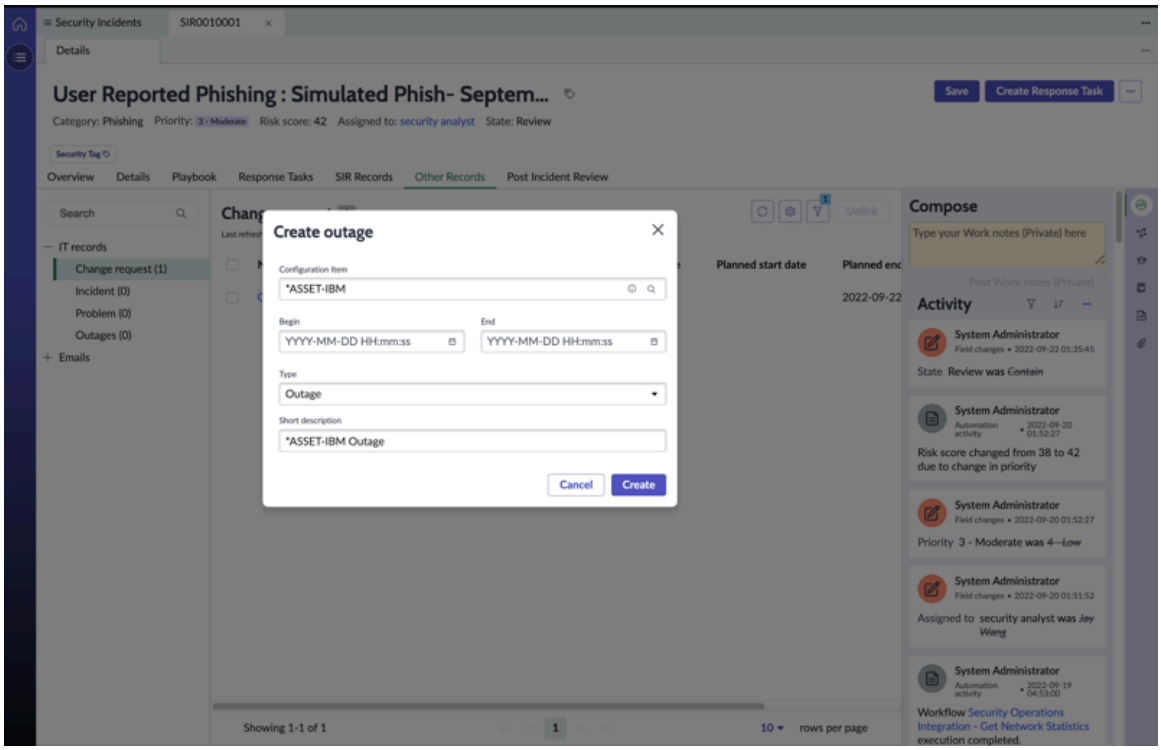
Antes de Iniciar

Função necessária: sn_si.analyst

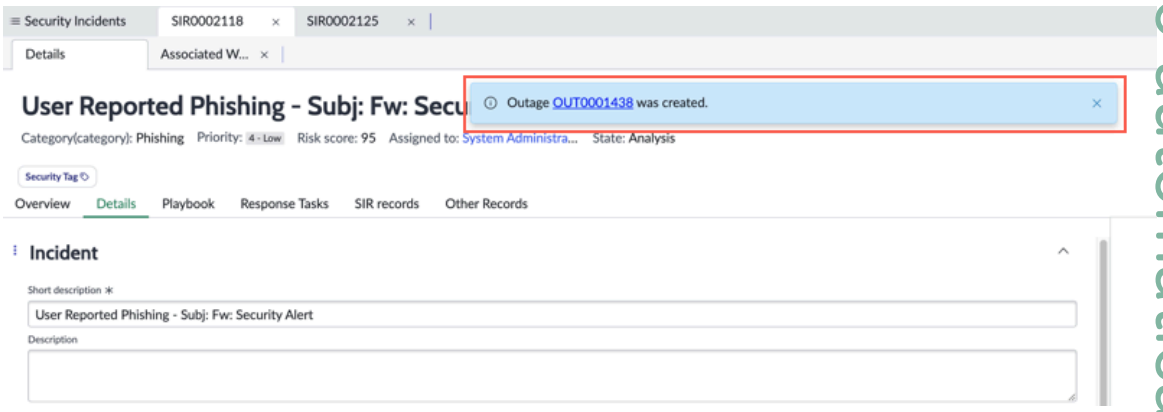
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique em **Criar indisponibilidade** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira os detalhes, como Item de configuração, Data de início, Data de término, Tipo e Descrição resumida.
5. Clique em **Criar**.



Tradução automática

Compor e-mails

Como analista, você pode compor e-mails diretamente de incidentes de segurança.

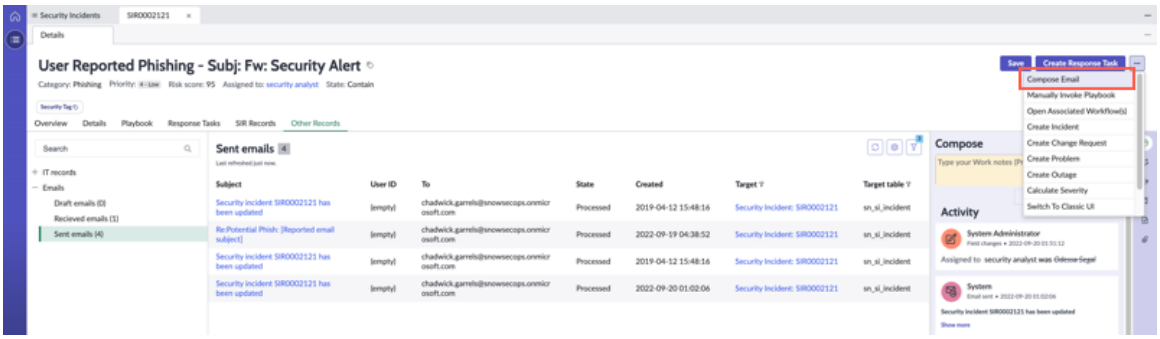
Antes de Iniciar

Função necessária: sn_si.analyst

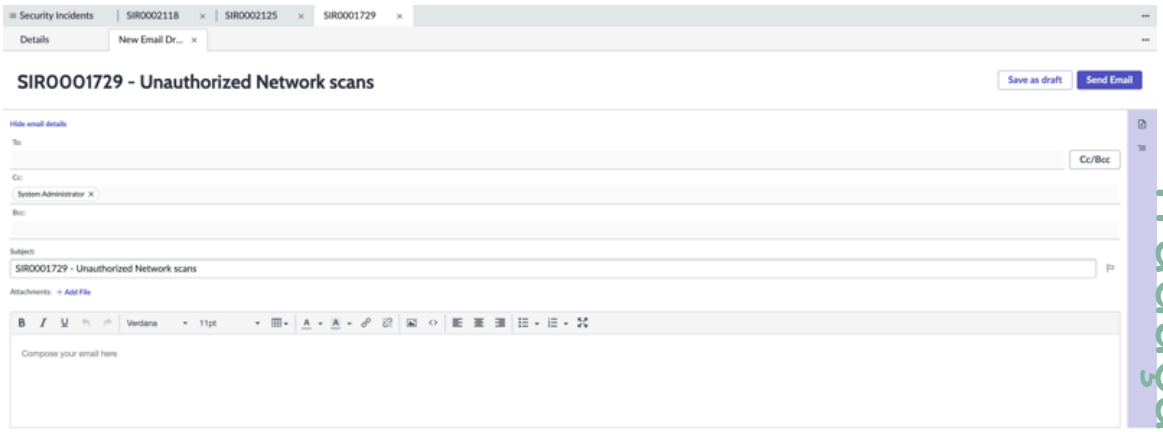
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione e abra o incidente para o qual você deseja redigir um e-mail.
3. Clique no estouro e selecione **Compor e-mail** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

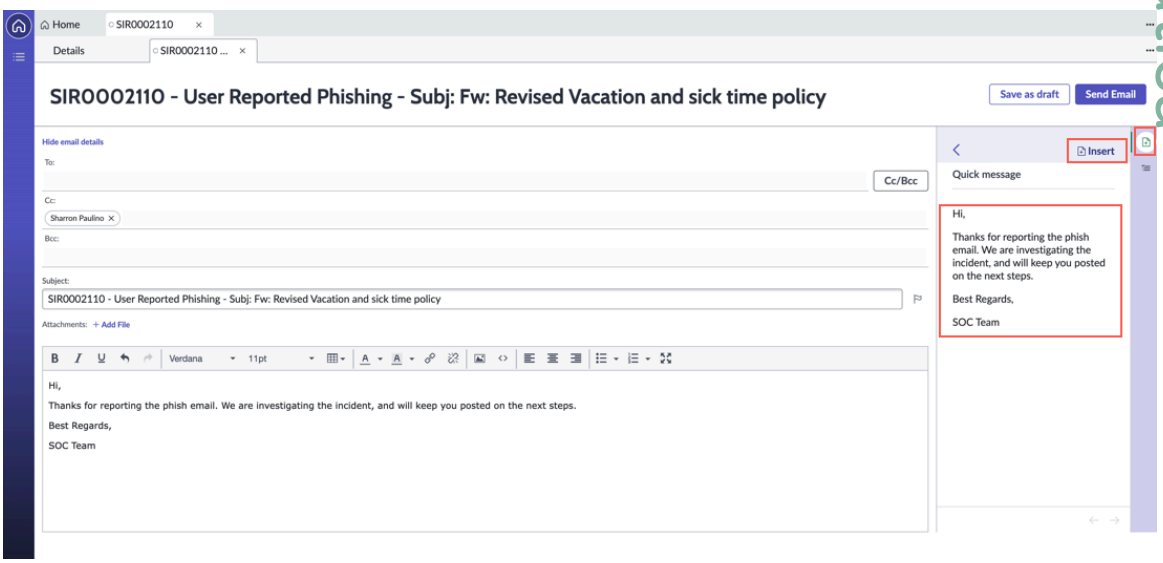


4. Insira **.** e. **CC** campo.



5. **Adicionar** anexos, se houver.

6. No formulário E-mail, clique em **Mensagens rápidas** para exibir as mensagens rápidas que são exibidas no lado direito do **Compor e-mails** seção.
   As mensagens rápidas disponíveis são exibidas. Selecione a mensagem e clique em **Inserir** . As mensagens são inseridas no corpo do e-mail.



7. Escreva seu e-mail e clique em **Enviar e-mail** .

Tradução automática

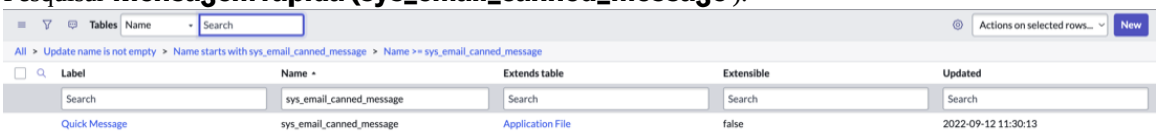
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode salvar um e-mail como rascunho. Esses rascunhos de e-mails estarão disponíveis na guia Outros registros.

Como configurar Mensagens rápidas:

a. Navegar até **Definições do Sistema** > **Tabelas**.

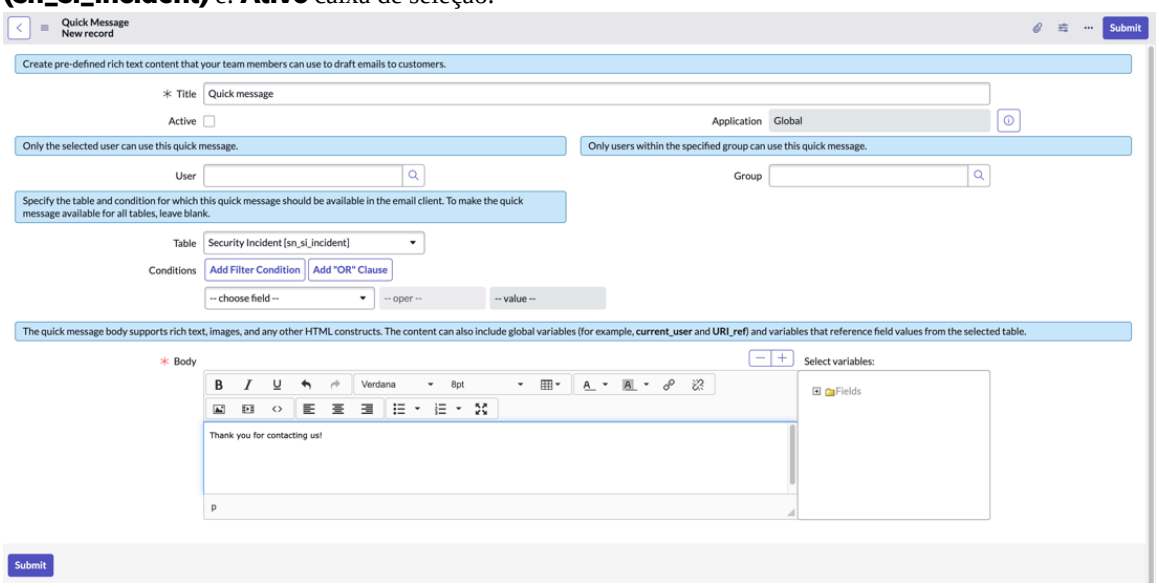
b. Pesquisar **Mensagem rápida (sys_email_canned_message**).



c. Ir para **Links relacionados** > **Mostrar lista**.

d. Criar **Novo** .

e. Insira **Título** , **corpo da mensagem** . selecione **Tabela: Incidente de segurança (sn_si_incident)** e. **Ativo** caixa de seleção.



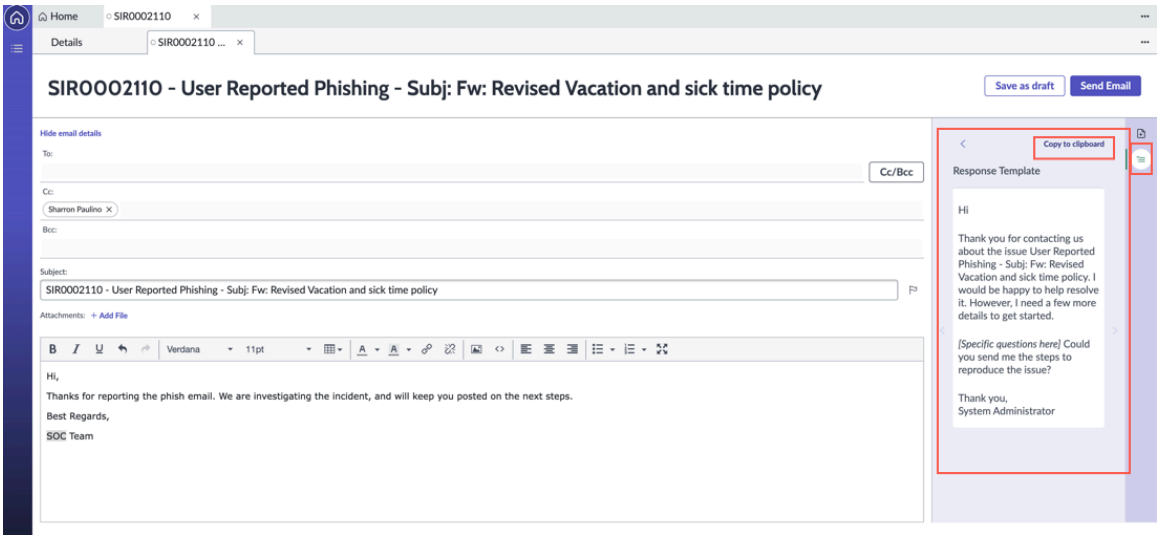
f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, a mensagem rápida aparece no menu contextual.

8. Clique em **Modelos** para adicionar qualquer modelo, se necessário.

9. Selecione **Modelo de resposta** e clique em **Copiar para a área de transferência** e aplicar o modelo, se necessário.

Tradução automática

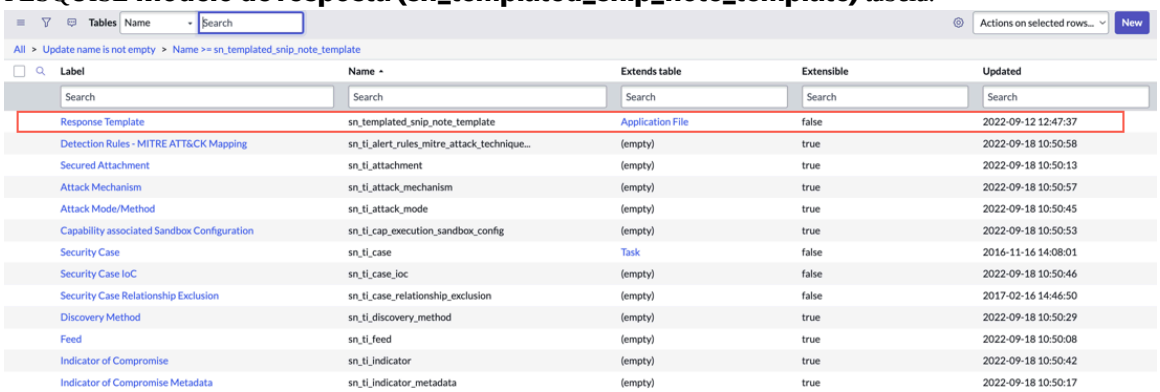
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como configurar Modelos de resposta:

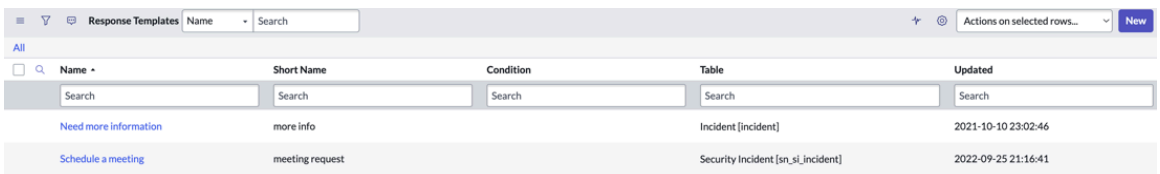
a. Navegar até **Definições do Sistema** > **Tabelas**.

b. PESQUISE **Modelo de resposta (sn_templated_snip_note_template)** tabela.



c. Ir para **Links relacionados** > **Mostrar lista**.

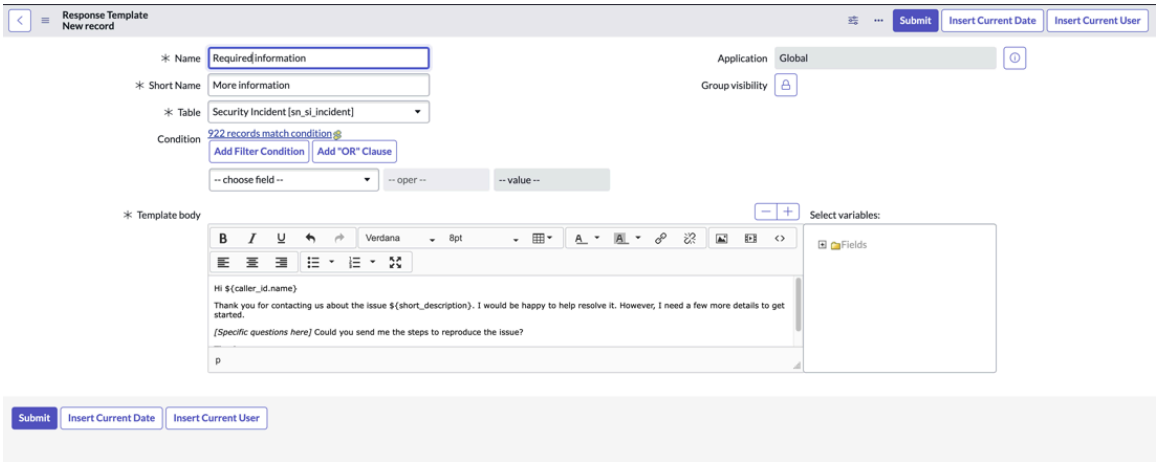
d. Criar **Novo** .



e. Insira **Nome** , **Nome curto** . selecione **Tabela: Incidente de segurança (sn_si_incident)** e. **Corpo do modelo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, o novo modelo aparece no menu contextual.

Resposta do incidente de segurança Revisão pós-incidente

A revisão pós-incidente aparece quando um incidente é movido para o estado Revisão.

Para obter informações mais detalhadas sobre como conduzir as atividades pós-incidente, consulte Relatório de análise pós-incidente

A revisão pós-incidente consiste nas seguintes seções:

1. Avaliações
2. Relatórios

No espaço Resposta a incidentes de segurança, você poderá solicitar e fazer avaliações usando essas duas novas ações de IU.

Nome	Descrição
Avaliações	Avaliação exibe todas as avaliações associadas ao incidente de segurança Outras avaliações. O analista poderá fazer avaliações e solicitar avaliações. • **Fazer avaliações** : Clique em **Fazer avaliações** para fazer as avaliações (se aplicável) e concluir a avaliação. Antes de concluir a avaliação, o estado do incidente de segurança é Pronto para realizar e a data de vencimento do incidente é indicada em vermelho. • Solicitar avaliações: Clique em **Solicitar avaliação** para quaisquer avaliações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	adicionais e você pode adicionar os novos usuários que deseja solicitar. **Nota:** Os usuários que já solicitaram não aparecerão nesta seção. Qualquer avaliação para este incidente foi configurada com base nas condições definidas na Revisão pós-incidente, sendo obrigatória ou opcional.
Relatórios	Modifique as configurações de tempo de execução e gere o relatório. Selecione a instância Relatório, modifique os filtros e salve o relatório. O analista pode visualizar e baixar o relatório PIR.

Integração do TISC no SIR Workspace

A seção a seguir inclui informações sobre a integração da Central de segurança do Inteligência contra ameaças no contexto do espaço SIR.

Enviar dados do Espaço SIR para o TISC

Saiba como os dados são colaborados e compartilhados entre os espaços do Centro de segurança de inteligência contra ameaças (TISC) e Resposta a incidentes de segurança (SIR) seguindo os procedimentos explicados nas seções a seguir.

Propriedades do sistema para enviar dados

Revise as propriedades do sistema para integrações do TISC para combinar com o SIRW. Você pode configurar essas propriedades para controlar como ambas as aplicações gerenciam as integrações.

Principais considerações

As propriedades do sistema para integrações do TISC fornecem opções de configuração avançadas sobre como a aplicação lida com observáveis e aprimoramentos.

1. Para definir as propriedades do sistema de integrações de TISC no SIRW, navegue até **Propriedades do sistema** Para Inteligência contra ameaças e acesse a tabela [sys_properties].
2. As propriedades do sistema controlam e manipulam o comportamento de cada operação de envio de dados individual.
3. Quando a propriedade está habilitada, os dados são enviados automaticamente quando os dados de observáveis ou aprimorados são gerados no Espaço SIR.
4. Se a propriedade estiver desabilitada, os dados serão enviados manualmente e permitirão que os usuários enviem dados usando as ações de IU do Espaço SIR.

As listas a seguir mostram as propriedades do sistema para integração TISC - SIR:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Enviar dados observáveis automaticamente e manualmente do SIR: Habilite a propriedade sn_ti.allow_observable_and_enrichrichment_records_push para enviar os dados automaticamente ou manualmente. Se desabilitada, esta propriedade desabilitará o modo automático e manual para todos os dados enviados pelo SIR.
- Resultados da pesquisa de ameaças por push: Habilite esta propriedade do sistema sn_ti.automatic_push_threat_lookup_results para enviar dados de pesquisa de ameaças automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de pesquisa de ameaças manualmente.
- Enviar resultados da pesquisa de vistas para o TISC: Habilite sn_ti.automatic_push_sighting_results_to_tisc Esta propriedade do sistema para enviar dados de pesquisa de vistas automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de pesquisa de vistas manualmente.
- Observáveis por push: Habilite sn_ti.automatic_push_observable_to_tisc Esta propriedade do sistema para enviar dados de observáveis automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados dos observáveis manualmente.
- Resultados de aprimoramento por push: Habilite sn_ti.automatic_push_enichment_results esta propriedade do sistema para enviar automaticamente os dados de resultados de aprimoramento para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de resultados de aprimoramento manualmente.

Adicionar incidente de segurança ao caso TISC

Adicione incidentes de segurança aos registros de caso do TISC.

Antes de Iniciar

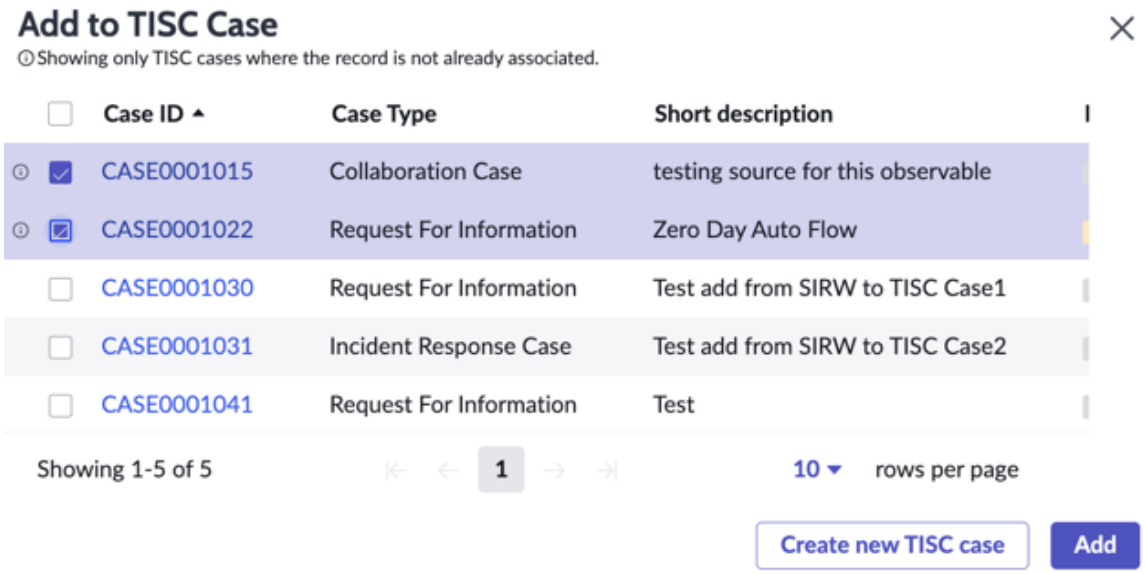
Função necessária: sn_si.analyst, sn_sec_tisc.case_write

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente ou navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Clique em **Mais ações** ícone.
4. Clique em **Adicionar ao caso TISC** ação.
   A caixa de diálogo Adicionar ao caso do TISC é exibida e mostra somente os casos do TISC em que o incidente ainda não está associado.
5. Selecione o(s) caso(s) em **Adicionar ao caso** caixa de diálogo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Crie um novo caso TISC se não houver registros de caso. Para obter mais informações sobre como criar caso(s), consulte Criação de casos usando Workbench de analista de ameaças.

6. Clique em **Adicionar**.
7. Clique no registro do caso para exibir o caso no TISC a partir da mensagem informativa exibida ou do **Atividade** fluxo.

Nota: Para exibir os incidentes de segurança vinculados, clique no registro de caso específico do incidente de segurança **Atividade** fluxo. Ao clicar nele, você será direcionado para o registro do caso no espaço do TISC e os incidentes de segurança serão adicionados **Artefatos** Do módulo Gestão de casos.

Adicionar observáveis ao caso do TISC

Adicionar observáveis aos registros de caso do TISC.

Antes de Iniciar
Função necessária: sn_si.analyst, sn_sec_tisc.case_write

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente ou navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Clique em **Registros relacionados** no espaço.
   Você pode executar a ação de adicionar observáveis aos casos do TISC usando várias guias do Espaço de resposta do incidente de segurança.

Nota: Você pode navegar até

- Página de detalhes de observáveis na guia Registros relacionados.
- **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** Para adicionar observáveis ao caso do TISC.

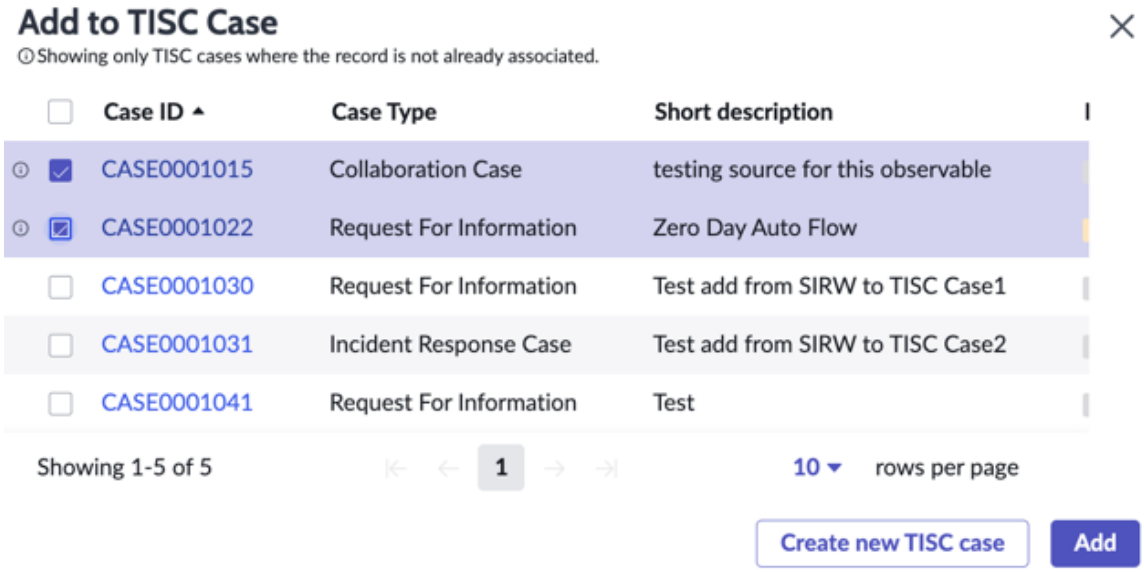
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Por exemplo, selecione **Inteligência sobre ameaça** > **Observáveis Associados**.
5. Selecione um ou vários observáveis para adicionar os observáveis selecionados aos registros de caso.

> **Nota:** Você também pode clicar em qualquer um dos registros de observável e ele abre a página de detalhes de observáveis em uma guia diferente. Você pode adicionar registros de caso a partir daqui clicando em Adicionar ao caso TISC.

6. Clique em **Ações de capacidade** botão dividir.
7. Selecione **Adicionar ao caso TISC** .
8. Selecione o(s) caso(s) em **Adicionar ao caso** caixa de diálogo.



> **Nota:** Crie um novo caso TISC se não houver registros de caso. Para obter mais informações sobre como criar caso(s), consulte Criação de casos usando Workbench de analista de ameaças.

9. Clique em **Adicionar**.
10. Clique no registro do caso para exibir o caso no TISC a partir da mensagem informativa exibida ou do **Atividade** fluxo.

> **Nota:** Se o observável não tiver um observável TISC correspondente, o observável selecionado no espaço SIR será enviado para o TISC automaticamente e, posteriormente, será adicionado aos registros de caso TISC selecionados. Para exibir os observáveis vinculados, clique no registro de caso específico no **Atividade** fluxo. Ao clicar nele, você será direcionado para o registro do caso no espaço do TISC e os observáveis serão adicionados **Artefatos** Do módulo Gestão de casos.

Resultado
Você enviou com sucesso os dados observáveis para a Gestão de casos da Central de segurança do Inteligência contra ameaças.

Enviar observáveis para o TISC

Usando este recurso, o analista de segurança pode enviar os dados observáveis do SIR para o TISC. Usando o contexto do TISC, você pode verificar se os observáveis estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

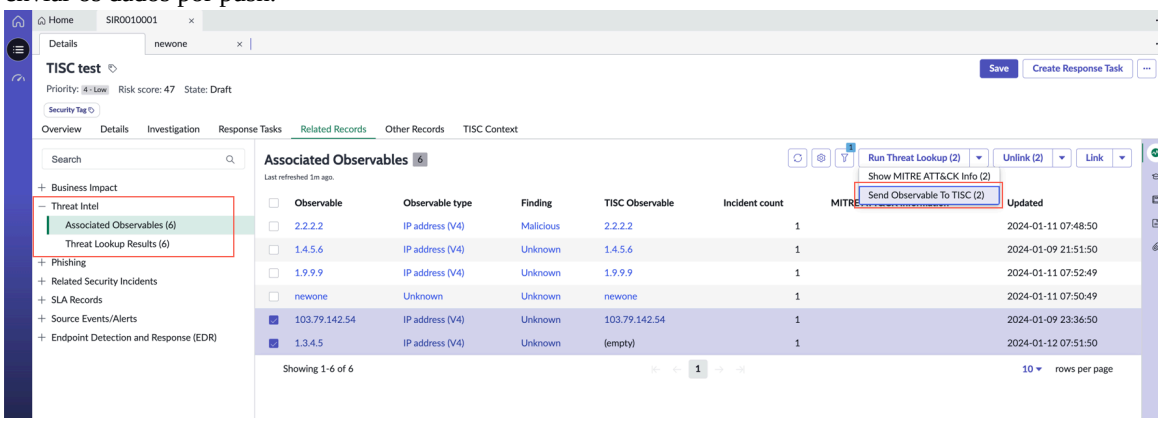
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Abra um incidente de segurança.
3. Selecione **Registros relacionados** Para executar a ação de capacidade de integração do TISC.

Nota:

- Você também pode navegar até **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** para executar a operação de envio.
- Em **Investigação** , selecione **Exibir informações relacionadas** para exibir todos os dados de pesquisa de ameaças, pesquisa de vistas e aprimoramento associados para o observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

4. Por exemplo, selecione **Inteligência sobre ameaça** > **Observáveis Associados** Para executar a operação de envio e enviar manualmente os dados para o TISC.
5. Selecione um ou mais registros observáveis para executar **Enviar observável para o TISC** operação para enviar os dados por push.



6. Selecione **Enviar observável para o TISC** .
7. Na tela Enviar observáveis para o TISC, forneça o seguinte:

Adicione informações aos observáveis do TISC

Campo	Descrição
Confiança	A pontuação de confiança dos observáveis.
TLP	O valor de TLP (Traffic Light Protocol, protocolo de semáforo) para os observáveis.
Anotações	Anotações para os observáveis.
Marcadores de TISC	Marcadores para os observáveis enviarem. Você pode adicionar marcadores personalizados que são adicionados aos observáveis.

8. Selecione **"Enviar"**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

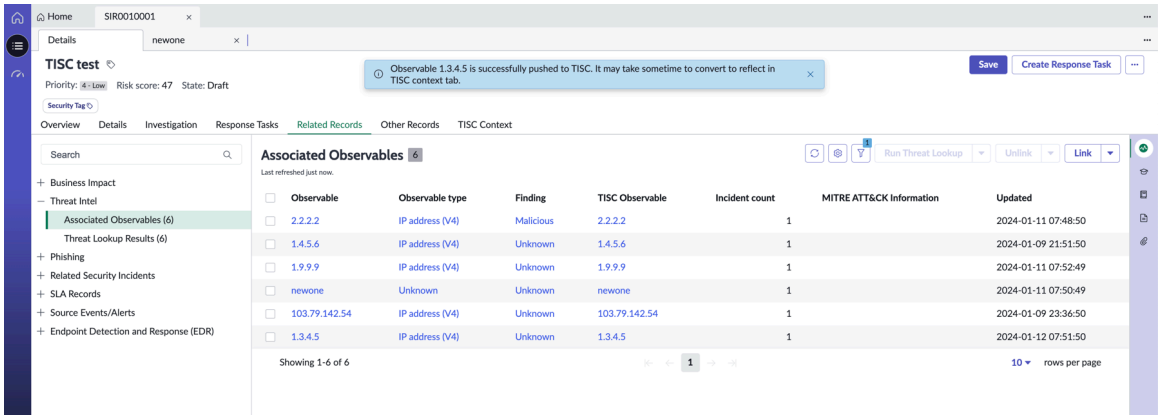
Nota:

- Se o observável selecionado não estiver presente no TISC, primeiro o observável será criado como origem do observável e, depois que o observável de origem criar o registro do observável do TISC, o registro do observável será associado automaticamente ao observável recém-criado.
- Uma vez que a operação de push do observável é executada, uma mensagem informativa é exibida.

  Os seguintes observáveis foram enviados com sucesso para o TISC. Pode levar algum tempo para refletir na guia Contexto do TISC. 0.0.0.0

- Se já existir um TISC observável, uma mensagem de erro será exibida.

  Os seguintes observáveis já existem no TISC: 0.0.0.0



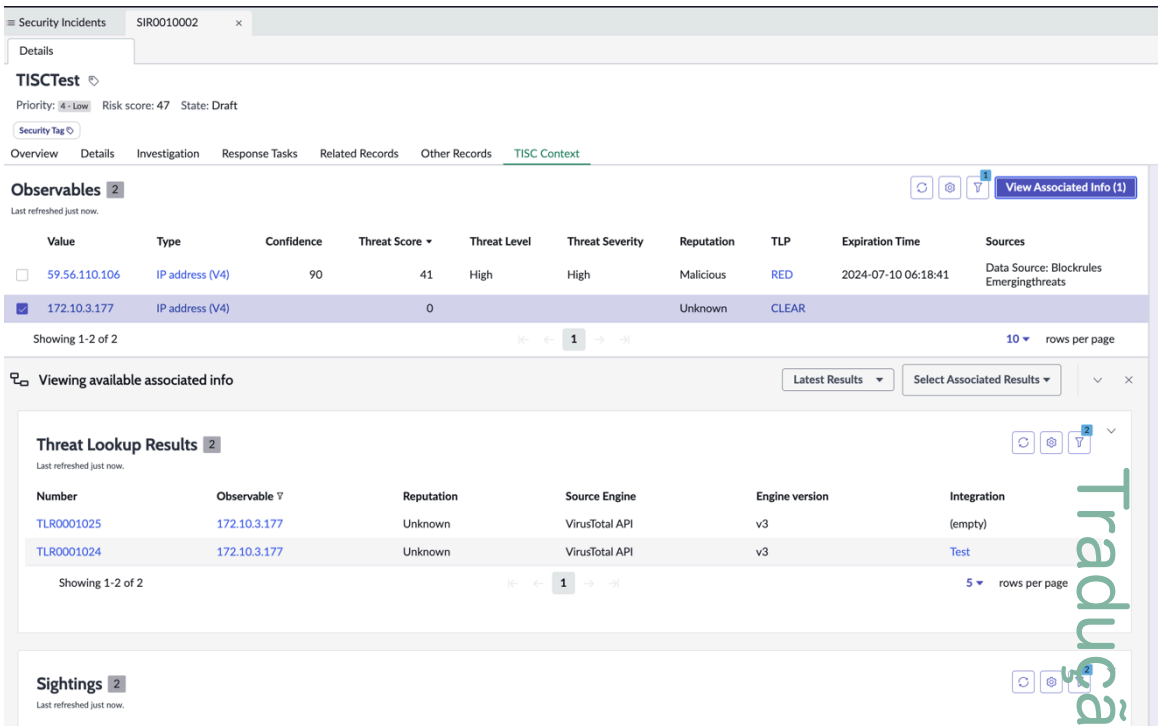
9. Selecione **Contexto do TISC** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: :

- Agora, você verá o observável que é enviado por push para o TISC a partir da aplicação SIR.



- **Em uma operação de push manual** : Os dados observáveis só podem ser enviados por push se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de push automática** : Os dados observáveis ou de aprimoramento serão enviados automaticamente quando associados a um incidente de segurança.

  Nota: . **Enviar observável para o TISC** a opção desaparece quando o fluxo automatizado é habilitado.

- **Contexto do TISC** Mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas DO SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento de observável associados dos observáveis selecionados.

10. Exibe os resultados.

Enviar pesquisa de ameaças para o TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de ameaças do SIR para o TISC. Usando o contexto do TISC, você pode verificar se os resultados da pesquisa de ameaças estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

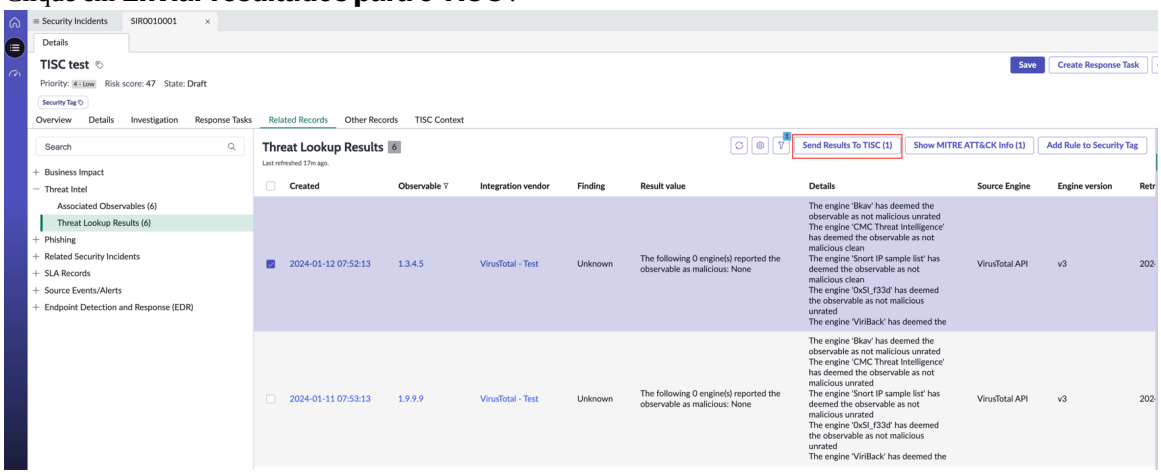
Procedimento

1. Navegue até **Registros relacionados** No espaço SIR para executar a ação de capacidade de integração do TISC.

Nota:

- Você também pode navegar até **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** para executar a operação de envio.
- Em **Investigação** clique em **Exibir informações associadas** para exibir todos os dados de pesquisa de ameaças, pesquisa de vistas e aprimoramento associados para o observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Inteligência sobre ameaça** > **Resultados da Pesquisa de ameaças** Para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de resultados da pesquisa de ameaças.
4. Clique em **Enviar resultados para o TISC** .



Nota:

- Se o observável de pesquisa de ameaças selecionado não estiver presente no TISC, primeiro no modo manual, o observável será criado como origem do observável e, depois que o observável de origem criar o registro do observável do TISC, o registro do observável será associado automaticamente ao observável recém-criado. Além disso, a pesquisa de ameaças selecionada também será enviada para o observável de pesquisa de ameaças recém-criado no modo manual.
- Em um modo automático, os observáveis não serão enviados por push se o observável estiver presente, e as pesquisas de ameaça serão enviadas automaticamente. Se os observáveis não estiverem presentes, as pesquisas de ameaça não serão enviadas por push.

5. Uma mensagem de confirmação é exibida O observável (1,9.78,242) do registro de pesquisa de ameaças selecionado não existe no TISC. Levará algum tempo para criar o observável e associar automaticamente o registro de pesquisa de ameaça observável no TISC.
Depois que isso for processado e enviado, você poderá ver os resultados.

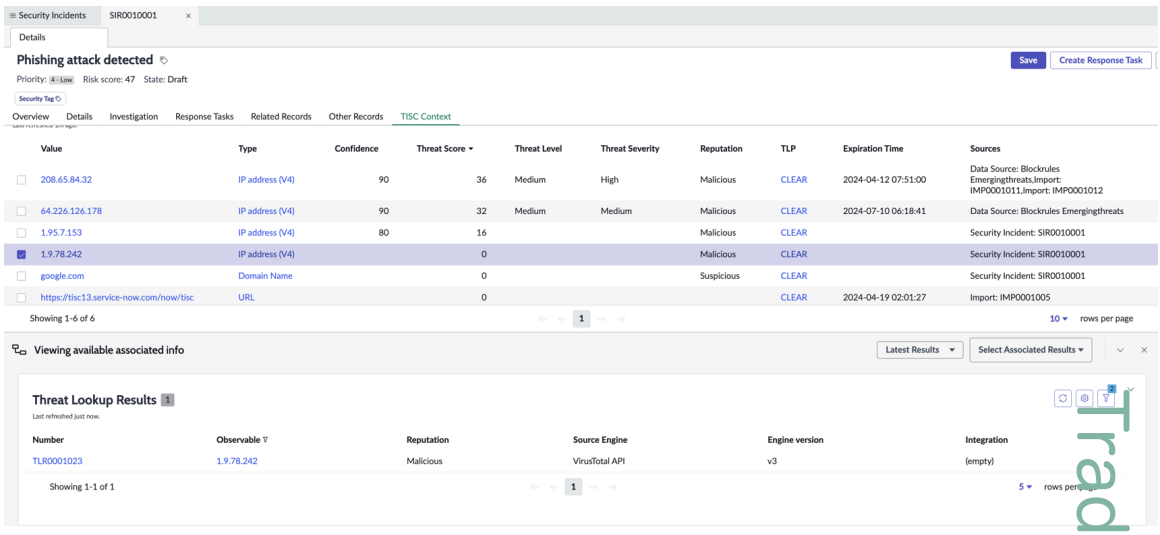
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Contexto do TISC** .

Nota: :

- Agora, você verá o observável que é enviado por push para o TISC a partir da aplicação SIR.



- **Em uma operação de push manual** : Os dados observáveis só podem ser enviados por push se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de push automática** : Os dados observáveis ou de aprimoramento serão enviados automaticamente quando associados a um incidente de segurança.
- **Contexto do TISC** Mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas DO SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento de observável associados dos observáveis selecionados.

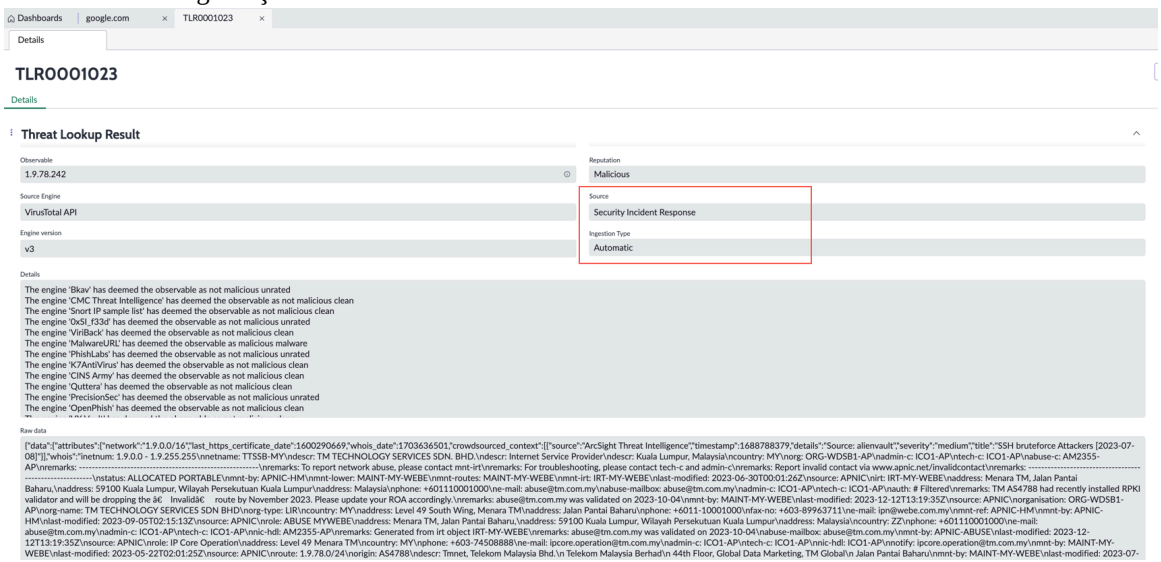
7. A exibição de lista exibe todos os resultados da pesquisa de ameaças, no entanto, selecione qualquer registro e clique em **Exibir informações associadas** botão.

8. Exiba os resultados da pesquisa de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Clique em qualquer registro de resultados de pesquisa de ameaça para exibir o registro na exibição de formulário, que também mostra o push ou **Tipo de ingestão** (automático ou manual) e. **Origem** Resposta do incidente de segurança.



Enviar pesquisa de vistas para o TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de vistas do SIR para o TISC. Usando o contexto do TISC, o analista pode verificar se os dados de pesquisa de vistas estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados sempre que necessário.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegue até **Registros relacionados** No espaço SIR para executar a ação de capacidade de integração do TISC.

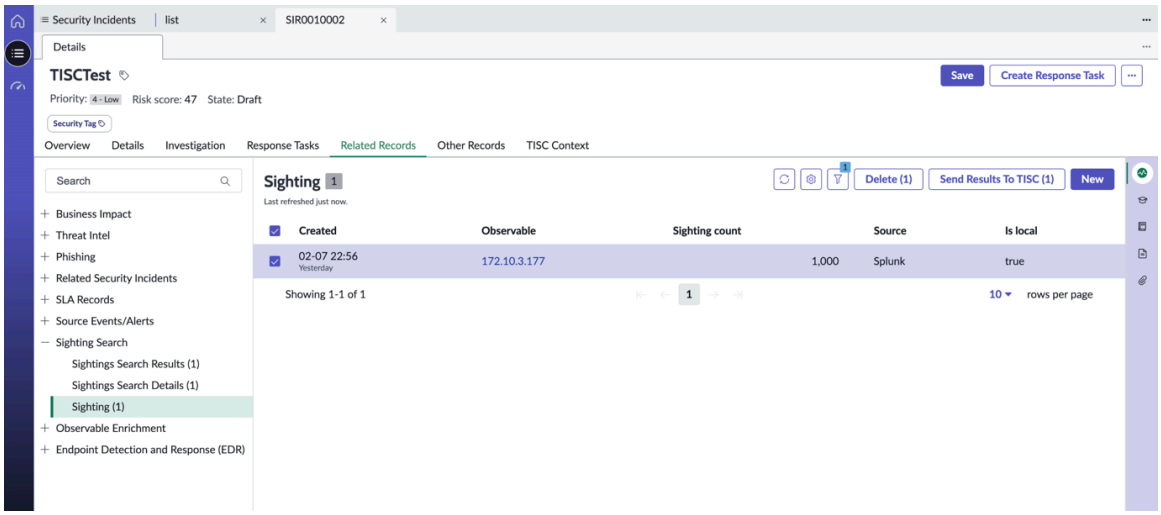
Nota:

- Você também pode navegar até **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** para executar a operação de envio.
- Em **Investigação** clique em **Exibir informações associadas** para exibir todos os dados de pesquisa de ameaças, pesquisa de vistas e aprimoramento associados para o observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Pesquisa de Vistas** > **Resultados da pesquisa de detecções** Para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de Resultados da pesquisa de vistas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

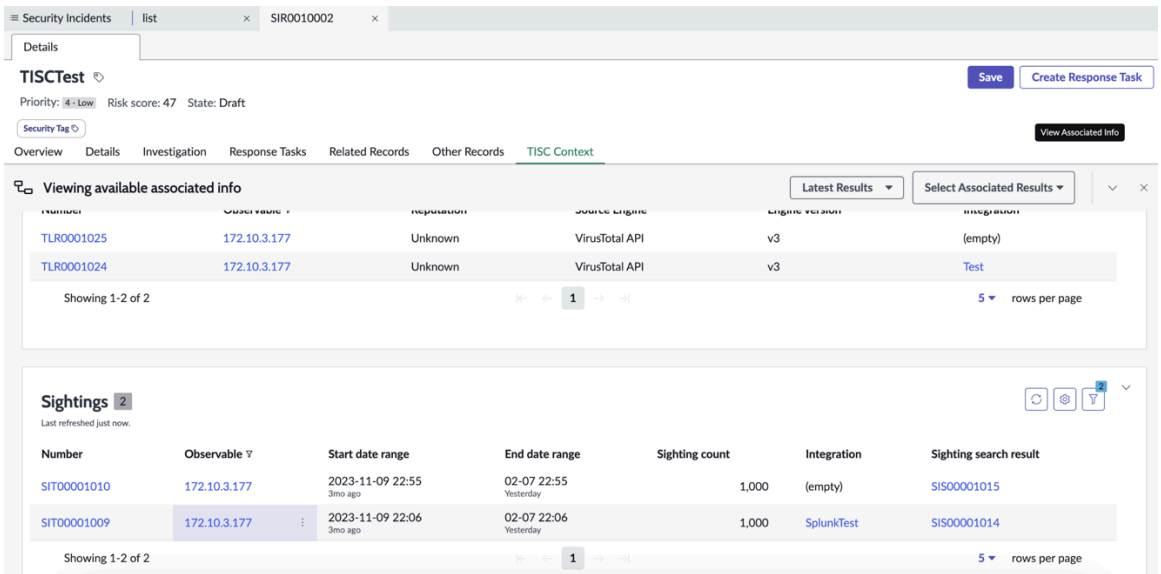


4. Clique em **Enviar resultados para o TISC** .

Nota:

- Se o observável de pesquisa de vistas selecionado não estiver presente no TISC, no modo manual, primeiro o observável será criado como fonte do observável e, depois que o observável de origem criar o registro do observável do TISC, o registro do observável será associado automaticamente ao observável recém-criado. Além disso, a pesquisa de vistas selecionada também será enviada para o observável de pesquisa de ameaças recém-criado no modo manual.
- Em um modo automático, os observáveis não serão enviados por push se o observável estiver presente, e as pesquisas de ameaça serão enviadas automaticamente. Se os observáveis não estiverem presentes, as pesquisas de ameaça não serão enviadas por push.

5. Selecione **Contexto do TISC** .



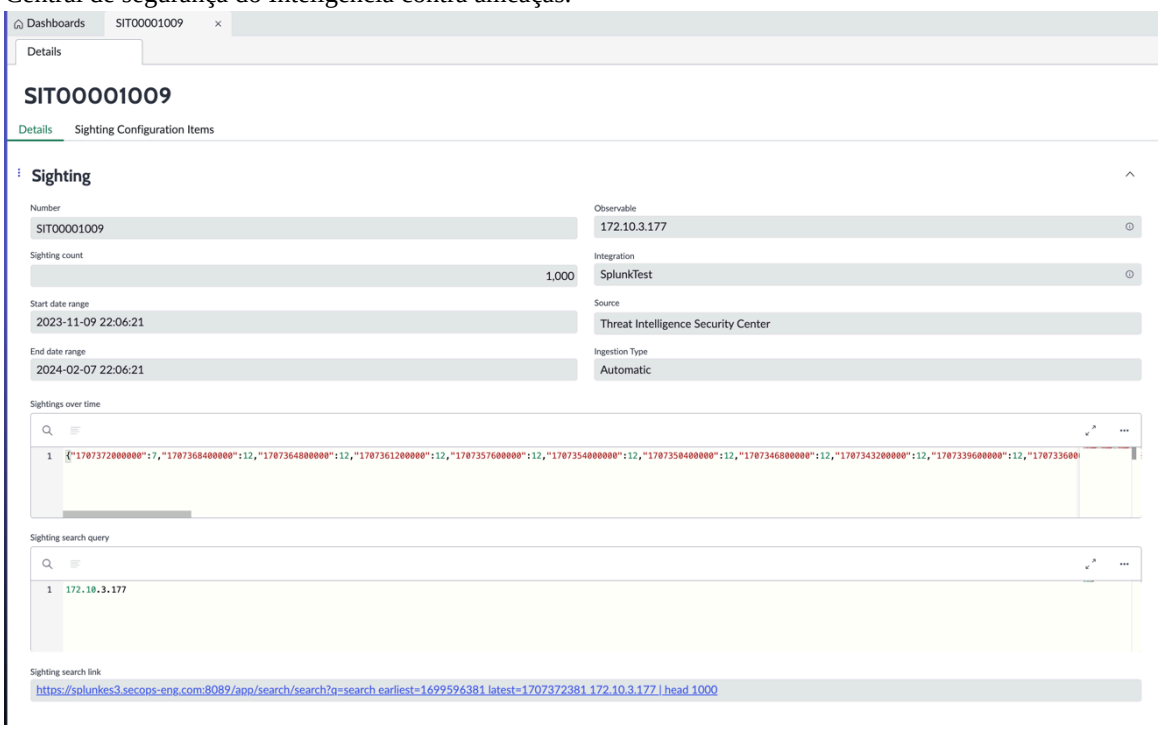
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: :

- Agora, você verá o observável que é enviado por push para o TISC a partir da aplicação SIR.
- **Em uma operação de push manual** : Os dados observáveis só podem ser enviados por push se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de push automática** : Os dados observáveis ou de aprimoramento serão enviados automaticamente quando associados a um incidente de segurança.
- **Contexto do TISC** Mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas DO SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento de observável associados dos observáveis selecionados.

6. Depois que o registro for processado, selecione-o e clique em **Exibir informações associadas** .
7. Exibe os resultados.
8. Clique em qualquer registro de resultados de pesquisa de vistas para exibir o registro na exibição de formulário, que também mostra o push ou **Tipo de ingestão** (automático ou manual) e. **Origem** Será a Central de segurança do Inteligência contra ameaças.



Enviar aprimoramento de observável para o TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de vistas do SIR para o TISC. Usando o contexto do TISC, o analista pode verificar se os dados de pesquisa de vistas estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados sempre que necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

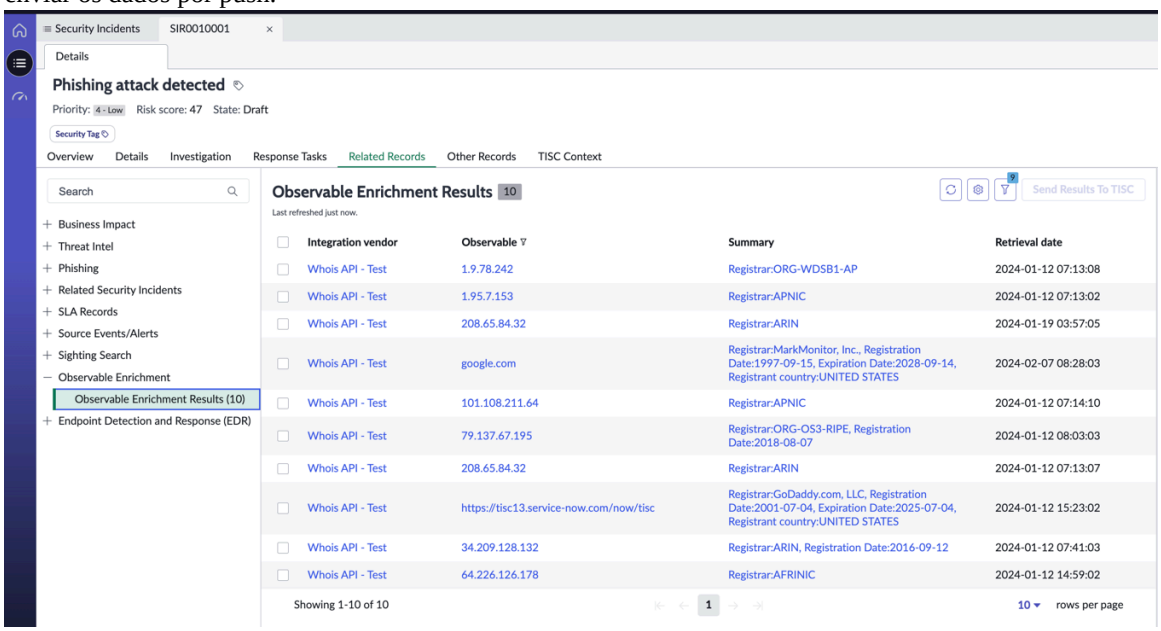
Procedimento

1. Navegue até **Registros relacionados** No espaço SIR para executar a ação de capacidade de integração do TISC.

Nota:

- Você também pode navegar até **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** para executar a operação de envio.
- Em **Investigação** clique em **Exibir informações associadas** para exibir todos os dados de pesquisa de ameaças, pesquisa de vistas e aprimoramento associados para o observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Aprimoramento de Observável** > **Resultados de enriquecimento observável** Para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros observáveis para executar **Enviar resultados para o TISC** operação para enviar os dados por push.



4. Clique em **Enviar resultados para o TISC** .

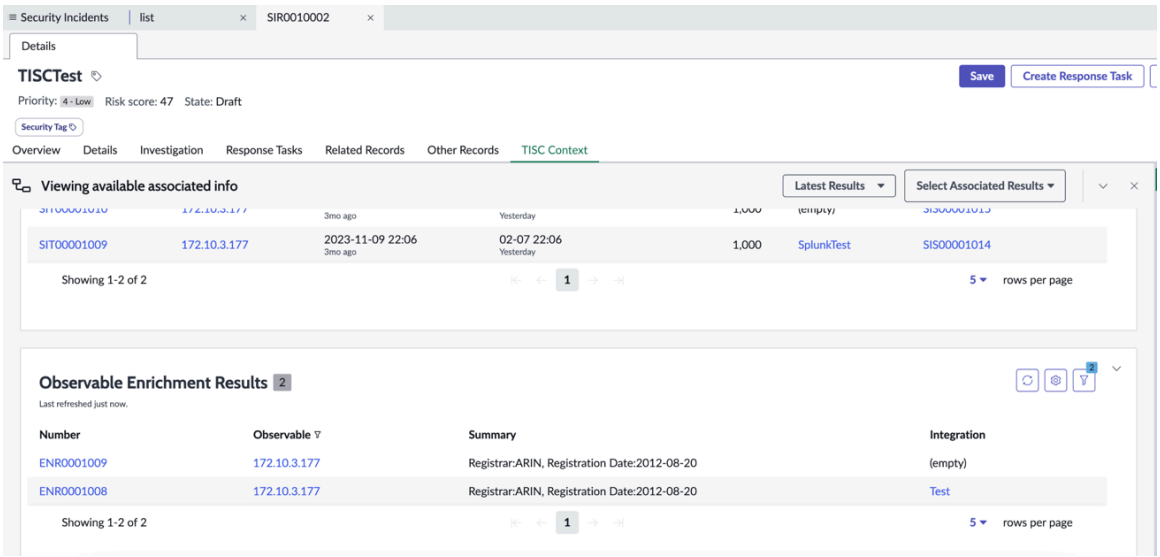
Nota:

- Se o observável selecionado não estiver presente no TISC, primeiro o observável será criado como origem do observável e, depois que o observável de origem criar o registro do observável do TISC, o registro do observável será associado automaticamente ao observável recém-criado.
- Uma vez que a operação de push do observável é executada, uma mensagem informativa é exibida O Observable 0.0.0.0 foi enviado com sucesso para o TISC. A conversão pode levar algum tempo para refletir na guia Contexto do TISC .

5. Selecione **Contexto do TISC** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: :

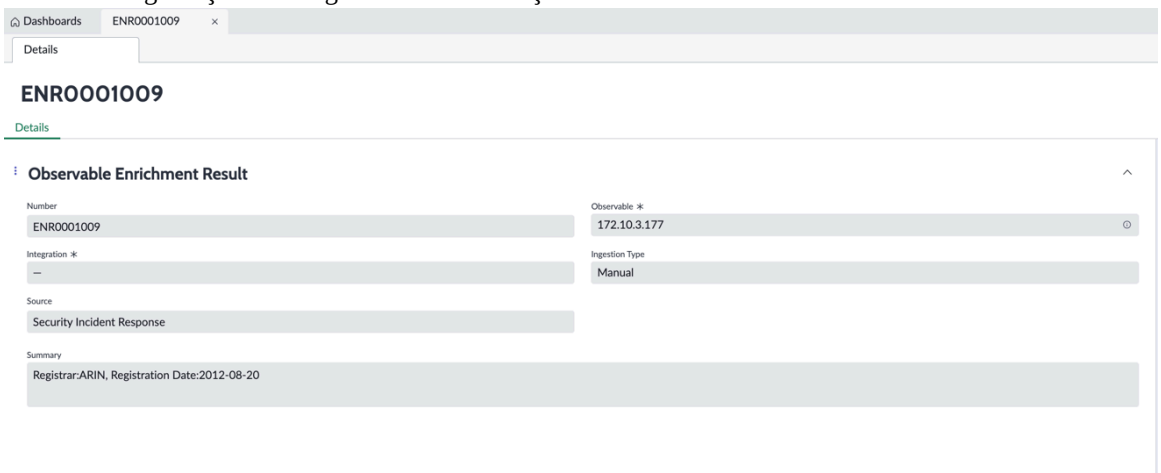
- Agora, você verá o observável que é enviado por push para o TISC a partir da aplicação SIR.
- **Em uma operação de push manual** : Os dados observáveis só podem ser enviados por push se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de push automática** : Os dados observáveis ou de aprimoramento serão enviados automaticamente quando associados a um incidente de segurança.
- **Contexto do TISC** Mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas DO SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento de observável associados dos observáveis selecionados.

6. Exibe os resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em qualquer registro de resultados de aprimoramento de observável para exibir o registro na exibição de formulário, que também mostra o push ou **Tipo de ingestão** (automático ou manual) e. **Origem** Será a Central de segurança do Inteligência contra ameaças.



Trabalhar com o contexto do TISC

O contexto do TISC facilita a exibição de dados de inteligência contra ameaças, como observáveis, no espaço de resposta a incidentes de segurança.

Isso ajuda os analistas de segurança a detectar, investigar e responder a incidentes de segurança com mais eficácia no espaço.

O contexto do TISC no espaço Resposta a incidentes de segurança permite que os analistas de segurança adicionem incidentes de segurança ou observáveis aos casos do TISC diretamente do espaço, também exibam os resultados de aprimoramento e exibam informações relacionadas a observáveis que são agentes de ameaça, padrões de ataque, campanhas e assim por diante.

Usando esta seção, você pode fazer o seguinte:

1. Associe observáveis a um caso de TISC.
2. Exibir informações de observáveis associados.
3. Exibir resultados de aprimoramento de observáveis.

Para obter informações e procedimentos mais detalhados, consulte as seções a seguir e, para obter mais informações sobre como a integração funciona entre os espaços TISC e SIR, consulte Integração do TISC com o SIR Workspace em Central de segurança de inteligência contra ameaças.

Adicionar observáveis ao caso do TISC

Use esta seção para adicionar incidentes de segurança ou observáveis a um caso TISC.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

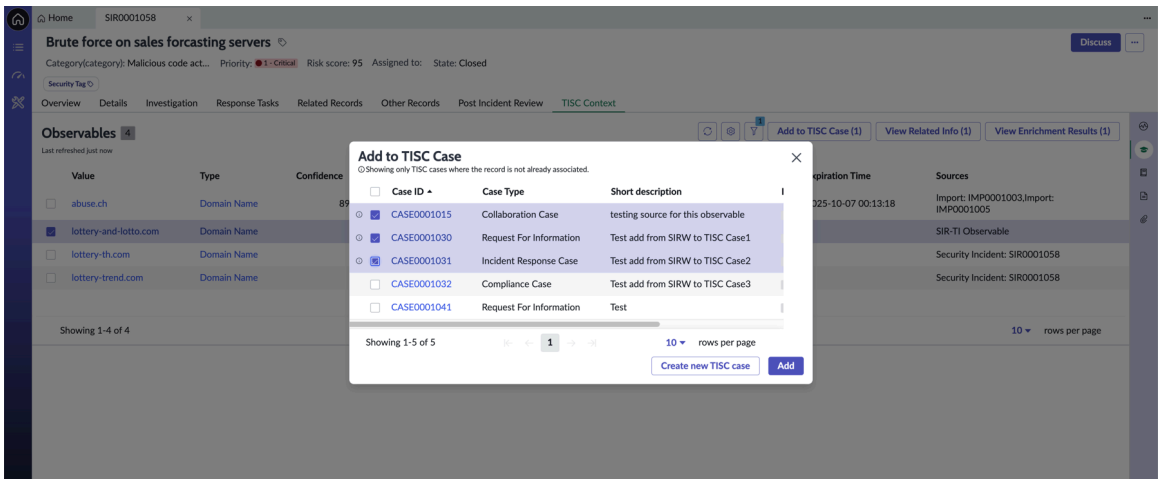
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isso também pode ser feito pesquisando o ID do incidente ou filtrando usando a seção Filtros rápidos ou navegando por um estado de incidente.

3. Selecione **Contexto do TISC** guia.
4. Clique em **Adicionar ao caso TISC** botão.
   A caixa de diálogo Adicionar ao caso do TISC é exibida e mostra somente os casos do TISC em que o registro ainda não está associado.
5. Selecione os observáveis.
6. Selecione Caso(s) e clique em **Adicionar** para adicionar os casos aos observáveis e associá-los ao incidente de segurança.



Nota: Você também pode criar um novo caso clicando em **Criar novo caso TISC** caso você não tenha nenhum caso existente.

As seguintes mensagens de confirmação são exibidas:

- Os observáveis a seguir foram adicionados como artefatos com sucesso.
- Os observáveis a seguir são enviados para o TISC e serão adicionados posteriormente aos registros de caso(s) do TISC selecionados.

Nota: O processamento e a associação das atividades de observáveis são publicados no fluxo de atividades como e quando a associação é concluída.

7. Exiba os registros de casos associados fazendo login no Espaço da Central de segurança do Inteligência contra ameaças para obter outras etapas.
   Para obter mais informações, consulte Integração do TISC com o SIR Workspace.

Nota:

No espaço Resposta do incidente de segurança, você também pode associar observáveis a registros de caso do **Investigação** e. **Registros relacionados** guias.

Nota: Para associar observáveis de **Investigação** , siga o procedimento abaixo e para associar de **Registros relacionados** explicado aqui Adicionar observáveis ao caso do TISC.Você também pode navegar até **Investigação** e navegue até **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** Para adicionar observáveis ao caso do TISC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir informações relacionadas do TISC

Use esta seção para exibir as informações relacionadas, como agentes de ameaça relacionados, padrões de ataque, campanhas e casos do TISC no espaço SIR.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente ou navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Quando o incidente estiver aberto, navegue até **Contexto do TISC** guia.
   Exibição de informações relacionadas à exibição:

   Nos detalhes do incidente, você pode exibir informações relacionadas em várias seções.

   a. Selecione um ou mais observáveis.

   b. Clique em **Exibir informações relacionadas** botão.
   Esta seção exibe as informações associadas relacionadas aos observáveis selecionados.

Nome	Descrição
Agentes da ameaça	Mostra informações do TISC para agentes de ameaça relacionados aos observáveis selecionados.
Padrões de ataque	Mostra informações do TISC para padrões de ataque relacionados aos observáveis selecionados.
Campanhas	Mostra informações do TISC para campanhas relacionadas aos observáveis selecionados.
Casos	Mostra informações do TISC para casos de TISC relacionados aos observáveis selecionados.

Exibir resultados de enriquecimento

Use esta seção para exibir os resultados de aprimoramento de observáveis, como resultados de pesquisa de ameaças, vistas e resultados de aprimoramento de observáveis do TISC no espaço SIR.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Tudo**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente ou navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Quando o incidente estiver aberto, navegue até **Contexto do TISC** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibindo resultados de aprimoramento:

Nos detalhes do incidente, você pode exibir informações relacionadas em várias seções.

a. Selecione um ou mais observáveis.

b. Clique em **Exibir resultados de aprimoramento** botão.
Esta seção exibe os detalhes relacionados aos observáveis selecionados.

Nome	Descrição
Resultados da Pesquisa de ameaças	Lista todos os resultados de pesquisa de ameaças associados para observáveis TISC selecionados.
Detecções	Lista todas as vistas associadas para observáveis TISC selecionados.
Resultados de enriquecimento observável	Lista todos os resultados de aprimoramento de observáveis associados para observáveis TISC selecionados.

Relatórios em Resposta a incidentes de segurança

Todos os relatórios associados a um incidente de segurança estão disponíveis na seção Relatórios para análise e compartilhamento.

O analista será capaz de:

- Criar um relatório
- Edite um relatório
- Exclua um relatório

Criar um relatório

Os analistas podem criar um relatório no Resposta a incidentes de segurança para incluir o status de um incidente e compartilhá-lo por e-mail.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um incidente de segurança.
3. Selecione **Relatórios** .

   . **Relatório** a página exibe uma lista de todos os relatórios criados para o incidente selecionado.

4. Selecione **Novo**.
   . **Selecione Modelo** a página aparece com uma lista de todos os modelos publicados. A lista de modelos está disponível somente quando o administrador publicou modelos de relatórios. Para obter mais informações, consulte Crie um modelo de relatório em Resposta a incidentes de segurança.
5. Selecione um modelo de relatório.
   O relatório é aberto no modo de edição com os dados do incidente conforme configurado no modelo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Expandir** e insira/remova os campos desejados.
   - **Campos SIR comuns** : A lista de campos mais usados para um incidente.
   - **Todos os campos SIR** : Todos os campos relacionados a um incidente. Por exemplo, quando você está gerando um relatório de incidente e deseja adicionar um campo chamado Descrição resumida, é possível selecionar esse campo no **Todos os campos SIR** . Quando você adiciona um campo, a descrição resumida do incidente é exibida no relatório.
   - **Registros relacionados** : Os registros relacionados de um incidente específico. Por exemplo, se você quiser adicionar observáveis associados ao relatório, poderá adicioná-lo ao seu relatório. Esses registros relacionados são exibidos no formato de tabela
   - **Scripts** : Para adicionar a data e a hora do relatório, você pode adicionar o script de data e hora atual ao seu relatório. Esta ação adicionará a data e hora de criação do relatório no relatório.
7. Selecione **Visualização** para exibir uma visualização do relatório.
8. Selecione **Salvar conteúdo** para salvar as mudanças.
9. **Opcional:** Selecione o ícone editar detalhes do relatório para atualizar o nome e a descrição do relatório.
10. Selecione **Publicar** para publicar o relatório.
11. Selecione o ícone Compartilhar relatório no e-mail.
    a. Insira os e-mails do destinatário em **.** e. **Cc/Cco** campos.
    b. Atualize o e-mail **Assunto e corpo do e-mail** .
    c. Selecione **Enviar** para compartilhar o relatório por e-mail.

Edite um relatório

Os analistas podem modificar um relatório não publicado em Resposta a incidentes de segurança e compartilhe por e-mail.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um incidente de segurança.
3. Selecione **Relatórios** .

   . **Relatório** a página exibe uma lista de todos os relatórios criados para o incidente selecionado.

4. Abra o relatório a ser atualizado.
   O relatório é aberto no modo de edição com os dados do incidente conforme configurado no modelo.
5. Edite o relatório conforme necessário.
6. Selecione **Visualização** para exibir uma visualização do relatório.
7. Selecione **Salvar conteúdo** para salvar as mudanças.
8. **Opcional:** Selecione o ícone editar detalhes do relatório para atualizar o nome e a descrição do relatório.
9. Selecione **Publicar** para publicar o relatório.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Selecione o ícone Compartilhar relatório no e-mail .
    a. Insira os e-mails do destinatário em . e. **Cc/Cco** campos.
    b. Atualize o e-mail **Assunto e corpo do e-mail** .
    c. Selecione **Enviar** para compartilhar o relatório por e-mail.

Exclua um relatório

Você pode excluir um relatório em Resposta a incidentes de segurança que está no estado publicado ou rascunho.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um incidente de segurança.
3. Selecione **Relatórios** .

   . **Relatório** a página exibe uma lista de todos os relatórios criados para o incidente selecionado.
4. Abra o relatório a ser excluído.
5. Selecione **Excluir**.
   Uma mensagem de confirmação é exibida.
6. Selecione **Excluir** para excluir o relatório.

Colabore usando chamada em conferência ou bate-papo no Resposta a incidentes de segurança

Você pode colaborar com analistas e usuários afetados para resolver ou discutir sobre um incidente em Resposta a incidentes de segurança aplicação.

Tópicos relacionados

Inicie uma chamada em conferência na Resposta a incidentes de segurança

Inicie um bate-papo na barra lateral na Resposta a incidentes de segurança

Inicie uma chamada em conferência na Resposta a incidentes de segurança

Usando a chamada em conferência, os analistas de segurança podem colaborar com outros analistas e usuários afetados em tempo real. Essas chamadas facilitam a troca de informações para ajudar a resolver incidentes.

Antes de Iniciar

Certifique-se de ter instalado e ativado os seguintes apps e plug-ins:

- Notify (com.snc.notify).
- Notify componentes de IU para o app Espaços configuráveis.
- Visual Task Board plug-in (com.devsnc.snb_vtb)

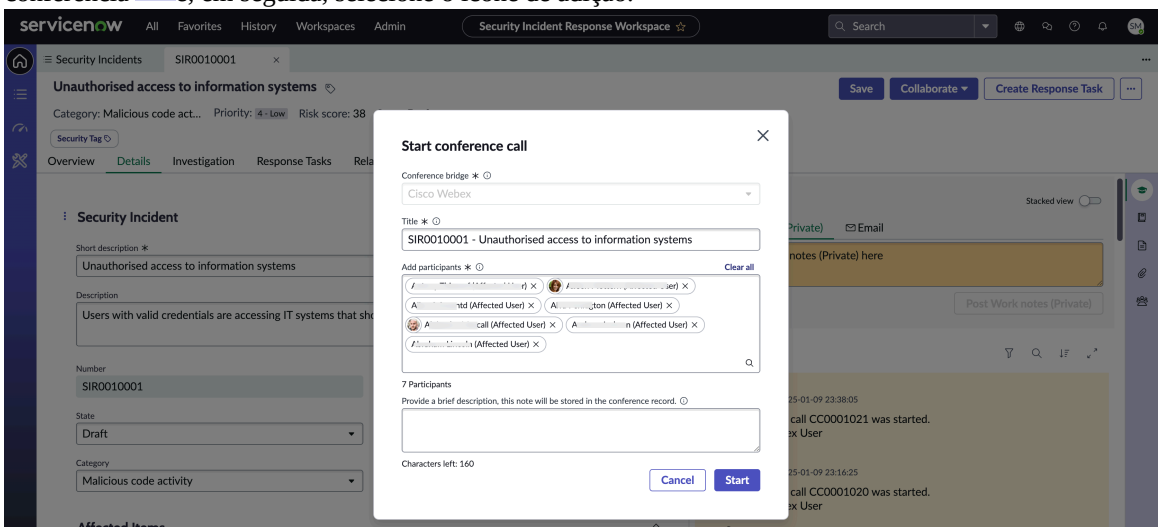
Função necessária: sn_si.analyst ou sn_si.manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um incidente de segurança para o qual você deseja iniciar uma chamada em conferência.
3. Selecione **Colaborar** e selecione **Iniciar uma chamada** ou você pode selecionar o ícone de chamada em conferência e, em seguida, selecione o ícone de adição.



O pop-up Iniciar chamada em conferência é exibido.

4. Selecione uma ponte de conferência no **Ponte de conferência** campo.
5. Forneça um título para a chamada em conferência no **Título** .

> **Nota:** Por padrão, o título do incidente é preenchido como o título da chamada. Você pode modificar o título padrão.

6. Adicionar ou remover participantes da chamada em **Adicionar participantes** .

> **Nota:** Com base na configuração nas configurações de Chamada em conferência, uma lista pré-preenchida de participantes é adicionada **Adicionar participantes** ou um **Recomendações** a lista de participantes está disponível. Para obter mais informações, consulte Gerenciar usuários e grupos de chamadas em conferência.

7. Forneça uma breve descrição para iniciar a chamada em conferência.
8. Selecione **Iniciar**.

A chamada em conferência começa na ponte de conferência selecionada. Todos os participantes recebem notificação por e-mail e por meio da ponte de conferência. Os participantes podem usar o link ou a notificação para ingressar na chamada.

9. Abra o incidente associado em Resposta a incidentes de segurança aplicação para exibir os detalhes da chamada em conferência.
10. **Opcional:** Selecione **Copiar convite** para adicionar participantes em uma chamada ativa.
11. Selecione **Encerrar chamada**.
    Quando o participante final sai da chamada em conferência, a chamada é encerrada
12. **Opcional:** Para reiniciar uma chamada em conferência, navegue até **Concluído** e selecione **Reiniciar** opção da chamada em conferência necessária.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione participantes à chamada em conferência ativa

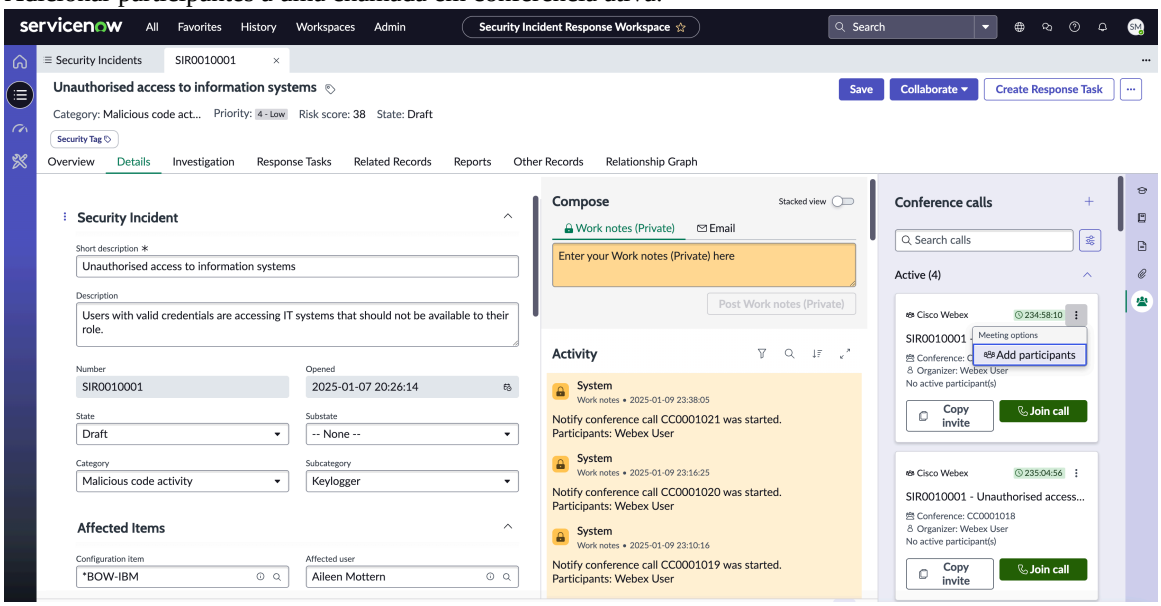
Você pode adicionar participantes a uma chamada em conferência ativa se não os tiver adicionado antes de iniciar a chamada em conferência.

Antes de Iniciar

Função necessária: sn_si.analyst,sn_si.manager

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra o incidente de segurança para o qual você deseja iniciar uma chamada em conferência.
3. Selecione o ícone de chamada em conferência para exibir os detalhes das chamadas em conferência.
4. Adicionar participantes a uma chamada em conferência ativa:



   - Selecione o ícone de opções de reunião ⋮ para a chamada em conferência ativa e selecione **Adicionar participantes** .
   - Selecione **Copiar convite** em **Chamadas em conferência** e compartilhe o convite com os participantes necessários.

Inicie um bate-papo na barra lateral na Resposta a incidentes de segurança

Usando a Barra lateral, os analistas de segurança podem colaborar com outras pessoas em tempo real com base em um registro baseado em tarefas ou interação do Espaço. Essas discussões da barra lateral facilitam a troca de informações e conhecimento para ajudar a resolver problemas com mais rapidez e com resultados de maior qualidade.

Antes de Iniciar

Função necessária: sn_si.read

Verifique se você ativou o plug-in Omni-Experience Standard Feature Set. Para obter mais informações, consulte Instalação de Barra lateral .

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione a Exibição de lista ícone.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra um incidente de segurança para o qual você deseja iniciar uma discussão na barra lateral.
4. Selecione **Colaborar** e selecione **Iniciar bate-papo** .
   A caixa de diálogo Iniciar uma discussão na barra lateral é exibida.

   Nota: A integração da Sidebar com o Microsoft Teams permite que os usuários da Barra lateral e do Microsoft Teams se comuniquem entre si a partir de suas respectivas plataformas. Para obter mais informações, consulte Barra lateral e Microsoft Teams .

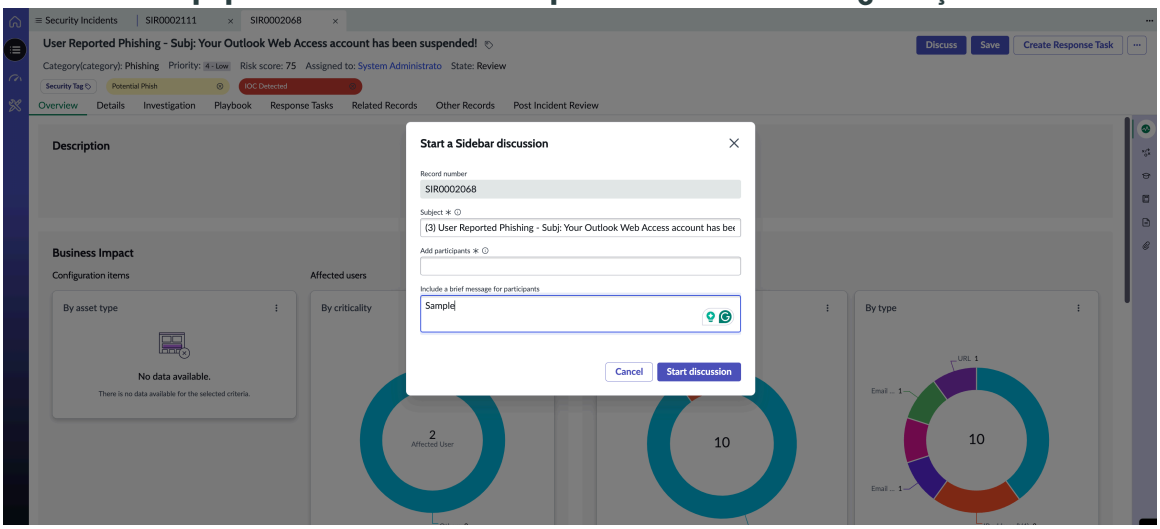
5. Na caixa de diálogo Iniciar uma discussão na barra lateral, preencha os campos.

Campo	Descrição
Número de registro	O número da tarefa ou incidente associado à discussão da barra lateral.
Assunto	Forneça um título para a discussão da barra lateral.
Adicionar participantes	Opção para adicionar participantes à discussão da barra lateral. Se você tiver integrado o bate-papo da barra lateral com o Microsoft Teams, também poderá adicionar participantes do Microsoft Teams. **Nota:** ○ É necessário adicionar pelo menos um participante para criar uma nova discussão. ○ Se a Barra lateral e o Microsoft Teams estiverem integrados, os usuários do Microsoft Teams serão diferenciados dos usuários da Barra lateral com um ícone do Microsoft Teams. ○ Por padrão, todos os usuários que têm acesso de leitura aos registros SIR também terão acesso aos bate-papos da barra lateral, mas isso pode ser controlado usando a consulta do membro. Para obter mais informações, consulte Configurar consulta de membro Barra lateral .
Inclua uma mensagem resumida	Envie um resumo curto do problema para que seja abordado na discussão da barra lateral.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inicie um bate-papo na barra lateral na Resposta a incidentes de segurança



6. Selecione **Iniciar discussão**.

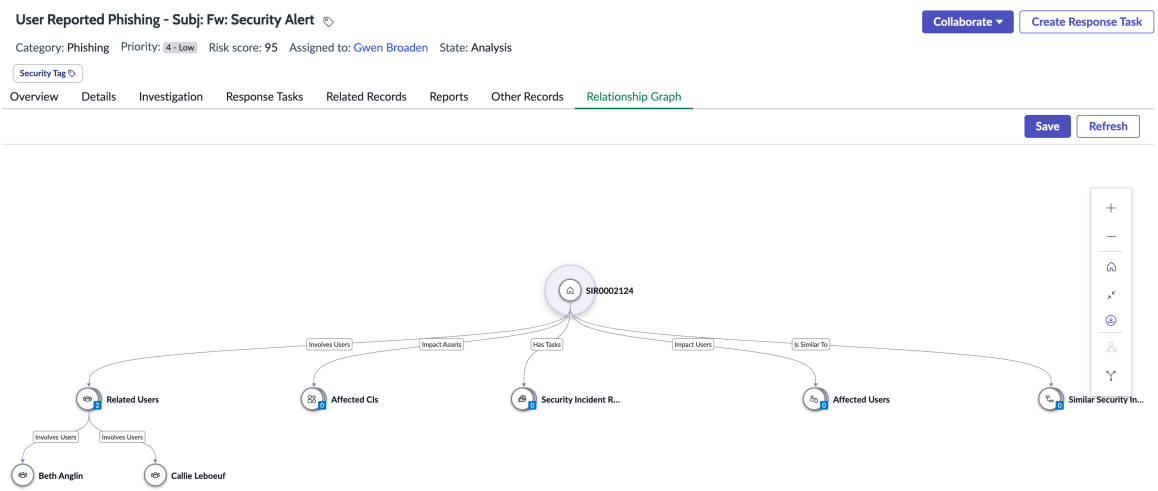
7. Você pode executar configurações adicionais, como ações rápidas.
   Para limitar o uso da ação, você pode usar **Aplicar ao grupo** campo na página de ação rápida. Para obter mais informações, consulte Como criar uma ação rápida .

Exibindo detalhes do incidente com um gráfico de relacionamento

Gráficos de relacionamento no Resposta a incidentes de segurança o espaço exibe visualmente as conexões entre um incidente de segurança e seus itens relacionados para ajudar você a analisar o contexto completo de um incidente de segurança.

Os itens relacionados a um incidente de segurança podem incluir observáveis associados, itens de configuração (ICs), incidentes de segurança semelhantes (SIRS), tarefas de resposta e outras listas relacionadas.

O exemplo de gráfico de relacionamento a seguir exibe detalhes de um incidente de segurança.



Quando você abre um gráfico de relacionamento para um incidente de segurança, as configurações disponíveis ficam visíveis por padrão. Você pode interagir com o gráfico da seguinte forma:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aplique zoom em qualquer objeto que se ajuste à tela e arraste os nós.
- Adicione subnós para cada nó, se disponíveis, e exiba os detalhes dos subnós.
- Oculte qualquer nó ou subnó do gráfico.
- Exibir detalhes de um subnó.

Personalize um gráfico de relacionamento

Visualize e analise incidentes de segurança e seus dados associados em um gráfico de relacionamento.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Espaços** > **Espaços de resposta a incidentes de segurança** > **Administração**.
2. Selecione **Gráfico de relacionamento** e, em seguida **Configurações do Gráfico de Relacionamento** .
3. Selecione **Novo**.
4. No formulário, preencha os campos.

Configurações do gráfico de relacionamento

Campo	Descrição
Nome da tabela relacionada	A tabela da qual você deseja buscar os dados observáveis do incidente de segurança, como a tabela Associar observável [sn_ti_observable] ou Incidente de segurança [sn_si_incident].
Rótulo de nó	O rótulo do nó do observável que aparece no gráfico de relacionamento. O valor fornecido automaticamente depende da tabela relacionada selecionada.
Ativo	Opção para habilitar a configuração.
Rótulo de nó de dados	O rótulo primário e secundário a serem exibidos no nó da lista relacionada selecionada.
Visível padrão	Opção para exibir o rótulo do nó de dados.
Rótulo de relacionamento	O relacionamento entre um nó e nó de link a ser exibido no gráfico de relacionamento.

5. Selecione **Save** (Salvar).

Crie um gráfico de relacionamento para um incidente

Crie um gráfico de relacionamento de nó em Resposta a incidentes de segurança Para que você possa analisar melhor um incidente de segurança, correlacionando-o com observáveis mal-intencionados, itens de configuração (ICs), incidentes de segurança semelhantes (SIRS), tarefas de resposta e outras informações relacionadas.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para obter informações sobre como criar um gráfico de relacionamento personalizado em vez de usar um gráfico predefinido, consulte Personalize um gráfico de relacionamento.

Nota: As mudanças no gráfico de relacionamento não são salvas automaticamente.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um incidente de segurança.
3. Selecione **Gráfico de relacionamento** guia.
4. No gráfico de relacionamento, selecione e mantenha pressionado (ou clique com o botão direito do mouse) o nó primário e selecione **Adicionar nós** .
5. Selecione um ou mais nós de categoria para exibir no gráfico de relacionamento, como Usuários relacionados, ICs afetados, incidentes de segurança semelhantes (SIRS) ou usuários afetados.

   Nota: Você pode selecionar vários nós de categoria.

6. Selecione e mantenha pressionado (ou clique com o botão direito do mouse) um nó de categoria e selecione **Vincular nós** para adicionar dados associados ao nó da categoria.

   Nota: Você pode aplicar filtros para reduzir o número de itens na lista.

   Uma lista de todos os registros relacionados para o nó da categoria selecionado é exibida. Por exemplo, se você selecionar **Usuários afetados** na categoria de nó, uma lista de todos os usuários afetados por este incidente é exibida.
7. Selecione os registros desejados na lista e selecione **Adicionar** .
8. Selecione **Adicionar**.
9. **Opcional:** Se necessário, desmarque as mudanças selecionando **Atualizar** .
10. Selecione **Save** (Salvar).

    Nota: As mudanças nos filtros também são salvas quando você salva o gráfico de relacionamento.

11. **Opcional:** Exiba os detalhes de um subnó.
    a. Selecione um subnó.
    b. Selecione **Mostrar detalhes** .
12. **Opcional:** Baixe o mapa para o seu sistema.

    a. Se apenas uma parte do mapa estiver visível na tela e você quiser que a tela inteira seja incluída no PDF, selecione o ícone Ajustar à tela ( ).

       Nota: Somente a parte do mapa que aparece na tela é incluída no arquivo PDF.

    b. Selecione o ícone de mapa de exportação ( ).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Vídeo que mostra como editar um gráfico de relacionamento para adicionar nós e subnós de categoria

https://player.vimeo.com/video/1095955062?h=593c16e2b6&badge=0&autopause=0&player_id=0&app_id=58479

Playbook de incidentes de segurança

Invoque o fluxo do playbook de incidentes de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados pelo Flow Designer existentes, ele continuará funcionando e as atividades continuarão sendo renderizadas como tarefas de resposta.

Há duas maneiras de associar o playbook ao incidente de segurança:

- Invocar automaticamente o playbook
- Adicionar playbook manualmente

Invocar playbook automaticamente

Para que um Playbook seja invocado automaticamente, um processo precisa ser definido usando **Designer de automação de processos (PAD)** e quando a condição do gatilho é atendida, a guia playbook é renderizada automaticamente com as atividades do playbook que estão sendo exibidas.

Adicionar playbook manualmente

Para que um Playbook seja invocado manualmente, navegue até o menu suspenso Ação de IU do formulário e selecione **Adicionar Playbook** . Para obter mais informações, consulte, Adicionar Playbook

Nota: Se já houver um playbook disponível, os novos playbooks adicionados serão executados paralelamente aos playbooks existentes.

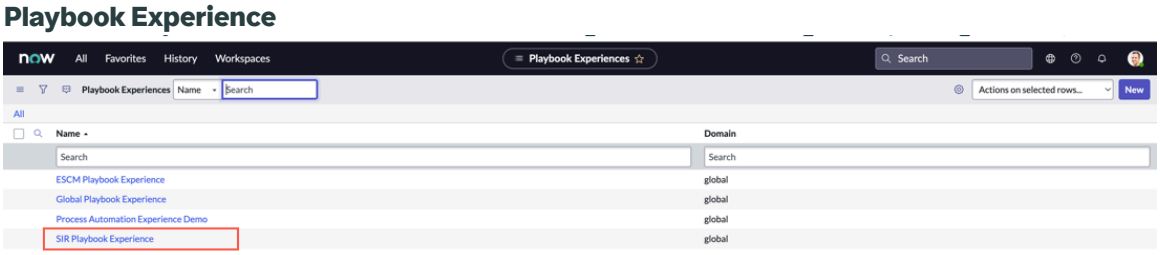
- No playbook, o analista pode filtrar os cartões do playbook por status.
- O analista pode cancelar um playbook selecionando-o no ícone de reticência.
- Em cada atividade, o analista poderá executar as ações definidas nos cartões de atividade, como Ignorar, Marcar como concluído, Cancelar ou Ações de Orquestração, como Enviar para área restrita, Pesquisar e-mails e assim por diante.
- Cada uma dessas ações é definida na definição da atividade, e o cartão completo visível é personalizável no momento da criação da própria definição da atividade.

Nota: Todas as definições de atividades futuras e as próximas etapas a serem executadas são exibidas com um ícone de cadeado e estão no modo somente leitura para o usuário. O modo de exibição do playbook é controlado por uma configuração conforme explicado abaixo.

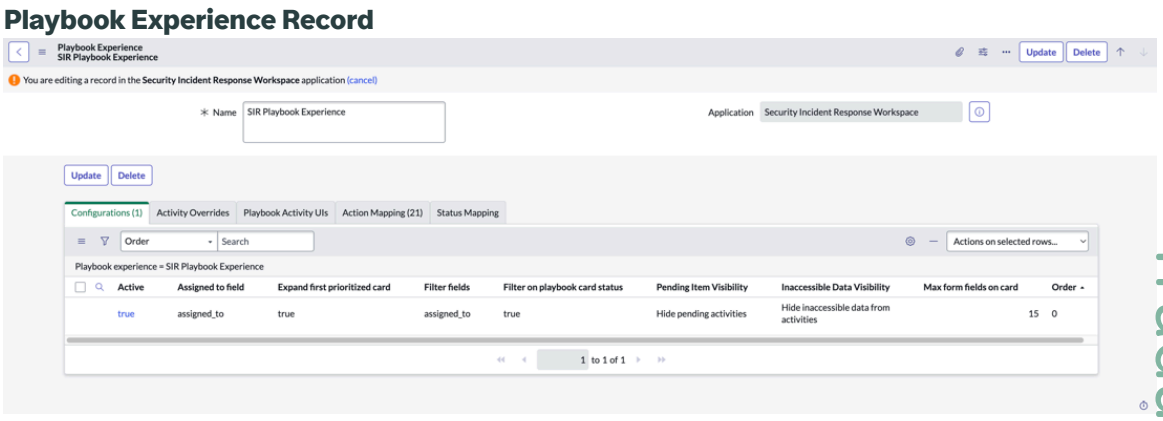
1. Navegar até **Tudo** > **Playbook Experiences**.
2. Na página Playbook Experiences, selecione um **SIR Playbook Experience** .

Tradução automática

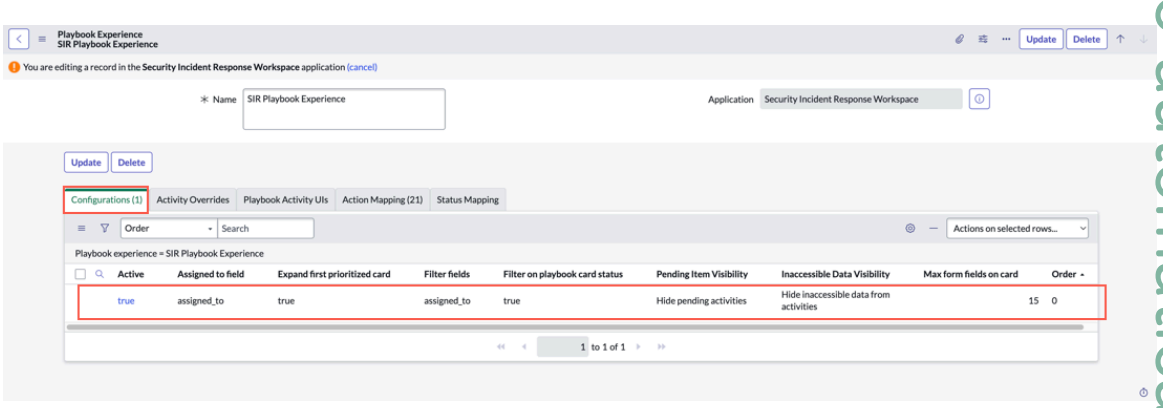
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



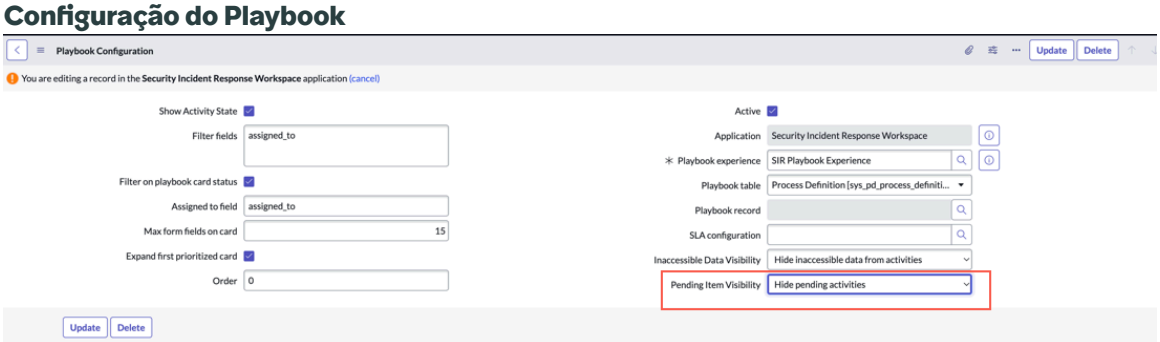
. **SIR Playbook Experience** a página é exibida.



3. Clique em **Configuração** registro.



4. Na guia Configuração, clique em Configuração do SIR Playbook Experience.



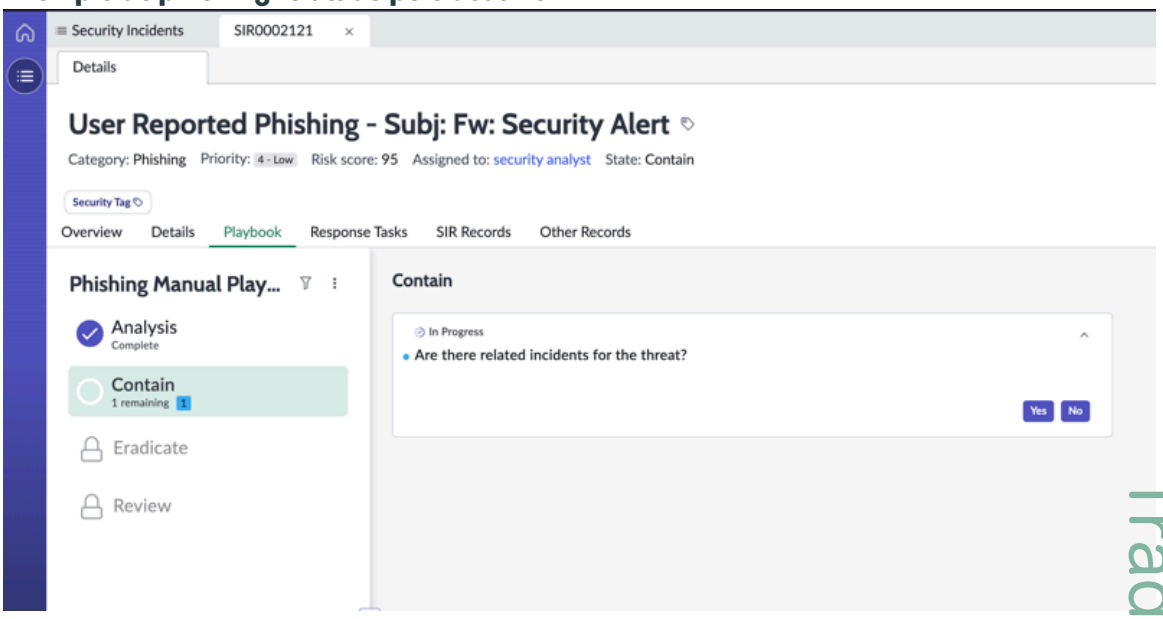
5. Navegue até **Visibilidade do item pendente** lista suspensa do campo, selecione a opção desejada e salve o registro. Escolhas das seguintes opções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

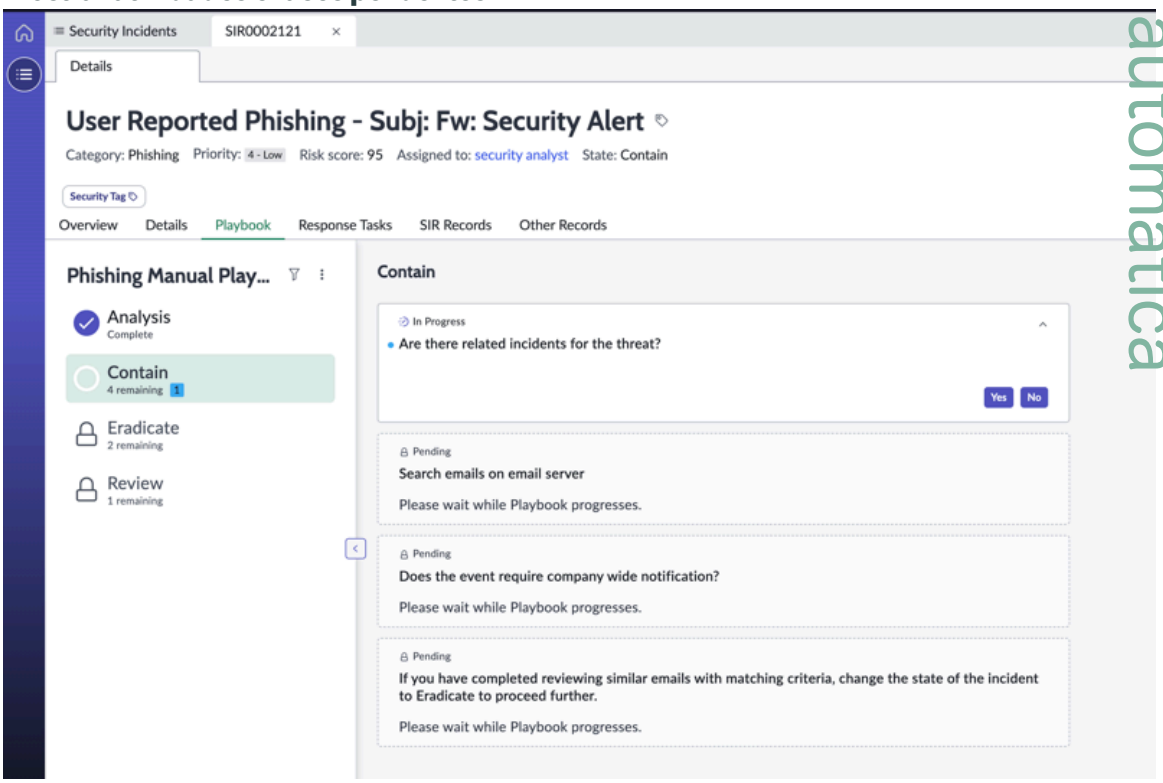
- **Ocultar atividades pendentes** : Selecione esta opção para ocultar as atividades pendentes que você deseja ver na seção Playbook do espaço.

Exemplo de phishing relatado pelo usuário



- **Mostrar fases e atividades pendentes** : Selecione esta opção para mostrar fases e atividades pendentes que você deseja ver na seção Playbook do espaço.

Mostrar atividades e fases pendentes

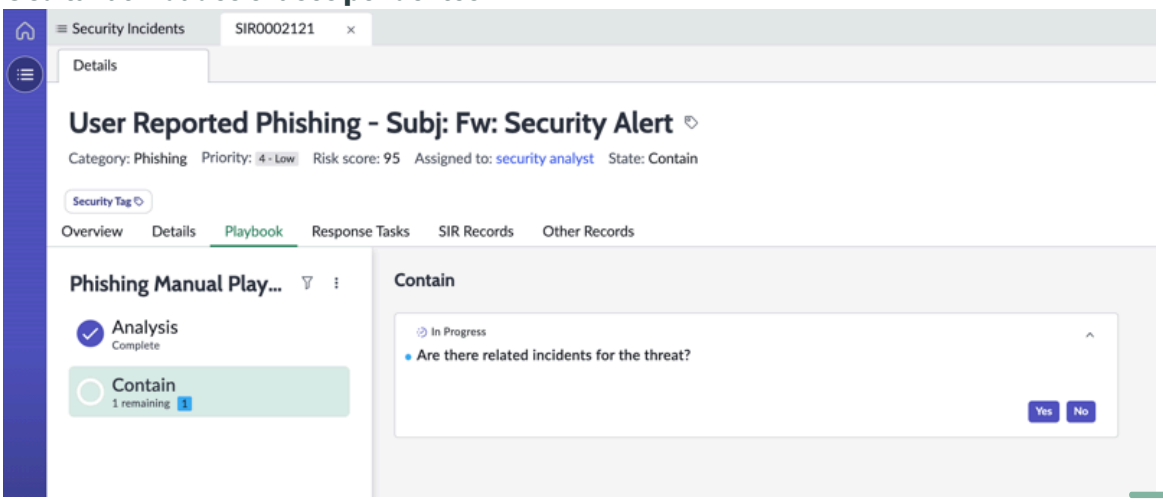


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

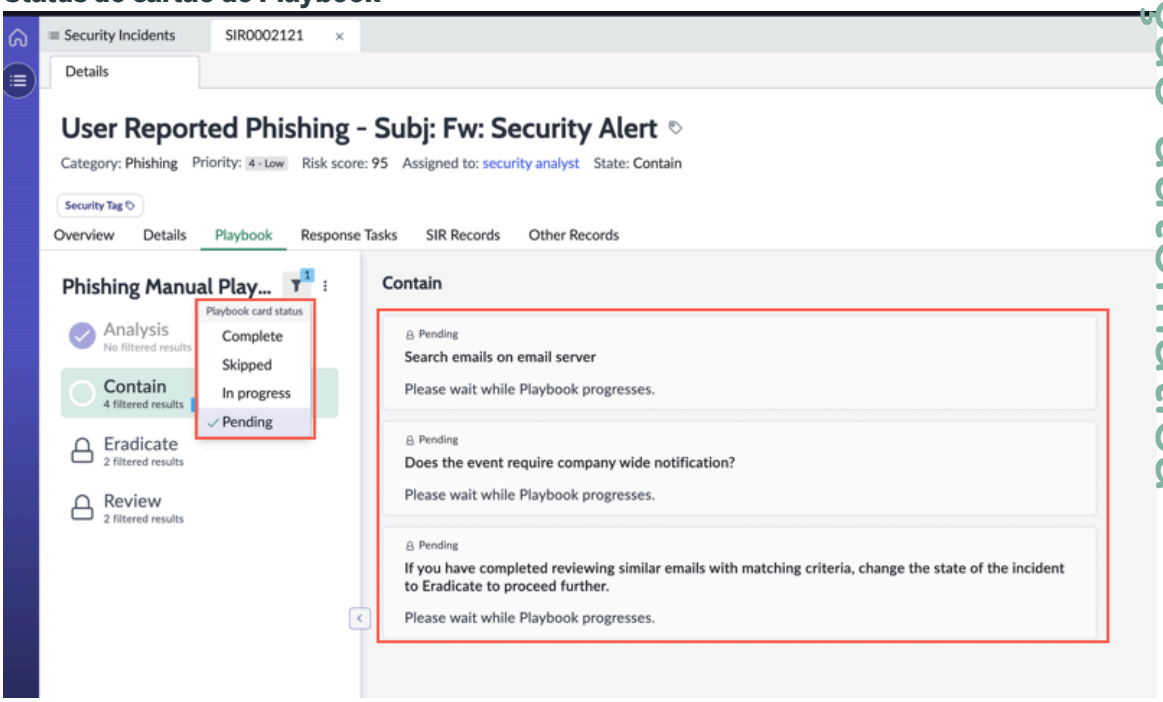
- **Ocultar atividades e fases pendentes** : Selecione esta opção para ocultar as atividades e fases pendentes que você deseja ver na seção Playbook do espaço.

Ocultar atividades e fases pendentes



6. Na seção Playbook, use a opção de filtro para filtrar as atividades por status do cartão Playbook (definição de atividade).

Status do cartão do Playbook



Adicionar Playbook

Use esta seção para adicionar o playbook manualmente.

Antes de Iniciar

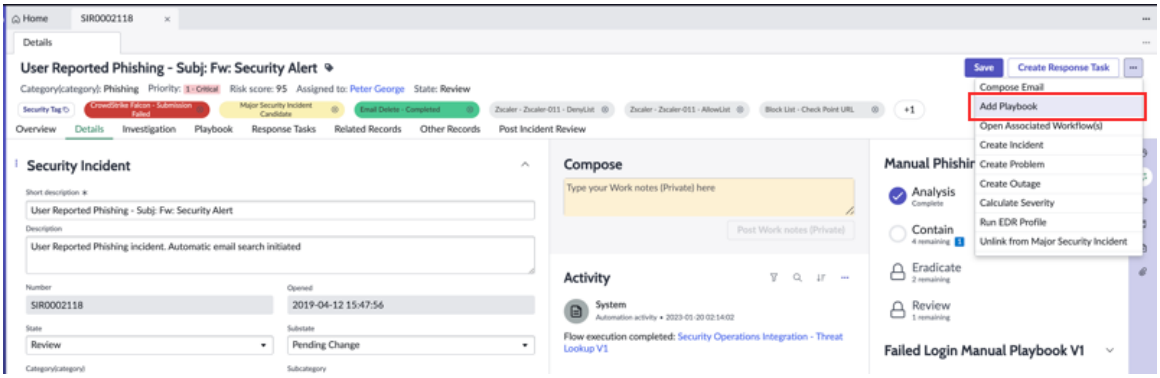
Função necessária: sn_si.analyst

Tradução automática

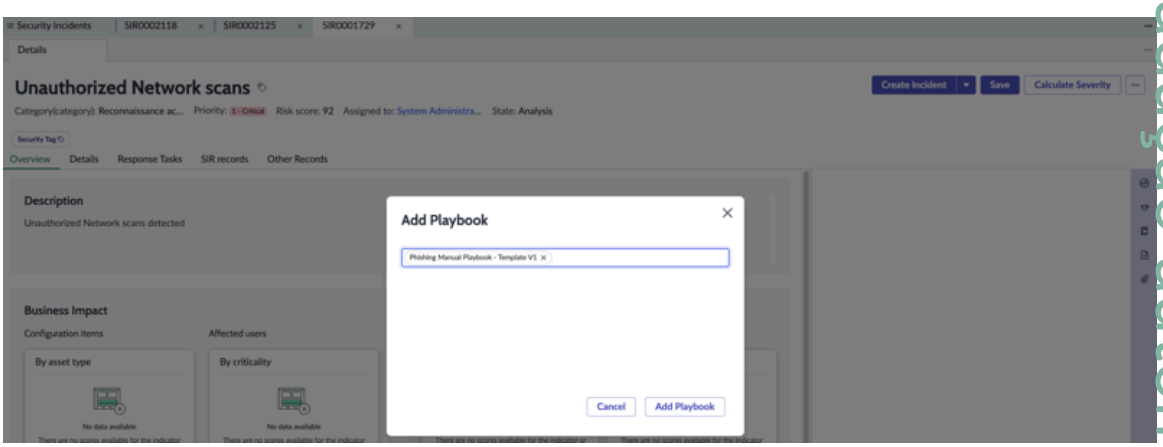
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Espaço de trabalho do analista de segurança**.
2. Abra um registro de incidentes
3. Clique em **Adicionar Playbook** .



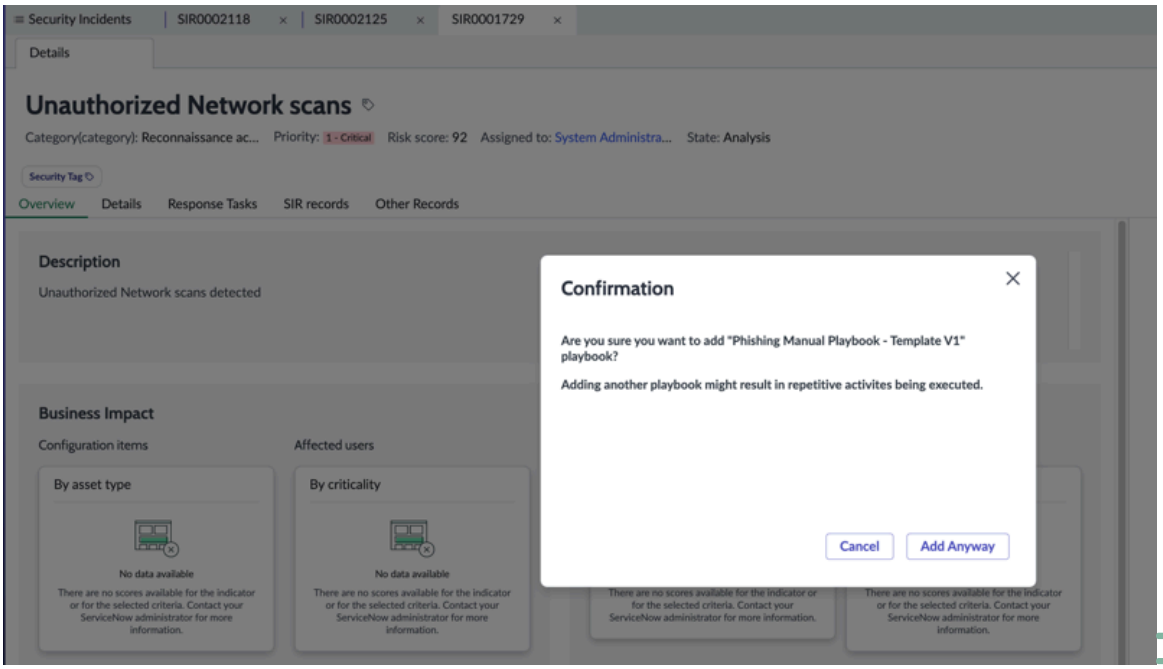
. **Adicionar Playbook** a caixa de diálogo é exibida.



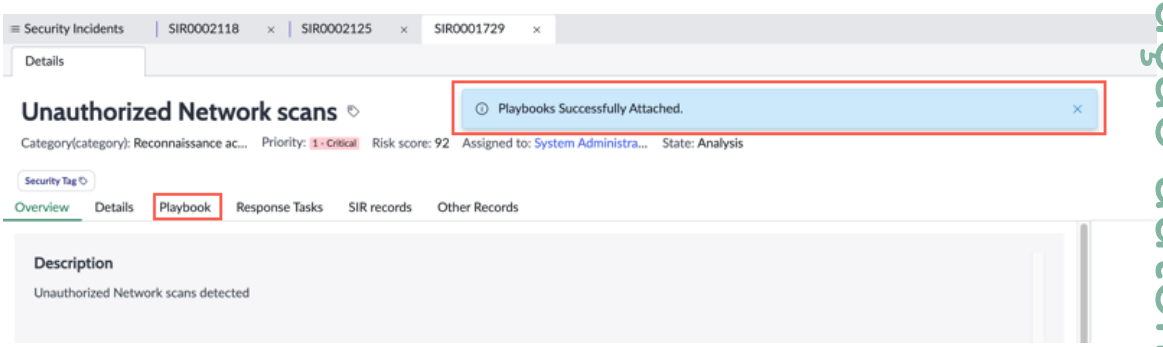
4. Selecione o modelo de playbook.
5. Clique em **Adicionar Playbook** .
   Uma caixa de diálogo de mensagem de confirmação é exibida para você confirmar.
6. Clique em **Adicionar mesmo assim** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



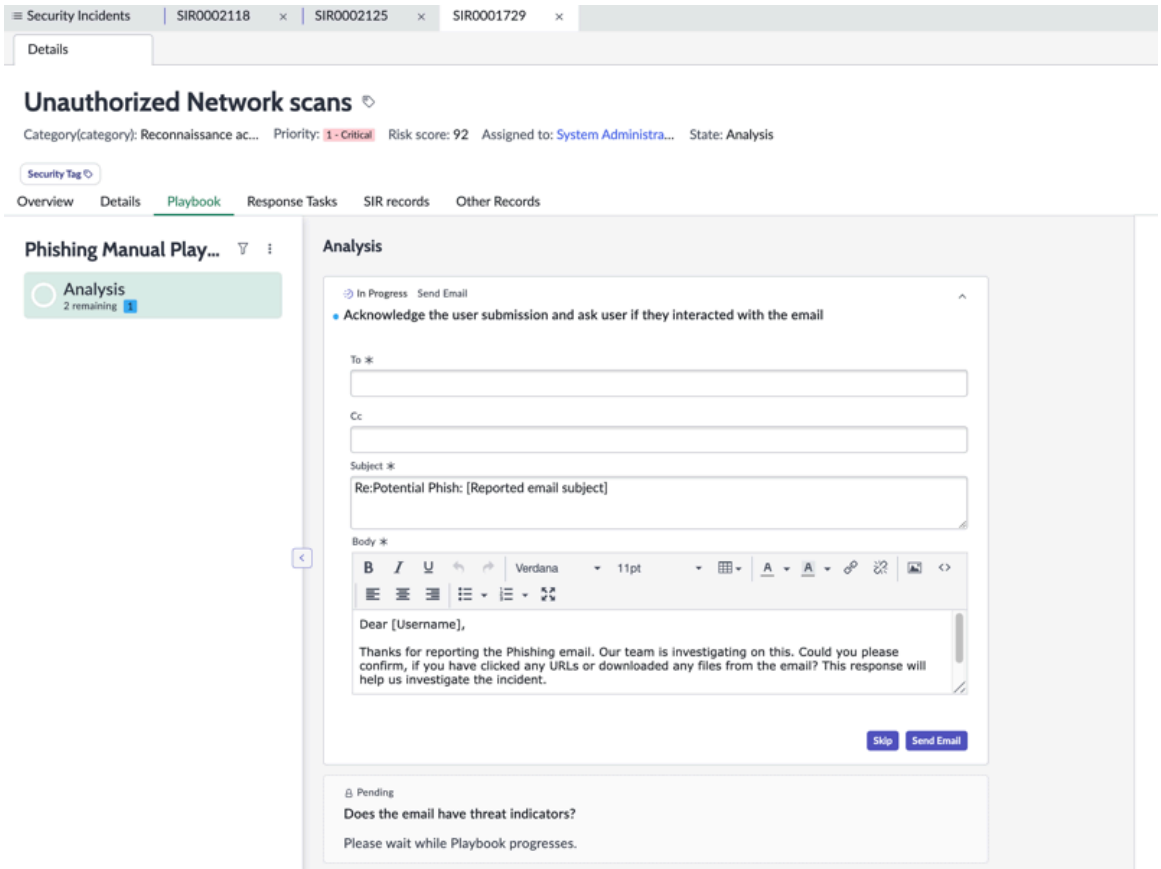
7. . **Playbook** adicionado ao lado de **Detalhes** guia.



8. Clique em **Playbook** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Execute a série de atividades conforme listado para passar para o próximo nível.

> **Nota:** Se um incidente de segurança estiver associado a um playbook, até que o playbook associado seja encerrado ou cancelado, o usuário não poderá associar novamente o mesmo playbook ao mesmo incidente de segurança.

Pré-requisitos para os Playbooks

Você precisa das seguintes funções e plug-ins para criar os Playbooks.

Função necessária: administrador

- Habilite o plug-in Designer de automação de processos (PAD) [com.glide.pad.license].
- Habilite os seguintes plug-ins para uma experiência de playbook:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Habilitar spoke de Operações de segurança para fluxos de acesso [com.snc.secops.spoke].
- PAD Commons da Gestão de casos de segurança empresarial.

Certifique-se de ter lido a documentação da plataforma em Explorando playbooks e. Designer de automação de processos antes de começar com este guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recriando playbooks existentes em Workflow Studio

Você não pode converter fluxos existentes diretamente em playbooks no Workflow Studio. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados.

Você não tem permissão para converter fluxos existentes diretamente em playbooks no Workflow Studio. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados. Usando esses subfluxos ou ações granulares, você deve criar definições de atividade. Depois de criar essas definições de atividade, elas são adicionadas como atividades na fase na definição do processo. Você pode reutilizar definições de atividade em vários playbooks.

Você pode personalizar cada atividade para renderizar as ações necessárias dentro delas e como o cartão deve ser exibido ao criar a definição da atividade. A atividade pode mostrar clientes de e-mail, tabelas, ações, artigos da base de conhecimento, URLs, e assim por diante. Você pode definir como a definição de atividade e a ação ou subfluxos subjacentes são criados.

Para obter mais informações, consulte as seções a seguir.

- Definições de atividades
- Designer de automação de processos

Definições de Atividades

. ServiceNow AI Platform fornece algumas definições de atividade no sistema de base. Para os playbooks do sistema de base do SIR Workspace, há algumas definições de atividade definidas no sistema de base na aplicação Commons PAD DO Enterprise Security Case Management.

Função necessária: sn_si.admin.

Esta é a lista de definições de atividade que fazem parte do sistema de base:

Definição de Atividade	Tabela	Descrição	Aplicação
Aguardar condição sem experiência	Global[global]	Aguarde a condição sem experiência	PAD Commons da Gestão de casos de segurança empresarial
Enviar para área restrita FCS X	Incidente de segurança [sn_si_incident]	Enviar para área restrita	PAD Commons da Gestão de casos de segurança empresarial
Enviar e-mail	Incidente de segurança [sn_si_incident]	Atividade Enviar e-mail para playbooks SIR.	PAD Commons da Gestão de casos de segurança empresarial
Pesquisar E-mail	Incidente de segurança [sn_si_incident]	Pesquisar e-mails no servidor de e-mail	PAD Commons da Gestão de casos de segurança empresarial
Atualizar estado da tarefa	Incidente de segurança [sn_si_incident]	Atualize o estado da tarefa	PAD Commons da Gestão de casos de segurança empresarial
Excluir e-mail	Incidente de segurança [sn_si_incident]	Excluir e-mails	PAD Commons da Gestão de casos de segurança empresarial

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de Atividade	Tabela	Descrição	Aplicação
Resultado Sim Não	Tarefa [task]	Resultado esperado	PAD Commons da Gestão de casos de segurança empresarial

Exemplo de definição de atividade: Enviar e-mail

A seguir está um exemplo de definição de atividade Enviar e-mail.

Básico

Os detalhes básicos capturam o nome (rótulo), a aplicação, a descrição, a tabela e de todas as aplicações a partir das quais ele pode ser acessado.

Adicione o plano de automação, a experiência de atividade e o envio. Depois de enviar, edite o documento para adicionar mais detalhes em cada guia.

Plano de Automação

O Plano de automação associa a ação de back-end ou os subfluxos criados usando o Flow Designer. Este exemplo usa: **Enviar e-mail - Atividade ESCM** subfluxo.

Este subfluxo permite o envio de um e-mail. Ele tem a lógica principal para enviar um e-mail. Todos os campos de entrada e de saída estão definidos.

Todos os campos de entrada são mostrados na seção do plano de automação. Cada campo de entrada pode ser habilitado para ficar visível somente para o administrador, no modal padrão, no modal padrão e no painel de configuração:

- **Somente visibilidade do administrador** : quando definido como administrador, somente o administrador pode exibi-lo.
- **Incluir no modelo padrão** : quando definido para exibir no modal padrão, ele aparece somente no modal de propriedades.
- **Incluir no modelo padrão e no painel de configuração** : Quando definido para exibir no modal padrão e no painel de configuração, ele aparece no painel de configuração DO BLOCO, bem como no modal de propriedades. Para obter mais informações, consulte Definições de atividade

Você pode definir os campos de entrada no momento da própria definição da atividade, desde que não seja necessário alterar esses valores no momento da configuração. Isso ajuda o responsável pelo processo de negócios a economizar tempo ao configurar uma atividade em um processo.

Experiência de Atividade

A guia Experiência de atividade define como o cartão de atividade é renderizado no tempo de execução. O sistema de base fornece os seguintes tipos de experiência:

- Aprovação
- Item do catálogo
- Criar Registro
- Instrutivo
- Conhecimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Lista
- Notificação
- Registro

Com base no tipo de experiência selecionado, os campos adicionais são preenchidos. Para obter mais informações, consulte ServiceNow AI Platform documentação.

Neste exemplo, **Registro** o tipo está selecionado.

Nota: Por exemplo, se você quiser renderizar uma tabela, poderá escolher a lista como o tipo de experiência.

Registro Associado

Use este registro para armazenar os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: Dados de fluxo
- Registro associado: Vl
- Tabela de status da experiência: Dados de fluxo
- Registro de status da experiência: Vl

Neste exemplo, a tabela de dados de fluxo é usada para capturar os dados de tempo de execução. Os dados de tempo de execução podem variar com base no caso de uso. Neste exemplo, os dados de tempo de execução são campos como Para, Cc, Assunto e corpo. Para cada caso de uso, uma definição de dados de fluxo precisa ser criada para definir o tipo de dados de tempo de execução.

1. Navegue até o painel esquerdo e insira **sys_flow_data_definition.list** . Ele exibe a lista de definições criadas para a tabela de dados de fluxo.

Registro associado

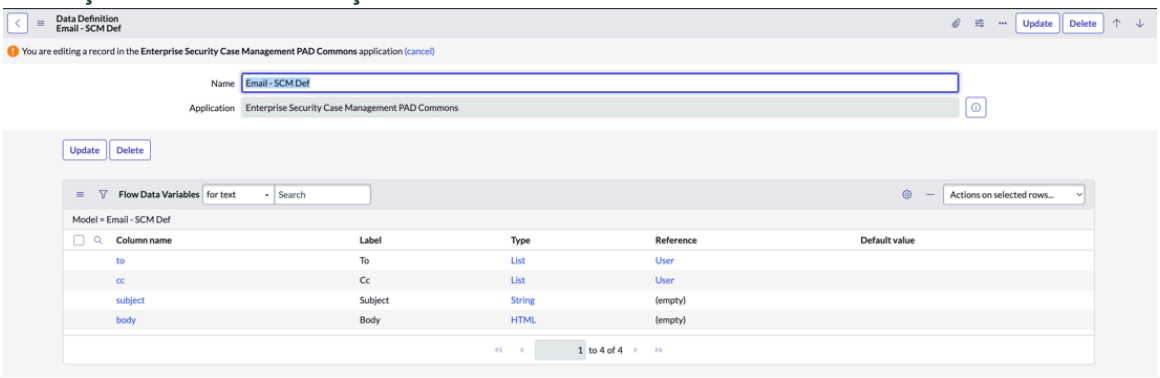


2. Aberto **Definição de e-mail - Definição do SCM** para exibir a definição relacionada a este exemplo.

Tradução automática

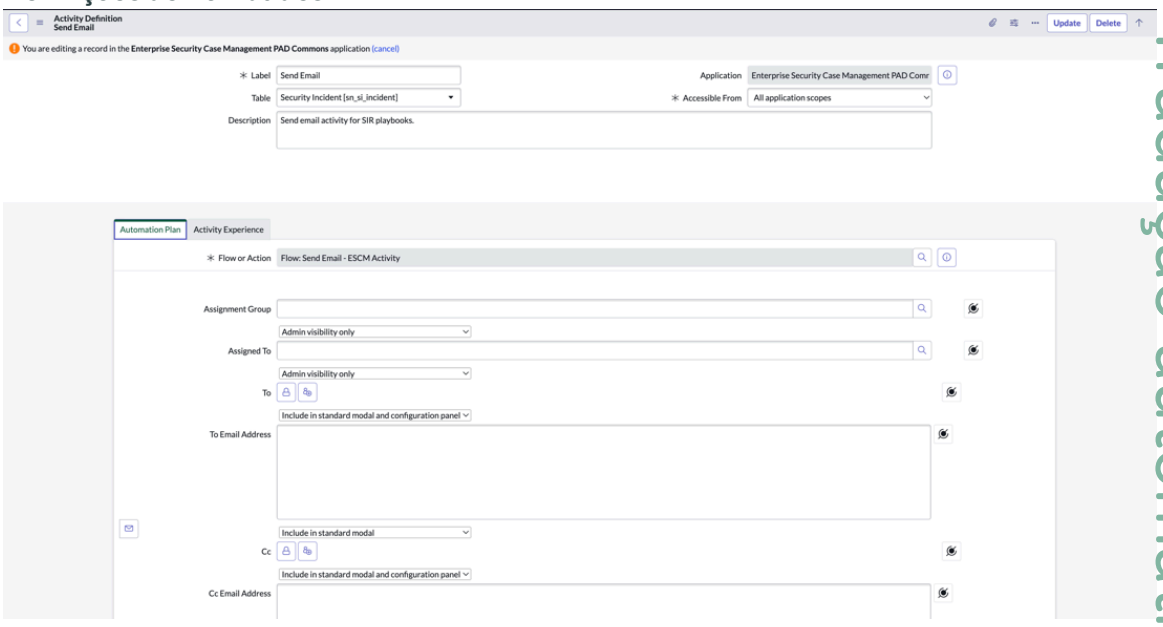
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de e-mail - Definição do SCM



Esta definição de dados de fluxo deve ser usada pelo subfluxo ou pela ação associada a esta definição de atividade (consulte o plano de automação) para capturar os dados de tempo de execução.

Definições de Atividades



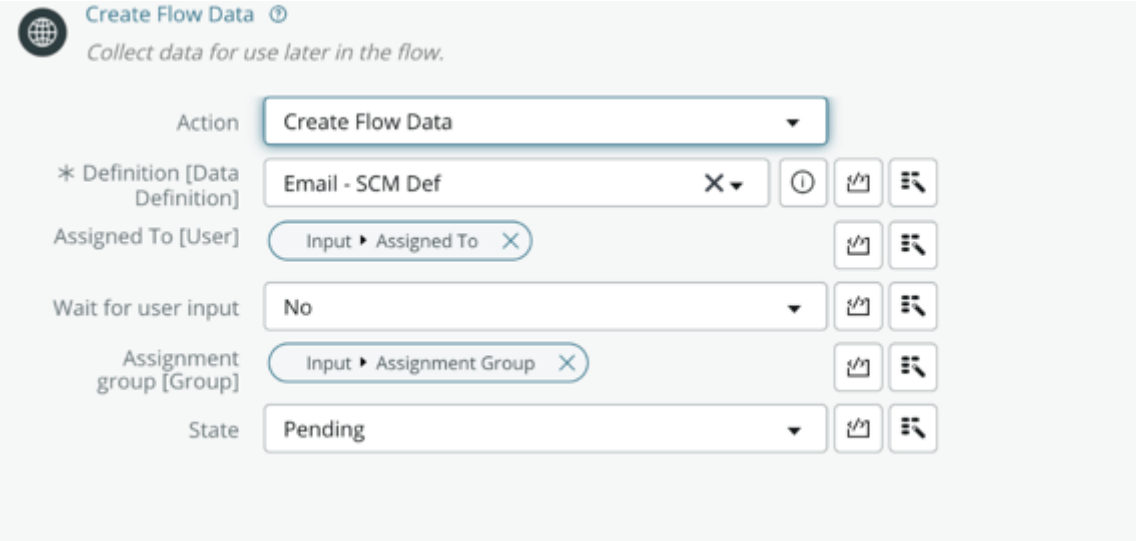
3. Neste exemplo, abra o subfluxo: **Enviar e-mail - Atividade ESCM** . Em **Criar dados de fluxo** etapa, a definição de dados de fluxo que você criou é mapeada em relação a. **Definição**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campo. Este registro de dados de fluxo é usado no subfluxo. Neste exemplo, o status do cartão de atividades (status da experiência) é capturado na tabela de dados de fluxo.

Enviar e-mail - Atividade ESCM



Nota: Se você quiser capturar os dados de tempo de execução em um registro de tabela diferente da tabela de dados de fluxo, digamos, por exemplo, em uma tarefa de resposta. Você pode selecionar a tabela associada como Tabela de tarefas de resposta. O registro associado deve ser definido como o registro de tarefa de resposta criado pelo subfluxo.

Da mesma forma, a tabela de status da experiência captura o status do cartão de atividades. No sistema de base, o campo estado da tabela de dados de fluxo é mapeado para o status do cartão de atividades. Portanto, quando a tabela de dados de fluxo é usada para capturar o status da experiência, ela atualiza automaticamente o status do cartão de atividades. Você também pode usar uma tabela diferente da tabela de dados de fluxo para capturar o status da experiência.

Por exemplo, se você quiser mapear o status da tarefa de resposta para o status do cartão de atividades, isso será possível. Para fazer isso:

1. Navegar até **Tudo** > **Playbook Experiences**.

Playbook Experiences

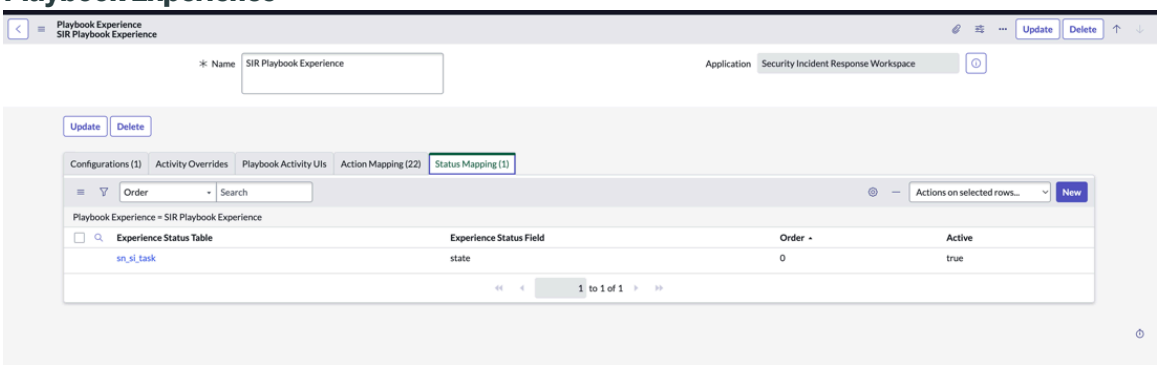


2. Aberto **SIR Playbook Experience** .
3. Aberto **Mapeamento de status** lista relacionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook Experience



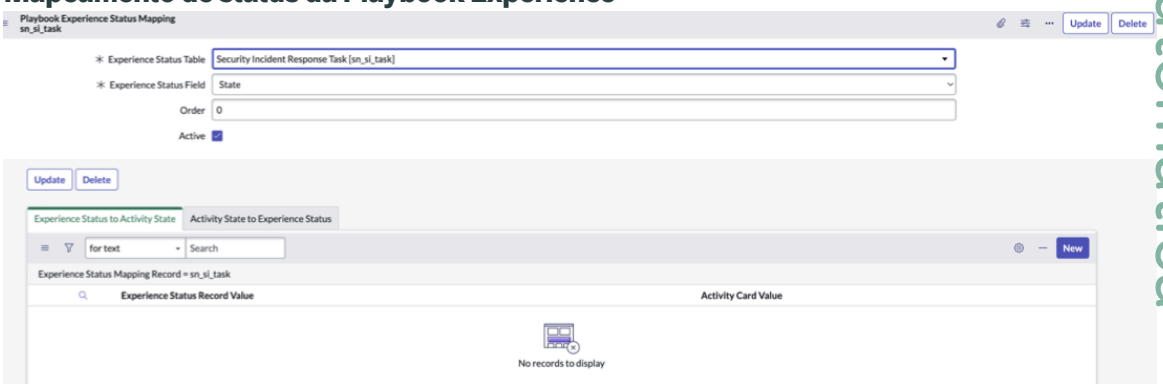
4. Insira **Tarefa de resposta** Em relação ao campo Tabela de status da experiência.
5. Insira **Estado** No campo Status da experiência.

Status da experiência



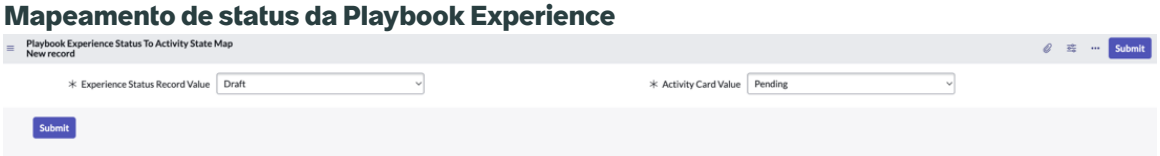
6. Clique em **Enviar**. O registro é criado.

Mapeamento de status da Playbook Experience



7. Em Status da experiência para Estado da atividade, mapeie os estados da tarefa de resposta para o status do cartão de atividade.
8. O lado esquerdo mostra os estados da tarefa de resposta e o lado direito mostra o status do cartão de atividades.

Mapeamento de status da Playbook Experience



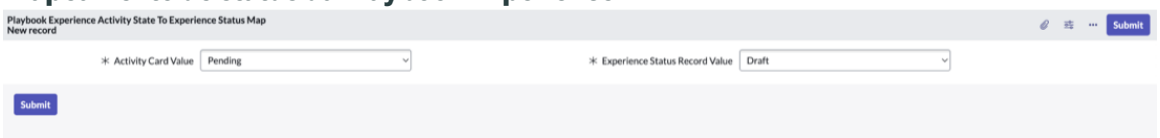
9. O mapeamento pode ser bidirecional. Na lista relacionada Estado de atividade para experiência, mapeie os status corretamente. Esta etapa é o inverso da etapa anterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nesse caso, o lado esquerdo mostra o status do cartão de atividades e o lado direito mostra o status da tarefa de resposta.

Mapeamento de status da Playbook Experience



Detalhes

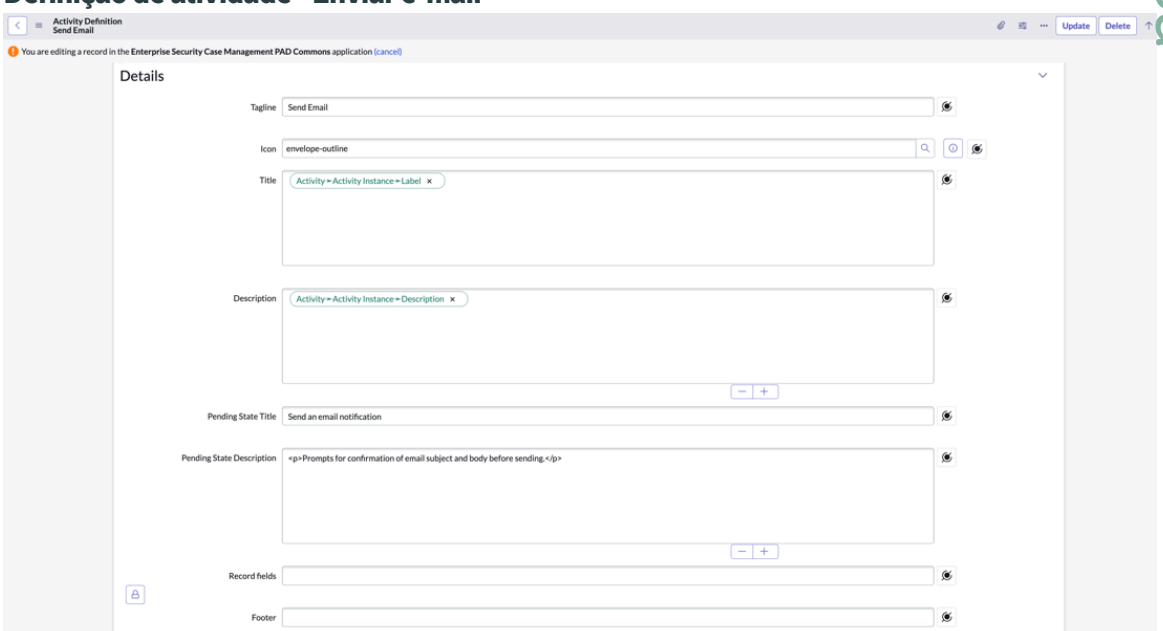
- Marcador: Enviar e-mail
- Ícone: Contorno do envelope (não mostrado na interface do usuário)
- Título: **Atividade** > **Instância de atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente no tempo de execução.
- Descrição: **Atividade** > **Instância de atividade** > **Descrição**. Aqui, selecionamos a descrição da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente no tempo de execução.
- Estado pendente: Envie uma notificação por e-mail. Este é o título quando a atividade está no status Pendente.
- Descrição do estado pendente: Solicita a confirmação do assunto e do corpo do e-mail antes de enviar. Esta é a descrição do cartão de atividade quando o status é campos de registro pendentes: Há campos de registro selecionados neste exemplo.

  Campos de registro são uma lista separada por vírgulas de nomes de campos a serem exibidos para o registro associado em uma lista de pares nome-valor. Os dados são obtidos previamente no servidor, a referência com pontos é compatível com e. **CanRead()** #as permissões são avaliadas em cada campo.

- Rodapé: Não há rodapé definido para este exemplo.

  Rodapé é um texto em uma área cinza do rodapé do cartão. Você pode adicionar qualquer informação significativa à mostrada.

Definição de atividade - Enviar e-mail



Tradução automática

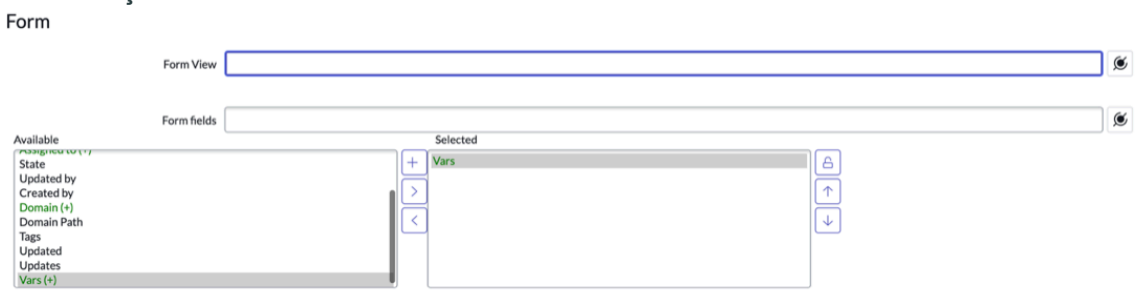
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário

- Exibição do formulário: Collect_data
- Campos de formulário:

Este exemplo usa a exibição collect_data para mostrar os campos que devem ser apresentados ao usuário para inserir entradas. A exibição collect_data é uma exibição fornecida pela plataforma correspondente à tabela de dados de fluxo. Como alternativa, você pode deixar a Exibição de formulário como vazia e selecionar Variáveis na lista de valores disponíveis em Campos de formulário. (clique no ícone de cadeado para abrir a lista de valores disponíveis).

Visualização do formulário



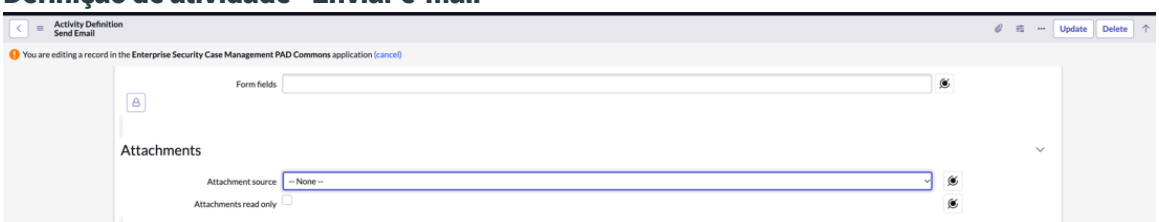
Anexos

Neste exemplo:

- A origem do anexo está vazia.
- Anexo Somente leitura não selecionado.

1. Origem do anexo - menu suspenso. Que anexos mostrar no cartão: Aqueles anexados ao registro primário, ao registro associado ou a nenhum.
2. Anexo somente leitura - Verdadeiro ou Falso. Impedir que o usuário renomeie ou exclua os anexos existentes.

Definição de atividade - Enviar e-mail



Recursos

Neste exemplo,

- Mostrar ANS - Desmarcado
- Mostrar check-list - Desmarcado
- Automatizado - Desmarcado

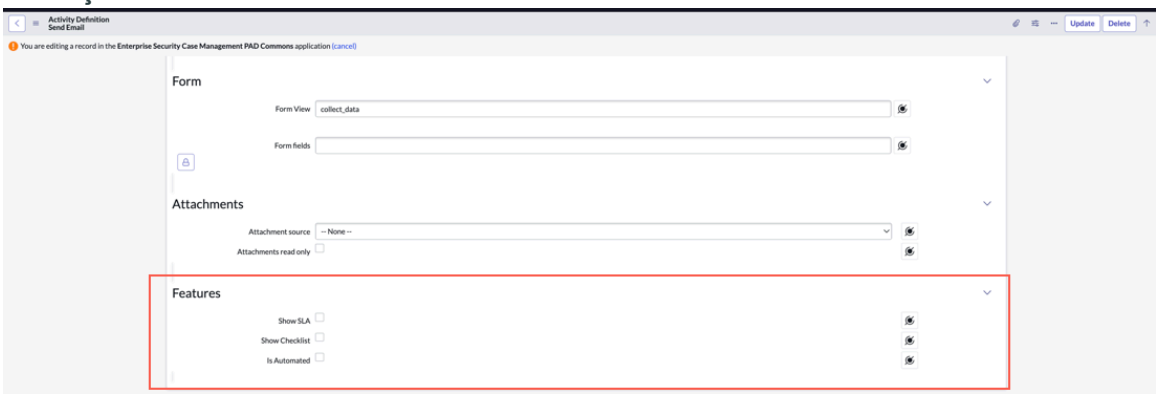
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mostrar ANS: Verdadeiro/Falso. Renderiza um temporizador de ANS no cabeçalho do cartão para o registro associado. O ANS é escolhido de acordo com o registro de Configuração de ANS especificado na configuração do Playbook.

1. Mostrar check-list#- Verdadeiro ou Falso. Renderiza qualquer check-list anexada ao registro associado. A check-list é editável e as mudanças são salvas sem exigir uma ação declarativa.
2. É automatizado - Verdadeiro ou Falso. Se verdadeiro, então **slogan** #e. **ícone** #será substituído pelo texto **Tarefa automatizada** e um ícone automatizado.

Definição de atividade - Formulário Enviar e-mail

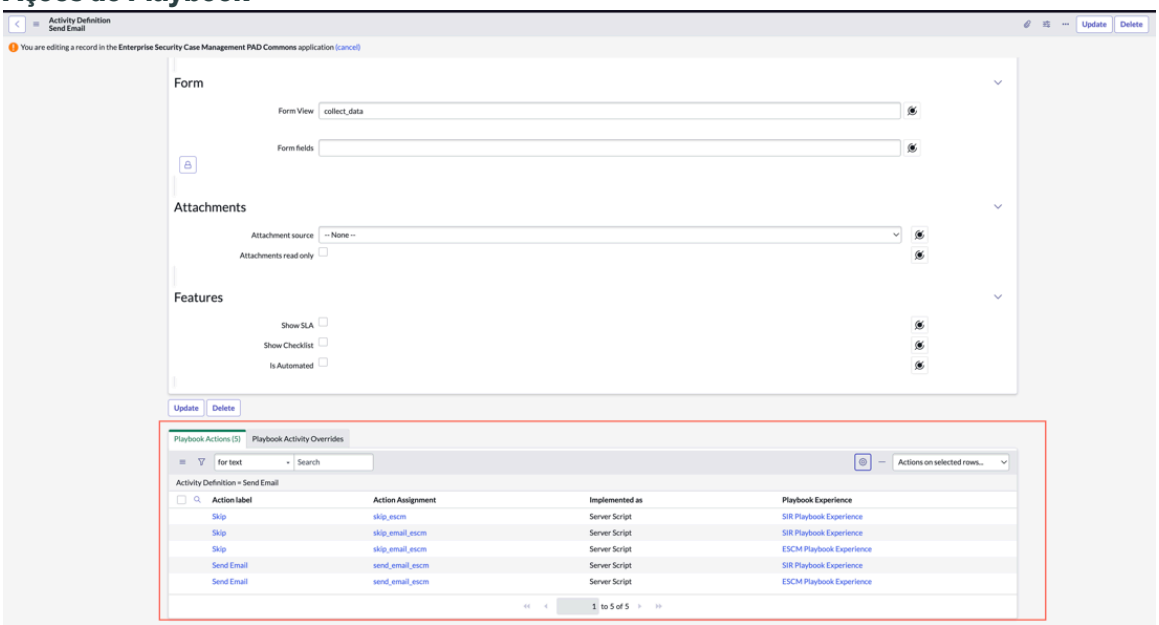


Ações do Playbook na Definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade. Este exemplo tem **Ignorar** e **Enviar e-mail** como ações.

Para adicionar uma nova ação ao cartão de atividade, você deve criar um registro no **Ações do Playbook** lista relacionada presente na parte inferior da página.

Ações do Playbook



1. Clique em **Nova**.
2. Selecione a ação de atividade existente no campo Atribuição de ação.
3. Selecione **SIR Playbook Experience** No campo Playbook Experience.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

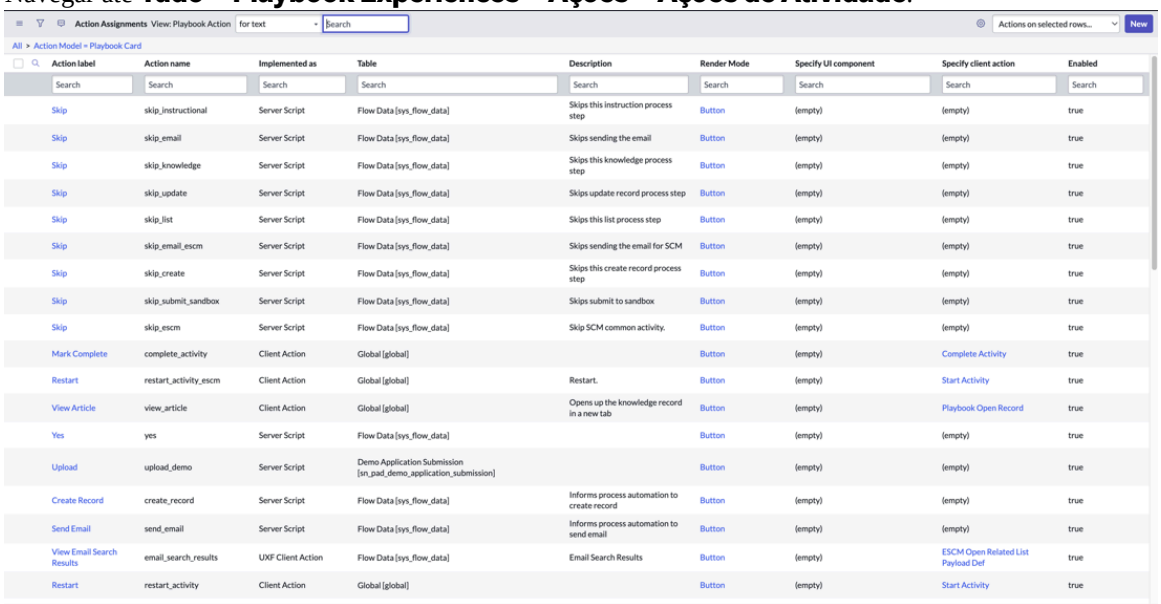
Criar uma Ação de Atividade

A seguir está o procedimento para criar uma ação de atividade.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Playbook Experiences** > **Ações** > **Ações de Atividade**.



2. Clique em **Nova**.

   Consulte ServiceNow AI Platform documentação para saber como criar essas ações. Neste exemplo, Ignorar é implementado como um script de servidor.

3. **Substituição do Playbook:**

   Se você quiser substituir o tipo de experiência de atividade existente, isso será possível. Para obter mais informações, consulte ServiceNow AI Platform documentação. Não há substituições do Playbook para este exemplo.

Enviar para área restrita FCS X

Enviar para a área restrita CSF X é um exemplo de um processo de definição de atividade.

Básico

Os detalhes básicos capturam o nome (rótulo), a aplicação, a descrição, a tabela e a partir da qual todas as aplicações podem ser acessadas.

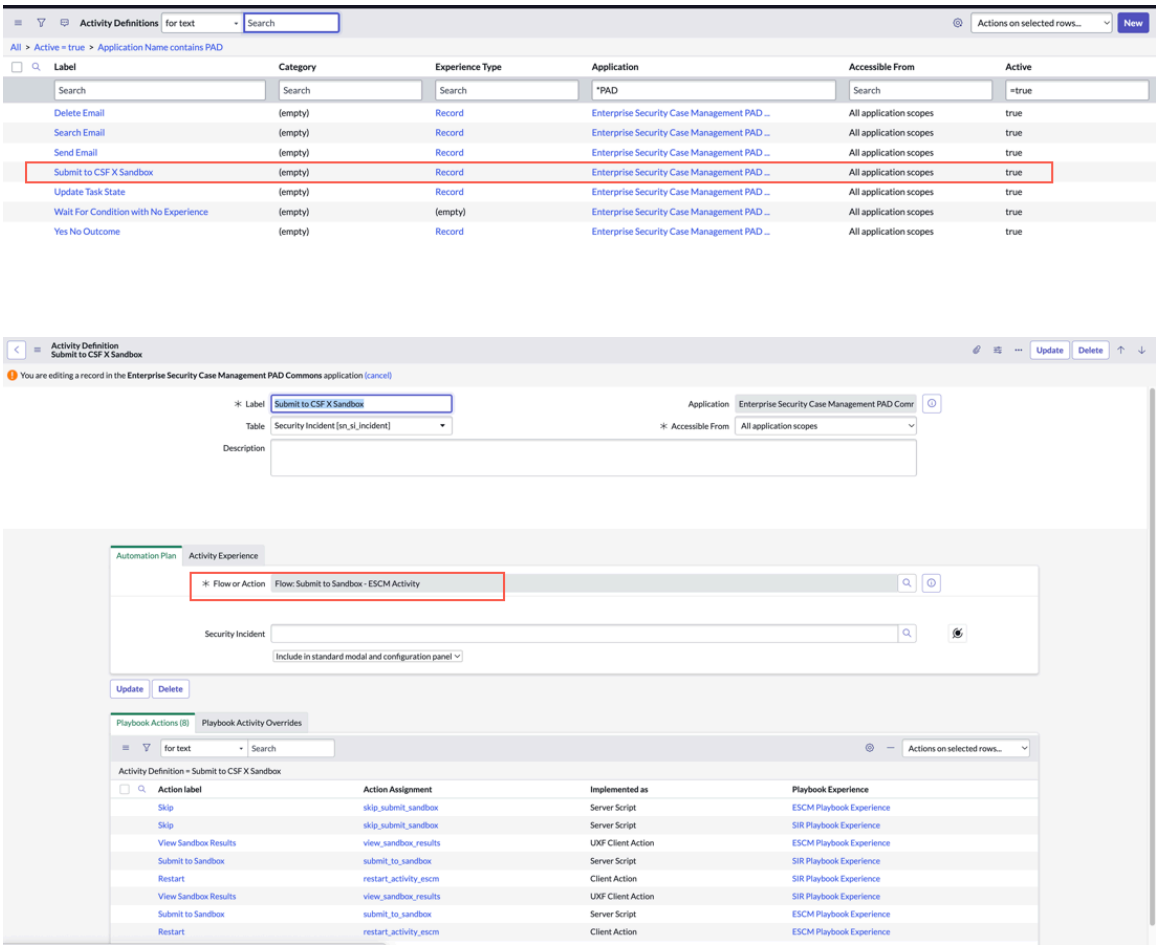
Adicione o plano de automação, a experiência de atividade e o envio. Depois de enviado, edite o documento para adicionar mais detalhes em cada guia.

Plano de Automação

O Plano de automação associa a ação/subfluxo de back-end criado usando o designer de fluxo. Este exemplo usa **Enviar para área restrita - Atividade ESCM** subfluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este subfluxo permite o envio de observáveis mal-intencionados para a área restrita. Todos os campos de entrada e de saída estão definidos.

Incidente de segurança é o campo de entrada.

Experiência de Atividade

Neste exemplo, **Registro** o tipo está selecionado.

Registro Associado

O registro associado armazena os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: Dados de fluxo
- Registro associado: VI
- Tabela de status da experiência: Dados de fluxo
- Registro de status da experiência: VI

Detalhes

- Marcador: Enviar e-mail
- Ícone: Contorno do envelope
- Título: **Atividade** > **Instância de atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente no tempo de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Descrição: VI (a saída de subfluxo é mapeada)
- Estado pendente: Em branco
- Descrição do estado pendente: Em branco
- Campos do Registro
- Rodapé

Formulário

- Exibição do formulário: Em branco
- Campos de formulário: Em branco

Anexos

Neste exemplo:

- Origem do anexo - Nenhuma
- Anexo somente leitura - Desmarcado

1. Origem do anexo - Este é um menu suspenso. Que anexos mostrar no cartão: Aqueles anexados ao registro primário, ao registro associado ou a nenhum.
2. Anexo somente leitura - Este é verdadeiro/falso. Impedir que o usuário renomeie ou exclua os anexos existentes.

Recursos

Neste exemplo,

- Mostrar ANS - Desmarcado
- Mostrar check-list - Desmarcado
- Automatizado - Desmarcado

Ações do Playbook na Definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade.

Este exemplo tem Ações Ignorar, Exibir resultados da área restrita, Enviar para área restrita e Reiniciar.

Para adicionar uma nova ação ao cartão de atividade, você precisa criar um novo registro na lista relacionada Ações do Playbook presente na parte inferior da página.

Substituição do Playbook

Não há substituições do Playbook para este exemplo.

Playbooks de amostra para o SIR Workspace

Você pode criar ou configurar playbooks para o SIR Workspace de forma rápida e fácil sem escrever código complicado. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo. Você pode invocar o fluxo do playbook de incidentes de segurança automaticamente ou manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Resposta do incidente de segurança fornece os seguintes playbooks com o sistema de base:

- Playbook para phishing manual
- Playbook para phishing automatizado
- Playbook para malware manual
- Playbook para malware automatizado
- Playbook para falha de login manual

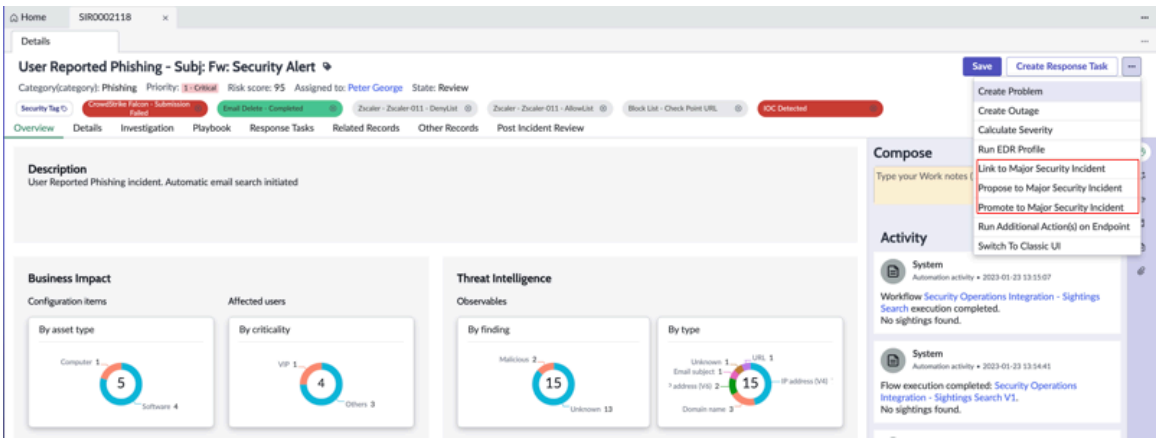
Trabalhar com registros MSI

Usando o espaço Resposta a incidentes de segurança, você pode propor, promover ou vincular incidentes de segurança como incidentes de segurança graves quando os incidentes são identificados como ameaça crítica para a organização.

Depois de instalar Gestão de incidentes graves de segurança(MSIM) no seu ServiceNow AI Platform, você pode lidar com a transição de incidentes de segurança para incidentes graves.

. Gestão de incidentes graves de segurança(MSIM) As ações de IU são exibidas no canto superior direito da faixa do formulário de incidente de segurança do espaço SIR. Selecione a ação de IU conforme aplicável.

Nota: Algumas ações são contextuais. Por exemplo, a ação Desvincular está disponível somente quando o incidente de segurança já está proposto, promovido ou vinculado a um incidente de segurança grave.



Propor como incidente de segurança grave

Propor um incidente de segurança como um incidente de segurança grave (MSI).

Antes de Iniciar

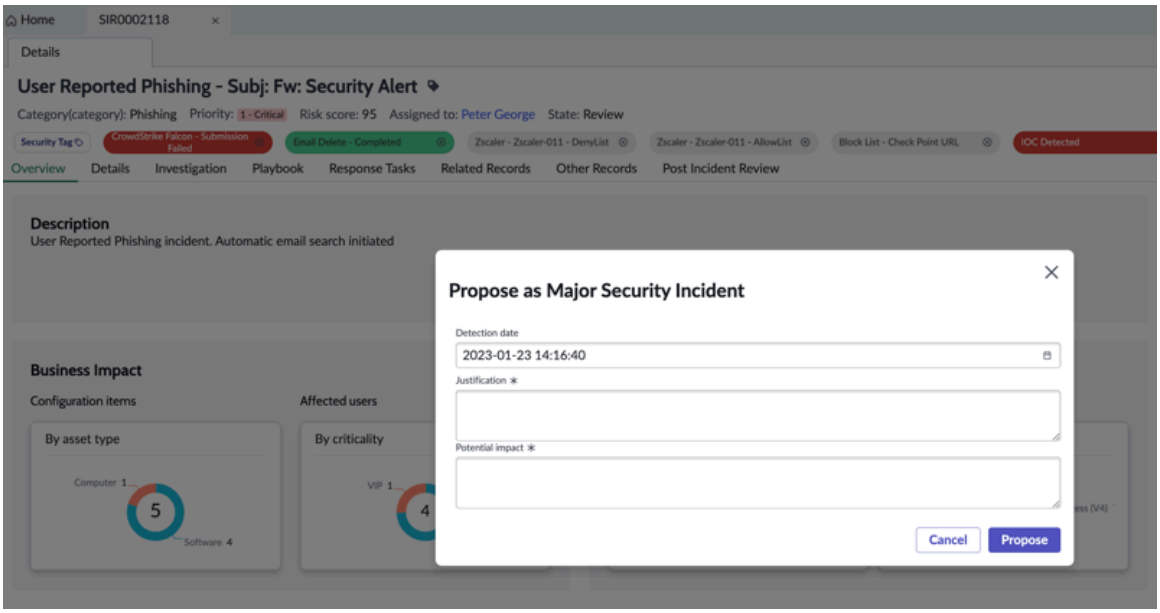
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique em **Propor incidente de segurança grave** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos como Data de detecção, Justificação e Impacto potencial.
5. Clique em **Propor** .
   O registro de incidente é proposto como candidato a incidente de segurança grave.
   Depois que o registro de incidente é proposto como candidato a incidente de segurança grave, **Candidato a incidente de segurança grave** o marcador é aplicado e exibido na faixa do formulário de incidente de segurança.

> **Nota:** Clique em **Desvincular do incidente de segurança grave** para desvincular o incidente se você não quiser propor ou não tiver nenhum impacto crítico. O incidente será desvinculado e será listado na exibição de lista para o analista de segurança para correção.

Promover a incidente de segurança grave

Promova um incidente de segurança a incidente de segurança grave.

Antes de Iniciar

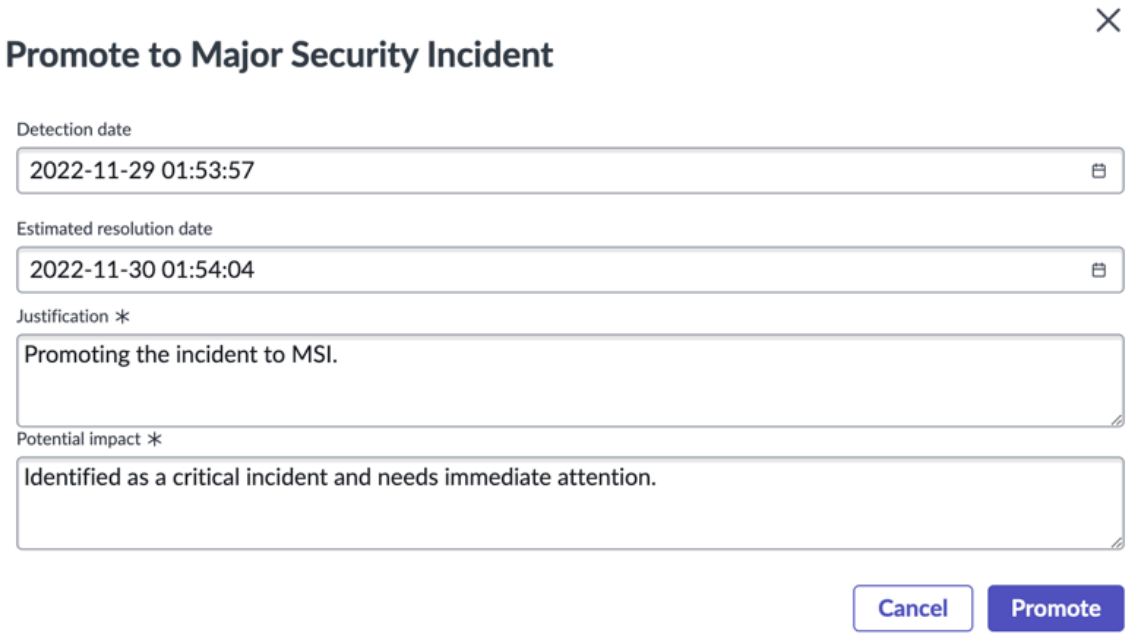
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique em **Promover a incidente de segurança grave** .
4. No formulário, preencha os campos como Data de detecção, Data de resolução estimada, Justificação e Impacto potencial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Promover** .
   O registro de incidente é promovido como um incidente de segurança grave.
   Depois que o registro de incidente é promovido como um incidente de segurança grave, **Incidente de segurança grave** o marcador é aplicado e exibido na faixa do formulário.

> **Nota:** Você também pode desvincular o incidente de segurança grave se o incidente não for crítico, o incidente será desvinculado e listado na exibição de lista para a correção do analista de segurança.

Link para o incidente de segurança grave

Vincular um incidente de segurança a um incidente de segurança grave como incidente(s) de segurança secundário(s).

Antes de Iniciar

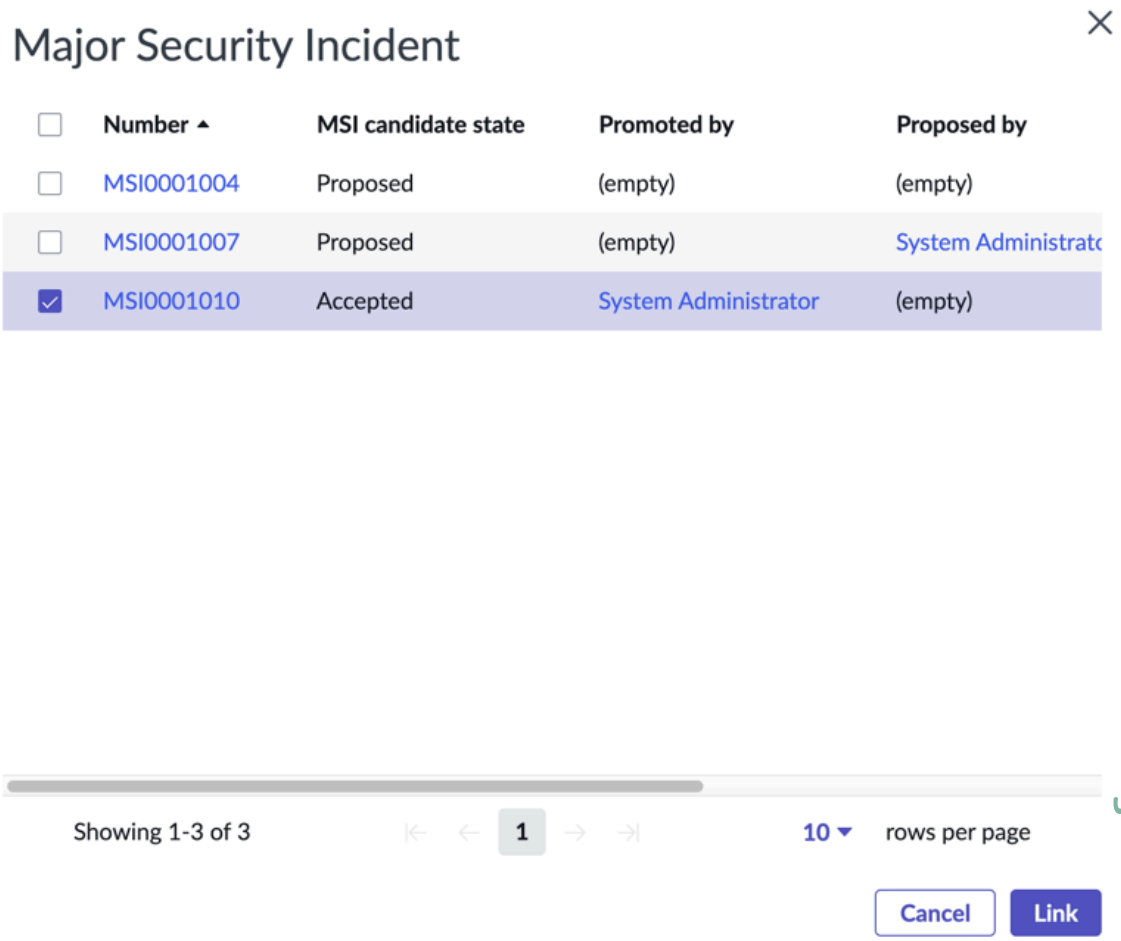
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique em **Link para Incidente de segurança grave** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

4. Selecione o(s) incidente(s) a ser vinculado(s) a um incidente de segurança grave.
5. Clique em **Vincular**.
6. O registro do incidente está vinculado como um incidente secundário do incidente de segurança grave. Depois que o incidente é vinculado como um incidente secundário a um incidente de segurança grave, **Incidente de segurança grave** o marcador é aplicado e exibido na faixa do formulário.

Trabalhar com ações de IU de formulário

A seguir estão as ações de IU exibidas no formulário de incidente de segurança.

Para navegar até as Ações de IU do formulário:

1. Ir para **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione qualquer incidente de segurança na exibição de lista.
3. Todas as ações de IU estão presentes no canto superior direito do formulário de incidente de segurança.

Ações de IU do formulário do espaço

Nome do Campo	Descrição
Discutir	Crie ou inicie uma discussão na barra lateral para o incidente de segurança.
Salvar	Salve ou atualize o registro de Resposta do incidente de segurança depois de fazer mudanças.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

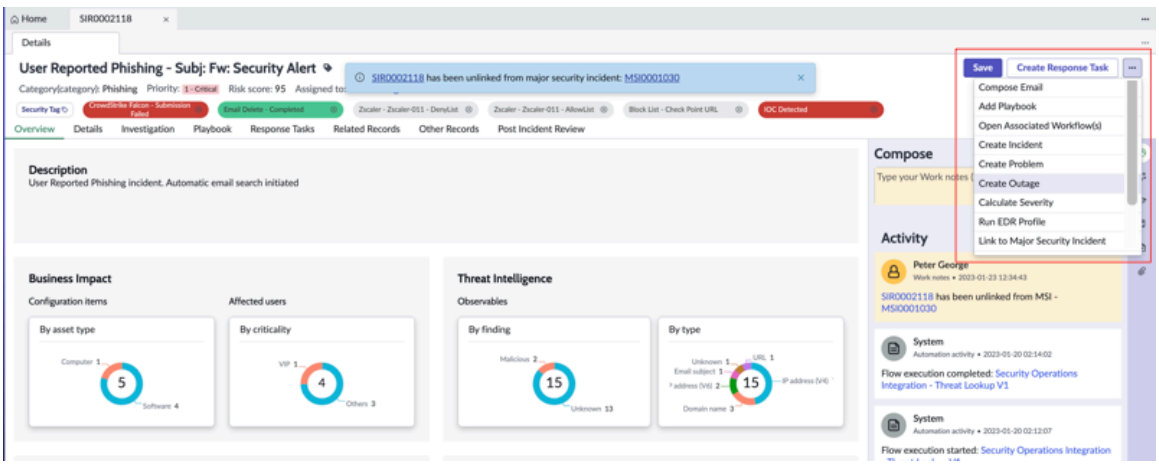
Nome do Campo	Descrição
Criar Tarefa de Resposta	Crie uma tarefa de resposta para o incidente de segurança.
Compor e-mails	Redigir e-mails para o incidente de segurança.
Adicionar Playbook	Adicione o playbook manualmente para o incidente de segurança.
Criar Incidente	Crie um incidente no incidente de segurança.
Criar caso de Atendimento ao cliente	Crie um caso de atendimento ao cliente para o incidente de segurança que será rastreado pela equipe de Gestão de atendimento ao cliente (CSM). **Nota:** Esta opção está disponível somente quando o Customer Service Management (CSM) está instalado.
Abrir fluxo(s) de trabalho associado(s)	Abra qualquer contexto de fluxo de trabalho associado ao incidente de segurança. Esta opção ficará visível somente se houver fluxos de trabalho.
Criar solicitação de mudança	Crie uma solicitação de mudança no incidente de segurança.
Criar Problema	Crie um problema no incidente de segurança.
Criar indisponibilidade	Crie uma indisponibilidade no incidente de segurança.
Calcular Gravidade	Calcule a gravidade de um incidente de segurança usando calculadoras predefinidas. A gravidade é calculada com base nas regras predefinidas nas calculadoras. A gravidade de um incidente é baseada na pontuação de risco, no impacto nos negócios e na prioridade.
Executar perfil de EDR	Selecione e execute o Perfil EDR para a integração necessária. **Nota:** Esta opção está disponível somente quando há integrações instaladas.
Link para o incidente de segurança grave	Vincular um incidente de segurança a um incidente de segurança grave.
Relatar evento de risco	Relate este incidente de segurança como um evento de risco à equipe de Gestão de riscos. A equipe de Gestão de riscos analisa o evento e garante que esses eventos e as perdas associadas não ocorram novamente. **Nota:** Esta opção está disponível somente quando a Gestão de riscos está instalada.
Desvincular de um incidente de segurança grave	Desvincular de incidente de segurança grave.
Propor como incidente de segurança grave	Propor um incidente de segurança como um incidente de segurança grave.
Promover a incidente de segurança grave	Promova um incidente de segurança como um incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Executar ações adicionais no endpoint	Execute ações adicionais no endpoint. **Nota:** Esta opção está disponível somente quando as integrações de endpoint estão instaladas. Por exemplo: FireEye HX
Criar um novo evento no MISP	Crie e modifique eventos no MISP automaticamente ou manualmente. **Nota:** Esta opção está disponível somente quando a integração MISP está instalada.
Associar técnica MITRE ATT&K.	Associe técnicas MITRE ATT&K ao incidente de segurança. **Nota:** Esta opção está disponível quando O MITRE ATT&K está instalado.
Mostrar informações do MITRE ATT&K.	Mostra as informações DO MITRE ATT&K associadas ao incidente de segurança. **Nota:** Esta opção está disponível quando O MITRE ATT&K está instalado.
Adicionar ao Caso de Segurança	Adicione o incidente de segurança a um caso de segurança existente ou novo. **Nota:** Esta opção está disponível quando Threat Intel está instalado.
Alternar para a IU Clássica	Permita que o analista alterne entre a IU clássica e nova para que ele também possa trabalhar nas funcionalidades existentes que ainda não estão disponíveis no novo espaço.
Cancelar	Cancelar um incidente de segurança. Depois de selecionar **Cancelar** todos os registros relacionados, como tarefas de resposta e incidentes de segurança secundários, também serão cancelados.
Excluir	Exclua um registro de incidente de segurança.

4. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Você pode ver as ações de IU na parte superior da página.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de fechamento de incidente de segurança

Feche o incidente de segurança atualizando o estado do incidente.

Antes de Iniciar

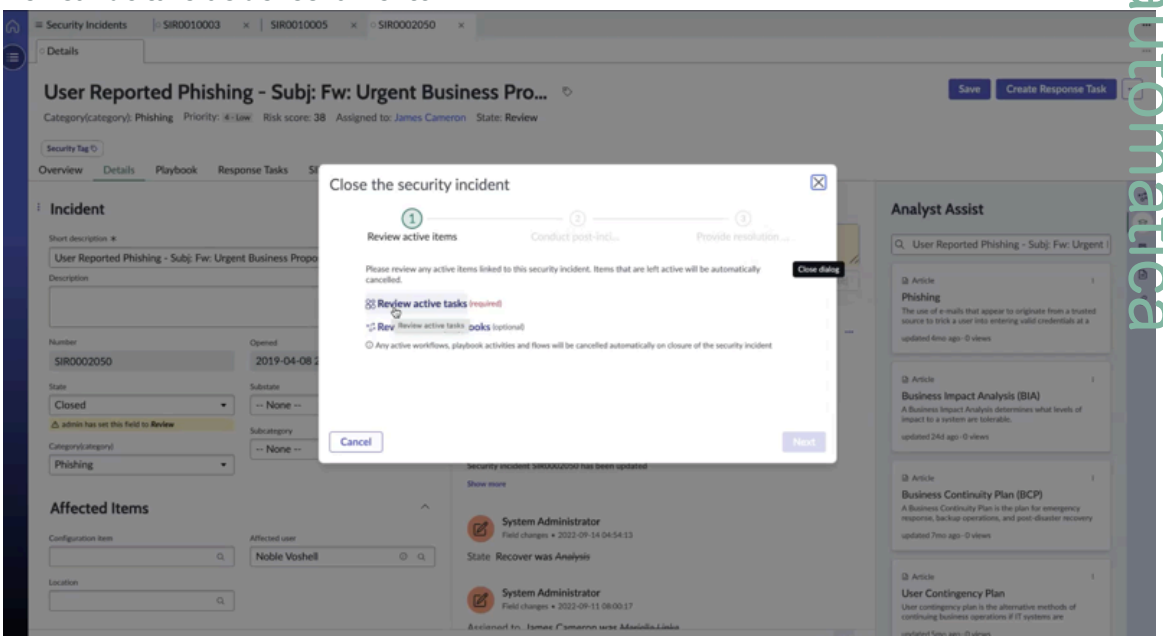
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Por exemplo, acesse **Listas** > **Incidentes de segurança** > **Incidentes em aberto**.
3. Abra um incidente que você deseja fechar.
4. Vá para **Detalhes** guia.
5. Detalhar o estado do incidente e selecionar **Fechar** .
6. Execute as atividades de fechamento.

   - Esta é uma etapa obrigatória para revisar qualquer tarefa antes de fechar um incidente de segurança. Todas as tarefas de resposta devem ser revisadas pelo analista e encerradas ou canceladas antes do fechamento como incidente de segurança. Quando o analista clica em **Revise tarefas ativas** , leva o usuário ao **Tarefas de resposta** guia. Uma mensagem de sessão é exibida solicitando que você está no processo de fechar um incidente de segurança. Clique em **continuar** .
   - Clique em **"Continuar"**. A primeira etapa - revisar as tarefas ativas no fechamento do incidente de segurança está concluída.

Revisando tarefas de fechamento



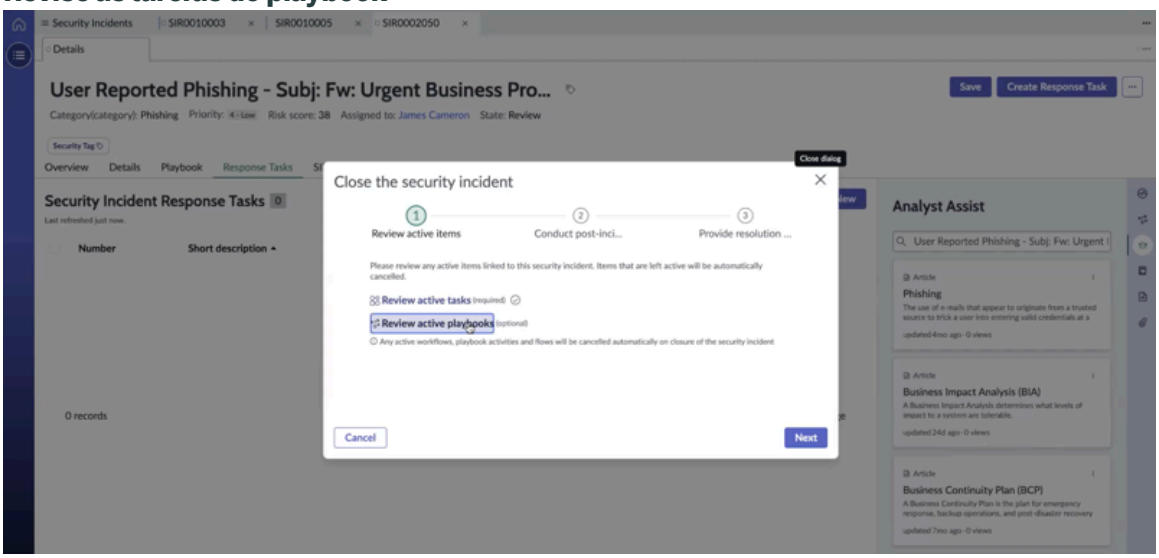
   - Passe para a próxima etapa para revisar os playbooks ativos para o analista revisar, que é uma etapa opcional. Você pode clicar no link para revisar a tarefa ativa do playbook e fechá-la conforme necessário.

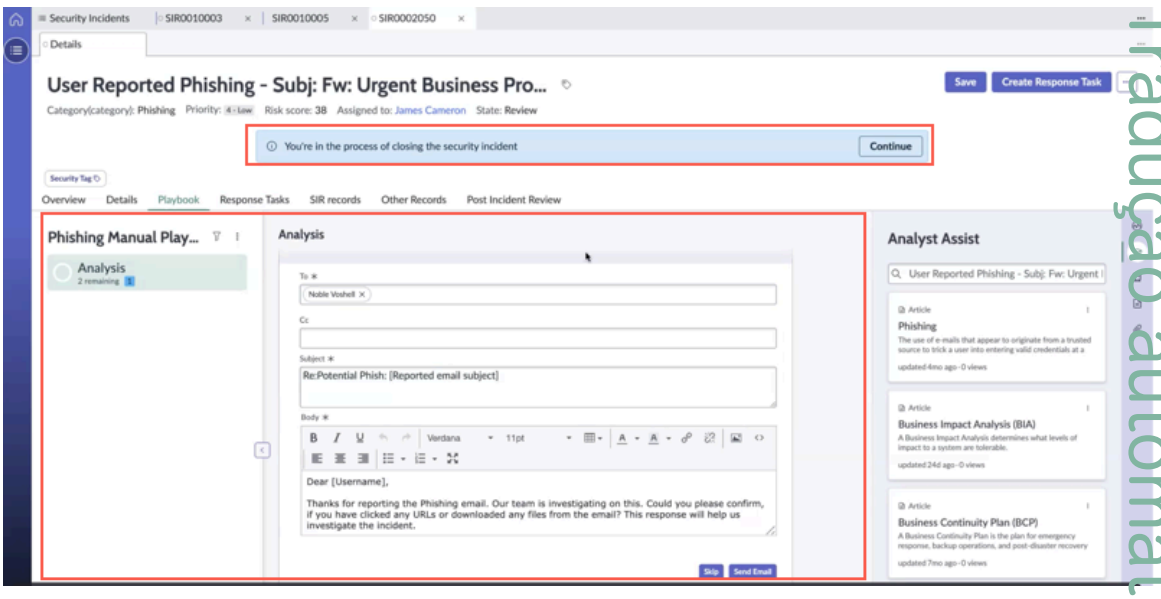
> **Nota:** Todos os fluxos de trabalho, atividades do playbook e fluxos ativos serão cancelados automaticamente no fechamento do incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revise as tarefas do playbook



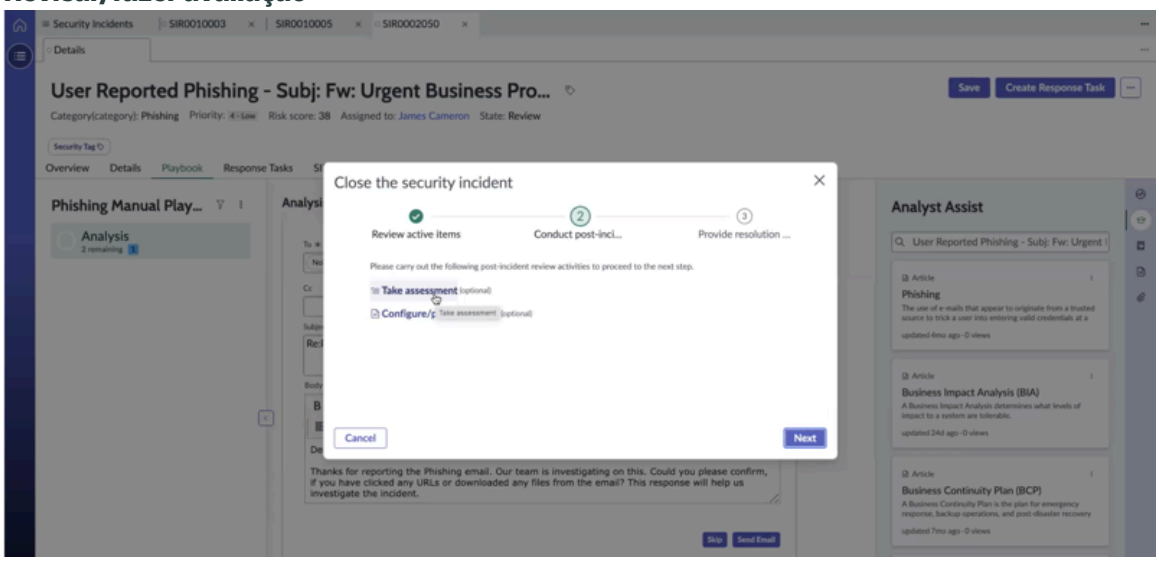


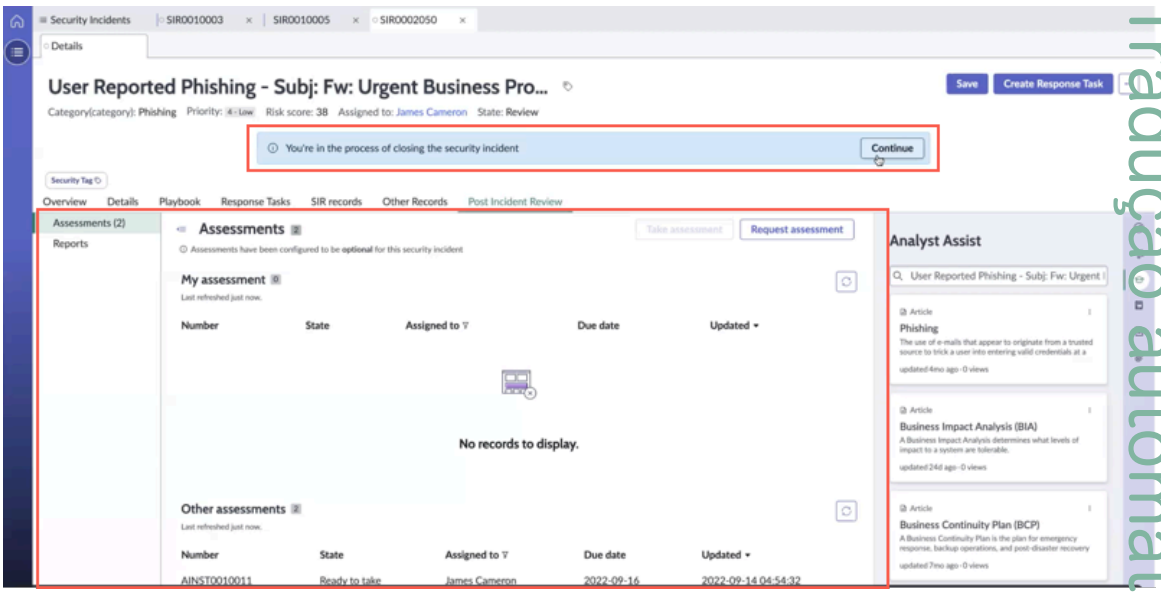
Tradução automática

- Relatório de revisão pós-incidente: Agora você será movido para revisar as atividades pós-incidente para prosseguir com o fechamento. Se a avaliação for opcional, ignore a etapa ou, se a avaliação for obrigatória, faça a avaliação e conclua-a.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revisar/fazer avaliação

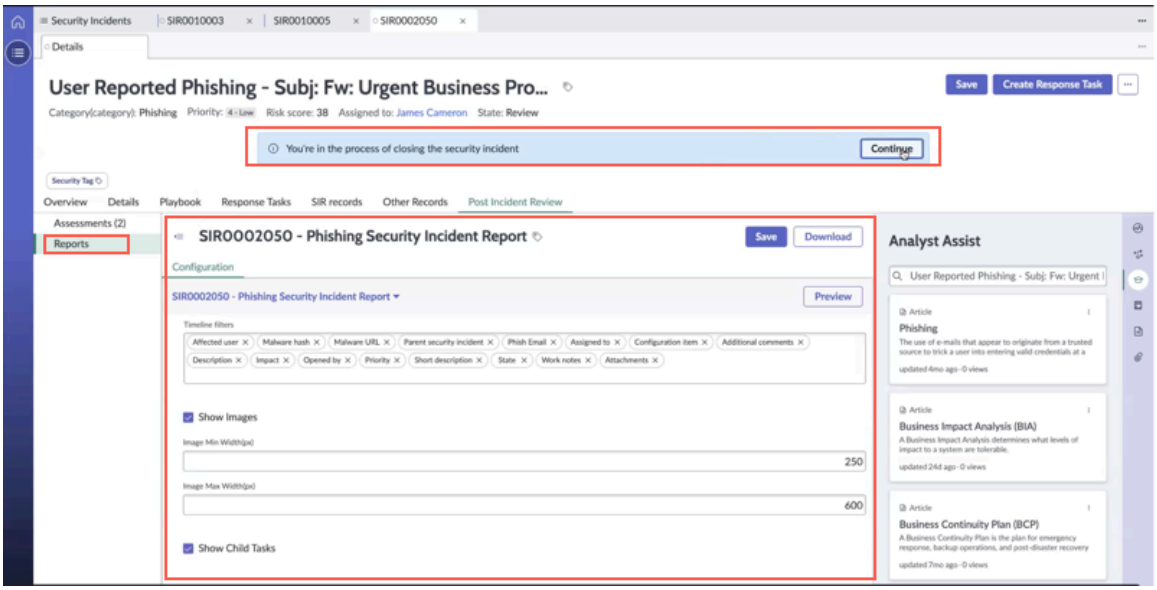




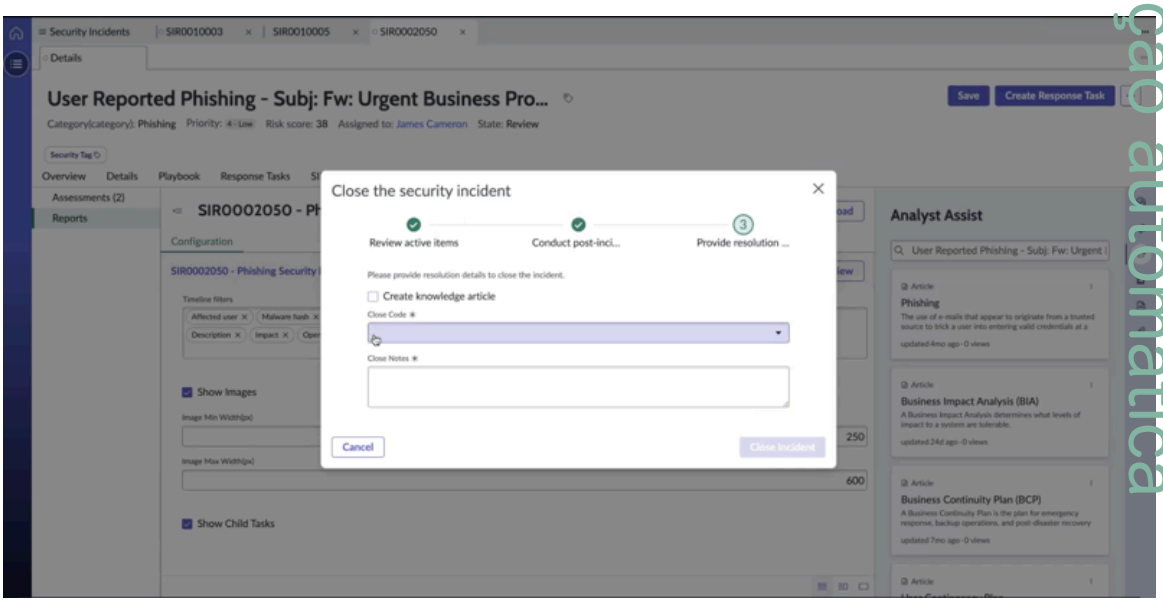
Tradução automática

- Configurar/visualizar relatório: Esta é novamente uma etapa opcional. Clique no link para revisar o relatório e prosseguir **Próximo** etapa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Fornecer detalhes da resolução: O analista pode marcar a caixa de seleção para criar artigos de conhecimento automaticamente.
- Forneça o código de fechamento, as anotações de fechamento e clique em **Fechar incidente** .



Nota: Se o analista cancelar **Feche o incidente de segurança** , em seguida, o analista pode navegar até **Detalhes** e mude o estado do incidente para **fechar** para continuar com o fechamento.

Exibição de painéis do Espaço SIR

Esta seção apresenta as métricas importantes para analisar seu Resposta a incidentes de segurança processo, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Na IU clássica, há alguns painéis padrão disponíveis na página inicial e. Performance Analytics Painéis que estão disponíveis quando Performance Analytics para Resposta a incidentes de segurança o plug-in está instalado. Agora, todos eles estarão disponíveis no novo espaço em **Painéis DO SIR** seção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis padrão na página inicial :

- Visão geral da resposta do incidente de segurança
  - Visão geral do analista
  - Visão geral do gerente (compatível com versões futuras)
  - Visão geral do CISO (compatível com versões futuras)
- **Análise da plataforma para** *`Resposta a incidentes de segurança`*
  - Explorador de incidentes de segurança
  - Painel do CISO (versão futura)
  - Gestão de incidentes de segurança
  - KPIs de Gestão de incidentes de segurança premium
  - Eficiência das operações de segurança
  - Análise sensível ao contexto – Painel de SI

Nota: Pode haver alguma repetição de painéis em análise padrão e de plataforma para painéis de resposta a incidentes de segurança, como o Painel do CISO. Quando o plug-in for instalado, haverá conteúdo adicional nesses painéis e não estará disponível como duplicado.

Os usuários precisam instalar o plug-in para que os painéis listados em Análise da plataforma para painéis de resposta a incidentes de segurança estejam presentes no espaço. Caso contrário, somente os painéis padrão estarão disponíveis.

Na versão atual do Espaço SIR, os painéis a seguir estão disponíveis em **Painéis DO SIR** seção. Os outros painéis ausentes estarão disponíveis em versões posteriores.

Painéis de resposta a incidentes de segurança

Painel	Descrição
Painel padrão	
Visão Geral de Análise de Segurança	Com este painel, os analistas de segurança podem exibir incidentes de segurança resumidos com base no trabalho de prioridade crítica do analista, no trabalho de alta prioridade, nos incidentes de segurança atribuídos ao analista, nas tarefas atribuídas aos analistas e na contagem de incidentes.
Performance Analytics (PA) para painéis de resposta a incidentes de segurança	
Explorador de incidentes de segurança	Com este painel, os gerentes e analistas de segurança podem exibir incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que gerentes e analistas obtenham rapidamente informações sobre a frequência em que os ataques estão ocorrendo e quais serviços de negócios são afetados.
Gestão de incidentes de segurança	Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento de incidentes de segurança, desde a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis de resposta a incidentes de segurança

Painel	Descrição
	análise/detecção inicial até a contenção, erradicação e recuperação.
Painel do CISO	Proposto para oferecer suporte na versão futura.
Eficiência das operações de segurança	Com este painel, gerentes e analistas podem exibir métricas gerais de eficiência e medir o desempenho do SOC.
KPIs de Gestão de incidentes de segurança premium	Com este painel, os gerentes de segurança podem rastrear e exibir o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.
Análise sensível ao contexto - S	Com este painel, gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento dos incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e encerrados no mesmo dia e a porcentagem de incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Acessar Painéis de SIR e PA

. **Painéis DO SIR** ícone exibido no lado esquerdo da página inicial do espaço.

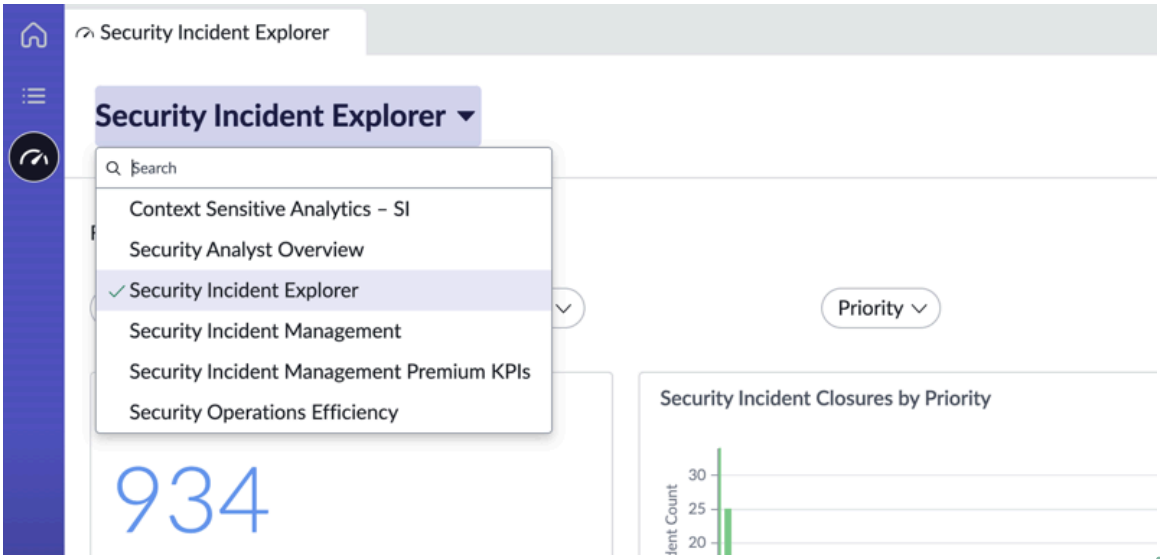
Nota: Usuários com acesso sn_si.manager ou sn_si.admin podem editar os painéis. Os usuários devem estar no mesmo escopo dos painéis em que o usuário está tentando fazer edições. Por exemplo, o painel de visão geral do analista de segurança está disponível no espaço SIR, então o usuário também deve estar no mesmo escopo do espaço SIR para fazer as edições no painel.

1. Navegar até **Espaços** > **Espaço de Gestão de incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione o Painel desejado na lista suspensa.



Você pode editar os painéis, adicionar novos elementos aos painéis e criar seus próprios painéis. Para obter mais informações sobre como usar painéis, consulte Trabalhar com painéis dinâmicos

Exiba o painel Visão geral do analista de segurança

Com este painel, os analistas de segurança podem exibir incidentes de segurança resumidos com base no trabalho de prioridade crítica dos analistas, no trabalho de alta prioridade, nos incidentes de segurança atribuídos ao analista, nas tarefas atribuídas aos analistas e na contagem de incidentes.

Antes de Iniciar

Por padrão, o painel Visão geral do analista de segurança é exibido para os usuários com acesso sn_si.analyst.

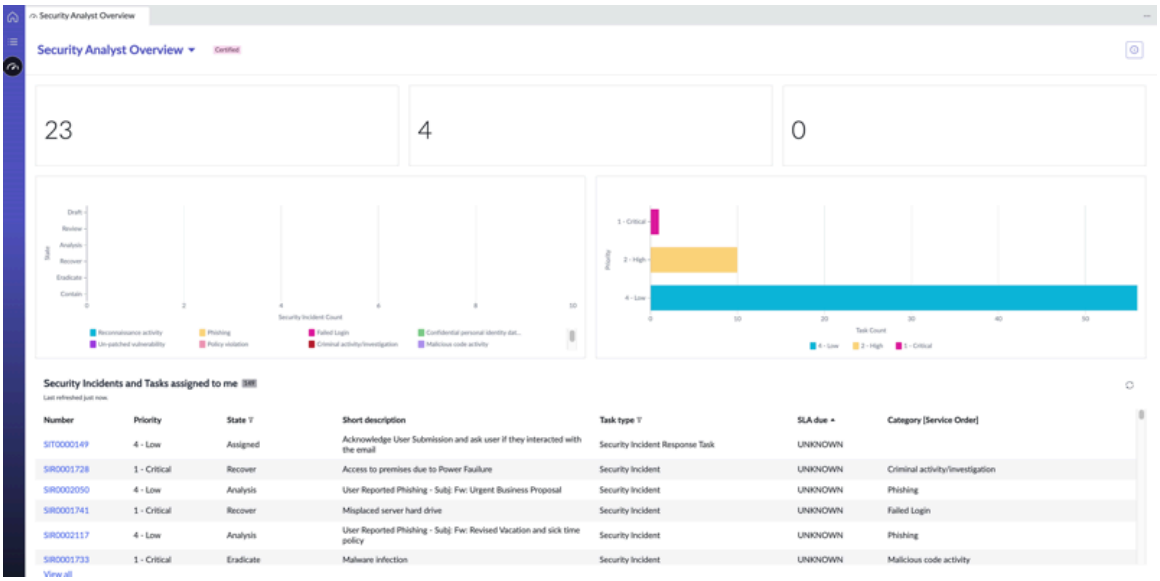
Função necessária: sn_si.analyst (Read), sn_si.manager ou sn_si.admin (Write)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do analista de segurança** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba o painel Visão geral do analista de segurança para obter mais ações. Para obter informações detalhadas sobre o painel Visão geral do analista de segurança, consulte Resposta a incidentes de segurança Soluções para Análise da plataforma e relatórios.

Exiba o painel do Security Incident Explorer

Com este painel, os gerentes de segurança podem exibir os incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios.

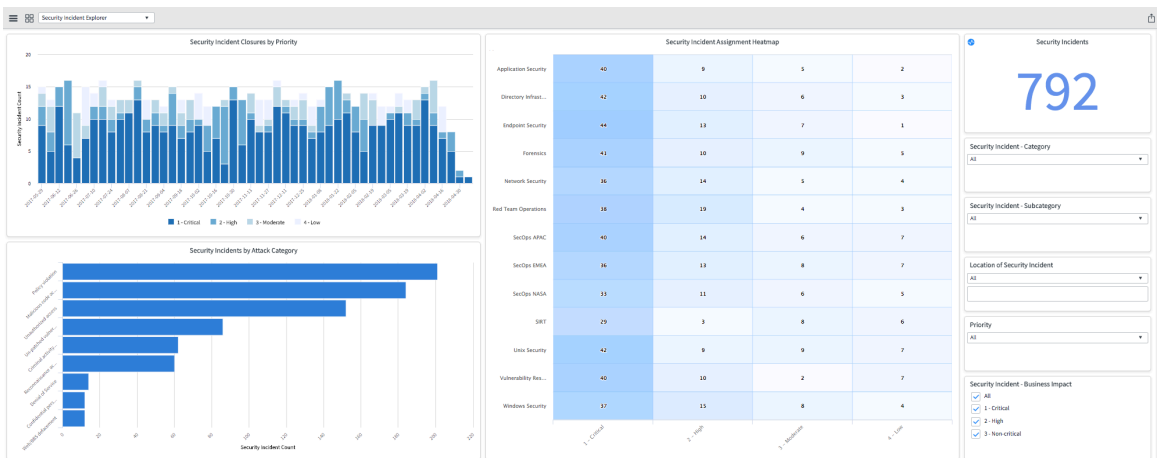
Antes de Iniciar

Por padrão, o painel do Security Incident Explorer é exibido para os usuários com acesso sn_si.manager.

Função necessária: sn_si.analyst (Read), sn_si.manager ou sn_si.admin (Write)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Explorador de incidentes de segurança** na lista suspensa.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exiba o painel do Security Incident Explorer para obter mais ações. Para obter informações detalhadas sobre o painel do Security Incident Explorer, consulte Painel do Security Incident Explorer

Na versão atual, a seguinte lista de relatórios não é compatível com o painel do Explorador de incidentes de segurança:

- Mapa térmico de atribuição de incidente de segurança - A visualização de mapa térmico não está disponível.
- Mapa de incidentes de segurança - A visualização de mapa não está disponível.

Exiba o painel da Gestão de incidentes de segurança

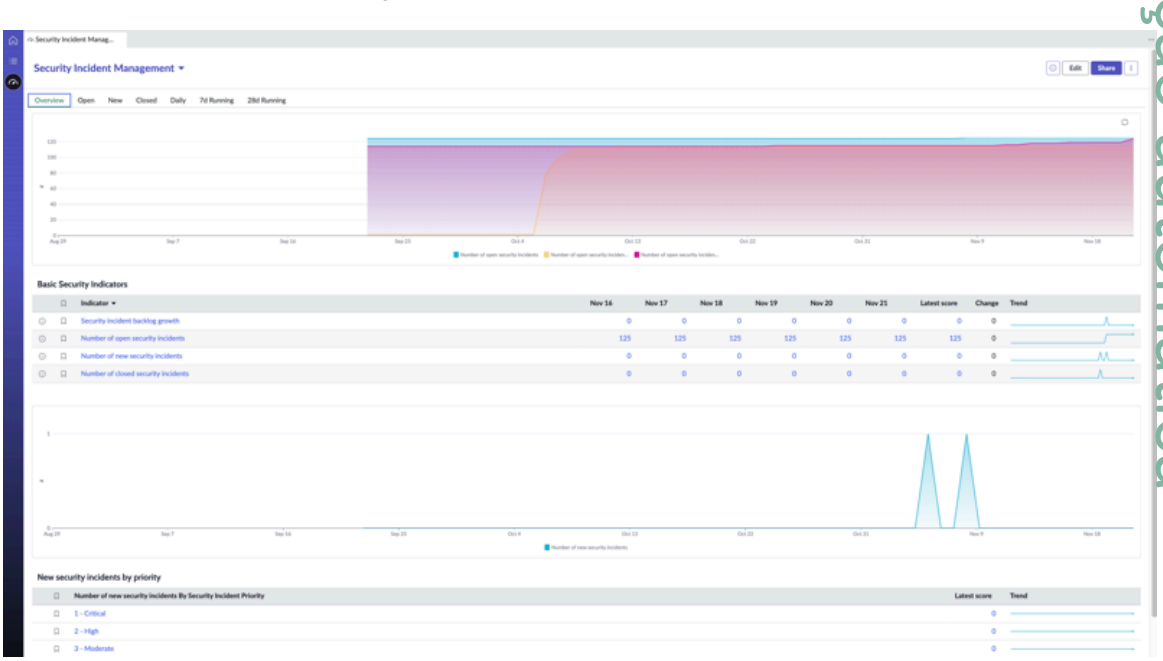
Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento de incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Gestão de incidentes de segurança** na lista suspensa.



Exiba o painel da Gestão de incidentes de segurança para obter mais ações. Para obter informações detalhadas sobre o painel Gestão de incidentes de segurança, consulte Painel da Gestão de incidentes de segurança

Exibir o painel Security Operations Efficiency

Os gerentes do Centro de operações de segurança (SOC) podem exibir métricas gerais de eficiência e medir o desempenho individual dos membros da equipe do SOC na organização.

Antes de Iniciar

Na versão atual, o relatório a seguir não é compatível com o painel Eficiência de operações de segurança:

Tradução automática

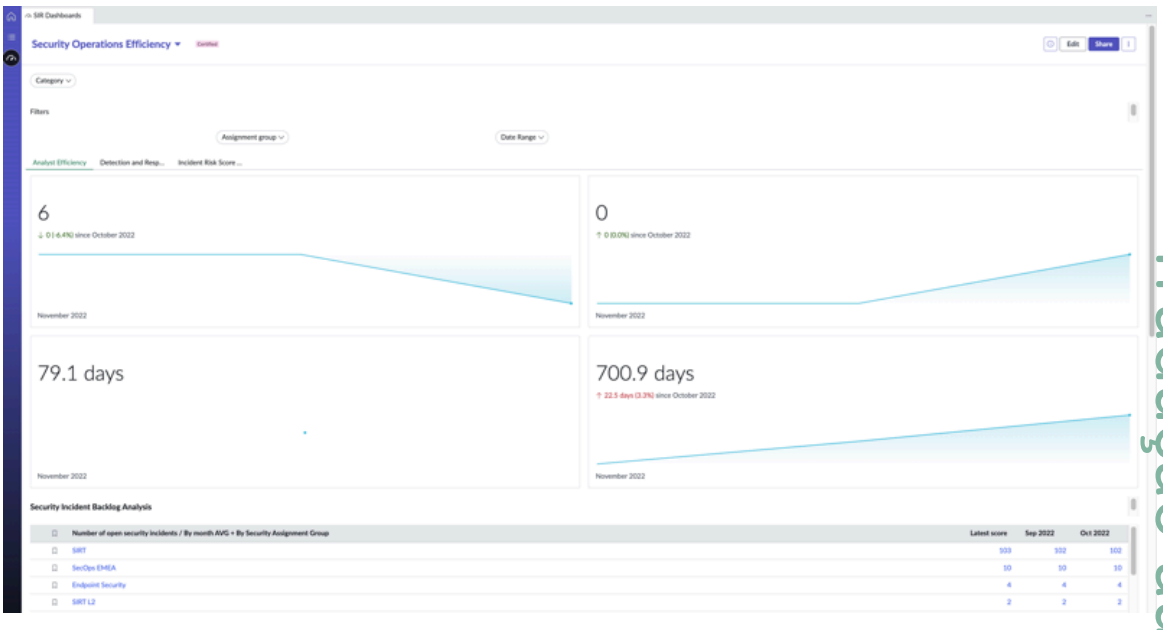
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A análise da fase do incidente de segurança - Workbench não está disponível

Função necessária: sn_si.analyst (Read), sn_si.manager ou sn_si.admin (write)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Eficiência das operações de segurança** na lista suspensa.



Exiba o painel Eficiência de operações de segurança para obter mais ações. Para obter informações detalhadas sobre o painel Eficiência de operações de segurança, consulte Painel de Eficiência de operações de segurança

Exiba o painel KPIs Premium de resposta a incidentes de segurança

Com este painel, os gerentes de segurança podem rastrear e exibir o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

Na versão atual, a lista de relatórios a seguir não é compatível com o painel KPIs Premium de Resposta a incidentes de segurança:

- Processo por estado - O Workbench não está disponível
- Processo por Idade - O Workbench não está disponível
- Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado - a visualização de mapa térmico não está disponível.
- Incidentes de segurança não atualizados por mais de 30 dias por grupo de atribuição e estado - A visualização de mapa térmico não está disponível.
- Incidentes de segurança com designado que não está ativo - a visualização de mapa térmico não está disponível.

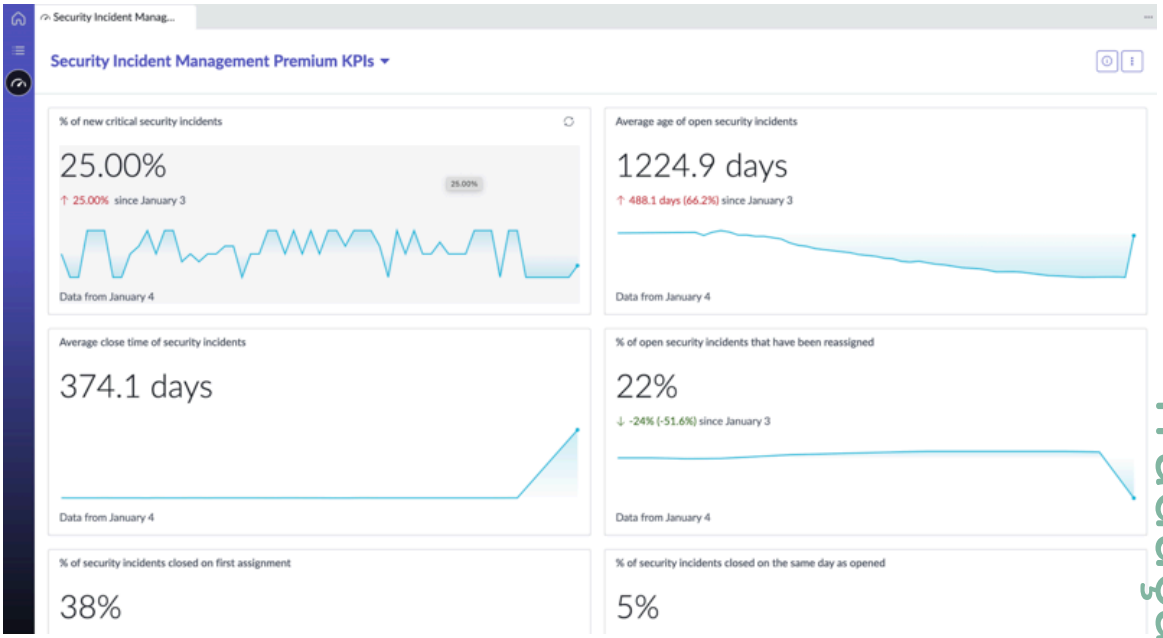
Função necessária: sn_si.analyst (Read), sn_si.manager ou sn_si.admin (write)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **KPIs Premium de Resposta a Incidentes de Segurança** na lista suspensa.



4. Exiba o painel KPIs Premium de resposta a incidentes de segurança para obter mais ações.
   Para obter informações detalhadas sobre o painel KPIs Premium de Resposta a incidentes de segurança, consulte Painel Premium da Gestão de incidentes de segurança

Exibir Análise sensível ao contexto - painel de SI

Com este painel, gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento dos incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e encerrados no mesmo dia e a porcentagem de incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Antes de Iniciar

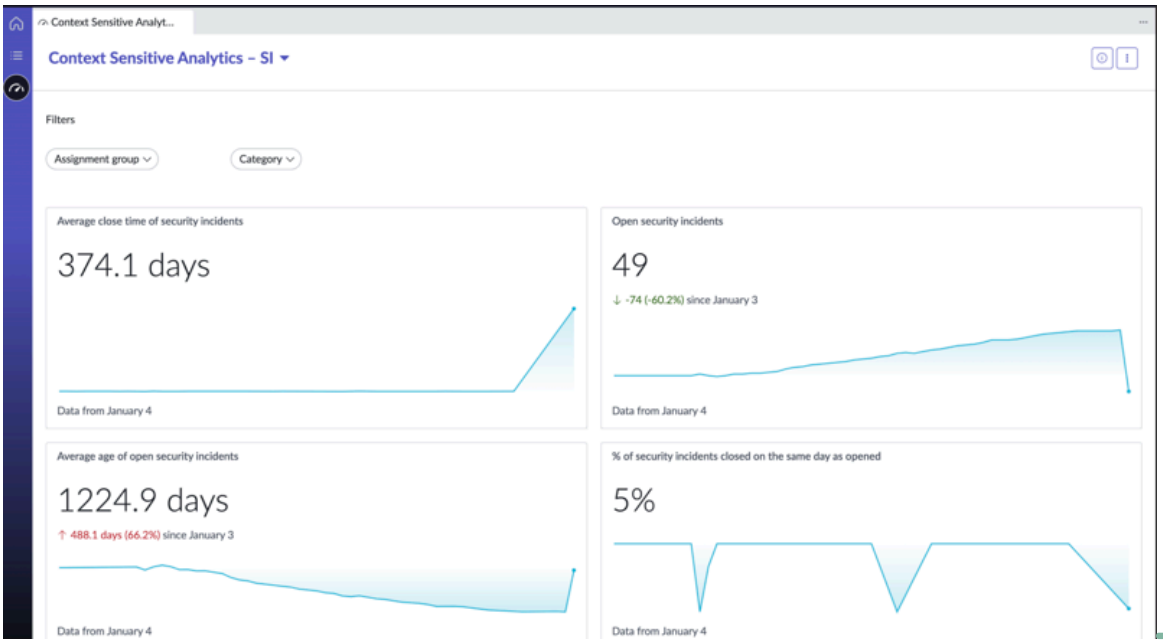
Função necessária: sn_si.analyst (Read), sn_si.manager ou sn_si.admin (write)

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Análise sensível ao contexto - SI** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel Análise sensível ao contexto - SI para obter mais ações.

Exibir painel do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de alto nível dos incidentes de segurança e tendências de incidentes semanais na instância na forma de gráficos. Esses gráficos ajudam você a exibir e analisar com eficácia o desempenho do SOC (Security Operations Center, centro de operações de segurança).

Antes de Iniciar

- Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.
- Certifique-se de ter o aplicativo Performance Analytics para Resposta de incidentes de segurança instalado.

Por Que e Quando Desempenhar Esta Tarefa

Nota: O painel do CISO e o painel Visão geral do CISO eram dois diferentes na IU clássica. Agora, os recursos dos dois painéis foram mesclados no painel do CISO.

O painel do CISO fornece informações importantes sobre seus incidentes de segurança semanalmente. Você pode configurar indicadores e coletar snapshots de dados dos incidentes que correspondem às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel.

Você pode visualizar as tendências semanais usando os widgets no painel do CISO. Os dados ou estatísticas das tendências de seus incidentes de segurança são coletados das propriedades do indicador de incidentes semanais que são definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Tempo médio para identificar (semanalmente)** : Este gráfico ilustra o tempo médio semanal necessário para identificar um incidente de segurança.
- **Tempo médio para conter (semanalmente)** : Este gráfico ilustra o tempo médio semanal necessário para conter um incidente de segurança.
- **Tempo médio para erradicar (semanalmente)** : Este gráfico ilustra o tempo médio semanal necessário para erradicar um incidente de segurança.

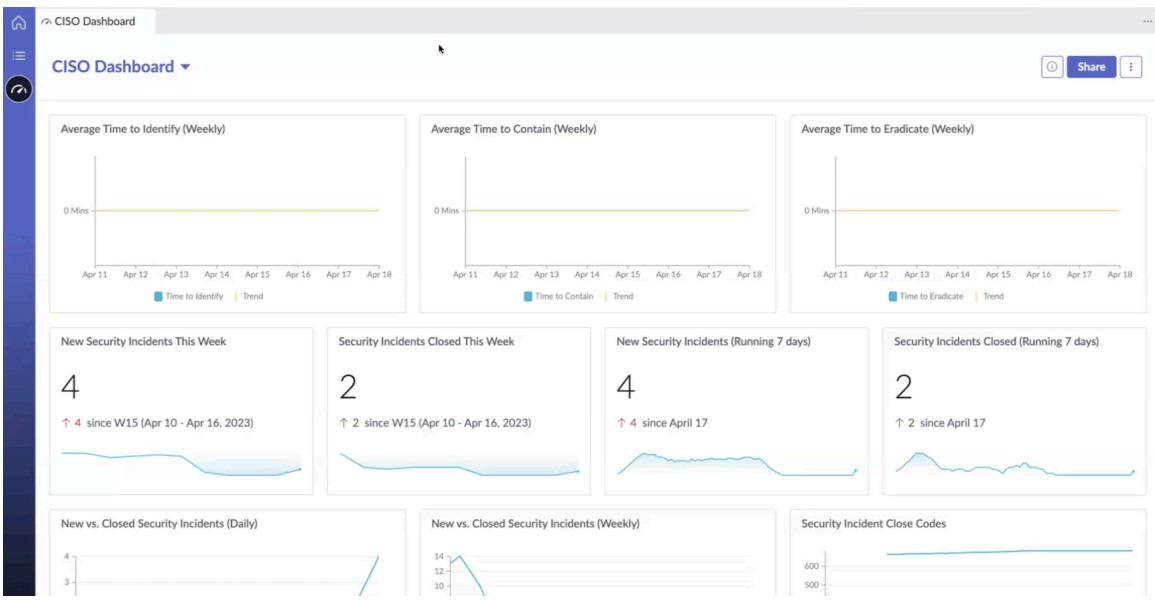
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Novos incidentes de segurança esta semana** : Este gráfico ilustra o número de novos incidentes de segurança esta semana.
- **Incidentes de segurança encerrados esta semana** : Este gráfico ilustra o número de incidentes de segurança encerrados esta semana.
- **Novos incidentes de segurança (em execução por 7 dias)** : Este gráfico ilustra o número de novos incidentes de segurança em execução por uma semana.
- **Incidentes de segurança encerrados (em execução por 7 dias)** : Este gráfico ilustra o número de novos incidentes de segurança encerrados, mas em execução por uma semana.
- **Incidentes novos versus encerrados (diariamente)** : Este gráfico ilustra a comparação entre os novos incidentes de segurança diários e os incidentes de segurança encerrados diariamente.
- **Incidentes novos versus encerrados (semanalmente)** : Este gráfico ilustra a comparação entre os novos incidentes de segurança semanais e os incidentes de segurança encerrados semanalmente.
- **Incidentes de segurança encerrados** : Este gráfico ilustra os códigos encerrados dos incidentes de segurança.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone no lado esquerdo da página inicial do espaço.
3. Selecione **Painel do CISO** na lista suspensa.



4. Exiba o painel do CISO para obter mais ações.

Exiba o painel Visão geral de relatórios do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de relatórios de alto nível dos incidentes de segurança e tendências de incidentes semanais na instância na forma de gráficos. Esses gráficos ajudam você a exibir e analisar com eficácia o desempenho do SOC (Security Operations Center, centro de operações de segurança).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.

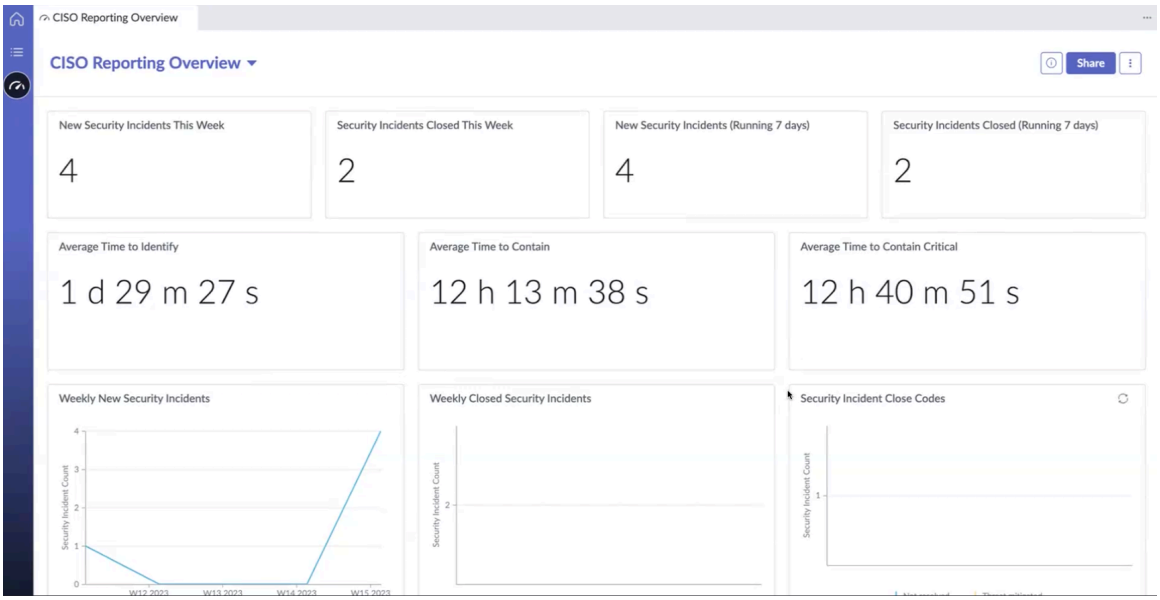
Por Que e Quando Desempenhar Esta Tarefa
O painel Visão geral de relatórios do CISO fornece informações importantes sobre os incidentes de segurança semanalmente, e você pode visualizar as tendências semanais usando widgets. Você pode obter informações importantes sobre os Relatórios do CISO usando os seguintes gráficos:

- **Novos incidentes de segurança esta semana** : Este bloco exibe o relatório do número de novos incidentes de segurança esta semana.
- **Incidentes de segurança encerrados esta semana** : Este bloco exibe o relatório do número de incidentes de segurança encerrados esta semana.
- **Novos incidentes de segurança (em execução por 7 dias)** : Este bloco exibe o relatório do número de novos incidentes de segurança que estão em execução por uma semana.
- **Incidentes de segurança encerrados (em execução por 7 dias)** : Este bloco exibe o relatório do número de novos incidentes de segurança encerrados, mas em execução por uma semana.
- **Tempo médio para identificar** : Este bloco exibe o relatório do tempo médio semanal necessário para identificar incidentes de segurança.
- **Tempo médio para conter** : Este bloco exibe o relatório do tempo médio semanal necessário para conter incidentes de segurança.
- **Tempo médio para conter Crítico** : Este bloco exibe o relatório do tempo médio semanal necessário para conter incidentes de segurança críticos.
- **Novos incidentes de segurança semanais** : Este gráfico ilustra o relatório dos novos incidentes de segurança semanais.
- **Incidentes de segurança encerrados semanalmente** : Este gráfico ilustra o relatório dos incidentes de segurança encerrados semanalmente.
- **Incidentes de segurança encerrados** : Este gráfico ilustra o relatório dos códigos encerrados dos incidentes de segurança.

Procedimento
1. Navegar até **Tudo** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do relatório do CISO** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel de Relatórios do CISO para obter mais ações.

Exiba o painel Visão geral do Gerenciador de incidentes de segurança

Este painel fornece aos gerentes uma visão geral de alto nível dos incidentes de segurança críticos ou de alta prioridade no nível da equipe, SLAs que estão prestes a expirar em 24 horas e tendências de incidentes semanais na instância na forma de relatórios e gráficos.

Antes de Iniciar

Função necessária:

- sn_si.admin - Editar e exibir painel.
- sn_si.manager - Exibir painel.

Por Que e Quando Desempenhar Esta Tarefa

Você pode analisar os incidentes de segurança críticos ou de alta prioridade, ou ANS que precisam de atenção imediata. Você também pode visualizar as tendências semanais usando os widgets no painel Visão geral do Gerenciador de incidentes de segurança. Os dados ou estatísticas das tendências semanais ou mensais de seus incidentes de segurança são coletados das tabelas de incidentes definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Incidentes de segurança críticos da equipe** : Este bloco exibe o número de incidentes de segurança críticos para a equipe esta semana.
- **Incidentes de alta segurança da equipe** : Este bloco exibe o número de incidentes de alta segurança da equipe esta semana.
- **ANS expirando em 24 horas** : Este bloco exibe o número de SLAs que expirarão em 24 horas.
- **Tempo médio para identificar** : Este bloco exibe o tempo médio semanal necessário para identificar incidentes de segurança.
- **Tempo médio para conter** : Este bloco exibe o tempo médio semanal necessário para conter incidentes de segurança.
- **Tempo médio para conter Crítico** : Este bloco exibe o tempo médio semanal necessário para conter incidentes de segurança críticos.

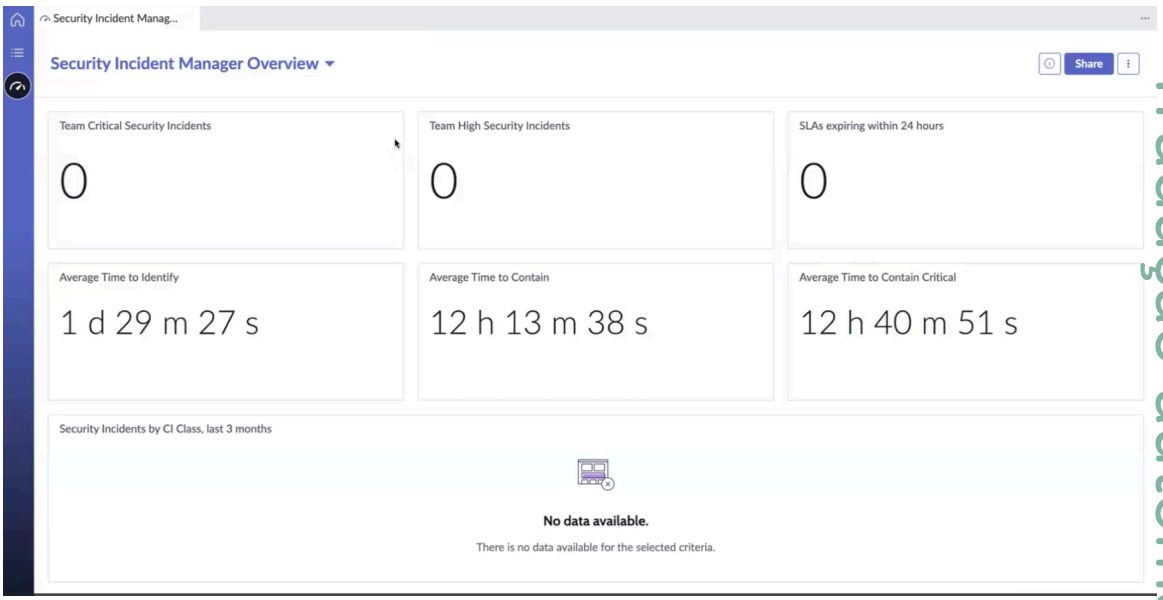
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incidente de segurança por classe de IC, últimos 3 meses** : Este gráfico ilustra as tendências de todos os incidentes de segurança com base na Classe de IC nos últimos três meses.
- **Tendência de todos os incidentes de segurança por categoria** : Este gráfico ilustra as tendências de todos os incidentes de segurança com base na categoria.
- **Tendência de todos os incidentes de segurança por prioridade** : Este gráfico ilustra as tendências de todos os incidentes de segurança com base na prioridade.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique em **Painéis DO SIR** ícone no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do Gerenciador de incidentes de segurança** na lista suspensa.



4. Exiba a Visão geral do Gerenciador de incidentes de segurança para obter mais ações.

Tradução automática

Exiba o painel Integridade da resposta do incidente de segurança

O recurso do painel Integridade da resposta a incidentes de segurança fornece uma exibição centralizada dos aspectos críticos relacionados à implementação do processo de resposta a incidentes, problemas/erros encontrados e métricas de desempenho. Ele serve como uma ferramenta vital para monitorar e otimizar a eficácia dos recursos de resposta a incidentes de segurança de uma organização.

Antes de Iniciar

Função necessária: sn_si.admin, ou sn_si.analyst ou sn_si.analytics_read - Exibir painel.

Por Que e Quando Desempenhar Esta Tarefa

Você pode monitorar a integridade dos incidentes de segurança usando os widgets e gráficos de tendências para cada aplicação. Essas estatísticas apresentam uma pontuação de integridade abrangente detalhando o estado da configuração e a eficácia da correção nas aplicações SIR. O painel Integridade da resposta do incidente de segurança oferece suporte às quatro guias a seguir:

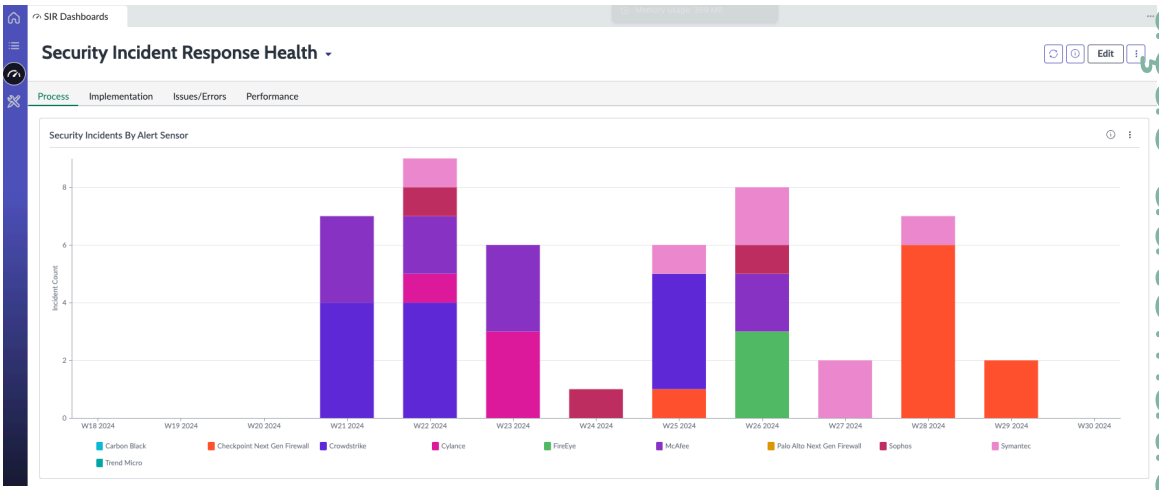
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Processo** : A guia exibe um resumo de todos os incidentes de vários sensores de alerta agrupados semanalmente.
- **Implementação** : Esta guia exibe as personalizações que os clientes executam em suas instâncias, abrangendo inclusões de script, regras de negócio, fluxos e upgrades.
- **Problemas/erros** : A guia exibe widgets destacando erros nos processos de integração, discrepâncias durante a ingestão de dados brutos de incidentes, erros HTTP de saída em aplicações SIR e quaisquer problemas que surjam durante a execução de playbooks.
- **Desempenho** : Esta guia exibe os problemas de desempenho nas aplicações SIR, incluindo lentidão nas consultas de desempenho, regras de negócios e scripts.

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione **Painéis DO SIR** Ícone na página inicial do espaço SIR.
3. Selecione **Painel de Integridade da resposta do incidente de segurança** na lista suspensa.
4. Selecione **Processo** para exibir o número de incidentes de segurança que foram acionados semanalmente para cada sensor de alerta no gráfico.

Guia Processo



Você pode executar as seguintes tarefas:

a. Selecione um sensor de alerta no gráfico para exibir os detalhes de KPI do número de incidentes de segurança acionados por sensores de alerta em uma semana.

b. Para obter os detalhes de KPI de uma semana específica, use **Calendário** opção.

c. Para comparar os incidentes de segurança acionados pelo sensor de alerta, selecione **Comparar registros** opção.

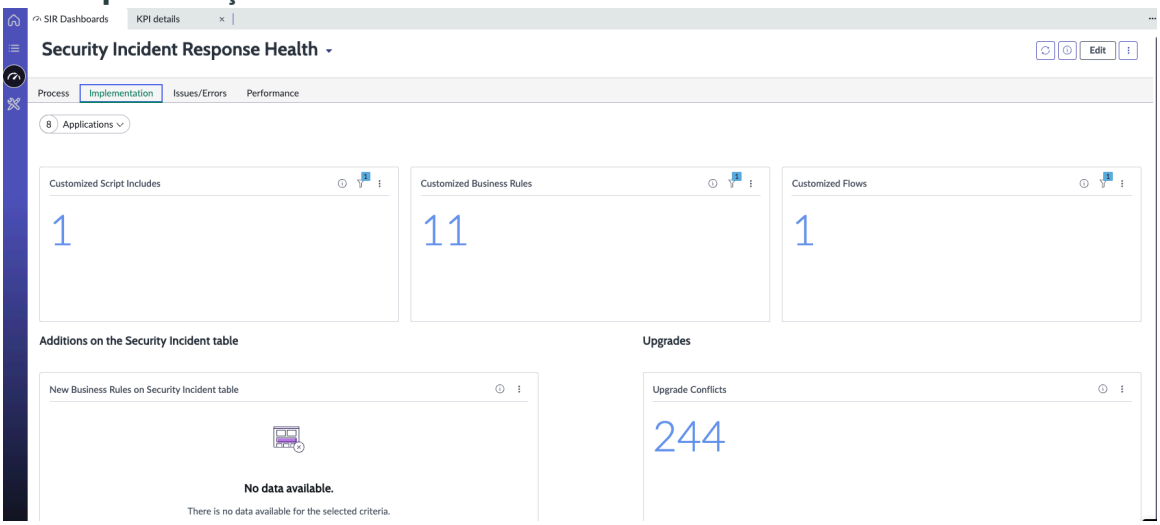
d. Para usar o Tipo de gráfico, Série temporal ou Análise, selecione **Opções de Gráfico** .

5. Selecione **Implementação** Para exibir o número de personalizações que foram criadas para os incidentes de segurança nas aplicações Resposta de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Implementação



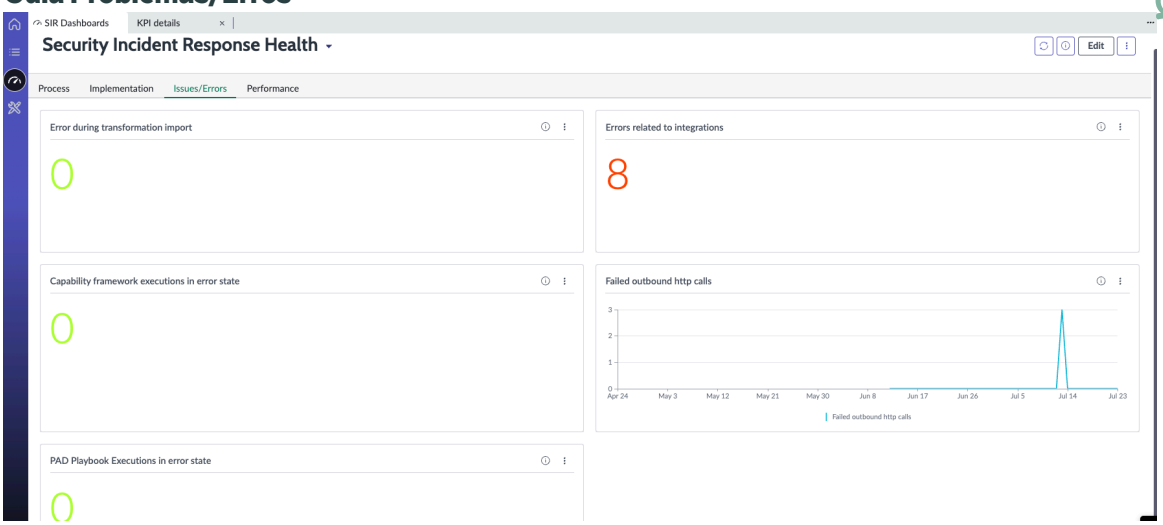
Implementação guia:

Você pode exibir o painel agregado para o número de personalizações que foram criadas para cada aplicação de Resposta de incidente.

- **Inclusões de script personalizadas** : Este widget exibe o número de scripts personalizados que foram adicionados com base em seus requisitos nas aplicações SIR.
- **Regras de negócios personalizadas** : Este widget exibe o número de regras de negócios personalizadas que foram adicionadas com base em seus requisitos nas aplicações SIR.
- **Fluxos personalizados** : Este widget exibe o número de fluxos personalizados que foram adicionados com base em seus requisitos nas aplicações SIR.
- **Nova regra de negócio na tabela Incidente de segurança** : Este widget exibe o número de regras de negócio que foram criadas na tabela Incidente de segurança.
- **Conflitos de upgrade** : Este widget exibe o número de conflitos que foram acionados durante upgrades nas aplicações SIR.

6. Selecione **Problemas/erros** Para exibir o número de problemas ou erros que foram acionados nas aplicações Resposta de incidentes de segurança.

Guia Problemas/Erros



Problemas/erros guia:

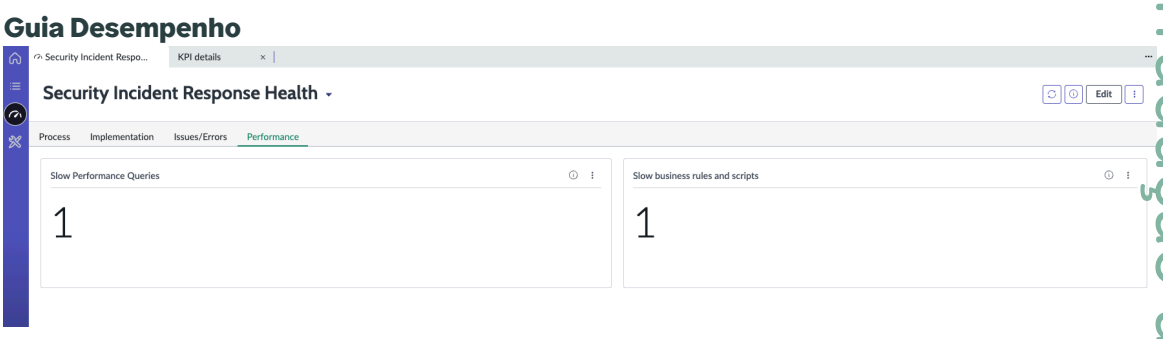
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir o painel agregado para problemas ou erros nas aplicações Resposta de incidentes de segurança.

- **Erros durante a importação de transformação** : Este widget exibe o número de erros que foram acionados durante a importação de transformação em aplicações SIR.
- **Erros relacionados a integrações** : Este widget exibe o número de erros que foram acionados durante as integrações DE SIR.
- **Execuções da estrutura de capacidade em estado de erro** : Este widget exibe o número de erros que foram acionados durante as execuções da estrutura de capacidade em aplicações SIR.
- **Chamadas HTTP de saída com falha** : Este widget exibe o número de chamadas HTTP de saída com falha que foram acionadas nas aplicações SIR.
- **Execuções DO Playbook do PAD em estado de erro** : Este widget exibe o número de erros de execução do Playbook PAD que foram acionados nas aplicações SIR.

7. Selecione **Desempenho** Para exibir o número de problemas de desempenho que foram acionados nas aplicações Resposta de incidentes de segurança.



Desempenho guia:

Você pode exibir o painel agregado para problemas de desempenho nas aplicações Resposta de incidentes de segurança.

- **Consultas de desempenho lentas** : Este widget exibe o número de consultas de desempenho nas aplicações SIR cujo tempo médio de execução é maior que 10 ms e a média de 1000 ou mais execuções.
- **Scripts e regras de negócios lentos** : Este widget exibe o número de regras de negócio e scripts nas aplicações SIR cujo tempo médio de execução é maior que 10 ms e a média de 1000 ou mais execuções.

8. Você pode usar **Atualizar** Ícone para atualizar os dados no painel Integridade da resposta do incidente de segurança.
9. Você pode usar **Exibir detalhes do painel** Ícone para exibir os detalhes do painel Integridade da resposta do incidente de segurança.
10. Você pode usar **Editar** Opção para modificar os detalhes do painel Integridade da resposta do incidente de segurança.
11. Você pode usar **Mais** Opção para executar ações adicionais no painel Integridade da resposta do incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação de incidente de segurança

Os incidentes de segurança podem ser criados manualmente a partir do formulário ou automaticamente por meio de eventos de segurança recebidos de ferramentas integradas de monitoramento de alertas de terceiros, como Splunk.

Importante: Os recursos mais recentes do Resposta a incidentes de segurança estão disponíveis exclusivamente em Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para o mais recente Resposta a incidentes de segurança ou Espaço de resposta a incidentes de segurança Versão para acessar e aproveitar recursos como transferência de turno, calculadora de pontuação de risco etc.

Se você tiver uma função de segurança, poderá usar qualquer um dos métodos a seguir para criar incidentes de segurança manualmente.

Métodos para criar incidentes de segurança manualmente

Método	Descrição
Criado manualmente a partir da lista Incidentes de segurança	Na lista Incidente de segurança, clique em **Novo** para criar um novo incidente de segurança.
Criado manualmente a partir do Catálogo de incidentes de segurança	Você pode criar incidentes de segurança selecionando uma das categorias de ameaças à segurança definidas no catálogo de incidentes de segurança.
Gestão de incidentes	No formulário Incidente em Gestão de incidentes, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de uma solicitação de segurança	No formulário Solicitação de segurança, clique em **Converter em incidente de segurança** para criar um novo incidente de segurança.
Criado manualmente a partir de um alerta de Gestão de eventos	No formulário Alertas de gestão de eventos, clique em **Criar incidente de segurança** para criar um novo incidente de segurança a partir de um alerta.
Criado manualmente a partir de um alerta	No formulário Alerta de gestão de eventos, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de um registro de vulnerabilidade (se o plug-in Resposta de vulnerabilidade estiver ativado)	No formulário Itens de vulnerabilidade, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.

Criação automática de incidentes de segurança

Em geral, os administradores de segurança são responsáveis por configurar regras de alerta usadas para gerar incidentes de segurança automaticamente.

Método de administrador de segurança para criar incidentes de segurança

Método	Descrição
Criado automaticamente usando regras de alerta	Incidentes de segurança podem ser criados com base em regras de alerta definidas em Gestão de eventos em seu datacenter aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação manual de incidente de segurança

Você pode criar um incidente de segurança no formulário Incidente de segurança, bem como de vários outros formulários.

Você pode criar incidentes de segurança com base em um registro existente nos seguintes formulários:

- Em qualquer lista de incidentes de segurança
- Formulário de incidentes
- Gestão de eventos Formulário de alerta
- Formulário Itens vulneráveis
- Formulário de solicitação de segurança

Crie um incidente de segurança na lista Incidentes de segurança

Além dos métodos automáticos para criar incidentes de segurança, você pode criá-los manualmente, conforme necessário.

Este vídeo mostra uma visão geral visual de como você pode criar um incidente de segurança na lista Incidentes de segurança.

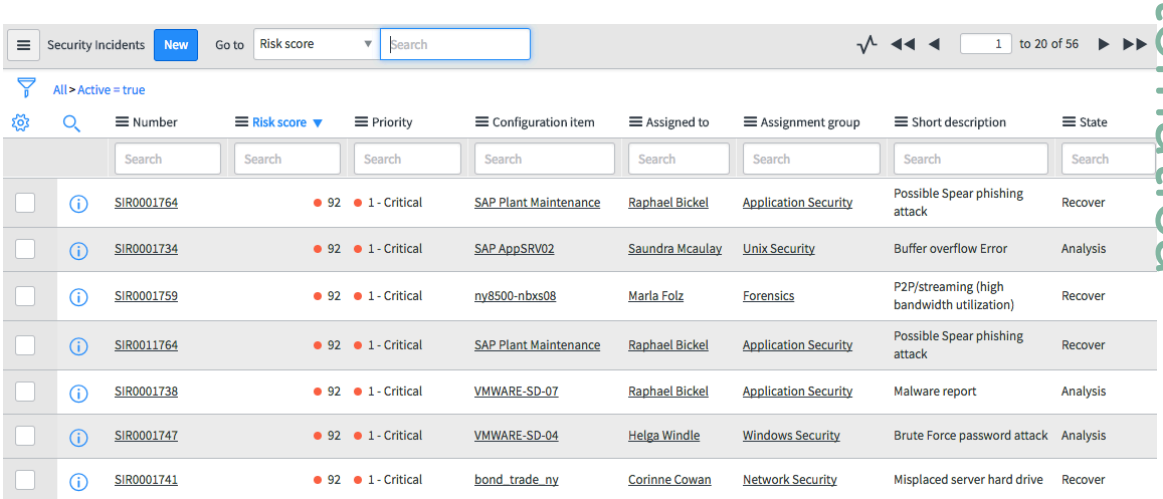
Crie um incidente de segurança na lista Incidentes de segurança

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

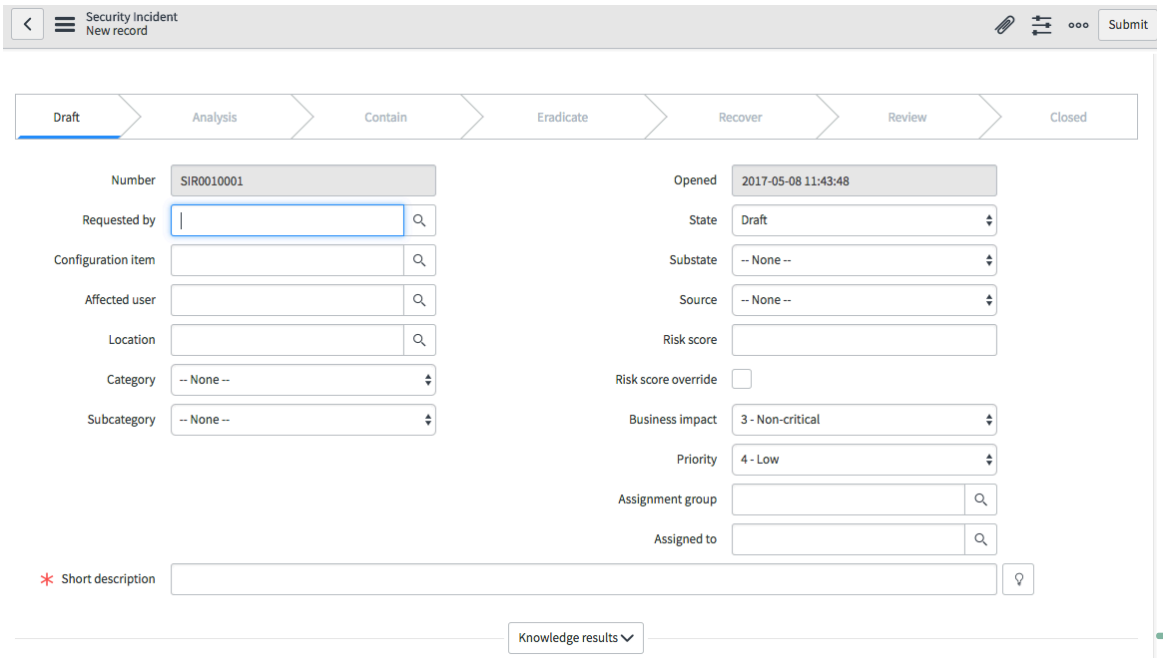
1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**).



2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No formulário, preencha os campos.

Campo	Descrição
Selecione marcador de segurança	Se necessário, selecione um Marcador de segurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo aparece somente depois que o incidente de segurança é salvo.
Número	[Somente leitura] O número do incidente de segurança.
Solicitação de	A pessoa que solicita que o trabalho seja realizado.
Item de configuração	O servidor, o computador, o roteador ou outro item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Local	O local do solicitante ou recurso. Se for um **Item de configuração** não está selecionado, este campo é preenchido previamente com o local do solicitante.
Categoria	A categoria que identifica o tipo de problema de segurança. Se uma categoria for selecionada, um fluxo de trabalho para analisar este problema será executado quando o registro for salvo. Por exemplo, se você selecionar **Negação de serviço** , O fluxo de trabalho Incidente de segurança - Negação de serviço - Modelo é executado. Para obter mais informações, consulte Modelos de fluxo de trabalho de Resposta a incidentes de segurança.
Subcategoria	A subcategoria que define o problema.
Aberto(a)	[Somente leitura] Exibe a data e a hora em que o incidente foi aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	O estado atual do incidente de segurança. Na criação do incidente de segurança, o padrão deste campo é **Rascunho** .
Subestado	Identifica se o incidente de segurança inclui um problema pendente ou uma mudança.
Origem	Identifica a origem do incidente de segurança, como e-mail, uma chamada telefônica ou monitoramento de rede.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Regra de Alerta	A regra no produto de segurança que acionou a criação deste incidente de segurança.
Pontuação de risco	Exibe a pontuação de risco calculada para este incidente de segurança. O valor é baseado na prioridade do incidente de segurança, no tipo de incidente de segurança (negação de serviço, spear Phishing ou atividade de código mal-intencionado) e no número de origens que acionaram uma pontuação de reputação com falha em um indicador. A pontuação de risco ajuda a priorizar o trabalho de incidentes de segurança para os analistas. Três propriedades de incidente de segurança permitem que você designe ainda mais um ponto codificado por cores para aparecer ao lado da pontuação de risco na exibição de lista para torná-los mais facilmente identificáveis. Se você fizer mudanças em determinados campos no incidente de segurança, como **Impacto nos negócios** ou **Prioridade** e salve o registro, o. **Pontuação de risco** é recalculado e exibido automaticamente. A mudança também é refletida nas anotações de trabalho e na lista relacionada Auditorias de pontuação de risco. **Nota:** A pontuação de risco também é recalculada quando os usuários afetados são associados a um incidente de segurança, serviços afetados ou itens vulneráveis. Você também pode inserir manualmente um novo **Pontuação de risco** . Isso pode ser útil se você quiser manter um incidente de segurança específico no topo da lista de incidentes de segurança que está analisando. Se você inserir um novo **Pontuação de risco** . **Substituição da pontuação de risco** a caixa de seleção é marcada automaticamente. Independentemente das mudanças feitas no incidente de segurança, uma pontuação de risco inserida manualmente não é recalculada automaticamente. **Nota:** Se você atualizou sua instância de uma versão anterior, as pontuações de risco foram calculadas para todos os incidentes de segurança em aberto. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.
Substituição da pontuação de risco	Marque esta caixa de seleção para substituir a atualização automática da pontuação de risco. A substituição será refletida nas anotações de trabalho.
Impacto nos negócios	Selecione a importância deste incidente de segurança para o seu negócio. O valor padrão é Não crítico. Se, depois que o registro de incidente de segurança for salvo, você alterar o valor em **Prioridade** fand/ou **Risco** . **Impacto nos negócios** recalculado.
Prioridade	Selecione a ordem na qual lidar com este incidente de segurança, com base na urgência. Se este valor for alterado depois que o registro for salvo, ele poderá afetar **Impacto nos negócios** cálculo.

Tradução automática

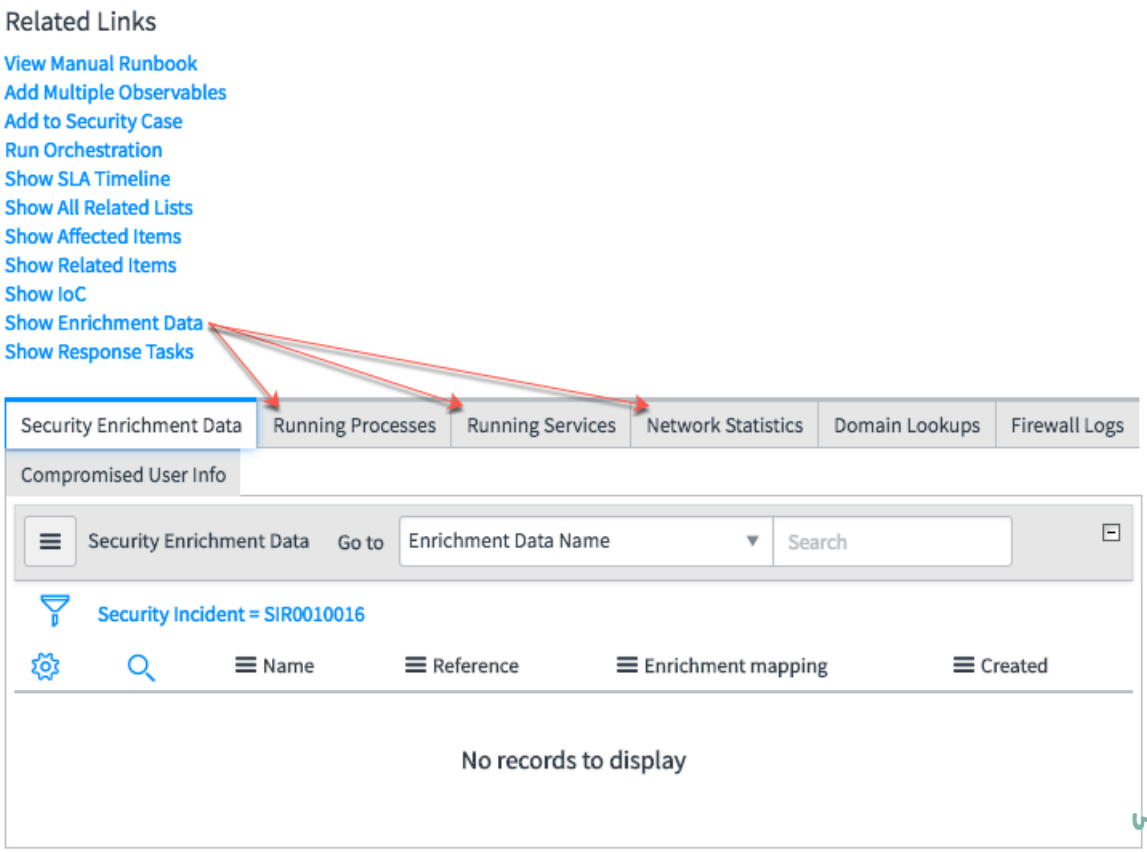
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	O grupo ao qual este incidente de segurança está atribuído.
Atribuição a	O indivíduo atribuído para analisar este incidente de segurança. As atribuições podem ser realizadas manual ou automaticamente. Para obter mais informações, consulte Atribuição de analistas de segurança.
Descrição resumida	Uma breve descrição do incidente de segurança.
Resultados de conhecimento	Conforme você digita a descrição resumida, os links para artigos relacionados da base de conhecimento são exibidos. Verificar as informações pode resolver o problema.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar** .
   Se você adicionou um novo IC ao incidente de segurança, os seguintes fluxos de trabalho de integração serão executados automaticamente:
   - Operações de segurança - Obter fluxo de processos em execução. Este fluxo de trabalho recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint.
   - Resposta a incidentes de segurança - Obter fluxo de trabalho de serviços em execução. Este fluxo de trabalho recupera uma lista de serviços em execução de ICs baseados no Windows.
   - Integrações de operações de segurança - Obter fluxo de estatísticas de rede. Este fluxo de trabalho recupera uma lista de conexões de rede ativas de um host ou endpoint.
5. Para exibir as informações recuperadas por esses fluxos de trabalho, clique em **Mostrar Dados de Aprimoramento** link relacionado e clique em qualquer uma das guias indicadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Fluxos de trabalho adicionais são executados com base nas integrações de terceiros que você ativou da seguinte forma Integração Carbon Black de operações de segurança - Obter fluxo de processos em execução

Tópicos relacionados

Configuração do Resposta a incidentes de segurança

Crie um incidente de segurança no Catálogo de incidentes de segurança

Os usuários em sua empresa podem usar o Catálogo de incidentes de segurança para solicitar vários tipos de análise relacionada à segurança.

Antes de Iniciar

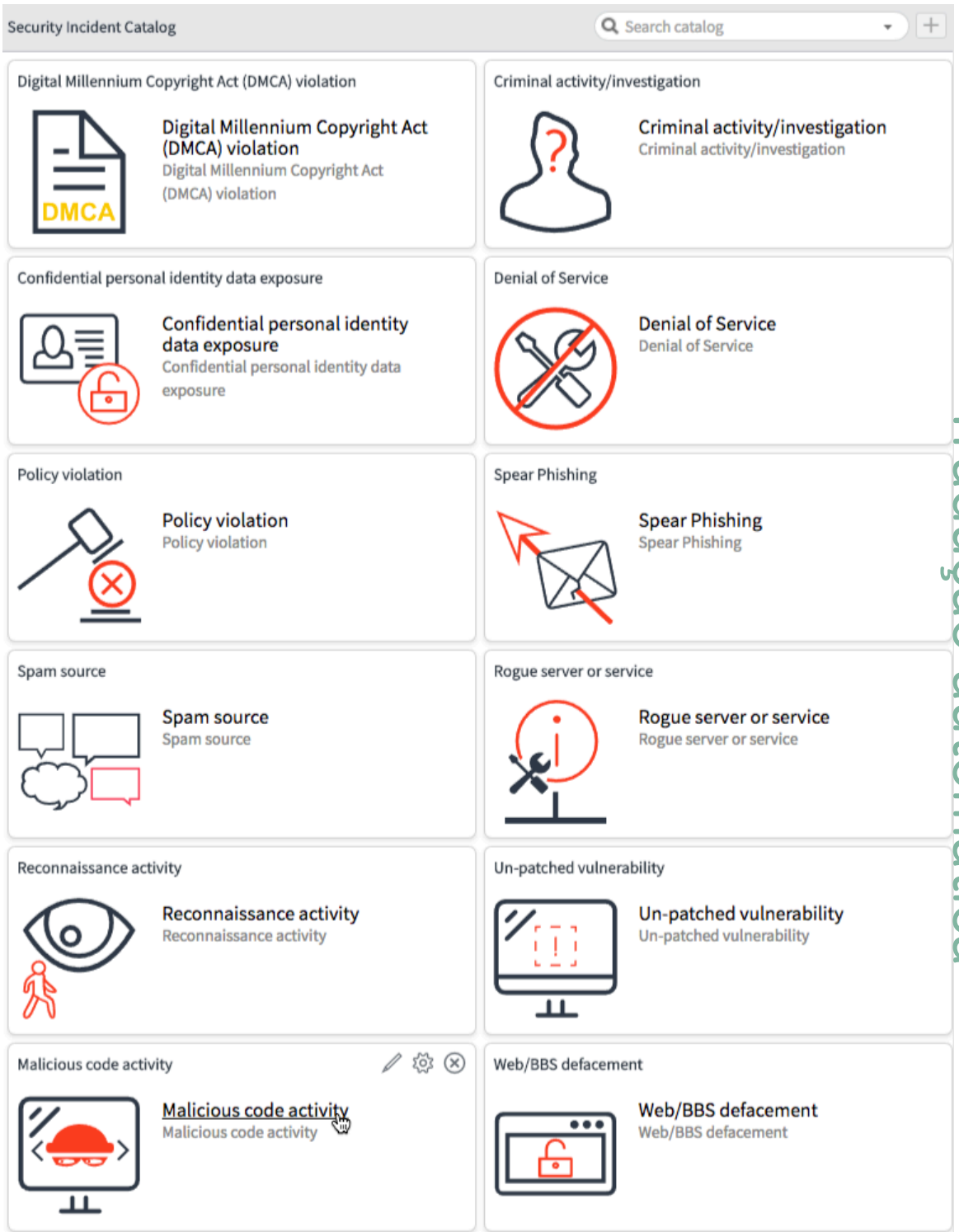
Função necessária: nenhuma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

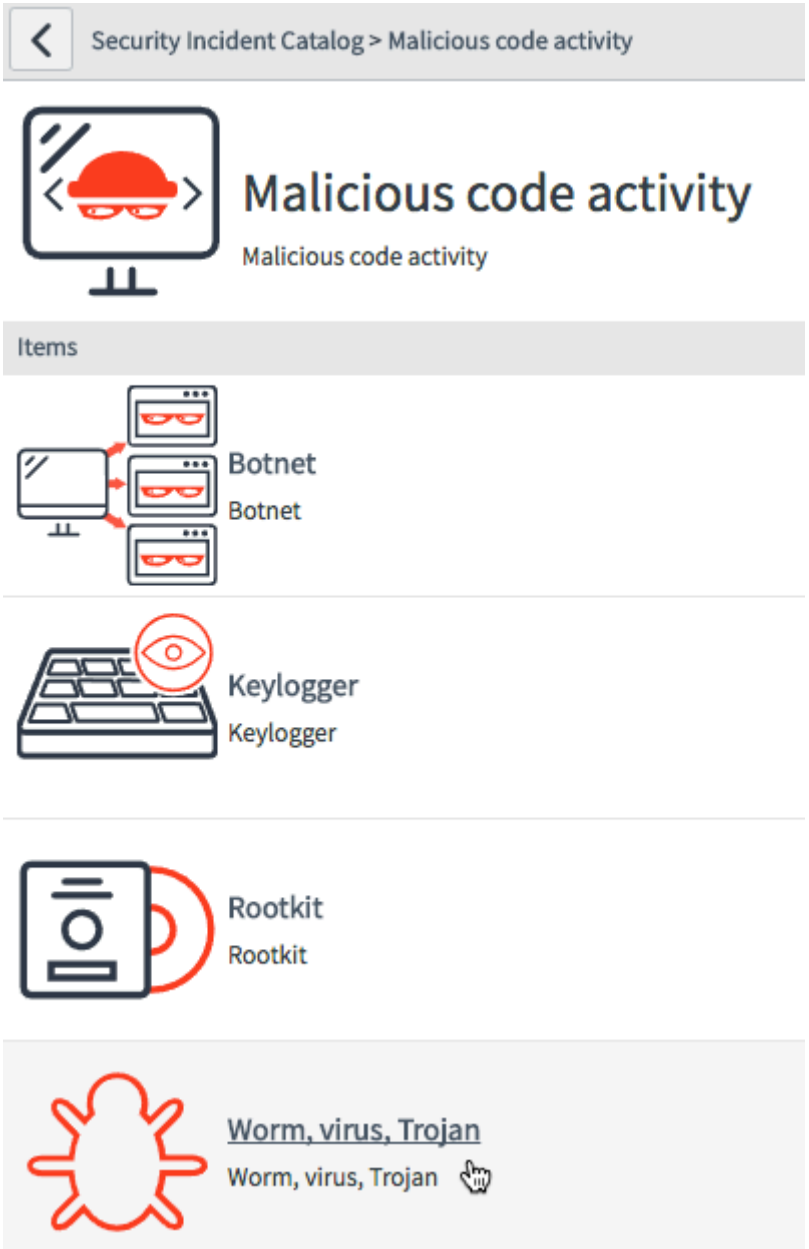
1. Navegar até **Tudo** > **Autoatendimento** > **Catálogo de incidente de segurança**.



2. Clique no item do catálogo para o qual você deseja fazer uma solicitação.
   Se o item selecionado no catálogo principal contiver subcategorias, a lista será mostrada. No exemplo a seguir, **Atividade de código mal-intencionado** selecionado.

Tradução automática

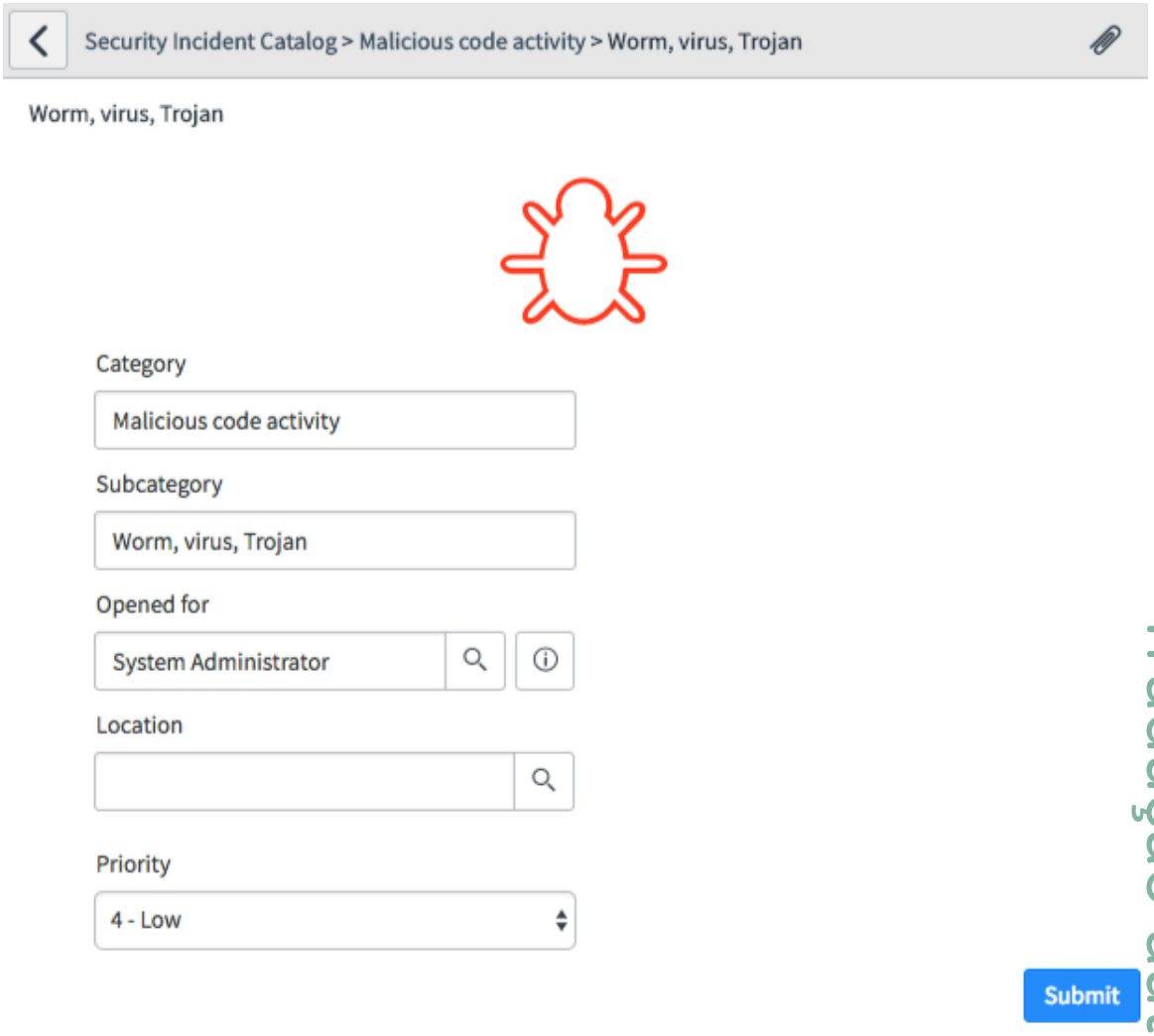
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique na subcategoria que melhor corresponde ao tipo de solicitação que você deseja fazer. Neste exemplo, **Worm, vírus, cavalo de troia** a subcategoria foi selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira as informações da solicitação e clique em **Enviar** .
   A solicitação é enviada para o departamento de Incidente de segurança.
5. Depois de enviar a solicitação, você pode rastrear o andamento navegando até **Autoatendimento** > **Minhas solicitações**e inserindo o número da solicitação.

Crie um incidente de segurança a partir de um alerta da Gestão de eventos

Quando a Gestão de eventos está ativada, você pode criar incidentes de segurança manualmente no formulário Alerta.

Antes de Iniciar

O plug-in Gestão de eventos requer uma assinatura separada e deve ser ativado pela equipe da ServiceNow. Este plug-in inclui dados de demonstração e ativa plug-ins relacionados, caso ainda não estejam ativos. A Análise de serviços é ativada automaticamente quando a Gestão de eventos é ativada.

Função necessária: evt_mgmt_admin, evt_mgmt_operator ou evt_mgmt_user

Procedimento

1. Navegar até **Tudo** > **Gestão de eventos** > **Todos os Alertas**.
2. Clique no alerta **Número** .
3. Clique em **Criar incidente de segurança** .
4. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação automática de incidentes de segurança

Ferramentas de monitoramento de terceiros, como Splunk, podem ser integradas com Resposta a incidentes de segurança para que os eventos de segurança importados dessas ferramentas gerem incidentes de segurança automaticamente. Você também pode importar dados de ferramentas de terceiros para alertas de segurança.

Para integrar ferramentas de monitoramento de alertas ao Resposta a incidentes de segurança, você deve usar REST API Para gravar na tabela Importação de incidentes de segurança [sn_si_incident_import]. Em seguida, usando **Transformação de incidente de segurança** mapas de transformação , A tabela de origem do conjunto de importação é mapeada para campos na tabela Incidente de segurança de destino [sn_si.incident].

Se você tentar importar registros de IC que não são reconhecidos pelo mapa de transformação, o script do mapa de transformação verificará o registro quanto ao seguinte (nesta ordem) na tentativa de fazer uma correspondência:

- sys_id
- Nome do IC
- nome de domínio totalmente qualificado
- Endereço IP

Nota: Se você achar que **Transformação de incidente de segurança** o mapa de transformação não é adequado para a ferramenta de monitoramento de alertas de terceiros que você está usando, duplique o mapa de transformação, crie um novo e edite os campos, conforme necessário.

Incidentes de segurança criados a partir de eventos e alertas

À medida que os eventos são importados das ferramentas de monitoramento de alertas, eles são processados primeiro por Gestão de eventose agrupados em alertas. Esses alertas podem ser usados para criar incidentes de segurança com base em regras de alerta personalizáveis ou revisados manualmente para selecionar os alertas a serem investigados como um incidente de segurança.

Você pode encontrar um exemplo de regra de alerta chamada **Crie incidentes de segurança a partir de alertas críticos** em Regras de Alertamódulo do Gestão de eventosaplicação. Esta regra de alerta cria automaticamente incidentes de segurança quando eventos críticos relacionados à segurança são recebidos de dentro ServiceNow ou de aplicações de monitoramento de terceiros. Depois que o incidente de segurança for criado, ele será atualizado conforme novos eventos forem recebidos. Você pode modificar o modelo de tarefa na regra de alerta para mudar os valores iniciais do incidente de segurança criado por esta regra de alerta. Para lidar com cada variedade distinta de incidente de segurança que você deseja criar, defina outras regras de alerta com condições diferentes.

Se você for um usuário com a função de administrador de segurança, poderá criar manualmente um incidente de segurança clicando em **Criar incidente de segurança** botão de qualquer alerta suspeito.

É importante que os eventos recebidos de ferramentas externas incluam as seguintes informações:

- O nó definido como o nome, endereço IP ou sys_id do IC que se torna o recurso afetado.
- A classificação de evento é definida como Segurança para diferenciá-los de outros eventos DE TI.
- A descrição do evento, que preenche a descrição do incidente de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As informações adicionais podem incluir informações extras que não se encaixam nos campos listados anteriormente ou em outros campos de evento, como categoria, vetores de ataque, URL de retorno ou ID de correlação. O formato é uma cadeia de caracteres que lista os nomes de campos junto com seus valores, usando o seguinte formato JSON:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Nota: Para cada campo e par de valor, se o campo no incidente de segurança em que o nome da coluna corresponde ao fieldName estiver vazio, ele será definido como fieldValue. Se o campo no incidente de segurança não estiver vazio, ele não será alterado. Em ambos os casos, o evento e todos os campos e valores codificados nas informações adicionais são registrados em uma entrada de anotações de trabalho descrevendo o evento. Se nada mudar no incidente de segurança, uma entrada de anotação de trabalho não será criada. Todos os campos em um incidente de segurança, incluindo campos personalizados adicionados à tabela, podem ser definidos.

Dados importados para alertas de segurança

Quando um evento é criado com mais dados codificados em JSON, esses dados são importados para qualquer campo com um nome que corresponda ao fieldName desse valor nos dados JSON.

Se você tiver dados em seu software de monitoramento de terceiros (por exemplo, Splunk) que não sejam comuns ao sistema de base, poderá adicionar novos campos à tabela Alerta para acomodar a importação de dados. O formato JSON para importar dados para alertas é o mesmo formato usado para criar incidentes de segurança a partir de eventos e alertas:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

A única diferença é que os dados no campo são sempre substituídos pelo fieldValue.

Quando os dados do evento de segurança são importados, eles preenchem os campos na tabela Alerta com nomes de campos correspondentes. Se o alerta for transformado posteriormente em um incidente de segurança, os mesmos dados de informações adicionais preencherão os campos correspondentes no incidente de segurança.

Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário

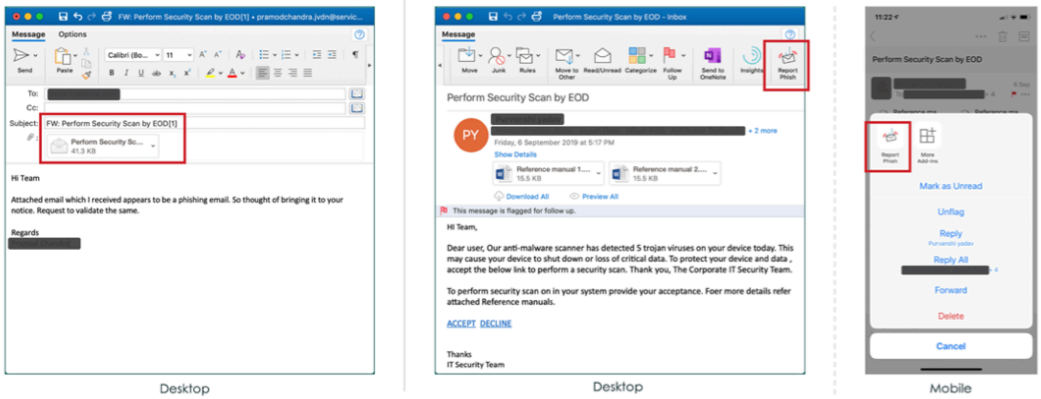
Use esse recurso para criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário.

A funcionalidade aprimorada de Phishing relatado pelo usuário inclui recursos de agregação, extração de cabeçalho de e-mail e configuração.

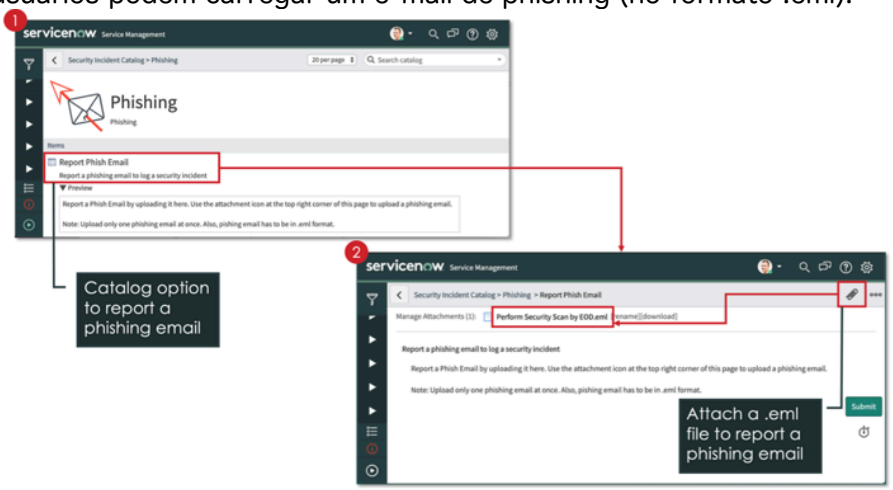
- Os usuários podem relatar e-mails de phishing de várias maneiras:
  - Os e-mails podem ser encaminhados como anexos.
  - . **Phishalarm** O plug-in (anteriormente conhecido como wombat) foi configurado com o cliente Microsoft Outlook, os usuários podem:
    - Clicar no botão **Relatar phishing**.
    - Encaminhar e-mails de phishing de um dispositivo móvel usando a opção **Relatar phishing**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Os usuários podem carregar um e-mail de phishing (no formato .eml).



- O phishing relatado pelo usuário inclui **lógica de negócios de agregação** que identifica e-mails de phishing duplicados relatados por usuários em uma organização. Os usuários podem usar este recurso para:
  - Agregar incidentes de phishing relatados pelo usuário duplicados ou semelhantes (campanhas de phishing iniciadas pela empresa).
  - Evite fazer a triagem de incidentes de phishing relatados pelo usuário duplicados e reduza o esforço manual envolvido na consolidação de incidentes.
  - Permita que os analistas de segurança trabalhem em um único incidente de phishing relatado pelo usuário.
- Fornece cabeçalhos de e-mail de phishing no incidente de phishing relatado pelo usuário.
  - Os analistas de segurança podem verificar as principais informações do cabeçalho de e-mail no incidente.
  - O esforço manual na coleta de informações de cabeçalho de outras fontes não é mais necessário.
- O e-mail de phishing original enviado é armazenado como um **Registro de e-mail de phishing** em uma nova tabela.
- Os analistas de segurança podem exibir detalhes do e-mail de phishing original, como conteúdo do e-mail de phishing, cabeçalhos e origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os administradores de segurança podem configurar e fazer algumas melhorias que incluem:
  - Configurações para extrair cabeçalhos de e-mail do corpo do e-mail (envios de **relatório de phishing**).
  - Filtros para capturar cabeçalhos selecionados.
  - Configurações para lidar com a associação de incidentes primários-secundários quando registros de e-mail de phishing duplicados são identificados.
  - Configurações do Flow Designer para modificar a lógica de negócios de agregação com base nos requisitos.

Configure regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para *`security@acme.com`* sejam categorizados como e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Configure regras de ingestão para phishing relatado pelo usuário.

Defina propriedades de phishing relatadas pelo usuário

Defina as informações do cabeçalho que precisam ser capturadas dos e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Defina propriedades de phishing relatadas pelo usuário.

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

Os e-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas. Para obter mais informações, consulte Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário.

Transformar e-mail de phishing em incidente de segurança

O fluxo Transformar e-mail de phishing em incidente de segurança converte ou transforma registros de e-mail de phishing em incidentes de segurança. Para obter mais informações, consulte Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança.

Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Exiba os detalhes do registro do incidente de segurança, incluindo as Listas relacionadas, anotações de trabalho e outras informações importantes. Para obter mais informações, consulte Registros de incidentes de segurança criados a partir de registros de e-mail de phishing.

Plug-ins e componentes necessários

O recurso de phishing relatado pelo usuário disponível nesta versão é uma versão aprimorada da funcionalidade de phishing relatada pelo usuário disponível na versão London. Consulte **Crie regras para validar ataques de phishing relatados pelo usuário** Na documentação de Londres para obter detalhes.

Instruções de instalação importantes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este aprimoramento substitui o design de phishing relatado pelo usuário existente. O novo design inclui as seguintes atualizações:

- Existente **Phishing relatado pelo usuário** As ações de entrada de e-mail (Tipo Encaminhar e Tipo Novo) foram desabilitadas.
- Um novo **Criar e-mail de phishing** a ação de entrada agora está disponível.
- . Transforme e-mails de phishing relatados pelo usuário em incidentes de segurançaé um novo fluxo que contém a lógica de negócios de criação e agregação de incidentes de segurança para o novo design. Você deve ativar este fluxo para que o novo design entre em vigor.
- As regras de phishing existentes relatadas pelo usuário foram preservadas durante o upgrade.

Nota: Se você usar ações de entrada de e-mail personalizadas e fluxos de trabalho personalizados para envios de phishing relatados pelo usuário, revise os designs antigo e novo para verificar se há funcionalidades conflitantes ou sobrepostas.

Detalhes de Aprimoramento de Phishing relatado pelo usuário A seguir estão os detalhes da melhoria:

- Relatar o e-mail de phishing de várias maneiras: Consulte Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário para obter detalhes. O e-mail de phishing é movido para `sn_si_phishing_email` tabela.
- Criação de registros de e-mail de phishing: Se as regras de correspondência de e-mail forem atendidas (consulte Configure regras de ingestão para phishing relatado pelo usuário. **Criar e-mail de phishing** a ação de entrada cria um registro de e-mail de phishing. Os cabeçalhos de e-mail analisados são armazenados no CM `sn_si_phishing_email_header` e associados ao e-mail de phishing como uma lista relacionada.
- Agregação de registros de phishing semelhantes em um único incidente de segurança: O. Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança o fluxo cria incidentes de segurança a partir dos registros de e-mail de phishing e agrega registros semelhantes em um único incidente. As condições de agregação podem ser modificadas conforme necessário neste fluxo.

Nota:

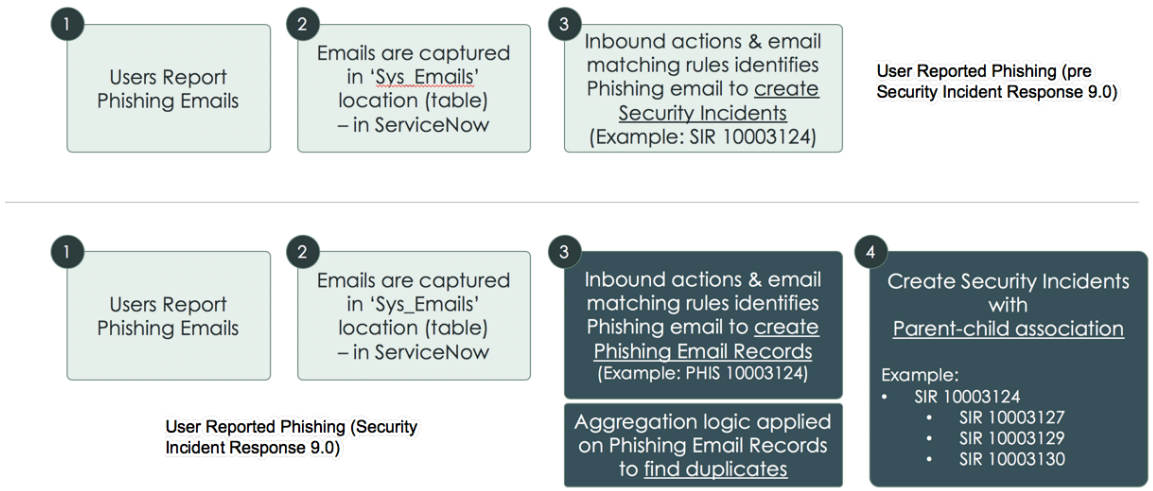
- . **Phishing relatado pelo usuário** As ações de entrada disponíveis antes da versão Security Incident Response 9,0 agora estão desabilitadas. Os incidentes de segurança não são mais criados por meio das ações de entrada desabilitadas.
- A aplicação Spoke do Security Operations deve ser instalada para que o novo design entre em vigor. Isso inclui Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança fluxo que está disponível em um estado inativo por padrão. Ative este fluxo para criar incidentes de segurança a partir dos registros de e-mail de phishing.

A imagem a seguir mostra as diferenças entre o antigo e o novo design:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

What Happens When User Reports A Phishing Email?



Para usar o recurso aprimorado de Phishing relatado pelo usuário, os seguintes plug-ins e componentes são necessários:

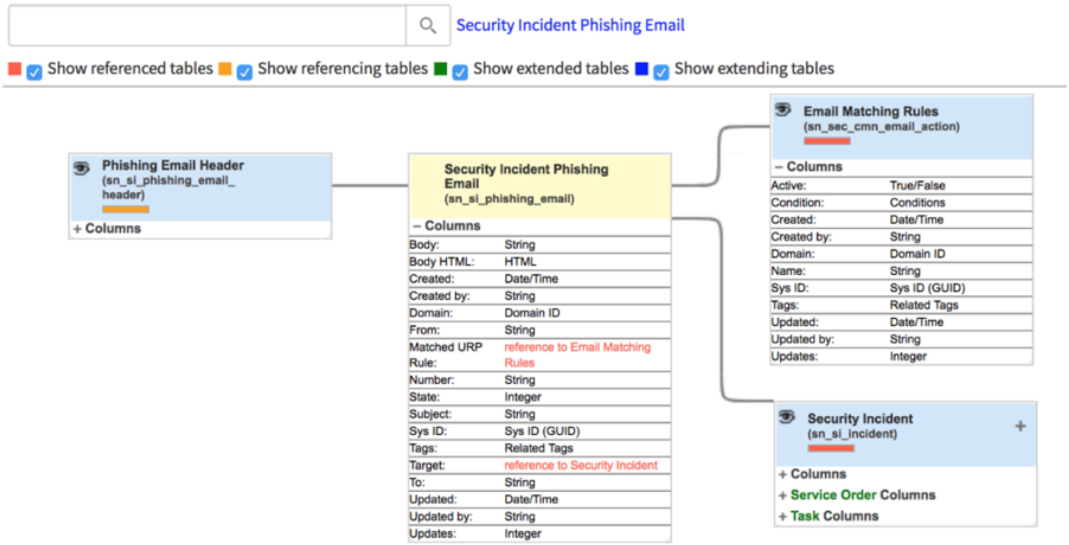
- Suporte de segurança Comum (`sn_sec_cmn`): Inclui:
  - Ação de entrada
  - Novo script EmailUserReportedPhishing
  - Tabela Regras de ingestão
- Resposta a incidentes de segurança (sn_si): Inclui:
  - Tabela de incidentes de segurança (sn_si_incident)
  - Tabela de e-mails de phishing de segurança (sn_si_phishing_email)
  - Tabela de cabeçalhos de e-mail de phishing de segurança (sn_si_phishing_email_header)
  - Produtor de registro de carregamento do EML
- Spoke de Operações de segurança

  Fluxos e subfluxos para agregar e-mails e transformar e-mails de phishing em incidentes de segurança.

A figura a seguir mostra a nova tabela de e-mails de phishing com referências à regra de URP correspondente e ao registro de incidente de segurança de destino (sn_si_incident).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configure regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para `security@acme.com` sejam categorizados como e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

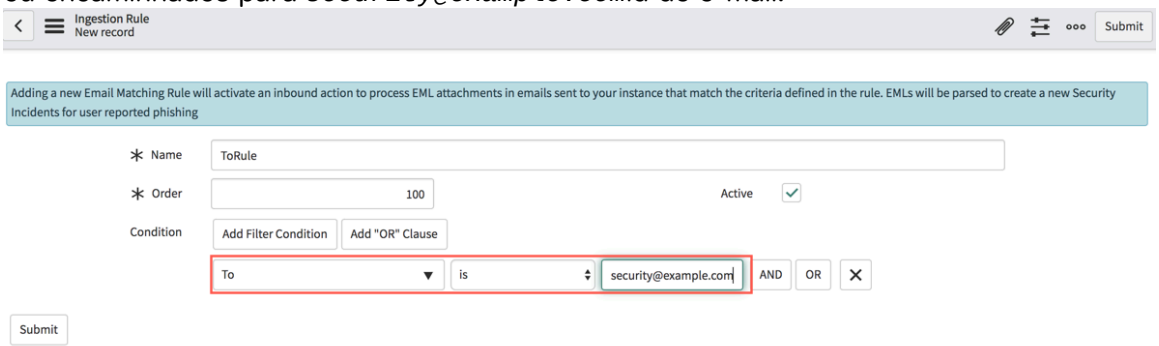
Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Processamento de E-mails** > **Regras de ingestão - Phishing reportado pelo usuário**.
2. Clique em **Novo** Para criar uma nova regra de correspondência de e-mail.
3. Insira um nome e defina uma ou mais condições para a regra.
4. Clique em **Enviar** para salvar a regra.
   A seguir estão algumas regras de exemplo:

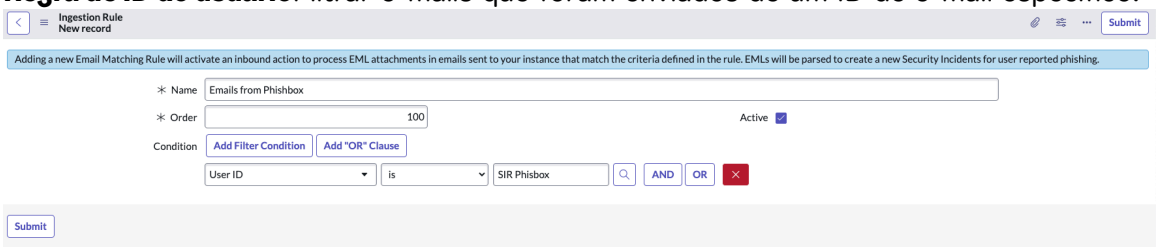
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Para Regra** Filtrar e-mails que foram enviados diretamente ou encaminhados para `security@example.com`id de e-mail.



- **Regra de ID do usuário**Filtrar e-mails que foram enviados de um ID de e-mail específico.



Defina propriedades de phishing relatadas pelo usuário

Defina as informações do cabeçalho que devem ser capturadas de e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Use essas opções para definir as seguintes configurações de phishing relatadas pelo usuário.

- Configuração para extrair cabeçalhos de e-mail do corpo do e-mail. (**Relatar Phish** envios.)
- Filtrar para selecionar cabeçalhos.
- Habilite ou desabilite a associação primário-secundário.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Processamento de E-mails** > **Propriedades do Phishing Reportado pelo Usuário**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Especifique a configuração para extrair cabeçalhos de e-mail do corpo do e-mail:
   - Insira uma cadeia de caracteres que identifique o início do cabeçalho do e-mail.
   - Insira uma cadeia de caracteres que identifique o final do cabeçalho do e-mail.

   Nota: Aplique essas configurações somente aos cabeçalhos capturados como parte do corpo do e-mail de phishing. Por exemplo, se **Phishalarm** O plug-in (anteriormente conhecido como wombat) foi configurado com o cliente Microsoft Outlook, quando o usuário clica em **Relatar Phish** , os cabeçalhos de e-mail são capturados de acordo com a configuração definida aqui. As informações do cabeçalho não serão capturadas se o e-mail de phishing for encaminhado como um anexo.

3. Especifique filtros para eliminar cabeçalhos que não são necessários para investigar o incidente de segurança.

   Insira uma lista separada por vírgulas de cabeçalhos de e-mail que devem ser capturados do e-mail de phishing relatado pelo usuário. Se você não especificar nenhum valor aqui, todas as informações do cabeçalho serão capturadas.

4. Habilite ou desabilite a associação primário-secundário.
   Por padrão, o **Sim** a opção está habilitada. Selecione **Sim** indicar que incidentes de segurança secundários devem ser criados quando os e-mails de phishing relatados pelo usuário são agregados. Se você selecionar **Não** os incidentes de segurança secundários não são criados, mas os e-mails de phishing relatados pelo usuário são associados ao incidente de segurança e o registro do incidente de segurança é atualizado. Consulte Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança para obter mais informações sobre como os incidentes de segurança secundários são criados.

5. Habilite ou desabilite a opção para exibir o conteúdo do e-mail de phishing no formato HTML.
   Por padrão, o **Sim** a opção está habilitada. Selecione **Sim** Para exibir o conteúdo do e-mail de phishing no formato HTML. Se você selecionar **Não** , O conteúdo do e-mail no formato HTML não ficará visível em um registro de phishing.

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

E-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas.

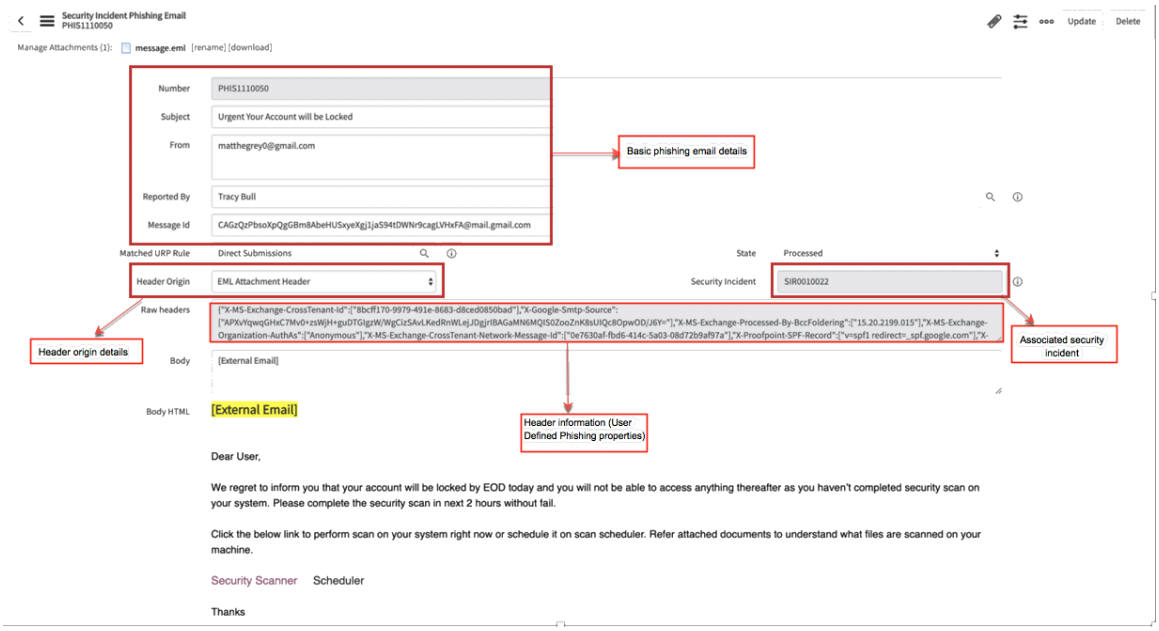
Quando um novo e-mail de phishing é relatado, as seguintes ações ocorrem:

- Um registro de e-mail é criado no `sys_email` tabela.
- . **Criar e-mail de phishing** A ação de entrada é executada no registro de e-mail e usa as Regras de correspondência de e-mail (consulte Configure regras de ingestão para phishing relatado pelo usuário para determinar se é um e-mail de phishing.
- Quando ele é identificado como um e-mail de phishing, um registro de e-mail de phishing é criado no `sn_si_phishing_email` tabela.
- Por fim, o. Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança o fluxo é aplicado para converter o registro de e-mail de phishing em um incidente de segurança.

Para exibir os detalhes do e-mail, navegue até **Incidente de segurança** > **Mostrar todos os e-mails de phishing**. Uma lista de registros de e-mail de phishing é exibida. Clique no link de data na coluna Criado para exibir o registro de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



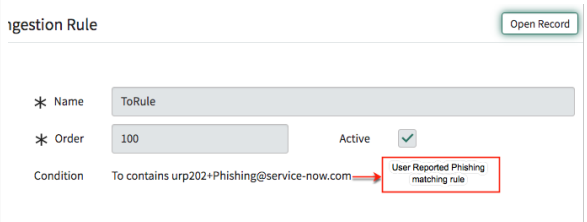
Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
Número	O número atribuído ao e-mail de phishing relatado pelo usuário.
Assunto	O assunto do e-mail. A regra de assunto é útil em campanhas ou testes de phishing simulados. Nesse caso, as organizações enviam e-mails enganosos para sua própria equipe para testar sua resposta a ataques de phishing e e-mail semelhantes. Em testes de e-mail de phishing simulados, se o cliente de e-mail do Microsoft Outlook com **Phishalarm** O plug-in (anteriormente conhecido como wombat) está sendo usado, o usuário pode clicar em **Relatar Phish** botão para denunciar o e-mail de phishing. O e-mail é enviado para a equipe de Operações de segurança com **Phishing simulado** Anexado ao assunto do e-mail. Isso é usado para identificar o e-mail como um e-mail de phishing simulado.
De	O endereço de e-mail de onde este e-mail de phishing se originou. Essas informações estarão disponíveis se o e-mail de phishing for encaminhado como anexo de arquivo .eml ou se os cabeçalhos originais estiverem incorporados no e-mail. Se o usuário encaminhou o e-mail de phishing diretamente, o endereço do remetente pode não estar disponível.
Relatado por	O ID de e-mail do usuário que relatou este e-mail de phishing. Clique em **Informações** ícone para exibir detalhes adicionais.
ID da mensagem	O ID atribuído à mensagem.
Regra de URP correspondente	A regra de phishing relatado pelo usuário que deve ser aplicada a este e-mail. Clique no ícone Informações para exibir detalhes adicionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

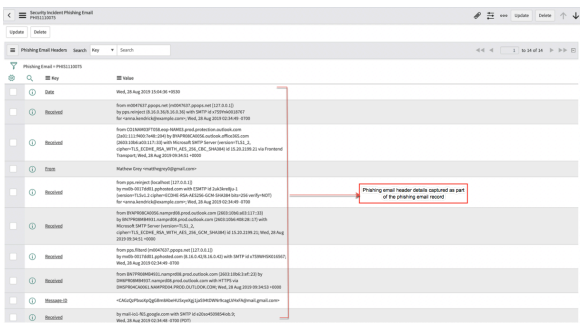
Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
 Como você pode ver, neste exemplo, o. **Condição** O campo mostra que ToRule é aplicado a este e-mail e um incidente de segurança é criado. Consulte Configure regras de ingestão para phishing relatado pelo usuário para obter mais informações sobre como definir regras de correspondência de e-mail.	
Estado	Quando um novo registro de e-mail de phishing é criado no `sn_si_phishing_email` , o campo Estado está definido como **Novo** . Quando este registro de e-mail é convertido em um incidente de segurança (consulte Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança), o campo Estado é atualizado para **Processado** .
Origem do cabeçalho	Este campo indica como os cabeçalhos de e-mail se originaram ou como o usuário relatou o e-mail de phishing: • **Cabeçalho do e-mail** : O usuário encaminhou o e-mail de phishing para a equipe de operações de segurança. • **Corpo do texto do e-mail:** ◦ O usuário clicou em **Relatar Phish** opção (se for **Phishalarm** O plug-in (anteriormente conhecido como wombat) foi configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatado pelo usuário definida, o e-mail de phishing é encaminhado para a equipe de operações de segurança. • **Cabeçalho do anexo do EML** : ◦ Anexo: O usuário encaminhou o e-mail como um anexo (arquivo .eml). ◦ Envio do catálogo de serviços: O usuário baixou o e-mail como um arquivo .eml para a área de trabalho e o carregou em um local especificado. O incidente de segurança é criado a partir do e-mail. • **Corpo do anexo do EML** : ◦ O usuário clicou em **Relatar Phish** opção (se for **Phishalarm** O plug-in (anteriormente conhecido como wombat) foi configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatado pelo usuário definida, o e-mail de phishing é encaminhado como um anexo para a equipe de operações de segurança.
Incidente de segurança	Este campo fica em branco quando o e-mail de phishing relatado pelo usuário é relatado pela primeira vez. . Transforme e-mails de phishing relatados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
	pelo usuário em incidentes de segurança o fluxo foi executado, este e-mail é convertido em um registro de incidente de segurança e o número desse registro é exibido aqui.
Cabeçalhos brutos	Este campo mostra as informações completas do cabeçalho extraídas do e-mail, conforme definido em Defina propriedades de phishing relatadas pelo usuário página. Os cabeçalhos são analisados em pares de valor de chave e exibidos na lista Cabeçalhos de e-mail de phishing.
	
Corpo da mensagem	Este é o corpo do e-mail de phishing relatado pelo usuário.

Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança

. **Transformar e-mail de phishing em incidente de segurança** o fluxo é um novo fluxo que converte ou transforma registros de e-mail de phishing em incidentes de segurança.

Antes de Iniciar

Nota: Para habilitar a funcionalidade Phishing relatado pelo usuário, você deve fazer uma cópia do fluxo#e.ativar . Se você criou ações de entrada personalizadas e fluxos personalizados para lidar com envios de phishing relatados pelo usuário, as modificações de fluxo sugeridas aqui não serão necessárias.

- Função necessária: sn_si.admin
- O spoke do Flow Designer deve ser instalado.

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é iniciado automaticamente quando um usuário relata um registro de e-mail de phishing com o Estado definido como **Novo** criado. Este fluxo contém a lógica para:

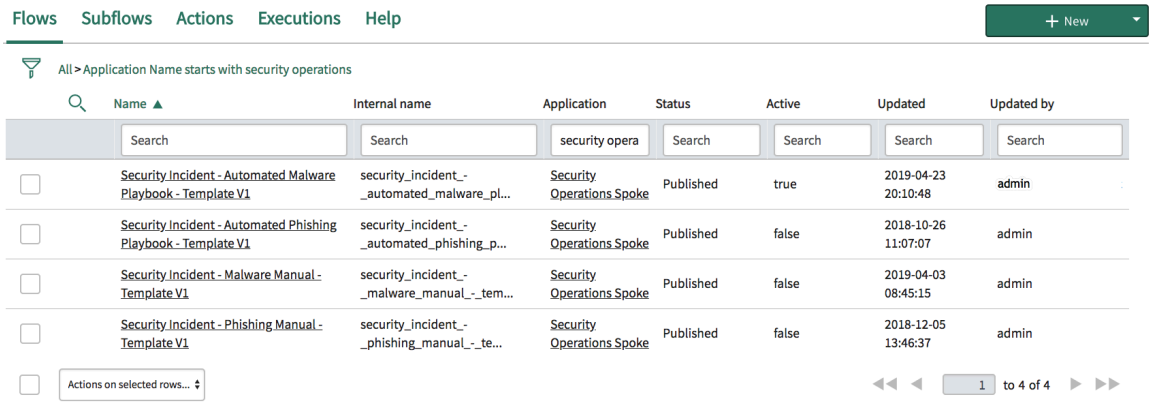
- Incidentes de segurança agregados.
- Atualize incidentes de segurança com anotações relevantes.
- Adicionar dados do cabeçalho.
- Crie incidentes secundários conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

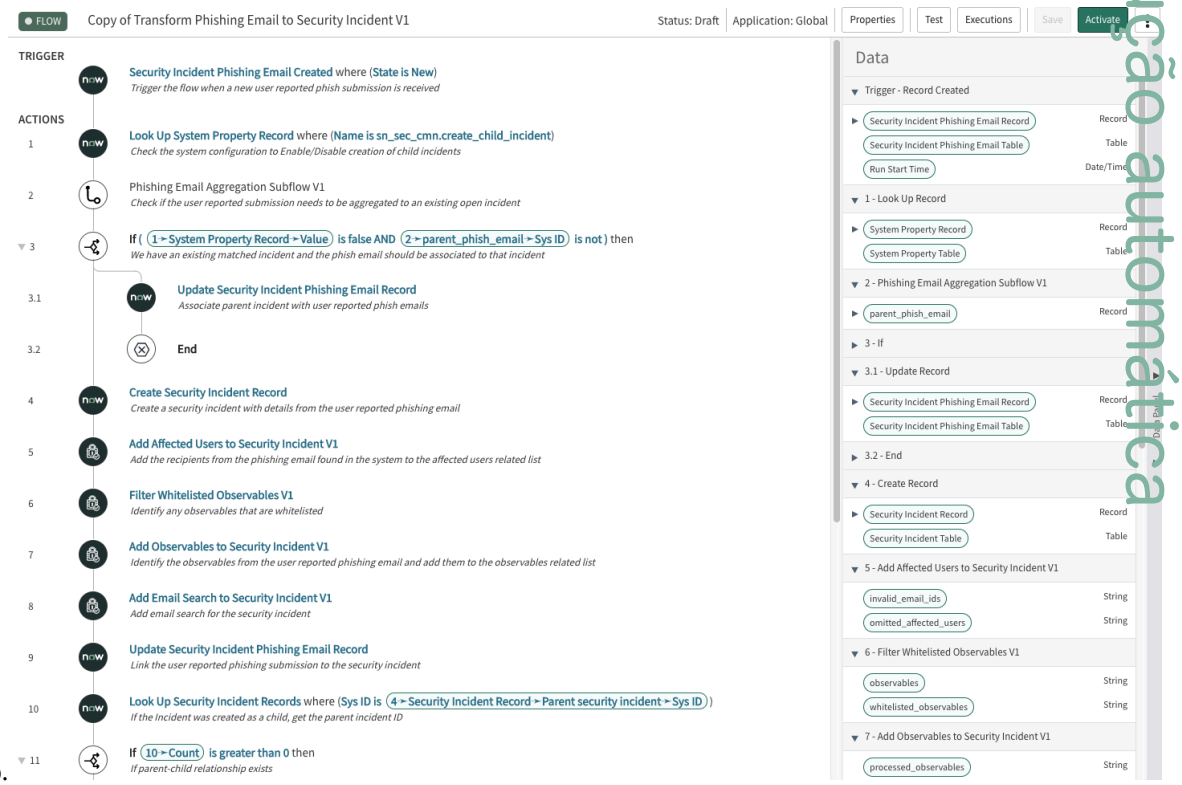
Procedimento

- Navegar até **Flow Designer** > **Designer** Para exibir os fluxos disponíveis com o spoke de Operações de segurança.



- Clique em **Transformar e-mail de phishing em incidentes de segurança** link para exibir o fluxo.
- Este fluxo é fornecido com o sistema de base e está em **Somente leitura** e não podem ser usados.

  Clique no ícone Mais , faça uma cópia do fluxo e abra-o para seu uso. Agora você pode fazer mudanças em seu fluxo, como modificar condições ou ações do gatilho ou adicionar e remover ações. Depois de fazer as mudanças necessárias, você deve ativar (consulte Ativar um Resposta a incidentes de segurança fluxo o fluxo para que ele possa ser executado.



  Esta figura mostra o gatilho e as etapas executadas com o fluxo. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

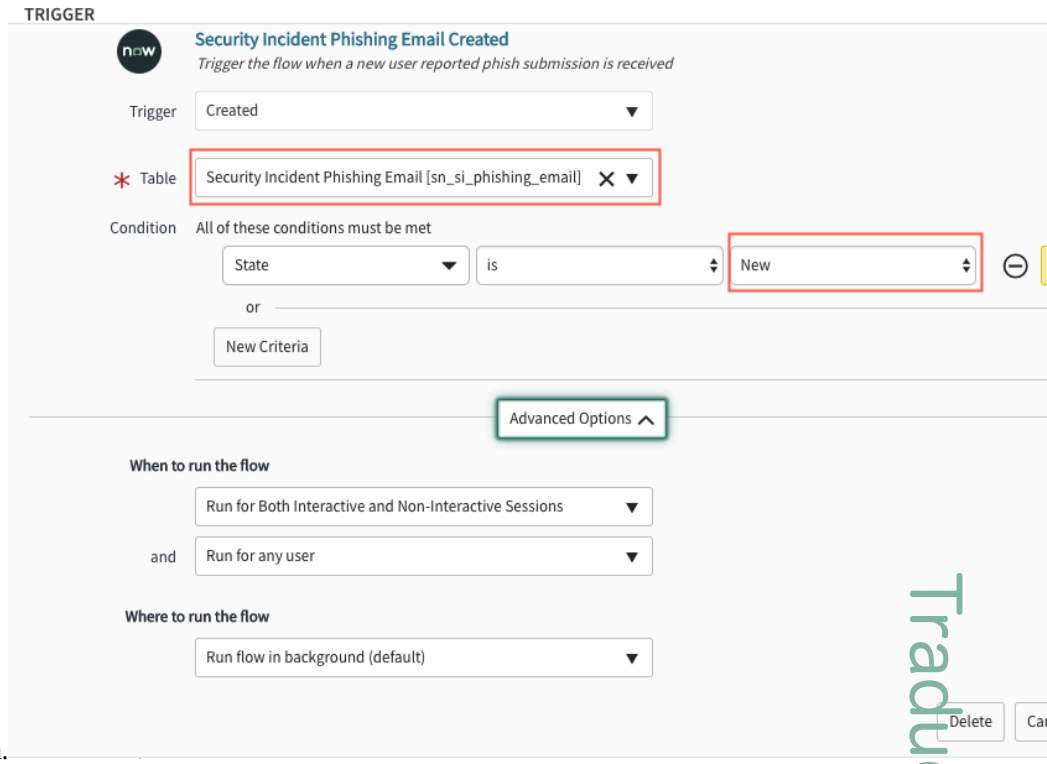
- Clique em **Gatilho** ícone.

  Na primeira etapa, você define ou define o gatilho para o fluxo. Especifique as condições para o gatilho e a tarefa a serem executados quando as condições

Tradução automática

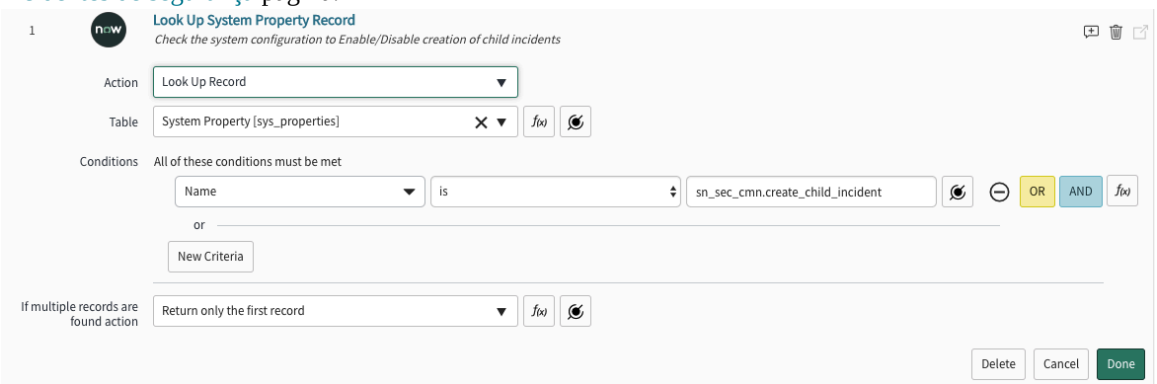
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

forem atendidas. Este fluxo é iniciado quando um **Novo** o registro é carregado no

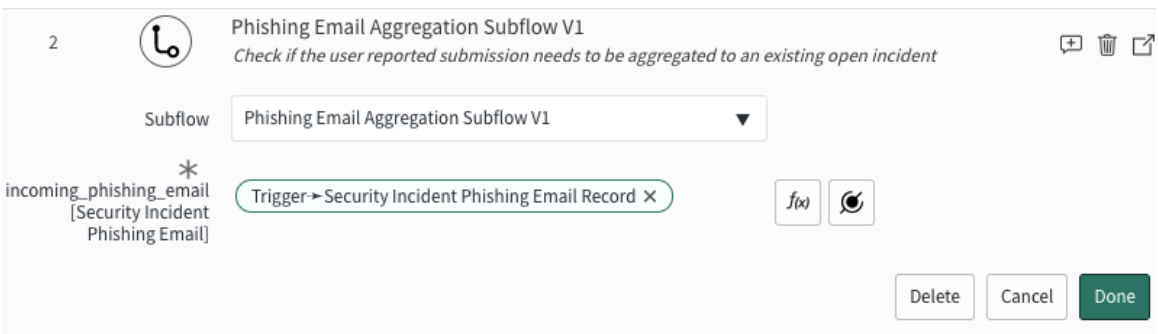


`sn_si_phishing_email`tabela.

- Na etapa 1, o fluxo verifica se **Criar incidentes secundários para envios de e-mail agregados?** o sinalizador está habilitado ou desabilitado em Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança página.



- Na etapa 2, o incidente de segurança primário mais antigo é identificado.
  Observe o ícone na etapa 2. Indica que o subfluxo Agregação de e-mail de phishing será executado como parte desta

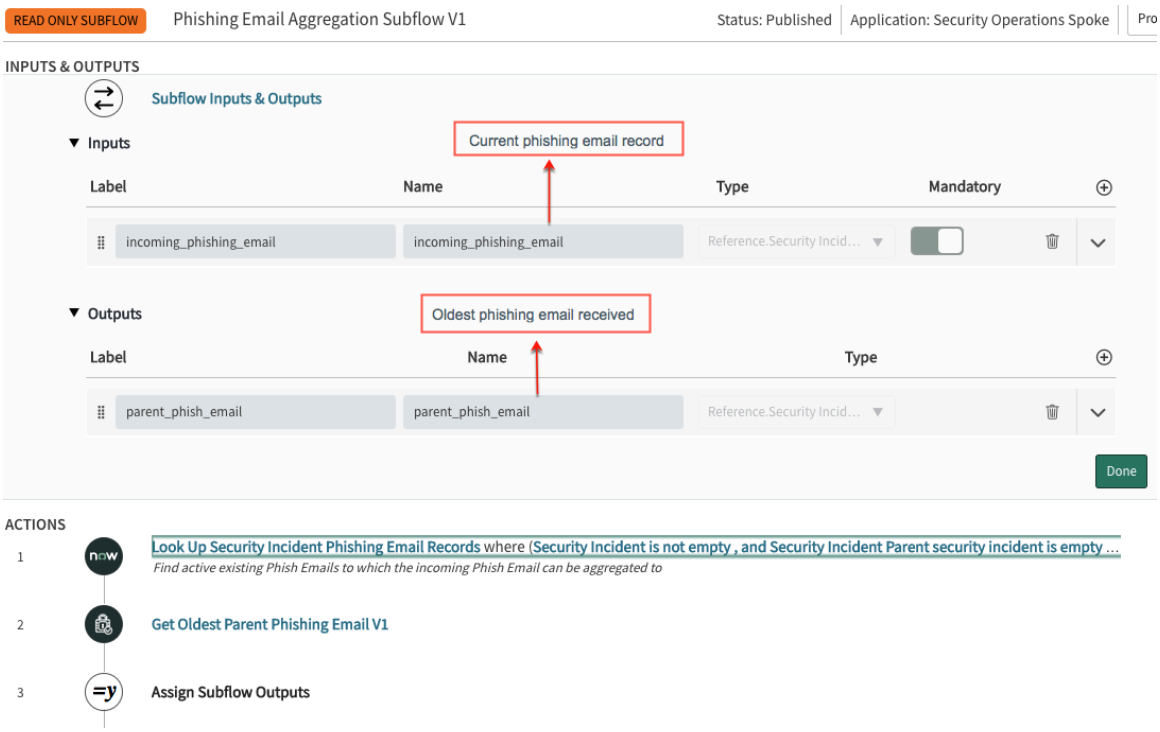


etapa.

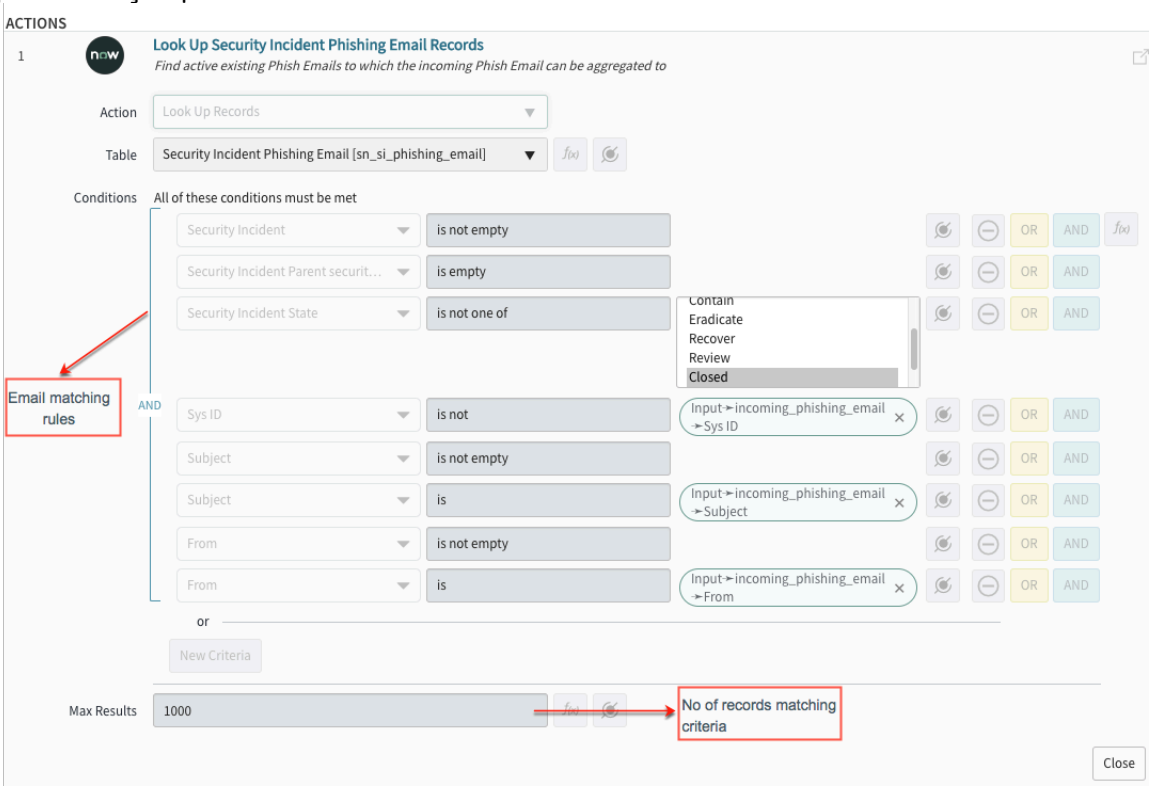
Clique no ícone do designer de ação para ver uma exibição detalhada da ação. Este subfluxo verifica o e-mail de phishing e o corresponde a um incidente de segurança existente com base nos critérios especificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Essas duas ações são executadas quando este subfluxo é executado. Clique no link da primeira ação para exibir detalhes adicionais.



Esta ação verifica os e-mails que correspondem aos critérios do novo e-mail de entrada com base em condições como:

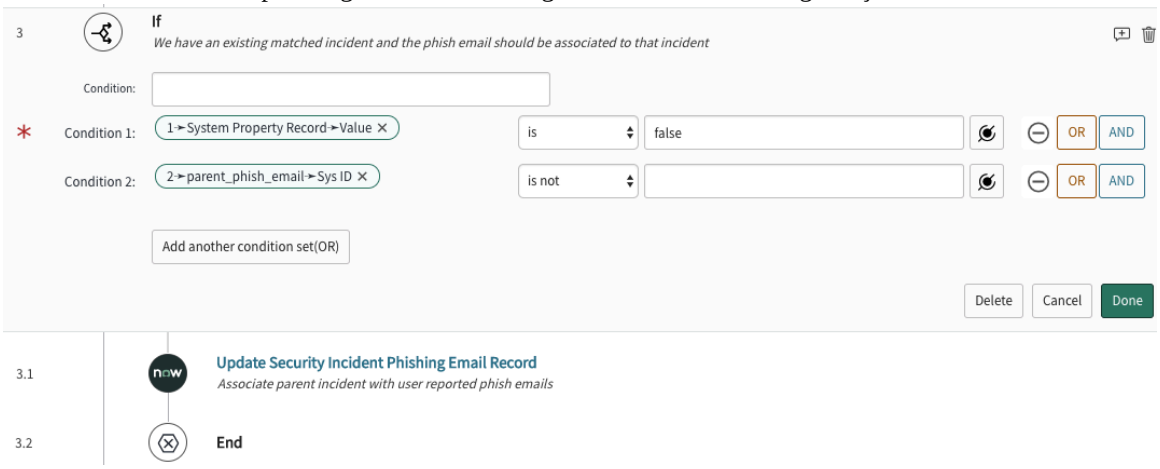
- O estado do incidente de segurança não é **Encerrado** .
- O valor de assunto ou de origem corresponde às condições da regra de correspondência de e-mail definidas (consulte Configure regras de ingestão para phishing relatado pelo usuário).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se essas condições forem atendidas, você poderá ver o número de registros que correspondem aos critérios no campo Máximo de resultados. O registro mais antigo ou o primeiro na lista é designado como o registro primário em relação ao qual os incidentes de segurança serão agregados.

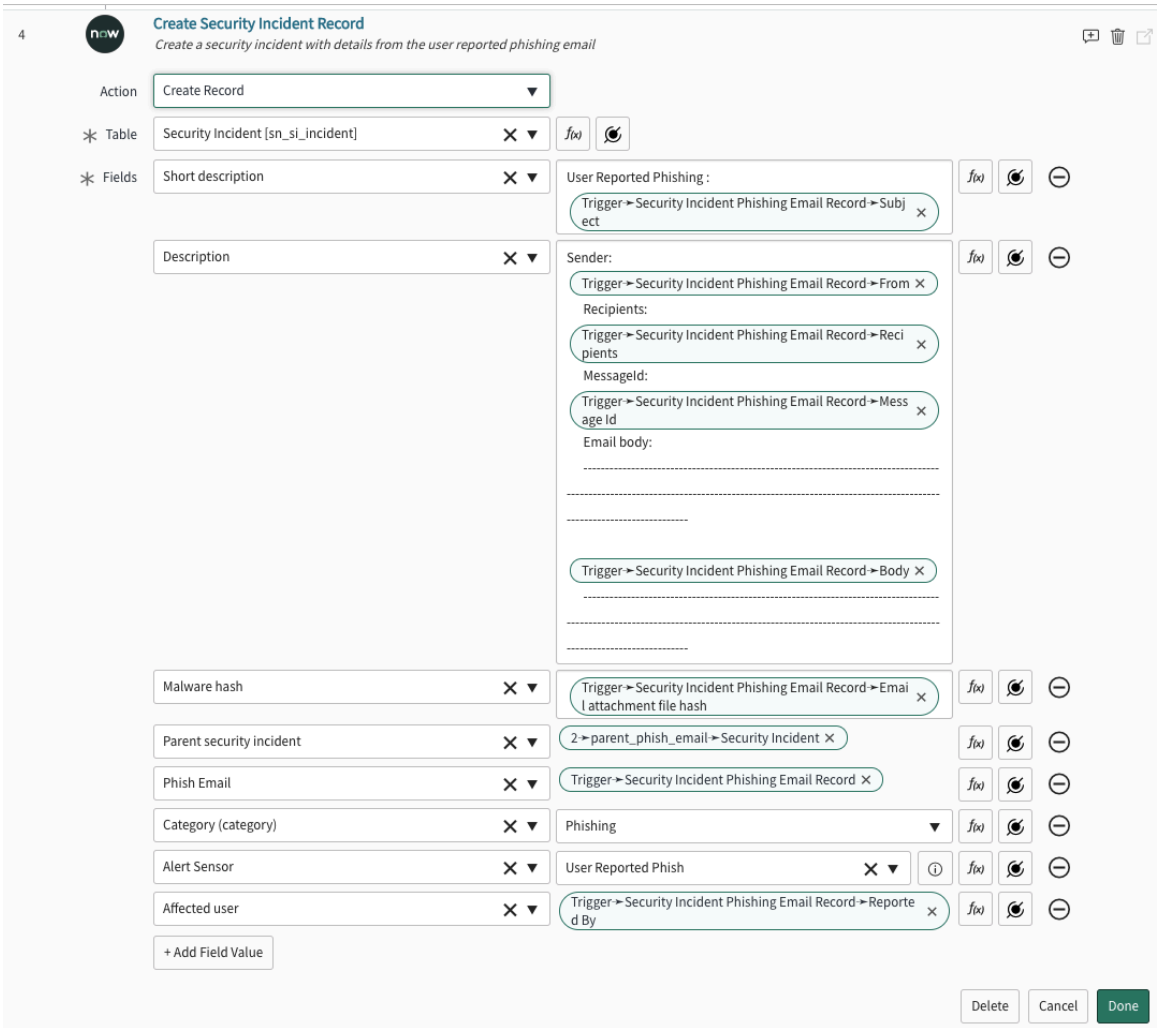
- A etapa 3 será aplicável somente se **Criar incidentes secundários para envios de e-mail agregados?** o sinalizador foi definido como **Não** em Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança página.
  Nesse caso, o e-mail de phishing é associado ao registro de incidente de segurança e o fluxo é encerrado.



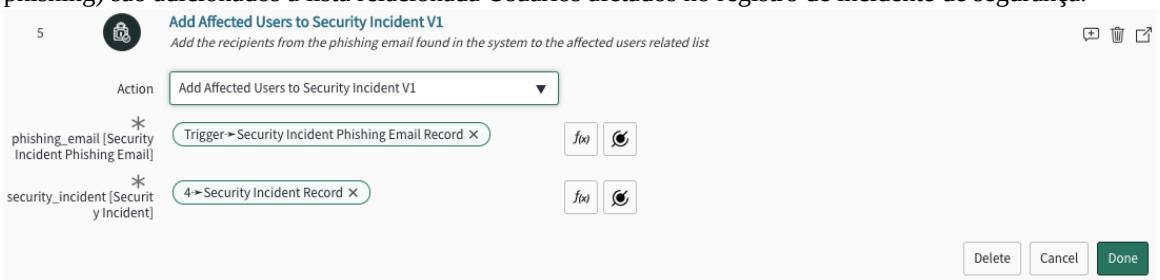
- . **Criar incidentes secundários para envios de e-mail agregados?** definido como **Sim** , o fluxo continua a ser executado e um novo incidente de segurança é criado com base no e-mail de phishing relatado pelo usuário.

Tradução automática

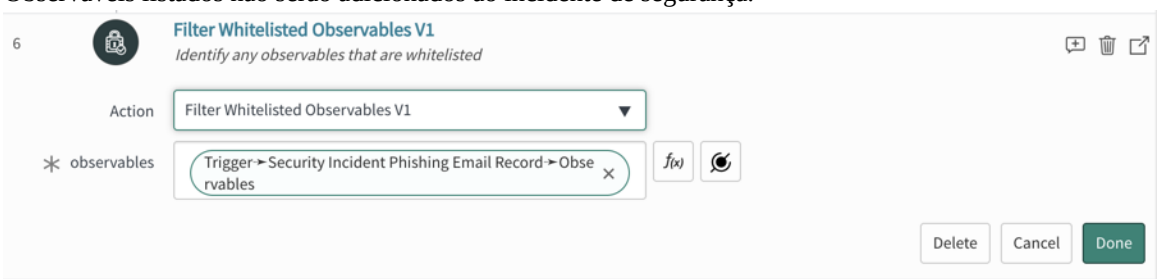
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Na etapa 5, os usuários que receberam o e-mail de phishing (funcionários na lista Para e CC do e-mail de phishing) são adicionados à lista relacionada Usuários afetados no registro de incidente de segurança.



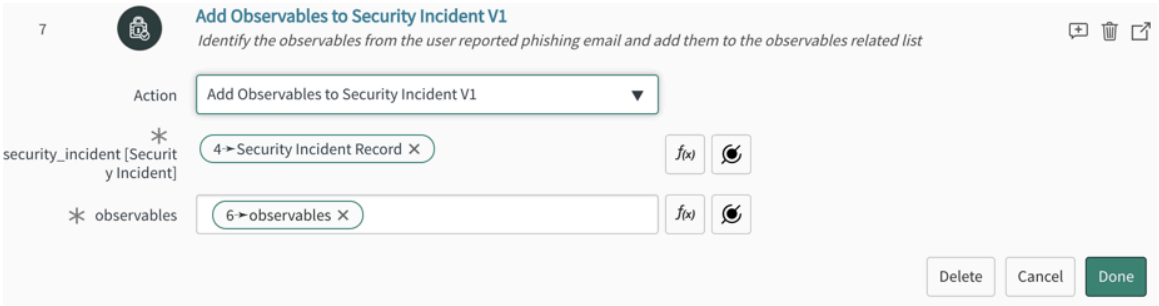
- Na etapa 6, Permitir observáveis listados são filtrados da lista de observáveis no incidente de segurança. Observáveis listados não serão adicionados ao incidente de segurança.



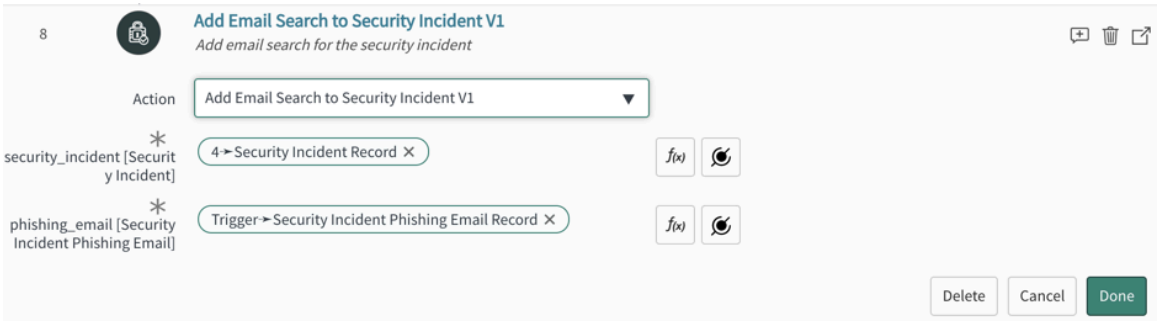
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

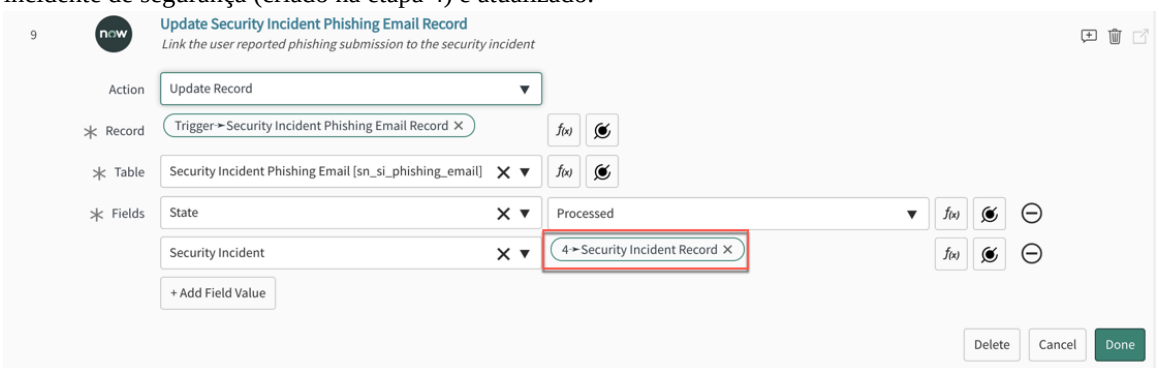
- Na etapa 7, observáveis desconhecidos do e-mail de phishing relatado pelo usuário são identificados e adicionados à lista relacionada de observáveis.



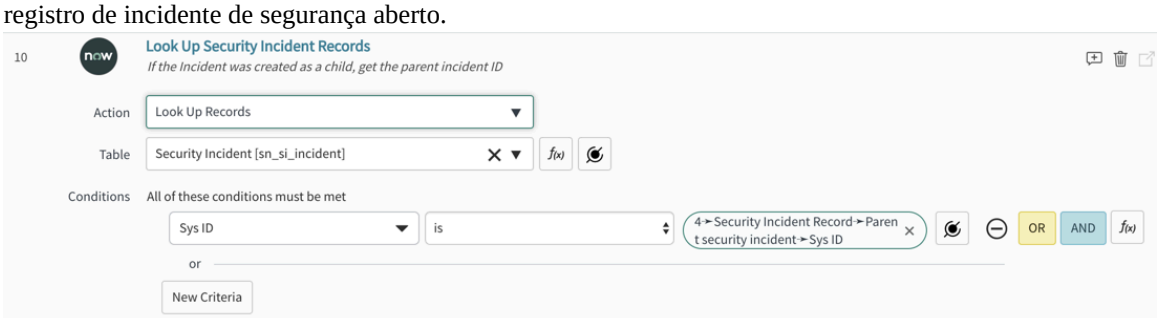
- Na etapa 8, uma consulta de pesquisa de e-mail é gerada, que é uma combinação do assunto e do endereço do remetente do e-mail.
  Essas informações são úteis para identificar os funcionários na organização que foram submetidos a phishing.



- Na etapa 9, o e-mail de phishing relatado pelo usuário é associado ao incidente de segurança e o registro do incidente de segurança (criado na etapa 4) é atualizado.



- Na etapa 10, o incidente de segurança primário é identificado e uma verificação é feita para ver se é um registro de incidente de segurança aberto.

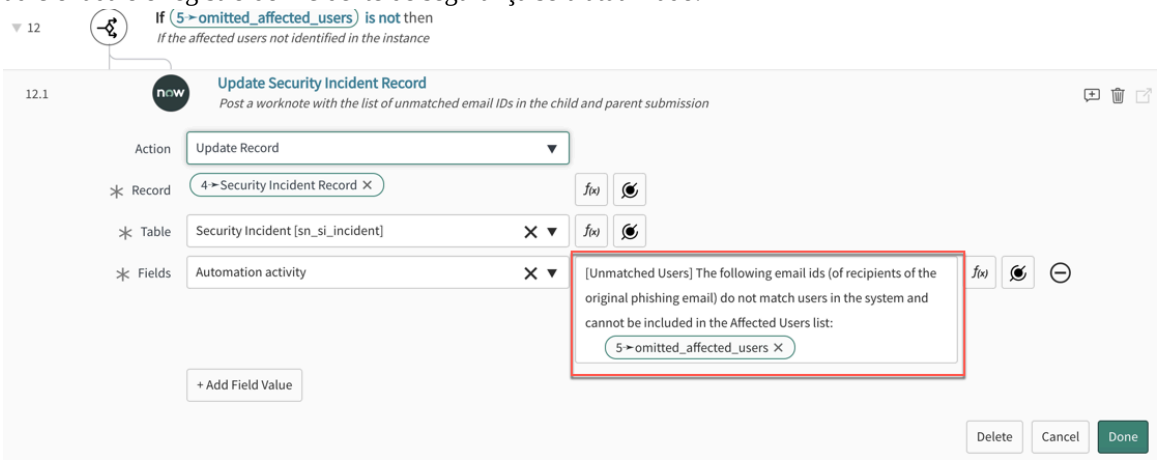


- Se a segurança primária estiver ativa, anotações serão adicionadas aos registros de incidente de segurança secundário e primário indicando como eles estão associados uns aos outros.

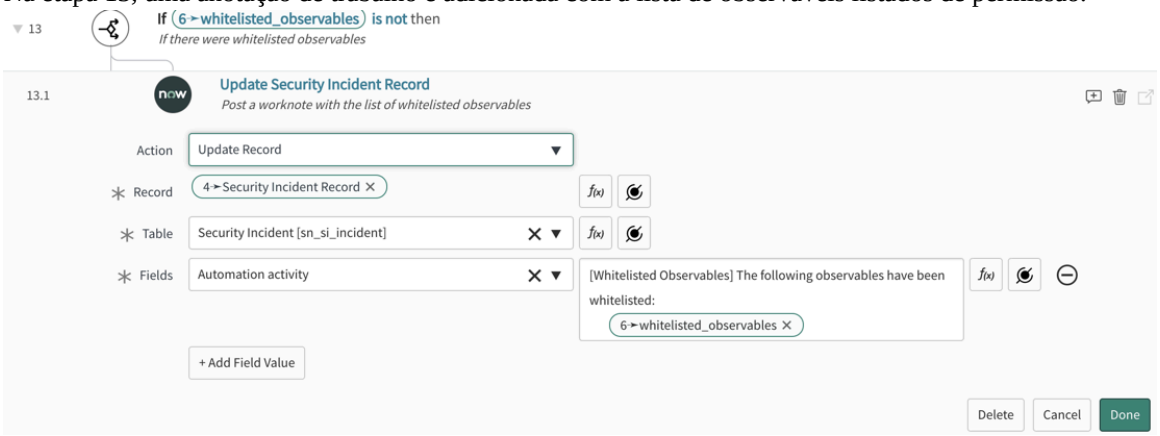
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na etapa 12, se nenhum usuário afetado for encontrado (na etapa 5 do fluxo), uma anotação de trabalho será adicionada e o registro do incidente de segurança será atualizado.



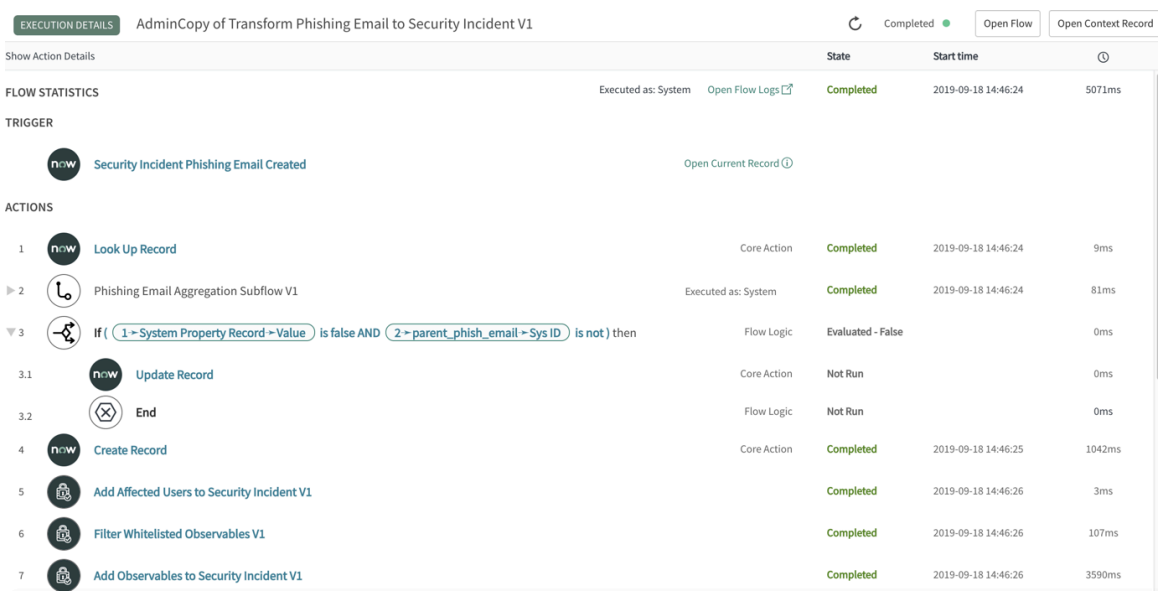
- Na etapa 13, uma anotação de trabalho é adicionada com a lista de observáveis listados de permissão.



O que Fazer Depois

Você pode clicar em **Teste** simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.



Tradução automática

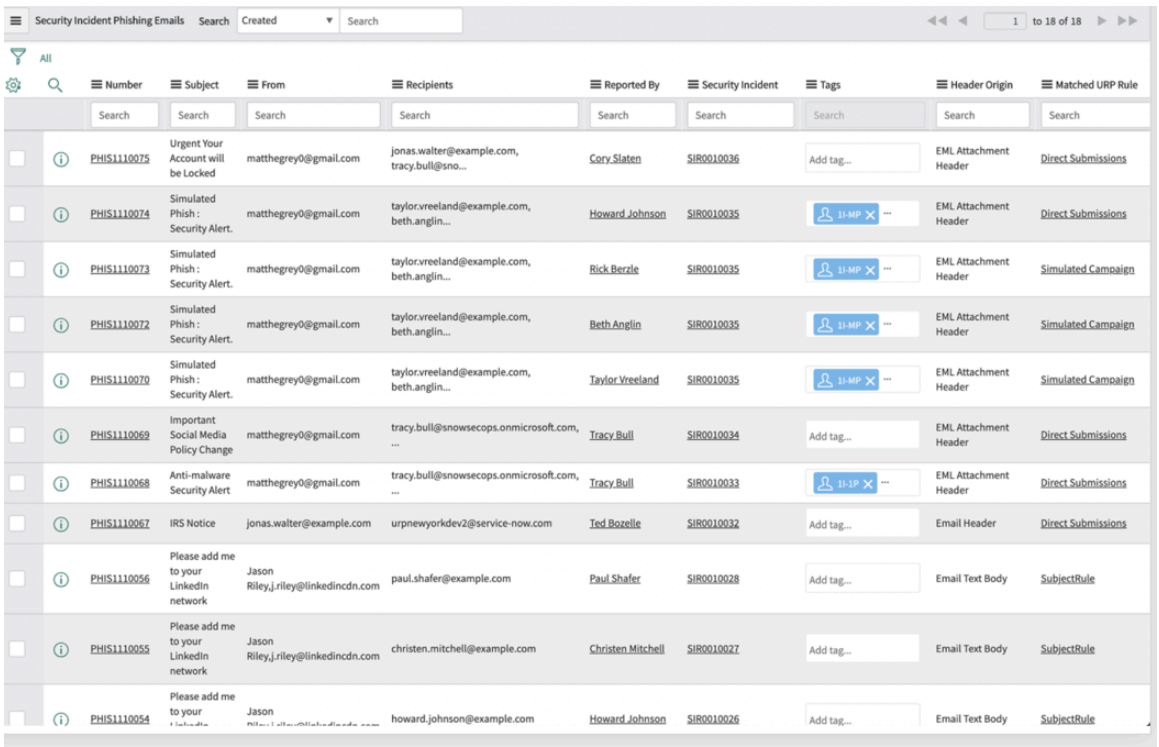
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o fluxo é executado, o registro de e-mail de phishing é convertido em um incidente de segurança. Veja Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

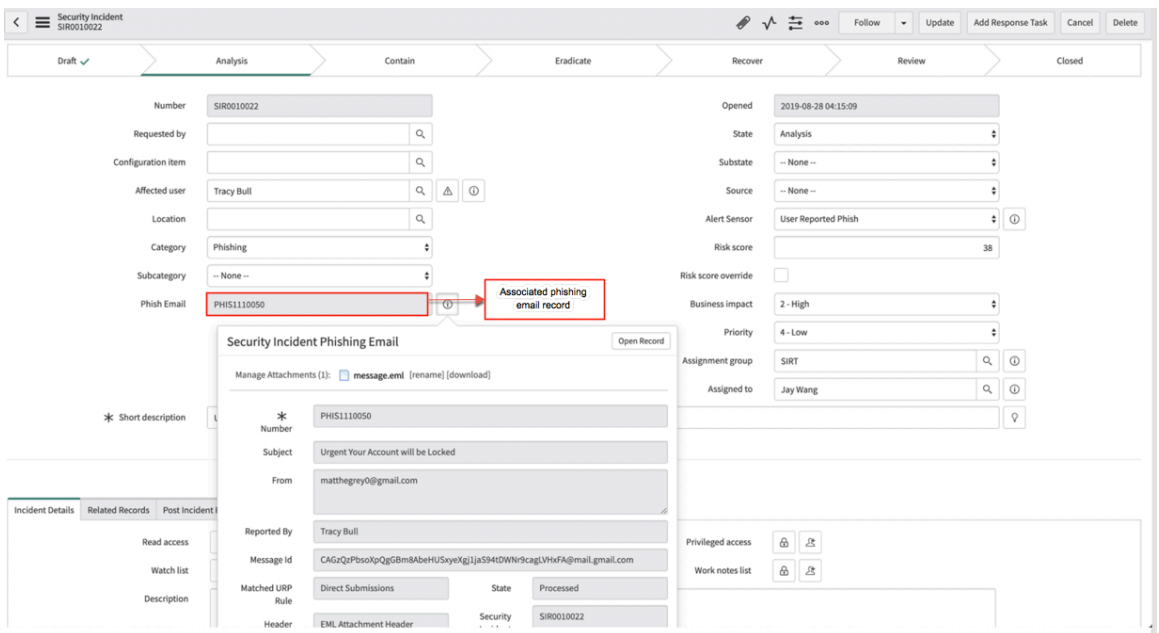
Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Registros de e-mail de phishing armazenados no `sn_si_phishing_email` as tabelas são convertidas em registros de incidentes de segurança.

Para exibir o incidente de segurança associado ao registro de e-mail de phishing, clique em **Incidente de segurança** > **E-mail de Phishing** > **Mostrar todos os e-mails de phishing**.



Clique no link na coluna Incidente de segurança associado ao registro de e-mail de phishing. Os detalhes do incidente de segurança são exibidos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

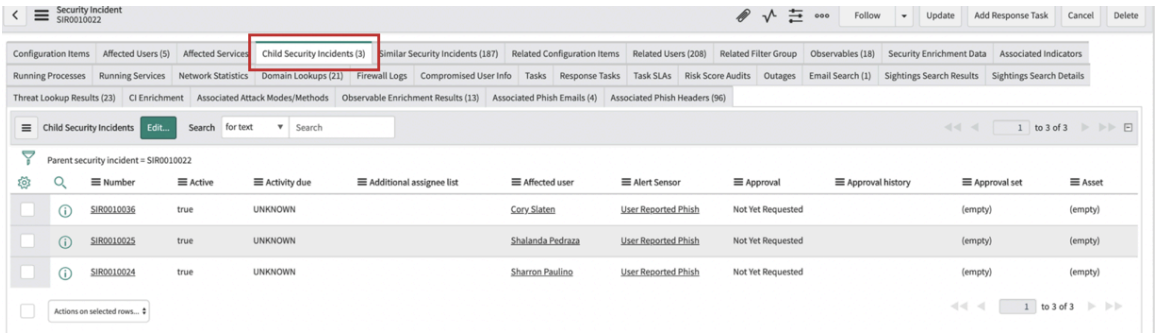
Listas relacionadas

Role para baixo até a seção Links relacionados do incidente de segurança e clique em **Mostrar todas as listas relacionadas** . Exiba detalhes como incidentes de segurança secundários, usuários afetados, e-mails de phishing associados.

Incidentes de segurança secundários

Clique em **Incidentes de segurança secundários** guia. Você pode ver uma lista de incidentes de segurança secundários associados ao incidente de segurança primário com base na lógica de agregação que foi aplicada. Para cada registro secundário adicionado, uma atividade automatizada do sistema é adicionada (na seção Anotação de trabalho) ao registro primário. Notifica o analista de segurança sobre o registro secundário agregado.

Nota: Você pode ver os incidentes de segurança secundários aqui somente se **Crie incidentes secundários para envios de e-mails agregados** o sinalizador está definido como **Sim** Na página Propriedades de phishing relatadas pelo usuário. Consulte Defina propriedades de phishing relatadas pelo usuário para obter detalhes.



E-mails de phishing associados

Clique em **E-mails de Phish associados** guia. Você vê uma lista de registros de e-mail de phishing (registros duplicados) associados ao registro de e-mail de phishing primário.

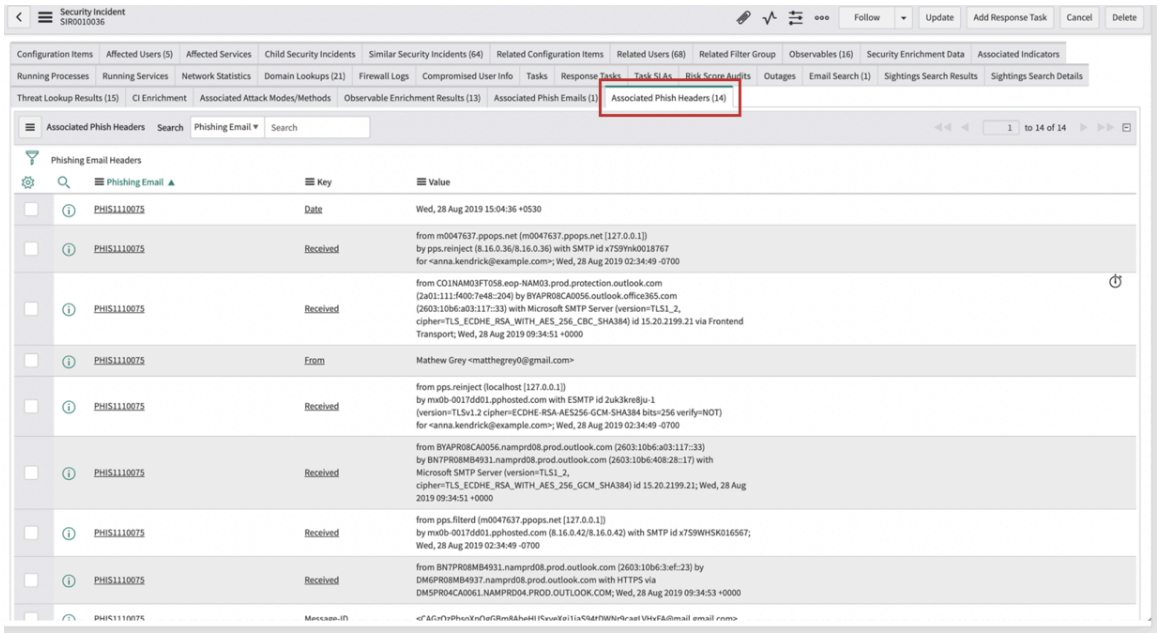


Cabeçalhos de e-mail de phishing associados

Clique em **E-mails de Phish associados** guia. Você vê os detalhes do cabeçalho do e-mail de phishing que foram capturados como parte do incidente de segurança. Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

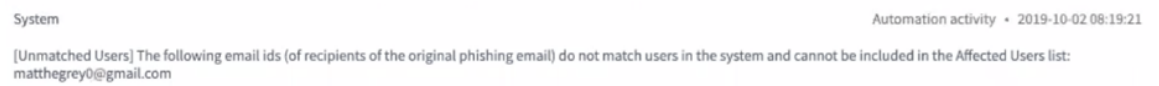


Observáveis de lista permitidos

. Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança o fluxo está sendo executado, você pode monitorar o status do incidente de segurança. Quando determinados observáveis são marcados como observáveis de lista permitidos, eles não são adicionados à lista relacionada de observáveis. Ao marcar os observáveis na lista de permissões, você pode garantir que somente os detalhes importantes sejam exibidos. Por exemplo, se www.google.com É um dos URLs que foi marcado como lista permitida, a seguinte mensagem do sistema é exibida. A lista de observáveis permitidos garante que somente os observáveis importantes sejam monitorados.

Capturar usuários incompatíveis

Alguns ids de e-mail na lista Para e CC do e-mail de phishing podem não pertencer a usuários da organização. Esses ids de e-mail são categorizados como usuários incompatíveis e não estão incluídos na lista relacionada Usuários afetados. Uma anotação de trabalho indicando que esses são usuários incompatíveis é exibida.



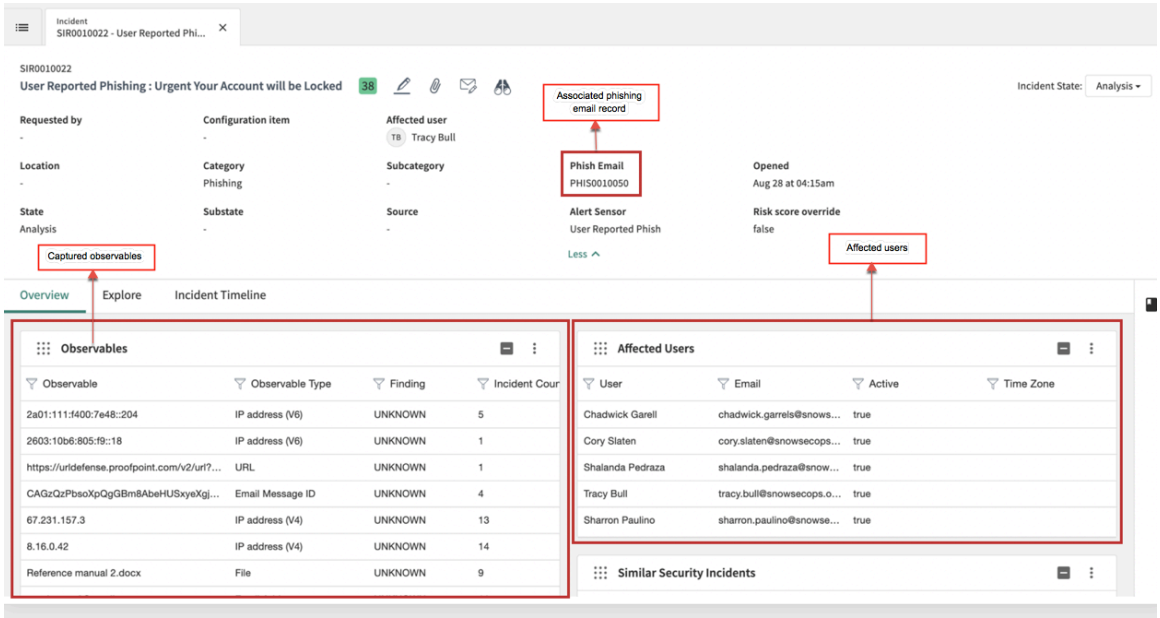
Phishing relatado pelo usuário no Espaço do analista de segurança

Você pode exibir incidentes de segurança associados aos registros de e-mail de phishing no Espaço do analista de segurança.

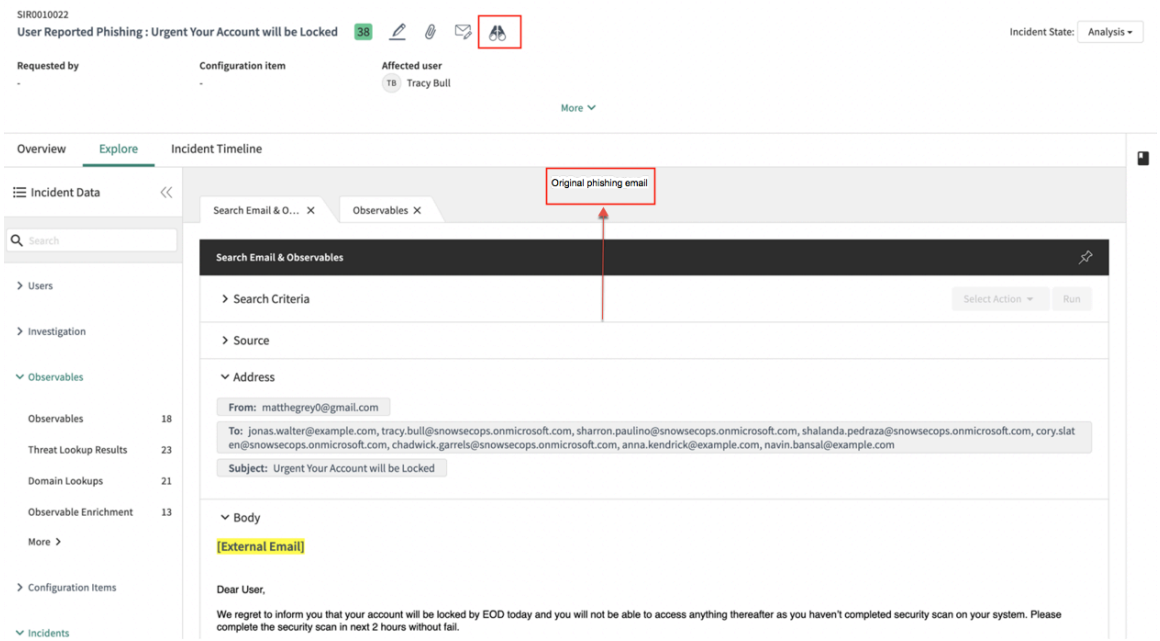
Navegar até **Incidente de segurança** > **Nova IU**. O espaço é aberto em uma guia separada do navegador. Clique no incidente de segurança associado ao registro de e-mail de phishing para exibir o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



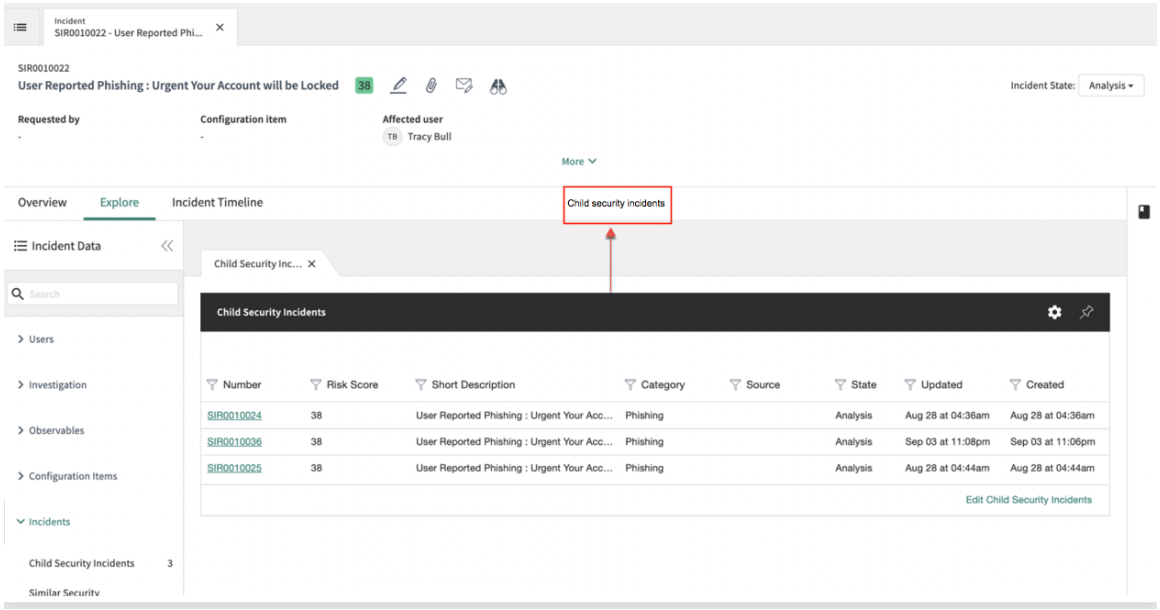
Clique no ícone de binóculos. O e-mail de phishing original é exibido.



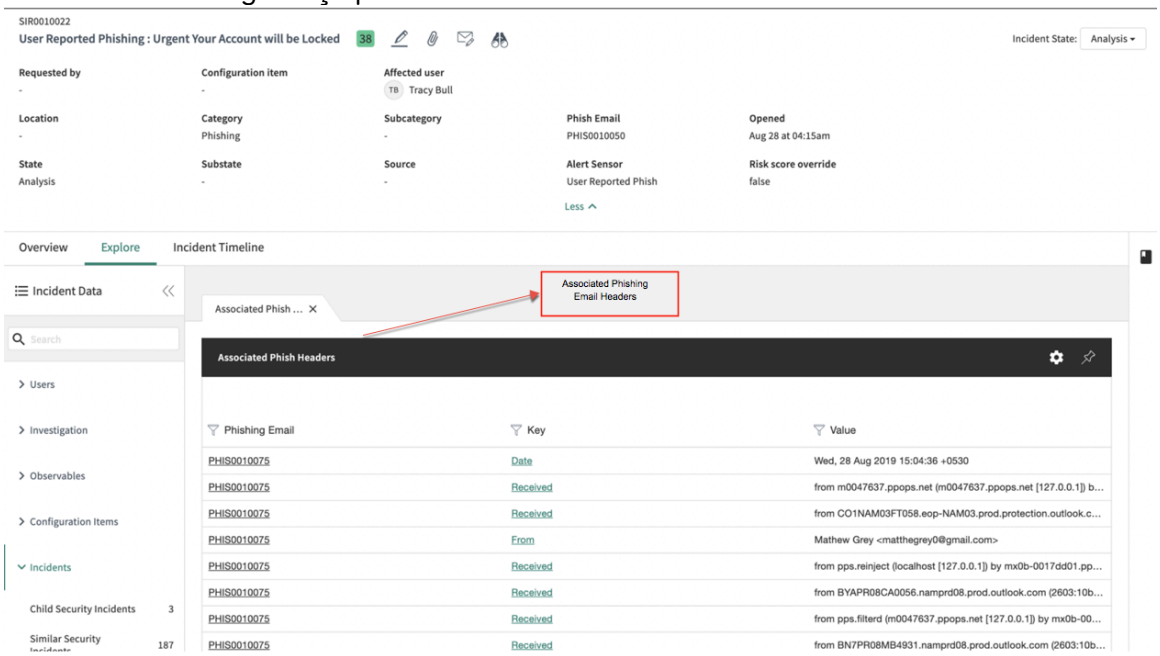
Em **Explorar** clique em **incidentes** > **Incidentes de segurança secundários**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



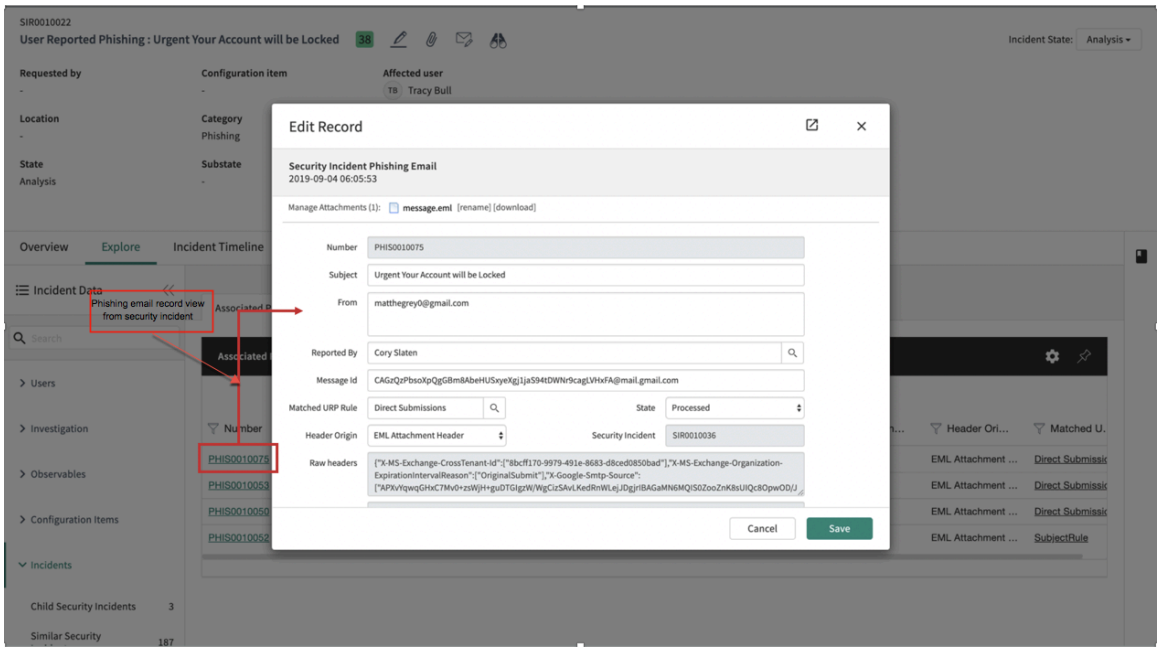
Clique **incidentes** > **Cabeçalhos de phishing associados** > . Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.



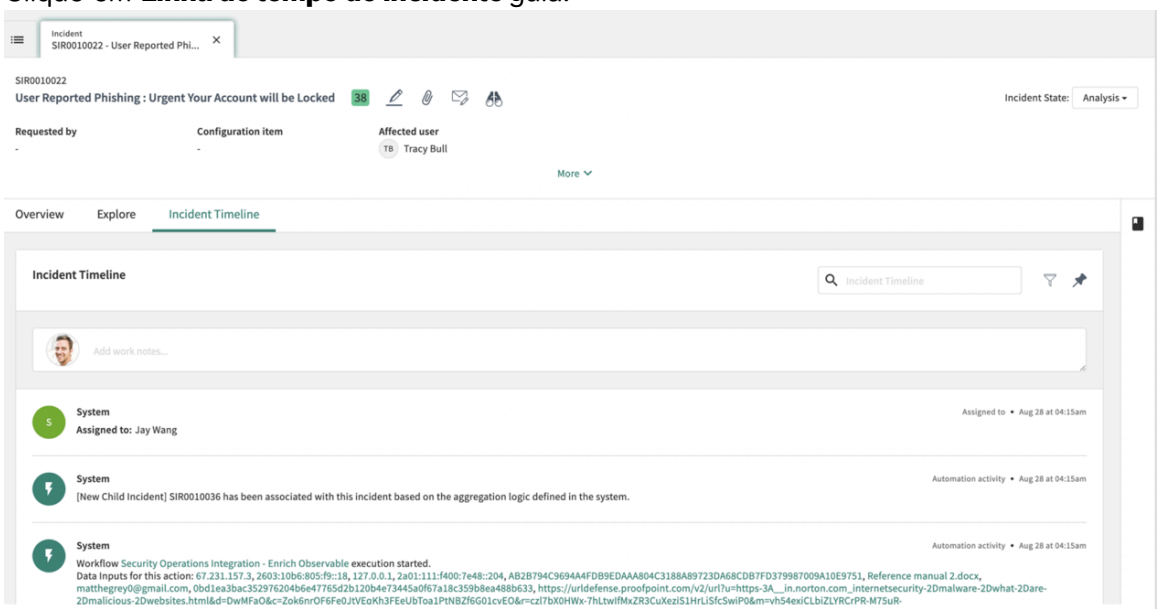
Clique no link do e-mail de phishing para exibir o registro de e-mail de phishing associado ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique em **Linha do tempo do incidente** guia.



Você pode exibir as atualizações do sistema que destacam:

- Registros secundários duplicados identificados.
- Observáveis de lista permitidos.
- Usuários incompatíveis que receberam o e-mail de phishing, mas não pertencem à lista de usuários afetados.

Perguntas frequentes

Esta seção aborda algumas das perguntas frequentes sobre o recurso aprimorado de Phishing relatado pelo usuário.

1. Instalei o novo spoke de resposta a incidentes de segurança, mas não consigo exibir nenhum incidente de phishing relatado pelo usuário.

   Por padrão, a funcionalidade de phishing relatado pelo usuário foi desabilitada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para habilitar este recurso, você deve fazer uma cópia do somente leitura Transforme e-mails de phishing relatados pelo usuário em incidentes de segurança e ative-o antes de usar.

2. Ao ingerir e-mails de phishing e convertê-los em incidentes de segurança, quais medidas de precaução são usadas para lidar com links e anexos maliciosos nos e-mails de phishing?

   . ServiceNow o scanner antivírus verifica anexos e links maliciosos. No entanto, para garantir que os analistas de segurança possam investigar os incidentes com precisão, o Resposta a incidentes de segurança a aplicação captura todos os artefatos que fazem parte de um e-mail de phishing. Mas a funcionalidade de phishing relatado pelo usuário silencia os links maliciosos no e-mail de phishing para que os analistas de segurança não cliquem acidentalmente nesses links. Em relação a anexos maliciosos, os analistas de segurança devem ser cautelosos ao baixá-los.

3. Capturamos todos os arquivos mal-intencionados que fazem parte dos e-mails de phishing para aprimoramento de incidentes de segurança?

   Sim, capturamos todos os arquivos dos e-mails de phishing. Esses detalhes estão disponíveis como parte dos observáveis de incidentes de segurança na forma de um hash de arquivo.

4. Enviamos arquivos e links maliciosos de e-mails de phishing para uma instância de área restrita para investigação?

   Atualmente, não oferecemos suporte a integrações de sandbox prontas para a investigação de arquivos e links maliciosos.

5. Há uma janela de tempo ou um gatilho que define a duração na qual os registros de e-mail de phishing duplicados de entrada são associados a um incidente de segurança primário?

   Registros de e-mail de phishing duplicados são agregados somente a um incidente de segurança primário ativo. Se o incidente primário for encerrado ou cancelado, o novo e-mail de phishing duplicado de entrada será criado como um novo incidente de segurança. Neste cenário, no novo incidente de segurança, você pode exibir o incidente de segurança primário encerrado ou cancelado no **Incidente de segurança semelhante** lista relacionada.

   Nota: Este comportamento pode ser configurado usando o Flow Designer.

6. O recurso Relatório de phishing do usuário oferece suporte ao uso somente do Microsoft Outlook **Phishalarm** Plug-in (anteriormente conhecido como wombat) para capturar detalhes do cabeçalho do e-mail?

   A funcionalidade relatada pelo usuário foi criada para analisar cabeçalhos de e-mail e está em conformidade com os padrões RFC822. Semelhante ao **Phishalarm** Plug-in (anteriormente conhecido como wombat), todos os outros plug-ins do Microsoft Outlook que capturam cabeçalhos de e-mail com base nos padrões RFC822 são compatíveis.

Criação de registro a partir de incidentes de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele. Você também pode criar um caso de atendimento ao cliente a partir de qualquer incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma mudança, incidente ou problema a partir de um incidente de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele.

Antes de Iniciar

Função necessária: sn.si_basic ou superior

Procedimento

1. Abra um incidente de segurança usando um desses métodos.
   - Abra um incidente de segurança existente navegando até **Incidente de segurança** > **Não atribuído** > **incidentes**e clicando em um incidente de segurança.
   - Navegue até para criar um incidente de segurança **Incidente de segurança** > **Não atribuído** > **incidentes**clique em **Novo** preencha o formulário e salve o registro.
2. Clique com o botão direito do mouse na barra de cabeçalho do incidente de segurança e clique em uma das seguintes opções:
   - **Criar Mudança**
   - **Criar Incidente**
   - **Criar Problema**

   Nota: Esta opção se aplica somente se a propriedade pop-up (sn_vul.popup) estiver habilitada. Quando você clica em um desses botões, uma janela de visualização é aberta para mostrar as informações do incidente de segurança que são usadas para criar a mudança, o incidente ou o problema. Ou seja, o item de configuração, sua localização, sua prioridade e as descrições curtas e longas. Se você estiver criando uma solicitação de mudança, poderá editar **Prioridade** , **Descrição resumida** e **Descrição** campos. Se você estiver criando um incidente, poderá editar o. **Impacto** , **Urgência** , **Descrição resumida** e. **Descrição** campos. Os campos na tela de incidente de segurança associada não são afetados.
3. Clique em **Enviar** para criar a mudança, o incidente ou o problema.

Crie um caso de Atendimento ao cliente a partir de um incidente de segurança

Resposta a incidentes de segurança fornecido com um mapeamento de campo padrão que mapeia um incidente de segurança para um Atendimento ao cliente(CS) Caso. Você pode criar um caso de CS a partir de qualquer incidente de segurança, editar o. **Prioridade** e também adicionar **Anotações opcionais** .

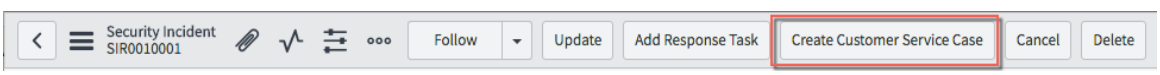
Antes de Iniciar

Função necessária: sn_si.basic e sn_customerservice_agent

Nota: . Atendimento ao cliente o plug-in deve ser ativado para executar esta tarefa.

Procedimento

1. Navegue até **Incidente de segurança** .
2. Abra o incidente de segurança ao qual você deseja adicionar um caso CS.
3. Clique em **Criar caso de Atendimento ao cliente** no cabeçalho superior.



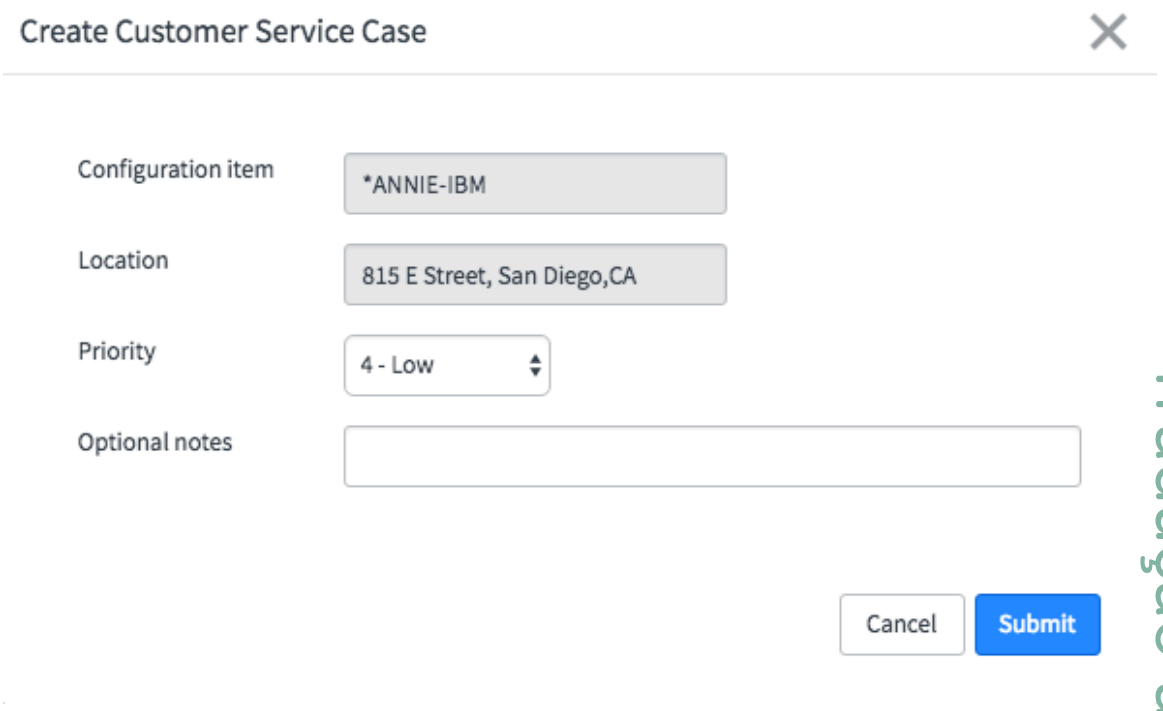
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A janela pop-up é preenchida previamente com informações do incidente de segurança com base no mapeamento de campo.

4. Você pode selecionar um novo **Prioridade** e adicione qualquer **Anotações opcionais** .

Nota: . **Prioridade** o campo substitui a configuração padrão. . **Anotações opcionais** são anexados ao incidente.



5. Clique em **Enviar**.
   Um caso de CS é criado e exibido na lista relacionada Casos de atendimento ao cliente no incidente de segurança.
6. Você pode clicar no link Caso de CS para acompanhar o caso.

Tópicos relacionados

Gestão de casos de atendimento ao cliente

Adicione um incidente de segurança a um caso de segurança

Se você determinar que um incidente de segurança requer um nível mais alto de análise, adicione-o a um caso novo ou existente.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

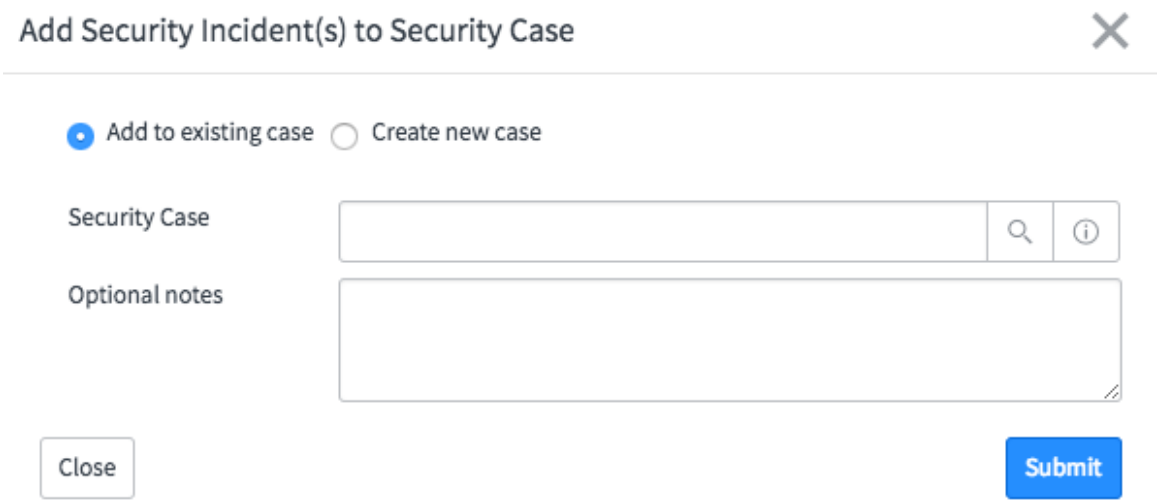
Função necessária: sn_si.admin, sn_ti.case_user_write

Procedimento

1. Navegue até o incidente de segurança que requer escalação clicando em **Incidente de segurança** > **incidentes** > **Atribuição a mim**e abra o incidente de segurança.
2. Clique em **Adicionar ao Caso de segurança** link relacionado.
   . **Adicionar Incidente(s) de Segurança ao Caso de Segurança** a caixa de diálogo é aberta.

Tradução automática

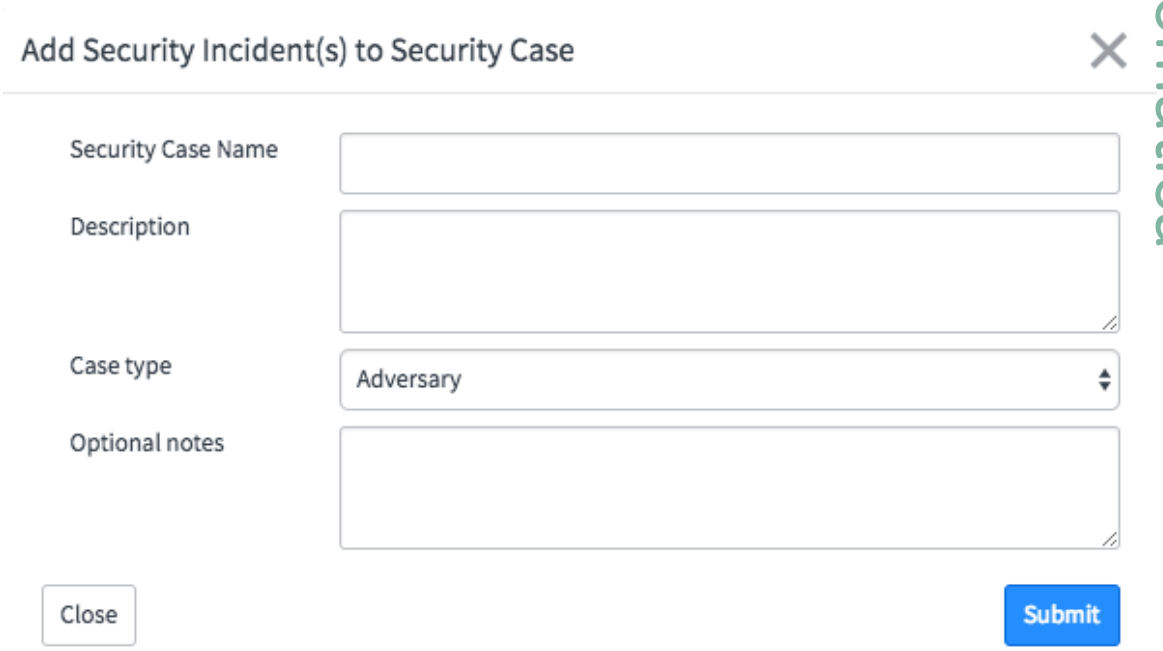
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Se você tiver um caso atribuído a você ao qual deseja adicionar este incidente de segurança, preencha os campos conforme apropriado e clique em **Enviar** .

Campo	Descrição
Caso de segurança	Selecione o caso de segurança.
Anotações opcionais	Conforme necessário, insira anotações adicionais que seriam de valor para o analista de caso.

4. Se você tiver um ou mais casos atribuídos a você, mas quiser criar um novo caso e atribuir o incidente de segurança a ele, clique em **Criar novo caso** para mostrar campos adicionais.



Nota: Se você não tiver nenhum caso atribuído a você, a tela acima será aberta primeiro.

5. Preencha os campos, se for o caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do caso de segurança	Insira o nome do novo caso de segurança.
Descrição	Insira uma descrição para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Anotações opcionais	Conforme necessário, insira anotações adicionais que seriam de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem aparece na parte superior do incidente de segurança, junto com um link para o novo caso.

Tópicos relacionados

Security Case Management

Criar tarefas de resposta

Após a criação de um incidente de segurança, você pode criar tarefas de resposta para rastrear ações separadas a serem executadas para responder ao problema de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegue até o local apropriado para abrir o incidente de segurança para o qual você deseja criar tarefas.
   Por exemplo:
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído a você, selecione **Incidente de segurança** > **incidentes** > **Atribuição a mim**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído à sua equipe, selecione **Incidente de segurança** > **incidentes** > **Atribuído à Equipe** > **incidentes**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança não atribuído, selecione **Incidente de segurança** > **incidentes** > **Incidentes não atribuídos**.
2. Abra o incidente de segurança para o qual você deseja adicionar tarefas de resposta.
3. Clique em **Adicionar tarefa de resposta** botão no cabeçalho do formulário.

   Nota: Para criar qualquer outra tarefa, clique em **Tarefas** Na Lista relacionada de incidentes.

4. Preencha os campos no formulário, conforme o apropriado.

Incidente de segurança

Campo	Descrição
Selecione marcador de segurança	Se você configurou e ativou marcadores de segurança , você pode selecionar um ou mais marcadores para adicionar metadados ao registro ou especificar o grau de sensibilidade da tarefa de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Número	[Somente leitura] O gerado automaticamente Resposta a incidentes de segurança número.
Primário	[Somente leitura] O número do incidente de segurança relacionado.
Item de Configuração	O item de configuração (recurso) afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Prioridade	A prioridade usada para determinar quando esta tarefa é executada.
Estado	O estado atual da tarefa de resposta de segurança. Na criação da tarefa, este campo é padronizado como **Rascunho** .
Habilidades	A habilidade necessária para executar esta tarefa. Clique no ícone de cadeado e selecione a habilidade necessária. Depois de concluir suas seleções, clique no ícone de cadeado novamente.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuição a	O indivíduo atribuído para executar a tarefa.
Descrição resumida	Uma descrição do Resposta a incidentes de segurança tarefa.
Descrição	Uma descrição da tarefa selecionada.
Notas de segurança	As anotações de trabalho criptografadas e não visíveis para o cliente.
Anotações de trabalho	As anotações de trabalho que não estão visíveis para o cliente.
Comentários adicionais	Comentários que você deseja que fiquem visíveis para o cliente.

5. Ao concluir suas entradas, clique em **Enviar** .

> **Nota:** Depois de criar Resposta a incidentes de segurança tarefas, você pode exibi-las usando qualquer uma das seguintes aplicações em **Tarefas de resposta** módulo:

- **Atribuído a mim** .
- **Atribuído à equipe** .
- **Mostrar tarefas em aberto**
- **Mostrar todas as tarefas**
- **Tarefas não atribuídas** .

Gerenciar Inteligência preditiva para phishing relatado pelo usuário

O recurso Inteligência preditiva para phishing relatado pelo usuário fornece uma solução significativa na triagem e priorização de e-mails de phishing relatados pelo usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta seção descreve o seguinte:

- Inteligência preditiva para phishing denunciado por usuários
- Plug-ins e componentes necessários
- Geração de veredito final para phishing relatado pelo usuário
- Solução de problemas de Inteligência preditiva para phishing relatado pelo usuário

Inteligência preditiva para phishing denunciado por usuários

Este recurso ajuda os analistas de segurança a fazer a triagem e priorizar os e-mails de phishing relatados pelo usuário.

A estrutura de Inteligência preditiva fornece soluções para treinar o sistema a prever, recomendar e organizar resultados de dados. Para obter mais detalhes sobre inteligência preditiva, consulte Inteligência preditiva . Usando essa estrutura, você pode criar modelos para prever automaticamente se um e-mail de phishing relatado pelo usuário é suspeito ou legítimo.

Usando dados históricos de incidentes de segurança de phishing relatados pelo usuário (cabeçalhos de e-mail, corpo do e-mail e resultados de triagem capturados por meio dos códigos de fechamento de incidentes de segurança), os analistas de segurança podem treinar o sistema para classificar os envios de phishing relatados pelo usuário de entrada como aqueles que precisam ser triados (provavelmente suspeitos) e aqueles que são envios legítimos.

Ao fazer a triagem automática dos e-mails recebidos, os analistas de segurança podem priorizar facilmente a fila de incidentes e se concentrar nos incidentes que provavelmente representarão um risco para a organização, além de gastar menos esforço em e-mails que provavelmente serão falsos positivos. O resultado da previsão também fornece uma pontuação de confiança na classificação para habilitar a priorização granular.

Plug-ins e componentes necessários

Para usar a Inteligência preditiva para phishing relatado pelo usuário, você deve instalar os seguintes aplicativos

Nome do plug-in	Versão mínima
Resposta a incidentes de segurança	9.0.1 ou 10.0.2
Inteligência preditiva	Versão Orlando
Inteligência preditiva para phishing denunciado por usuários	10.0.2

Nota: Os seguintes novos aprimoramentos estão disponíveis com o Security Incident Response 10,4:

- A capacidade de escolher códigos de fechamento de campos personalizados para treinamento de modelo.
- A capacidade de ativar explicitamente previsões após a criação do modelo.
- A capacidade de gerar um veredito final sobre o envio de phishing relatado pelo usuário usando uma tabela de decisão. (Requer o spoke de Operações de segurança 10,3.0)

Para usar os novos aprimoramentos, você deve fazer upgrade das seguintes aplicações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do plug-in	Faça upgrade para
Resposta a incidentes de segurança	10.0.4
Inteligência preditiva para phishing denunciado por usuários	10.3.1

Tabelas novas e atualizadas

- sn_sir_ml_urp_config (Novo): Contém a configuração da aplicação URP ML.
- sn_sir_ml_urp_feature (Novo): Registros extraídos da tabela de e-mail sn_si_phishing.
- sn_sir_ml_urp_feature_import (Novo): Usado para carregar dados históricos de e-mail de phishing.
- sn_si_incident (atualizado): Os seguintes novos campos foram adicionados:
  - Previsão aceita
  - Resultado da previsão
  - Pontuação de confiança
- **Inclusões de script**
  - URPMLUtil: Recupera a configuração, executa o trabalho de previsão e rastreia o processo de previsão.
  - URPMLProcessor: Extrai e processa dados da tabela sn_si_phishing_email.
  - URPMLAction: Executa o fluxo para aceitar o resultado da previsão.

Geração de veredito final para phishing relatado pelo usuário

As equipes de resposta a incidentes de segurança agora podem conduzir o veredito finalizado para um registro de phishing relatado pelo usuário com base nos resultados da inteligência preditiva e nas integrações de aprimoramento de ameaças.

Esta geração de veredito final é habilitada por meio de uma construção de tabela de decisão e aproveitada em um fluxo.

Pré-requisitos

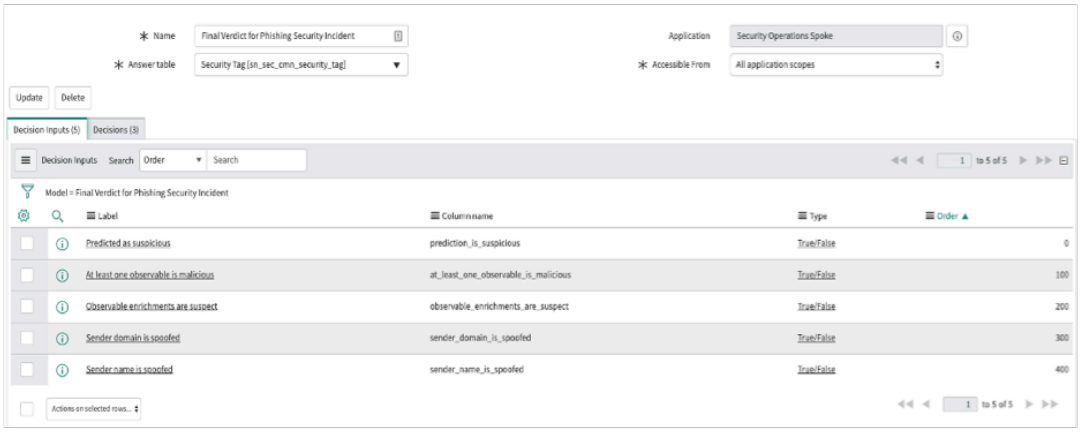
Todos os plug-ins listados em Plug-ins e componentes necessários foram instalados.

Navegar até **Inteligência preditiva para phishing** > **Veredito final** > **Veredito final para incidente de segurança de phishing**.

. **Entradas de decisão** mostra as diferentes condições que foram avaliadas para chegar ao veredito final.

Tradução automática

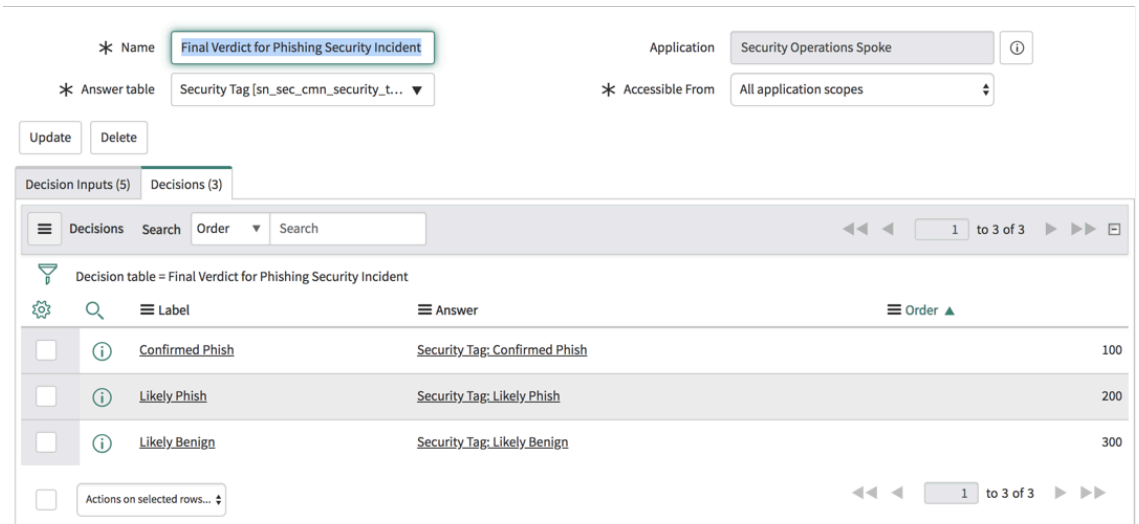
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As seguintes condições estão disponíveis com o sistema de base:

- Previsto como suspeito: Quando a inteligência preditiva classifica o e-mail de phishing relatado pelo usuário como **suspeito** .
- Pelo menos um observável é mal-intencionado: Quando um observável envolvido no incidente de segurança (por exemplo, URL, Domínio, IP, Hash) foi classificado como **mal-intencionado** por fontes de inteligência contra ameaças.
- O aprimoramento de observáveis é suspeito: Quando o aprimoramento em observáveis (por exemplo, recente registro de domínio de phishing, país de registro de domínio de phishing) é considerado suspeito.
- O domínio do remetente é falsificado: Quando o domínio de e-mail do phisher é suspeito de falsificar um domínio confiável.
- O nome do remetente é falsificado: Quando o endereço de e-mail do phisher suspeita de falsificar um funcionário confiável de uma organização.

. **Decisões** mostra as opções de veredito finais que podem ser obtidas para um determinado incidente de segurança.



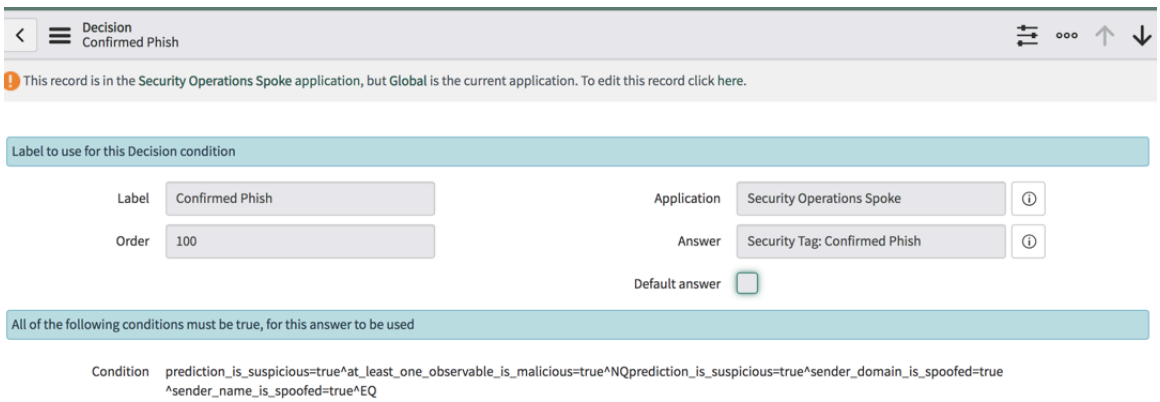
As seguintes decisões estão disponíveis com o sistema de base:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Phish confirmado: Quando as condições levaram ao veredito final como sendo um e-mail de phishing confirmado.
- Phish provável: Quando as condições levaram ao veredito final como uma possível tentativa de phishing.
- Provável benigno: Quando as condições levaram ao veredito final como uma submissão benigna.

Você pode ver as condições que foram avaliadas para cada uma das opções finais de veredito. Clique no link Rótulo para ver as condições.



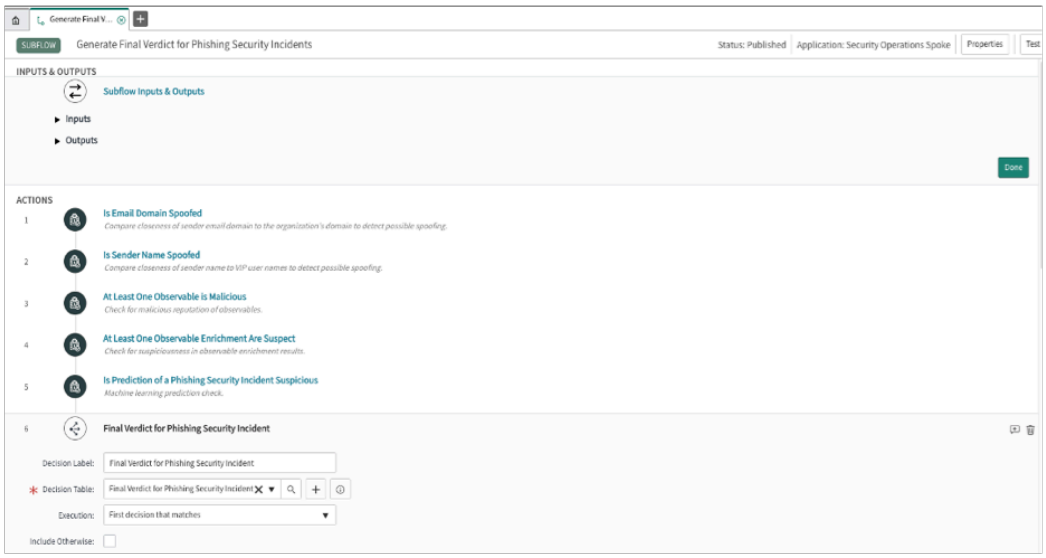
Você pode personalizar a tabela de decisão fornecida com o sistema de base ou criar sua própria tabela de decisão. Esta tabela de decisão pode ser aproveitada nos playbooks de resposta a incidentes de segurança. . **Gerar veredito final para incidentes de segurança de phishing** o subfluxo está disponível com o sistema de base. Este subfluxo gera automaticamente o veredito final de um incidente de segurança de phishing e aplica um marcador de segurança com base nessa decisão. Você pode incluir este subfluxo como parte do **Phishing automatizado** playbook.

As entradas para este subfluxo são:

- Incident_id: O sys ID do incidente de segurança de phishing.
- c_level_names: Lista separada por vírgulas de nomes (por exemplo, nomes de executivos na organização) que provavelmente estão sendo falsificados no ataque de phishing.
- Trusted_domains: Lista separada por vírgulas de domínios de e-mail confiáveis.
- Enrichment_keywords: Lista separada por vírgulas de palavras-chave que indicam a malícia do observável a partir dos resultados de aprimoramento.
- Sender_email (opcional): O endereço de e-mail do remetente do e-mail de phishing.

A saída desse fluxo pode ser **Phish confirmado** , **Phish provável** ou **Provável benigno** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solução de problemas de Inteligência preditiva para phishing relatado pelo usuário

Esta seção aborda alguns cenários de problemas comuns.

- Problema: Não consigo modificar a configuração da Inteligência preditiva.

  Solução: Verifique se você tem permissões para fazer isso. Você deve fazer login como um usuário com a função ml_admin para modificar os limites. Alguns cenários podem exigir privilégios ainda mais altos, como, por exemplo, você precisa modificar o limite de dados de treinamento. Para esses cenários, você deve entrar em contato com o Suporte ao cliente para obter assistência.

- Problema: Falha no treinamento do modelo.

  Solução: Verifique se os URLs do agendador DE ML foram configurados. Navegar até **Propriedades do sistema** > **Todas as Propriedades** e verifique se `glide.shared_service_scheduler.url` a propriedade foi configurada.

- Problema: Os resultados de previsão não estão disponíveis em um incidente de segurança.

  Solução:

  - Verifique se o URL da previsão foi configurado no `glide.prediction_service.url` Propriedade do sistema e verifique se o datacenter corresponde ao URL.
  - Verifique se o trabalho programado Prever e-mail de phishing relatado pelo usuário está ativo.

Configurar Inteligência preditiva para phishing relatado pelo usuário

Configure e prepare o modelo para identificar e-mails de phishing relatados pelo usuário.

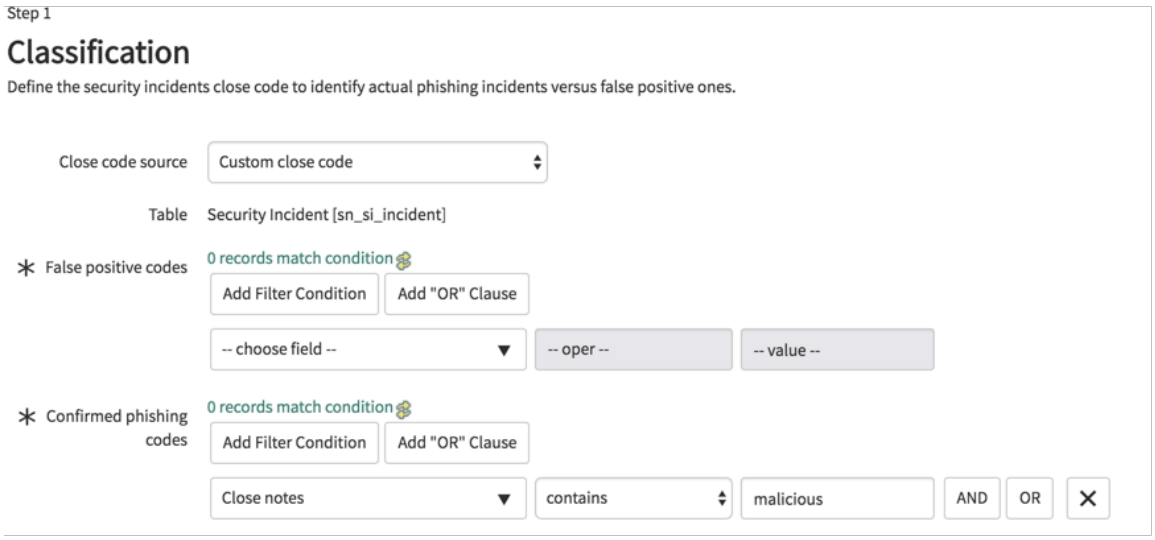
Antes de Iniciar
Função necessária: Ml_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência preditiva para phishing** > **Configuração**.
2. Na Etapa 1 da configuração, selecione uma das seguintes opções na lista Fechar origem do código:
   - Código de fechamento padrão: Selecione esta opção para especificar os códigos de fechamento de incidente de segurança padrão que devem ser usados pelo modelo de treinamento para identificar e-mails mal-intencionados e legítimos. Clique no ícone de cadeado e selecione um ou mais códigos de falso-positivo ou códigos de phishing confirmados.
   - Código de fechamento personalizado: Selecione a opção Código de fechamento personalizado se quiser definir códigos de fechamento de campos personalizados que podem ser usados como parte dos procedimentos de resposta a incidentes existentes. Para definir um código de fechamento, selecione um campo na tabela de incidentes de segurança e especifique uma ou mais condições de filtro.



3. Na Etapa 2, importe dados históricos que podem ser usados para treinar o modelo.
   Selecione a Fonte de dados para importar os dados históricos. Isso pode ser:
   - Tabela de e-mail de phishing relatado pelo usuário: Você pode ver o número de registros que podem ser importados como dados históricos. Selecione esta opção e clique em **Importação** .
   - Fonte de dados personalizada: Você pode anexar um único arquivo CSV formatado que contém registros de dados históricos. Selecione o arquivo e clique em **Importação** .

   Nota: O arquivo CSV importado deve conter os seguintes cabeçalhos:
   - Rótulo
   - Cabeçalho
   - Corpo do texto

   Cada registro deve conter um marcador malicioso ou legítimo na coluna Rótulo no arquivo CSV.

   Clique em **Cancelar importação** para parar de importar os dados. O processo de importação é cancelado e todos os registros importados até o momento são excluídos.
4. Depois de importar os dados históricos, clique no link para atualizar a página.
   Você pode importar mais dados de treinamento ou continuar com a próxima etapa.

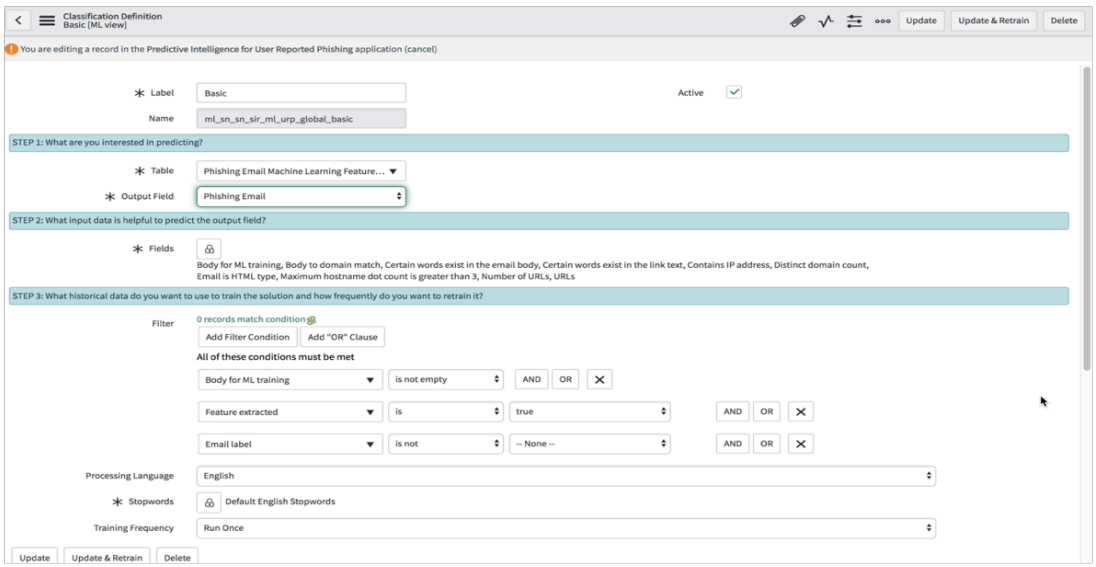
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na Etapa 3, verifique se o número de registros disponíveis para treinamento atende aos requisitos de limite mínimo.

   Nota: Os valores padrão para o número máximo e mínimo de registros de treinamento são exibidos. Esses limites podem ser modificados no Propriedades do aprendizado de máquina da plataforma página. Entre em contato com o Suporte ao cliente para obter assistência.

6. Se os dados de treinamento forem suficientes, clique em **Treinar modelo** .
   Você pode atualizar as entradas para treinamento na tela abaixo.



7. As entradas de previsão que você pode modificar incluem:
   - O que você está interessado em prever?
   - Que dados de entrada são úteis para prever o campo de saída?
   - Que dados históricos você deseja usar para treinar a solução e com que frequência deseja treiná-la novamente?

   Os valores padrão dessas entradas são exibidos. Você pode modificá-los e clicar em um dos seguintes:
   - **Atualização** Atualiza a definição do modelo de treinamento.
   - **Atualizar e treinar novamente** : Atualiza a definição do modelo de treinamento e treina novamente o modelo (aciona o. **Modelo de treinamento**).

8. Por fim, quando concluir o treinamento do modelo, clique em **Ativar previsão** caixa de seleção.
   As previsões agora são fornecidas em cada registro de phishing relatado pelo usuário usando esse modelo. Se você quiser parar de fornecer previsões sobre os registros de phishing relatados pelo usuário, limpe **Ativar previsão** marque a caixa e clique em **Desativar** .

Atribuição de analistas de segurança

Dependendo de suas configurações no SIR Tela Configuração de administração, você pode atribuir analistas de segurança a incidentes de segurança manualmente; automaticamente usando um fluxo de trabalho ou automaticamente usando atribuição automática.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição manual de analista

Você pode configurar o. Resposta a incidentes de segurança Tela Configuração de administração para exigir que os analistas de segurança sejam atribuídos manualmente sempre que alguém ou o SIR a aplicação cria um incidente de segurança ou gera uma tarefa de resposta de segurança.

Se um incidente de segurança ou tarefa de resposta não puder ser atribuído automaticamente, você poderá definir SIR Tela Configuração de administração para exigir a atribuição manual de analistas de segurança. Esta é uma boa opção se você tiver um número limitado de analistas de segurança para concluir solicitações ou se simplesmente não quiser atribuí-las automaticamente.

Atribuição de analista de segurança baseada em fluxo de trabalho

Você pode configurar o. Resposta a incidentes de segurança Tela Configuração de administração para usar um fluxo de trabalho selecionado para atribuir o analista de segurança sempre que alguém ou a aplicação SIR criar um incidente de segurança ou tarefa de resposta de segurança.

Na tela de configuração Administração de incidentes de segurança, você pode optar por usar um fluxo de trabalho para atribuir um analista a cada incidente de segurança ou tarefa de resposta de segurança. Esta opção é uma boa opção para organizações que usam um processo personalizado para resolver problemas de segurança ou têm um processo que pode ser automatizado.

Atribuição automática de analista de segurança

Você pode configurar o. Resposta a incidentes de segurança Tela Configuração de administração para atribuir automaticamente o analista de segurança sempre que alguém ou o SIR a aplicação cria um incidente de segurança ou uma tarefa de resposta de segurança. A atribuição automática permite que você defina, com base nas necessidades de sua organização, os critérios pelos quais os analistas são atribuídos automaticamente a incidentes de segurança.

Atribuição automática do agente com base nas classificações do agente

Se a atribuição automática estiver habilitada e um incidente de segurança ou uma tarefa de resposta for criada, ocorrerão as seguintes ações:

- Os analistas de segurança disponíveis são avaliados com base nos critérios definidos na configuração.
- Um analista de segurança apropriado é atribuído automaticamente à tarefa.
- A tarefa é movida para **Atribuído** estado.

Se a configuração estiver definida para considerar mais de um conjunto de condições, como habilidades, local, fuso horário ou área de cobertura do grupo, os analistas de segurança serão avaliados com base nas configurações da propriedade de ponderação e em outros critérios. Essas definições de configuração ajudam a atribuir agentes automaticamente com base em propriedades opcionais. As classificações calculadas são usadas para determinar o melhor agente para o incidente de segurança ou a tarefa de resposta. Qualquer combinação de métodos baseados em classificação pode ser habilitada na tela de configuração da aplicação.

Quando uma tarefa é criada, uma classificação para cada tipo de critério de seleção habilitado é calculada para cada agente disponível. O agente cuja classificação total é mais alta é considerado para atribuição automática.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As configurações das propriedades de ponderação de atribuição automática, encontradas em **Incidente de segurança** > **Administração** > **Propriedades**estão incluídos nos cálculos de classificação.

Esses valores ajudam a priorizar quais critérios de seleção de atribuição automática são mais importantes para sua organização. Defina os valores de prioridade entre 1 (menos importante) e 10 (importante).

Para obter um exemplo de como as propriedades de ponderação afetam as classificações do agente, consulte Atribuição automática do agente usando vários critérios de seleção.

Agendamento de plantão

O aplicativo Agendamento de plantão ajuda a garantir que membros da equipe de suporte dedicados estejam disponíveis para resolver problemas conforme eles surgem. Você pode configurar cronogramas de plantão, rotações de escala e políticas de escalação, escalar notificações para um grupo e determinar o contato atual para uma escalação. A aplicação identifica o membro atribuído e disponível de um grupo de suporte, por exemplo, ao atribuir um incidente. Para obter mais informações, consulte Agendamento de plantão .
A programação de plantão para Resposta a incidentes de segurança funciona da mesma maneira.

Atribuição automática de agente usando o local

Os agentes podem ser atribuídos automaticamente com base no local inicial em seu registro de usuário e no local das tarefas.

A atribuição automática por local é realizada quando **A seleção automática de agentes considerará a configuração do local dos agentes** a opção está habilitada.

Quando uma tarefa (incidente de segurança ou tarefa de resposta) é criada, o agente mais próximo do local da tarefa é considerado para a tarefa. Se a aplicação estiver configurada para que somente o local seja considerado, o agente mais próximo será atribuído automaticamente à tarefa.

Quando uma tarefa é criada, os locais do agente são comparados com os seguintes intervalos para determinar a classificação de cada local do agente.

Cálculo da classificação do local

Distância (mi.) do agente à tarefa	Classificação
0 a 0,1	1
0,11 a 0,5	0.9
0,51 a 5	0,7
5,1 a 10	0,5
10,1 a 20	0,4
20,1 a 30	0,3
30,1 a 40	0,2
40,1 a 100	0.1
> 100	0

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades, fuso horário ou programação, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é atribuído automaticamente para a tarefa. Consulte Atribuição automática do agente usando vários critérios de seleção para obter detalhes.

Atribuição automática do agente usando habilidades

Os agentes podem ser atribuídos automaticamente com base em suas habilidades e nas habilidades necessárias para executar a tarefa. Atribua habilidades aos registros de usuário usando **Habilidades** > **Usuários**.

A atribuição automática por habilidades pode ser realizada quando **A seleção automática de agentes para tarefas requer que eles tenham habilidades** a opção de configuração está definida como **todos** ou **alguns** .

Quando uma tarefa que inclui habilidades é atribuída automaticamente, as habilidades de um agente são comparadas com as habilidades necessárias para executar a tarefa. Uma classificação é calculada com base na opção de configuração de habilidades. Se a opção estiver definida como **alguns** , o agente com a correspondência de habilidades mais próxima é atribuído automaticamente à tarefa. Se a opção estiver definida como **todos** somente os agentes que possuem todas as habilidades necessárias são considerados. Se nenhum agente tiver todas as habilidades necessárias para executar a tarefa, ninguém será atribuído automaticamente.

Uma classificação de habilidades é calculada como:

Skills_agent/skills_task

Em que:

- Skills_agent é o número de habilidades possuídas pelo agente que correspondem às habilidades necessárias para a tarefa.
- Skills_task é o número total de habilidades necessárias para a tarefa.

Por exemplo, se uma tarefa requer quatro habilidades e o Agente A possui três delas e o Agente B possui duas delas:

- Classificação de habilidade do agente A é igual a 3/4 ou 0,75
- Classificação de habilidade do agente B: 2/4 ou 0,5

Se a aplicação estiver configurada para usar outros critérios de seleção, como local ou fuso horário, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática do agente usando vários critérios de seleção para obter detalhes.

Atribuição automática do agente usando fusos horários

Os agentes podem ser atribuídos automaticamente com base no fuso horário definido em seus registros de usuário e no fuso horário das tarefas.

. **A seleção automática de agentes considerará o fuso horário da tarefa** a opção de configuração está habilitada, a atribuição automática por fuso horário pode ser realizada.

Quando uma tarefa é criada, os agentes no fuso horário mais próximo do fuso horário da tarefa são considerados para a tarefa. Se a aplicação estiver configurada para que somente o fuso horário seja considerado, somente um agente no mesmo fuso horário poderá ser atribuído automaticamente à tarefa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: É importante que os fusos horários do agente e a tarefa sejam definidos corretamente.

Quando uma tarefa é criada, os agentes são classificados com base no fuso horário da tarefa e no fuso horário do agente usando a seguinte fórmula:

1 - [abs(Task_tz – Agent_tz) ÷ 12]

em que:

- abs é a função matemática para calcular o valor absoluto.
- Task_tz é o deslocamento entre o fuso horário da tarefa e o GMT.
- Agent_tz é o deslocamento entre o fuso horário do agente e o GMT.

Por exemplo, uma tarefa é criada na cidade de Nova York (GMT-4) e dois agentes estão disponíveis para executar a tarefa, um em Los Angeles (GMT-7) e um em Paris, França (GMT-1).

A classificação do agente em Los Angeles é calculada como:

1 - abs(((((-4) - (-7)) ÷ 12 ou 0,75

A classificação do agente em Paris é calculada como:

1 - abs(((((-4) - (-1)) ÷ 12 ou 0,58

Portanto, se a atribuição automática da tarefa for baseada somente no fuso horário, ela será atribuída ao agente de Los Angeles.

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades ou local, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática do agente usando vários critérios de seleção para obter detalhes.

Atribuição automática do agente usando áreas de cobertura do grupo

Os agentes podem ser atribuídos automaticamente com base na área de cobertura do grupo definida em seus registros de usuário.

Atribuição automática do agente usando vários critérios de seleção

Quando uma tarefa é criada, as classificações dos agentes são calculadas. Para obter mais informações, consulte:

- Atribuição automática de agente usando o local
- Atribuição automática do agente usando habilidades
- Atribuição automática do agente usando fusos horários

A atribuição automática é baseada no seguinte cálculo:

(Classificação criteria_1 x peso criteria_1) (classificação criteria_2 x peso criteria_2) (classificação criteria_3 x peso criteria_3) / Número de tipos de critérios usados em que:

O número de tipos de critérios usados é igual a 1, 2 ou 3, dependendo das configurações de local, habilidade e fuso horário usadas.

Este exemplo calcula a atribuição automática do agente com base no local e nas habilidades. O exemplo é baseado nas seguintes suposições.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- . **A seleção automática de agentes considerará a localização dos agentes** a opção de configuração está habilitada para a aplicação.
- . **A seleção automática de agentes requer que eles tenham algumas das habilidades necessárias para a tarefa** a opção de configuração está habilitada para a aplicação.
- . **Peso das habilidades** a propriedade está definida como 10 para a aplicação.
- . **Peso do local** a propriedade está definida como 5 para a aplicação.
- Os agentes A e B estão disponíveis para executar uma tarefa, e a tarefa requer quatro habilidades específicas.
- O local do agente A fica a 5 km do local da tarefa e possui três das quatro habilidades necessárias.
- O local do Agente B fica a 400 m do local e possui duas das habilidades necessárias.

A atribuição automática para os agentes usa este cálculo: (Classificação do local x peso do local) (classificação de habilidades x peso das habilidades)]/ 2

- O cálculo de atribuição automática do Agente A é: (0,7 x 0,5) (0,75 x 1)]/ 2: 0,55
- O cálculo de atribuição automática do Agente B é: (0,9 x 0,5) (0,5 x 1)]/ 2: 0,475

Neste exemplo, o Agente A é atribuído automaticamente à tarefa.

Espaço de mineração de processos para Resposta a incidentes de segurança

A Mineração de processos verifica por meio de logs de auditoria de incidentes de segurança e identifica fatores que contribuem para ineficiências, como várias reatribuições, tempos de espera prolongados e períodos de inatividade para incidentes de segurança. As organizações podem usar essas informações para lidar com as ineficiências.

Com a mineração de processos, você pode identificar as seguintes oportunidades de melhorias para seus incidentes de segurança.

Oportunidades com mineração de processos

Oportunidade	Descrição
Incidentes com pelo menos duas mudanças de grupo de atribuição	Incidentes para os quais o grupo de atribuição foi alterado duas ou mais vezes.
SIRT (Máximo de repetições é 2)	
Os incidentes levaram mais de 5 horas para escalar para alta prioridade	Incidentes para os quais a prioridade foi escalonada para uma prioridade mais alta após cinco horas.
Os incidentes levaram mais de cinco horas para serem analisados	Incidentes que estavam no estado de análise por mais de cinco horas.
Incidentes analisados em 30 minutos	Incidentes que estavam no estado de análise por menos de 30 minutos.
Revisão (o máximo de repetições é 2)	Incidentes que foram movidos para o estado de revisão por duas vezes.
Erradicar (o máximo de repetições é 2)	Incidentes que foram movidos para o estado Erradicado por duas vezes.

Pacote de conteúdo de mineração de processos para Resposta a incidentes de segurança adiciona um projeto pré-criado que inclui uma definição de modelo de processo predefinida

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para incidentes de segurança. Para criar um projeto, consulte Criar projeto de mineração de processos para incidentes de segurança.

Nota: Para usar a Mineração de processos no Resposta a incidentes de segurança, baixe e instale o pacote de conteúdo. Para obter mais informações, consulte Pacote de conteúdo para Resposta a incidentes de segurança .

Criar projeto de mineração de processos para incidentes de segurança

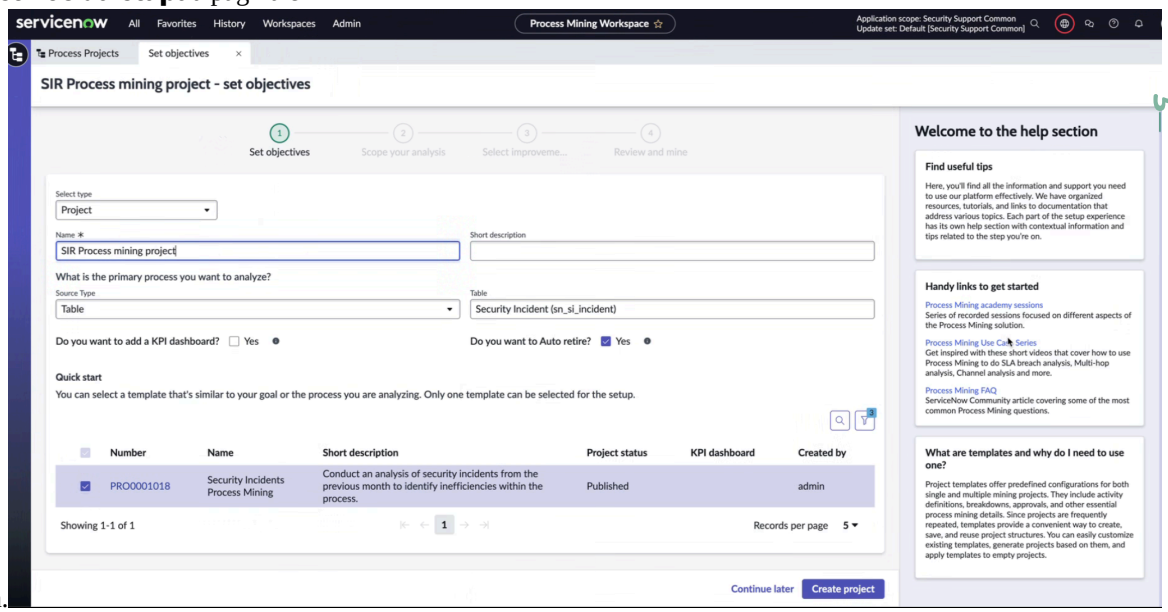
Crie um projeto no Espaço de mineração de processos usando as definições de modelos de processo de pré-compilação do pacote de conteúdo para verificar logs de auditoria de registros de incidentes de segurança e identificar ineficiências no ciclo de vida do incidente de segurança.

Antes de Iniciar

Função necessária: sn_process_optimization_analyst e sn_si_read

Procedimento

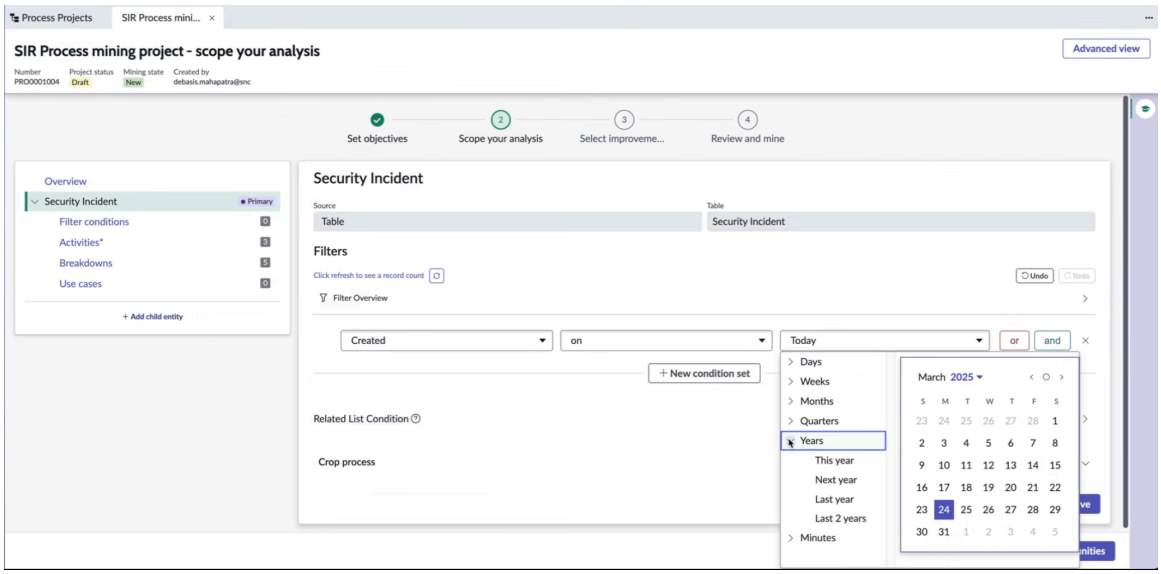
1. Navegar até **Tudo** > **Espaços** > **Espaço de mineração de processos**.
2. Selecione **Criar Novo Projeto** .
   . **Objetivos da etapa**a página é aberta.



3. Insira um nome de projeto de mineração de processos em **Nome** .
4. **Opcional:** Adicione uma descrição resumida sobre seu projeto em **Descrição resumida** .
5. Selecione **Tipo de origem** Como Tabela.
6. Selecione Incidente de segurança (sn_si_incident) em **Tabela** .
7. Selecione o modelo padrão e selecione **Criar projeto** .
   O painel do projeto aparece com todas as configurações definidas.
8. Selecione a edição (ícone) correspondente a **Escopo da análise** e configure os filtros para definir o número de registros a serem minerados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Selecione **Selecione oportunidades de melhoria** e configure as melhorias para seus incidentes de segurança.
   Uma lista de oportunidades de melhoria é exibida. Para obter informações sobre como configurar oportunidades de melhoria, consulte Trabalhar com oportunidades de melhoria .
10. Selecione **Revise e minere** e selecione **Projeto de mineração** .
11. Selecione **Mineração de amostra** ou **Mina completa** .
12. Selecione **Confirmar e minerar** para iniciar a mineração.
    A mineração é iniciada e o status da mineração é exibido.

Casos de uso de mineração de processos para incidentes de segurança

Os casos de uso de Mineração de processos a seguir fornecem vários métodos de análise que você pode usar para identificar ineficiências durante a resolução de incidentes de segurança.

Análise de vários saltos

Os incidentes de segurança que são reatribuídos várias vezes para equipes diferentes podem resultar em um atraso na resolução. Ao analisar os motivos das reatribuições desses incidentes de segurança e onde os incidentes são retidos por períodos mais longos, você pode melhorar a eficiência geral.

A seguir estão exemplos de etapas para obter a lista de incidentes de segurança que seguiram os caminhos mais longos:

1. Navegar até **Espaços** > **Espaço de mineração de processos**.
2. Selecione **Grupo de atribuição** .
3. Abra um projeto e navegue até **Workbench do analista** .

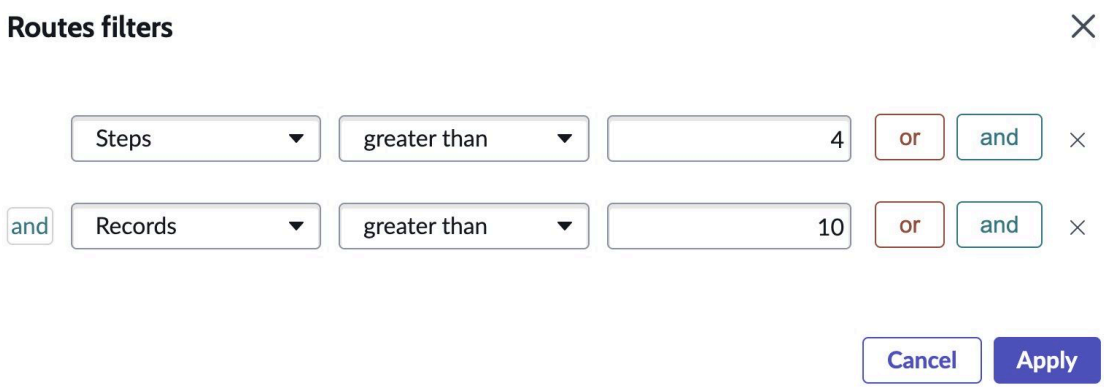
   Ao abrir um projeto de otimização de processo minerado, por padrão, o Workbench do analista é aberto.
4. Selecione **Análise de variação** .
5. Selecione o filtro ( ) e defina o filtro semelhante ao seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Etapas maiores que o número médio de etapas.
- Registros maiores que o número mínimo de registros que seguiram uma rota mais longa.

Nota: Você pode configurar os valores de acordo com seu requisito.



6. Selecione **Aplicar**.

   Todos os registros que correspondem aos critérios de filtro são exibidos. Selecione um registro para exibir a rota de fechamento do registro.

7. Selecione um registro e selecione **Mostrar rota** .

   A rota percorrida pelo registro é exibida. Você pode usar esta rota para identificar a etapa em que os incidentes foram retidos por uma duração maior do que o esperado.

Análise de violação de ANS

Você pode usar a mineração de processos para analisar incidentes de segurança que violaram um determinado ANS (Acordo de nível de serviço).

Exemplos de etapas a seguir para obter a lista de incidentes de segurança que violaram o ANS:

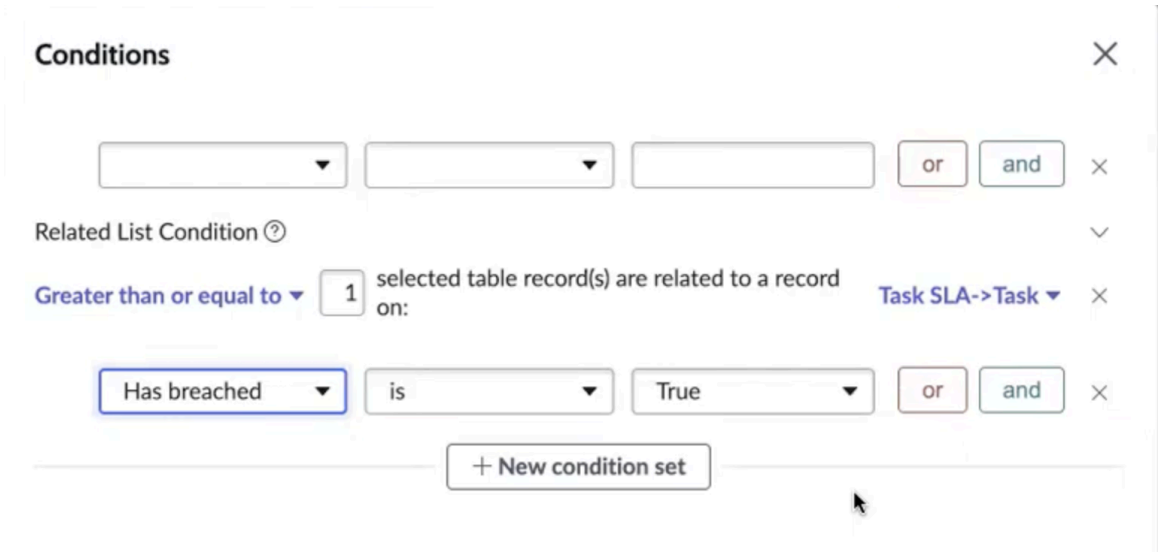
1. Navegar até **Espaços** > **Espaço de mineração de processos**.
2. Abra um projeto e navegue até **Workbench do analista** .

   Ao abrir um projeto de otimização de processo minerado, por padrão, o Workbench do analista é aberto.

3. Em Filtros avançados, selecione **Condições** .
4. Selecione a seta correspondente a. **Condição da lista relacionada** .
5. Defina as condições semelhantes às seguintes:
   - Use **Selecione** para selecionar `ANS de tarefa` tabela.
   - Defina o valor de **Maior que ou igual a.** campo para `1` .
   - Defina o valor de **Violou** . **Verdadeiro** .
   - Para identificar incidentes de segurança que violaram um ANS específico, defina um **Definição de ANS** filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Aplicar**.

   Todos os registros que correspondem às condições são exibidos. Selecione um registro para exibir a rota do registro para análise.

Análise de prioridade

Você pode usar a mineração de processos para revisar e melhorar o processo de atribuição de prioridade existente para seus incidentes de segurança.

A seguir estão exemplos de etapas para obter a lista de incidentes de segurança para os quais a prioridade foi modificada:

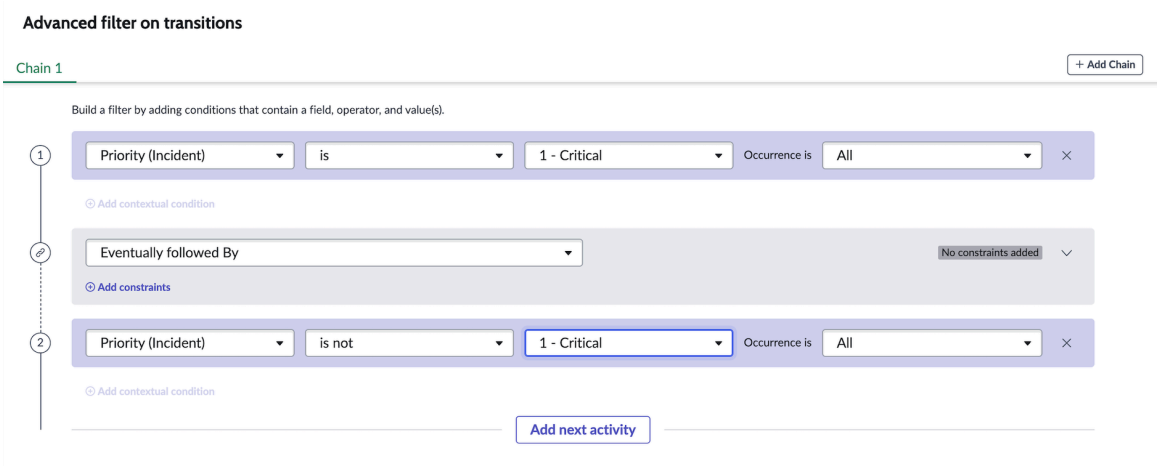
1. Navegar até **Espaços** > **Espaço de mineração de processos**.
2. Abra um projeto e navegue até **Workbench do analista** .

   Ao abrir um projeto de otimização de processo minerado, por padrão, o Workbench do analista é aberto.

3. Selecione **Prioridade** .
4. Em Filtros avançados, selecione **Transições** .
5. Em **Filtro avançado em transições** , configure o seguinte:
   a. A prioridade definida é 1 - Crítica.
   b. Selecione **Seguido por**
   c. A prioridade não é 1 - Crítica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Aplique todas as cadeias** .

   O mapa mostra todos os incidentes de segurança aos quais foi atribuída prioridade 1 e sua prioridade foi reduzida posteriormente.

Análise de gargalo

Você pode usar a mineração de processos para revisar as transições de estado de seus incidentes de segurança. Esta análise identifica as transições que não são usuais e o atraso causado por causa disso.

A seguir estão exemplos de etapas para executar a análise de gargalo:

1. Navegar até **Espaços** > **Espaço de mineração de processos**.
2. Abra um projeto e navegue até **Workbench do analista** .

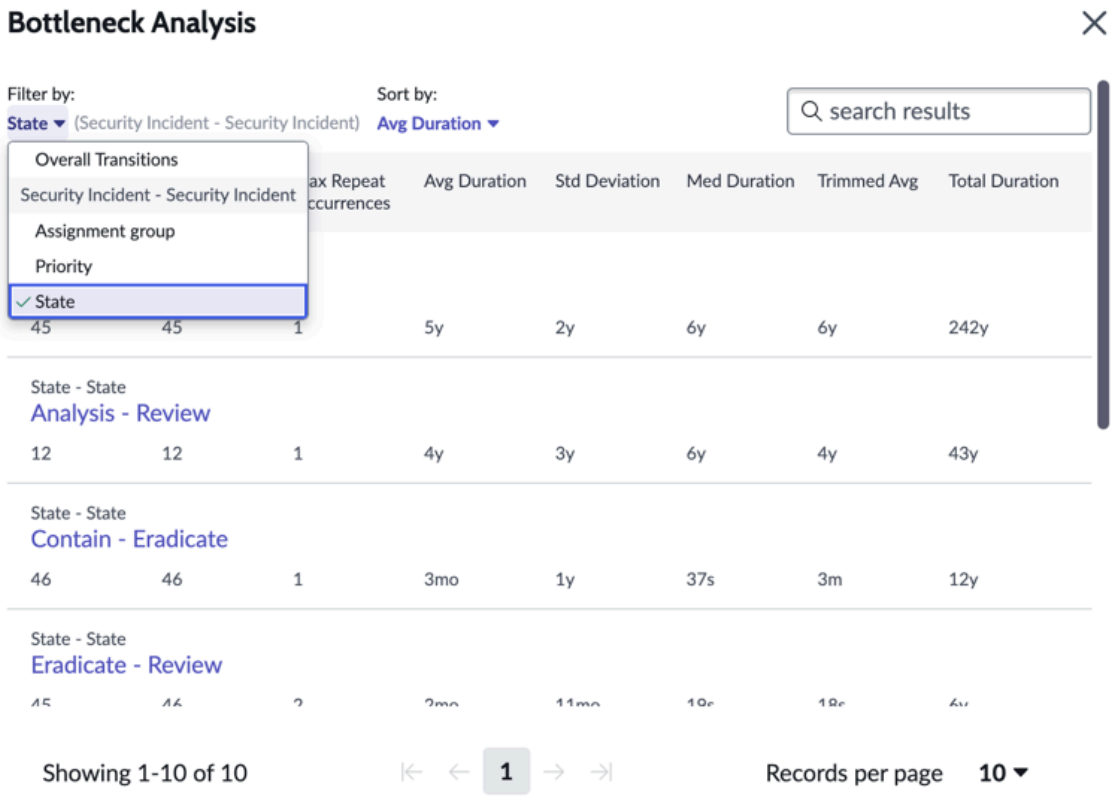
   Ao abrir um projeto de otimização de processo minerado, por padrão, o Workbench do analista é aberto.

3. Selecione **Análise de gargalo** em **Opções de modelo** .

   A tela exibe as transições de estado dos incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione **Filtrar por** para identificar transições de gargalo. Como alternativa, use a barra de pesquisa para pesquisar transições de gargalo. Por exemplo, para identificar incidentes que foram movidos para outros estados do estado Encerrado, use "Encerrado " ou "Encerrado -".

Muito tempo para iniciar do que resolver

Você pode usar a mineração de processos para revisar os incidentes que levam muito tempo para chegar ao estado Rascunho, mas que foram encerrados em um tempo relativamente menor.

A seguir estão exemplos de etapas para identificar incidentes de segurança que estavam no estado Rascunho por mais de dois dias e foram encerrados em 30 minutos após a mudança para o estado Análise:

1. Navegar até **Espaços** > **Espaço de mineração de processos**.
2. Abra um projeto e navegue até **Workbench do analista** .

   Ao abrir um projeto de otimização de processo minerado, por padrão, o Workbench do analista é aberto.

3. Em Filtros avançados, selecione **Transições** .
4. Em **Filtro avançado em transições** , configure o seguinte:
   a. Definido `Estado (incidente)` . `Rascunho` .
   b. Selecione **Seguido por**
   c. Selecione **Adicionar restrições** e definir **De** . 2 dias.
   d. Selecione **Adicionar próxima atividade** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Definido Estado (incidente) Em Análise .

f. Selecione **Seguido por**

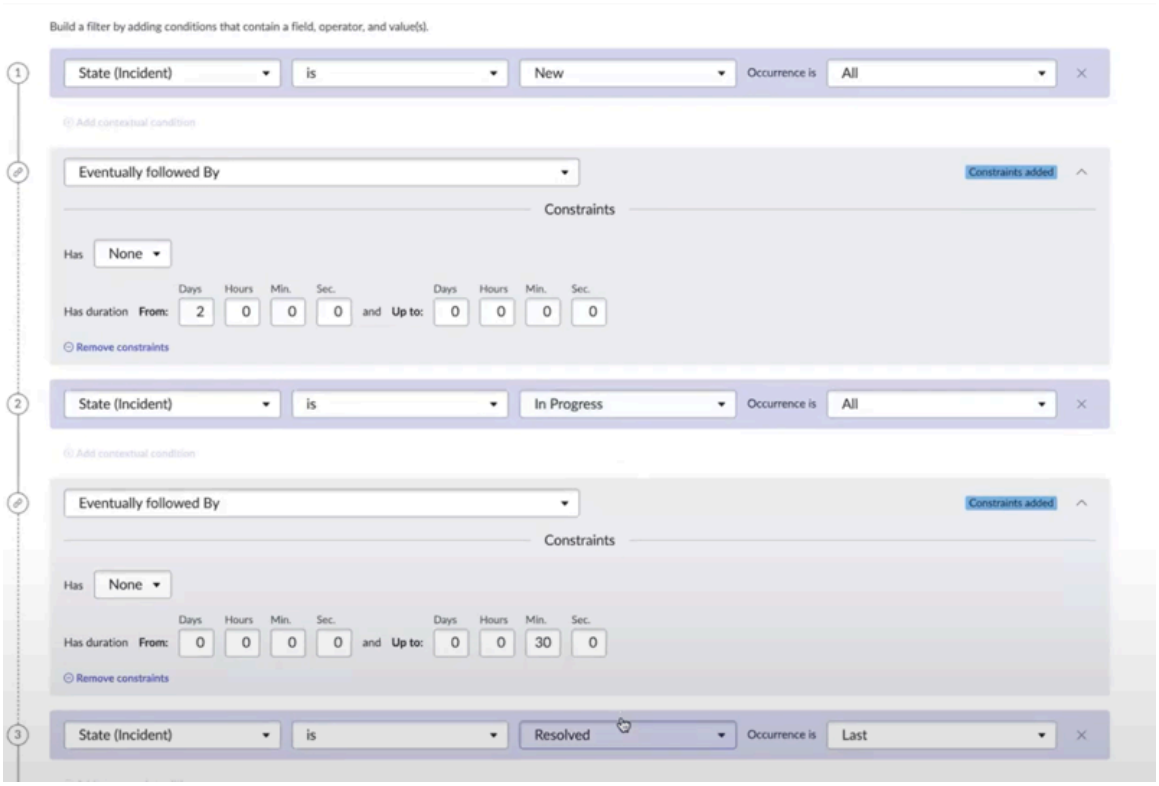
g. Selecione **Adicionar restrições** e definir **Até** . 30 minutos.

h. Selecione **Adicionar próxima atividade** .

i. Selecione **Seguido por**

j. Selecione **Adicionar restrições** e definir **Até** como 30 minutos.

k. Definido Estado (incidente) . Encerrado .



5. Selecione **Aplique todas as cadeias** .

6. Selecione **Filtros de detalhamento** e classifique por **Duração média mais longa** .

Gerenciar incidentes de segurança e solicitações de entrada

Depois que um incidente de segurança é criado, há vários tipos de informações que podem ser adicionadas e exibidas conforme sua análise do problema progride em direção à resolução.

Importante: Os recursos mais recentes do Resposta a incidentes de segurança estão disponíveis exclusivamente em Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para o mais recente Resposta a incidentes de segurança ou Espaço de resposta a incidentes de segurança Versão para acessar e aproveitar recursos como transferência de turno, calculadora de pontuação de risco etc.

Esta seção descreve o seguinte:

- Crie uma solicitação de entrada
- Gerenciar observáveis
- Gerencie pesquisas e verificações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Calcule a gravidade de um incidente de segurança
- Gerenciar atividades pós-incidente
- Fechar incidentes de segurança

Crie uma solicitação de entrada

Ao contrário dos incidentes de segurança, as solicitações de entrada geralmente têm prioridade mais baixa. Solicitações de pesquisa, verificação ou um novo selo são exemplos de solicitações de entrada.

Antes de Iniciar

Funções necessárias: sn_si.basic role ou superior

Procedimento

1. Navegue até um dos formulários de solicitações.
   Por exemplo, **Tudo** > **Incidente de segurança** > **Solicitações de Entrada** > **Atribuição a mim**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Solicitação de segurança

Campo	Descrição
Número	[Somente leitura] O número da solicitação de segurança gerado automaticamente.
Empresa	A empresa solicitante.
Local	O local do IC, se aplicável. Este campo é preenchido previamente quando o IC é selecionado.
Item de Configuração	O item de configuração afetado pela solicitação.
Prioridade	A prioridade da solicitação.
Aberto(a)	[Somente leitura] A data e a hora em que a solicitação foi aberta.
Estado	O estado atual da solicitação de segurança. Na criação da solicitação de segurança, o padrão deste campo é **Rascunho** .
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuição a	O indivíduo atribuído para executar o trabalho.
Descrição resumida	Uma breve descrição da solicitação de segurança, que está visível para o solicitante.
Descrição	A descrição completa da solicitação, que está visível para o solicitante.
Anotações de trabalho	Anotações de trabalho, visíveis para o solicitante.

4. Ao concluir suas entradas, clique em **Enviar** .
5. Se você precisar escalar a solicitação para um incidente de segurança, clique em **Converter em incidente de segurança** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar observáveis

Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicarão uma invasão. Observáveis típicos são endereços IP, hashes MD5 de arquivos ou URLs de malware ou nomes de domínio. Inteligência contra ameaças os dados da tabela observável estão disponíveis em um incidente de segurança.

As informações de observáveis incluem valor, tipo, contexto e carimbo de data/hora.

Você pode criar ou excluir observáveis manual ou automaticamente por meio de solicitações de pesquisa.

Um novo **Descoberta** a coluna foi adicionada ao **Resultados da pesquisa de ameaças** guia. Os valores possíveis são: Mal-intencionado e Desconhecido.

Se uma solicitação de pesquisa de IOC não encontrar um observável de incidente de segurança, ela será rotulada como Desconhecido.

Se uma solicitação de pesquisa de IOC encontrar um incidente de segurança observável, ela será rotulada como mal-intencionada.

Durante um upgrade, os itens existentes têm **Descoberta** Coluna definida como mal-intencionada.

Nota: Enquanto Inteligência contra ameaças os dados da tabela observáveis fazem parte de um incidente de segurança, nenhuma outra interação com o. Inteligência contra ameaças o módulo está incluído. Para obter a funcionalidade completa da ameaça, o Inteligência contra ameaças o plug-in está disponível por assinatura.

Tópicos relacionados

Crie um observável de incidente de segurança

Mostrar informações de IOC para um incidente de segurança

Você pode exibir informações de IOC, como observáveis e resultados de pesquisa de vistas associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir as informações relacionadas ao IOC.
2. Clique em **Mostrar IOC** link relacionado.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações sobre o incidente de segurança.

Tab	Descrição
Observáveis	Exiba ou adicione ou edite manualmente observáveis associados ao incidente de segurança. Para obter mais informações, consulte Gerenciar observáveis.
Indicadores associados	Se Inteligência contra ameaças estiver ativado, você pode exibir quaisquer outros indicadores associados a qualquer um dos mesmos registros de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tab	Descrição
Resultados da pesquisa de detecções	Contém resultados da pesquisa de vistas.
Detalhes de Pesquisa de detecções	Contém detalhes do registro de Pesquisa de vistas.
Pesquisas de ameaças	Armazena dados de aprimoramento de sistemas de detecção de malware. Esta guia aparece somente quando Inteligência contra ameaças o plug-in está instalado.
Modos/métodos de ataque associados	Se Inteligência contra ameaças estiver ativado, você pode exibir qualquer outro tipo de ataque associado a qualquer um dos mesmos registros de ameaça.
Solicitações de Verificação de Segurança	Se Inteligência contra ameaças estiver ativado, você pode exibir solicitações de verificação e pesquisa anexadas ao incidente de segurança.
Recursos com IoC Semelhante	Se Inteligência contra ameaças estiver ativado, você pode exibir quaisquer outros recursos com indicadores semelhantes.
Usuários com IOC Semelhante	Se Inteligência contra ameaças estiver ativado, você pode exibir outros usuários com indicadores semelhantes.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar** .

Crie um observável de incidente de segurança

Você pode criar e exibir um observável em um incidente de segurança e tomar as medidas apropriadas. Ter observáveis disponíveis no incidente de segurança é escalonável e reduz o tempo de resposta.

Antes de Iniciar

Função necessária:

- sn_ti_observable.write (gravação)
- sn_ti_observable.read (leitura)
- sn_ti_observable.admin (excluir)

Procedimento

1. Navegue até **Incidente de segurança** .
2. Escolha um incidente.
3. Clique em **Observáveis de incidentes de segurança** guia lista relacionada.
4. Clique em **Nova**.
5. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, você pode selecionar um ou mais marcadores para especificar o grau de sensibilidade do observável. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se for uma verificação de ameaça Em um endereço IP ou hash, malware retornado ou alguma outra falha, o endereço IP ou valor de hash é adicionado automaticamente à tabela observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação observável, como um endereço IP ou hash de arquivo. Esses tipos de observáveis são definidos em **Tipos de observáveis** módulo.
Contagem de incidentes	O número de vezes que o valor do observável foi encontrado.
É composição	Este campo é exibido somente depois que o registro do observável é salvo. . **Tipo de observável** está definido como qualquer coisa diferente disso **Composição do observável** e este novo observável é uma composição, marque esta caixa de seleção. . **Tipo de observável** já está definido como **Composição do observável** , a caixa de seleção é marcada e somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades: ○ **Mal-intencionado** : Indica que o observável é prejudicial para a organização. ○ **Suspeito** : Indica que o observável pode ser prejudicial para a organização. ○ **Limpo** : Indica que o observável não é prejudicial para a organização. ○ **Desconhecido** Indica que ainda não determinamos a descoberta do observável. ○ Valor padrão: Desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como mal-intencionados.
Operador	Este campo aparece somente quando **É composição** a caixa de seleção está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

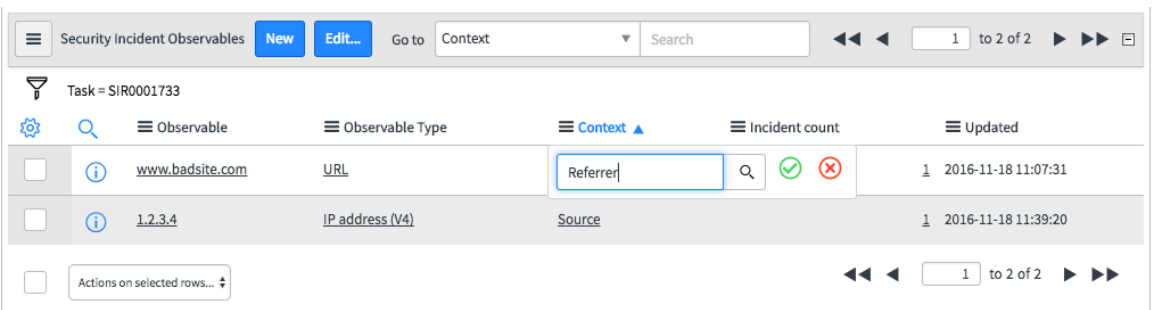
Campo	Descrição
	Defina este campo como **E.** se todos os observáveis secundários precisarem estar presentes para que um indicador associado seja considerado presente. Defina como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.
Não deve estar presente	Este campo é exibido somente depois que o registro do observável é salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Local	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregue mais dados de IOC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

6. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

7. Retornando ao incidente de segurança, as seguintes informações estão disponíveis.

Nota: Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. . **Itens de configuração relacionados** e. **Usuários relacionados** as guias da lista relacionada são atualizadas de acordo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Definição
Observável	O valor (por exemplo, endereço IP ou hash) associado ao observável.
Tipo de Observável	O tipo específico de observável.
Contexto	Selecionado pelo usuário. As opções são: ○ IP - Origem ou destino **Nota:** Se Inteligência contra ameaças e. Palo Alto Networks - Firewall se estiverem ativados, alterar ou adicionar um valor a este campo causará Obter fluxo de dados de log Operações de segurança Palo Alto Networks - Obter dados de log fluxo de trabalho a ser executado. O fluxo de trabalho recupera dados de log de ameaças aprimorados do firewall e os anexa ao incidente de segurança. As informações também são analisadas e exibidas no Logs do firewall seção em **Dados de aprimoramento** guia. ○ Referenciador **Nota:** Quando o usuário clica em um link em um e-mail de phishing, um referenciador é o URL do salto final antes que o URL do malware seja acessado.
Contagem de Incidentes	O número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Atualização em	Dados e hora em que a lista foi atualizada pela última vez.

Nota: . Inteligência contra ameaças o plug-in está instalado, você também pode exibir o observável no **Observáveis** lista no **Repositório IOC** .

Tópicos relacionados

Edite uma lista de observáveis de incidentes de segurança

Adicione vários observáveis de incidentes de segurança .

Gerenciar observáveis de arquivo

Gerenciar observáveis de arquivo fornece medidas de segurança rigorosas para armazenar os arquivos suspeitos e habilita os observáveis do tipo de arquivos para integração com a área restrita.

Antes de Iniciar

Função necessária: sn_ti_malicised_attachment_access (upload)

Carregue observáveis do tipo de arquivo:

- Automaticamente: Quando os incidentes de segurança são criados para os e-mails de phishing, os anexos no e-mail de phishing são criados como observáveis do tipo de arquivo.
- Manualmente: Um analista de segurança também pode carregar os arquivos suspeitos para criar observáveis do tipo de arquivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

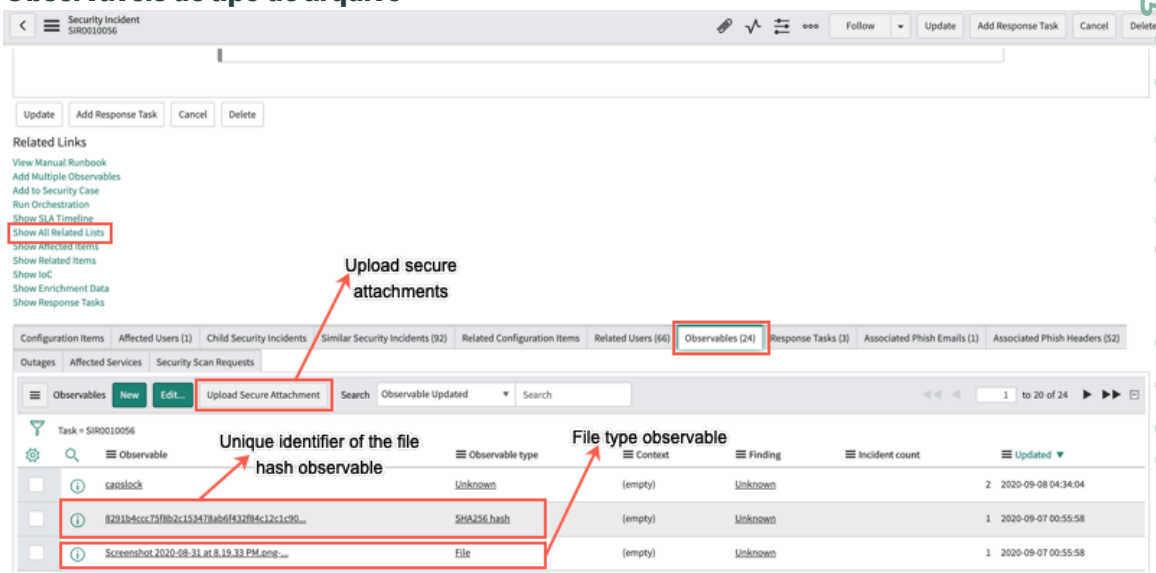
Você pode criar e exibir observáveis de tipo de arquivo para um incidente de segurança. Os arquivos suspeitos que fazem parte dos observáveis são armazenados em um local específico, que pode ser acessado pelo analista de segurança para baixar o arquivo somente com uma função específica.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** em **Mostrar todas as listas relacionadas** guia.

   Se houver anexos no e-mail de phishing, por padrão, esses anexos serão criados como observáveis do tipo de arquivo no incidente de segurança correspondente. Cada anexo é criado como dois observáveis, como tipo de arquivo e observável de hash de arquivo.
3. Para carregar os anexos seguros manualmente:
   - Clique em **Carregar anexo seguro** .
   - Em Carregar anexos seguros, clique em **Escolha o arquivo** para carregar um ou mais arquivos. Cada arquivo é considerado como um único registro observável.
   - Clique em **Criar observáveis de arquivo** para criar observáveis de tipo de arquivo, como um é o tipo de arquivo e outro é o hash de arquivo, que é um identificador exclusivo.

Observáveis de tipo de arquivo



Selecione o tipo de arquivo observável a ser processado para integrações adicionais, como área restrita e pesquisa de ameaças. Além disso, você também pode baixar os anexos do tipo de arquivo observável.

Nota:

A pesquisa de ameaças (VirusTotal) recupera o arquivo dos anexos protegidos para os novos observáveis de tipo de arquivo e as propriedades do sistema abaixo não são aplicáveis aos novos observáveis de tipo de arquivo.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para uma referência rápida, o tipo de arquivo observável é mapeado como secundário para o observável de hash e o observável de hash é mapeado como secundário para o observável de arquivo.

Se os anexos de e-mail de phishing excederem mais do que o tamanho definido, os observáveis não serão criados. Você deve modificar as propriedades do sistema para oferecer suporte aos arquivos de tamanho maior.

Propriedades do sistema de tamanho de arquivo

Propriedade do sistema	Descrição
glide.email.inbound.max_total_attachment_size_bytes	Se você estiver encaminhando o e-mail de phishing diretamente, use este valor de propriedades do sistema para aumentar o tamanho do arquivo de 18 MB para o tamanho de arquivo desejado.
.glide.attachment.max_get_size	Se você estiver encaminhando o e-mail de phishing como um anexo, use este valor de propriedade do sistema para criar as propriedades do sistema abaixo no escopo global para aumentar o tamanho do arquivo de 5 MB para o tamanho desejado.

Você também pode criar um novo tipo de arquivo observável da seguinte forma:

a. Clique em **Nova**.

b. Selecione **Tipo de observável Categoria: Arquivo**

c. Clique em **Upload** para anexar um arquivo.

Edite uma lista de observáveis de incidentes de segurança

Você pode editar quais observáveis na lista associados a um incidente de segurança serão exibidos.

Antes de Iniciar

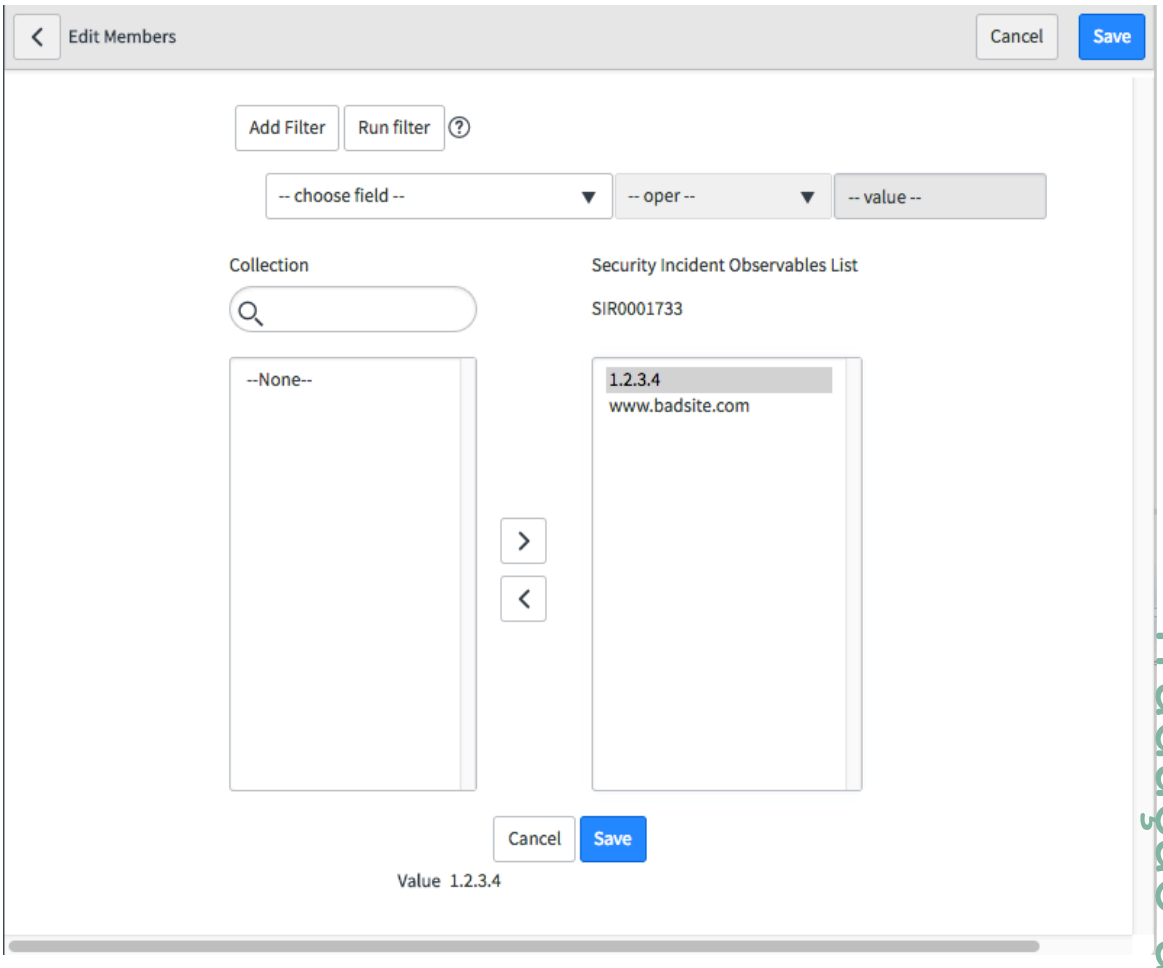
Função necessária: sn_si.basic

Procedimento

1. Navegue até **Incidente de segurança** .
2. Escolha um incidente.
3. Clique em **Observáveis de incidentes de segurança** guia lista relacionada.
4. Clique em **Editar**.
5. Adicionar ou remover observáveis da lista.
   Crie um filtro para listas longas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Salvar**.

Nota: Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. . **Itens de configuração relacionados** e. **Usuários relacionados** as guias da lista relacionada são atualizadas de acordo. Além disso, se o Inteligência contra ameaças o plug-in está ativado e você tem pelo menos um Integrações do Resposta a incidentes de segurança implementação de integração ativada, o. Integração de operações de segurança - Recurso de pesquisa de ameaças executa um ou mais fluxos de trabalho e as pesquisas de segurança contra ameaças são realizadas nos observáveis adicionados. Os resultados aparecem em **Resultados da pesquisa de ameaças** guia.

Tópicos relacionados

Adicione vários observáveis de incidentes de segurança .

Crie um observável de incidente de segurança

Adicione vários observáveis de incidentes de segurança .

Para economizar tempo, você pode adicionar vários observáveis de incidentes de segurança à lista de observáveis de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_ti_write

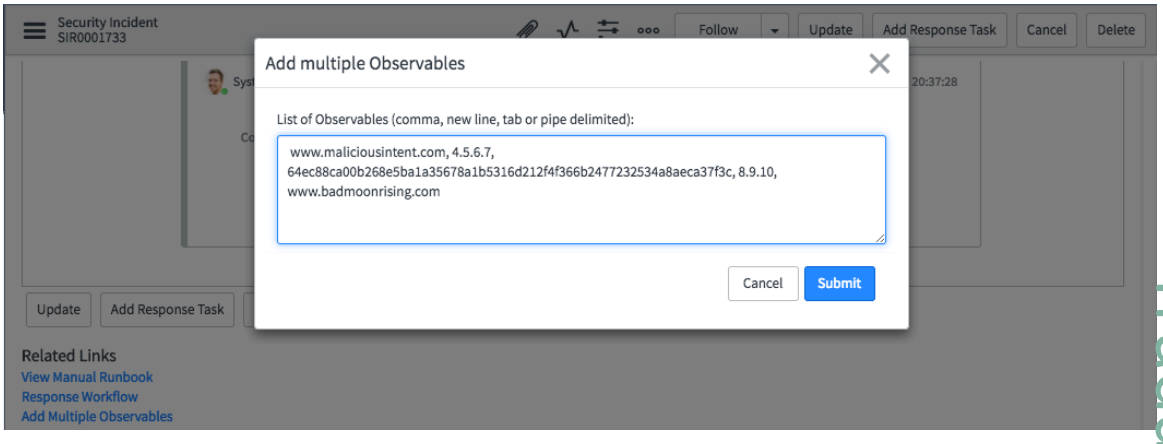
Nota: Ao adicionar vários observáveis de incidentes de segurança, as duplicatas são ignoradas durante o processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Incidente de segurança** .
2. Escolha um incidente.
3. Clique em **Adicionar vários observáveis** link relacionado.
4. Insira ou cole vários observáveis.
   As entradas podem ser de qualquer tipo de observável. Os formatos aceitos são: Vírgula, nova linha, guia ou separadores de tubo rígido.



> **Nota:** Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. . **Itens de configuração relacionados** e. **Usuários relacionados** as guias da lista relacionada são atualizadas de acordo.

Valores observáveis não detectados automaticamente são atribuídos ao tipo Desconhecido.

5. Clique em **Enviar.** .

Aprimoramento automático de dados de log observável de incidentes de segurança

Quando determinadas aplicações e integrações são configuradas, incluindo Inteligência contra ameaças e o. Palo Alto Networks - Firewall As informações de observáveis em um incidente de segurança podem ser enriquecidas automaticamente com dados de log de ameaças sempre que o IP de origem de seus observáveis for modificado.

Quando ocorre uma modificação, uma regra de negócios inicia um fluxo de trabalho que recupera dados de logs de ameaça no firewall e enriquece as informações de observáveis no incidente de segurança.

Para que os observáveis possam ser aprimorados, as etapas a seguir devem ser executadas.

- Inteligência contra ameaças deve ser ativado.
- . Firewall da Palo Alto Networks a integração deve ser ativada e configurada. Também pode incluir Configure credenciais SSH para o MID Server.

Após a conclusão dessa configuração, o ato de mudar o IP de origem dos observáveis associados a um incidente de segurança faz com que uma regra de negócio execute o. **Operações de segurança Palo Alto Networks - Obter dados de log** fluxo de trabalho. As atividades de fluxo de trabalho enfileiram uma consulta de pesquisa no firewall e retornam um ID de trabalho que é usado para recuperar dados de logs de ameaças do firewall e anexá-los como um arquivo XML ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

- Fluxo de aprimoramento de informações da sessão de foco automático
- Palo Alto Networks Fluxo de trabalho do Inicializador de firewall
- Operações de segurança Palo Alto Networks - Verificar e bloquear fluxo de trabalho de valor
- Obter fluxo de dados de log
- Obter fluxo de aprimoramento de dados do Wildfire

Publique observáveis em uma lista de observação de terceiros

Você pode publicar um ou mais observáveis ou indicadores associados em uma lista de observação de terceiros. Atualmente, a única implementação que oferece suporte a essa funcionalidade é o CrowdStrike Falcon Host.

Antes de Iniciar

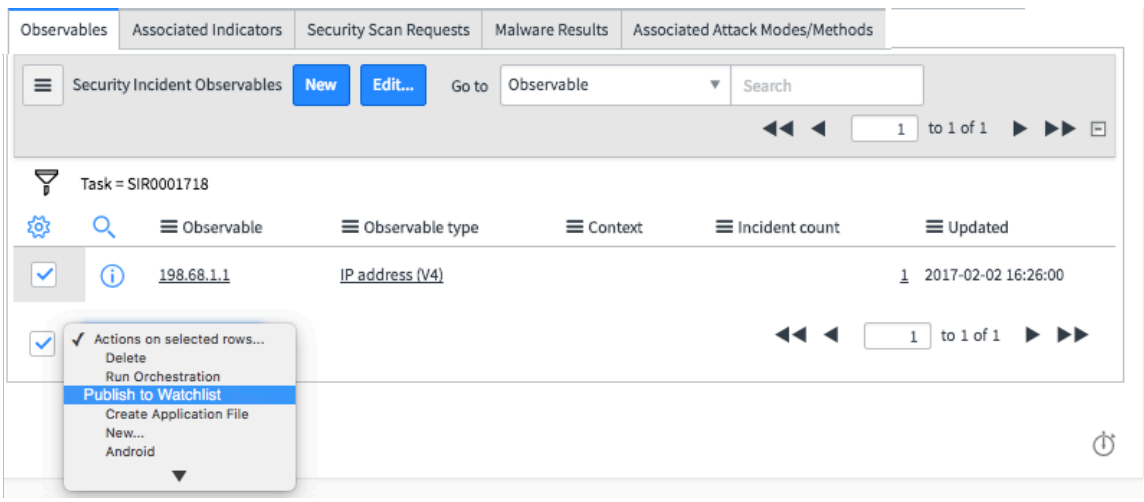
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Procedimento

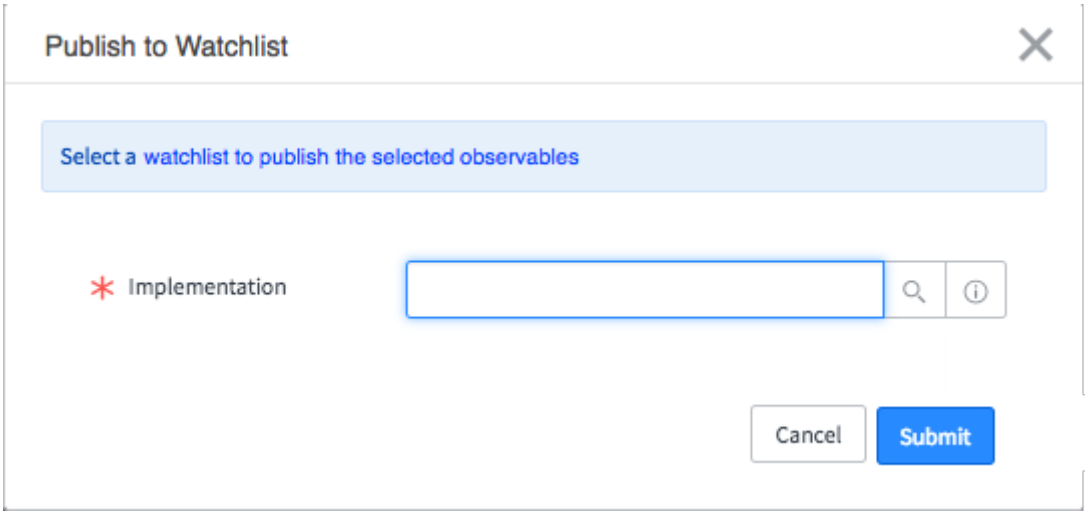
1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** em **Lista relacionada** guia.
3. Clique em **Publicar na Lista de observação** em **Ações nas linhas selecionadas...** menu suspenso.



A caixa de diálogo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira ou escolha a implementação.

> **Nota:** Um fluxo de trabalho é acionado pelo Integração de operações de segurança- Publicar na lista de observação Quando você seleciona a implementação do host do CrowdStrike Falcon.

5. Clique em **Enviar**.

Gerencie pesquisas e verificações

Você pode executar pesquisas e verificações de vulnerabilidade de incidentes de segurança e do catálogo de incidentes de segurança para identificar possíveis ameaças e vulnerabilidades.

Envie uma solicitação de Pesquisa de IOC de um incidente de segurança

Uma pesquisa de IOC é executada automaticamente sempre que observáveis são adicionados a um incidente de segurança. Se o incidente de segurança tiver anexos, eles poderão ser facilmente encontrados pressionando um botão.

Antes de Iniciar

Para pesquisas automáticas de IOC, o. Inteligência contra ameaças o plug-in deve ser ativado.

Função necessária: sn_si.basic

> **Nota:** Por padrão, o **Tipo de pesquisa** para **Arquivo** está inativo.

Procedimento

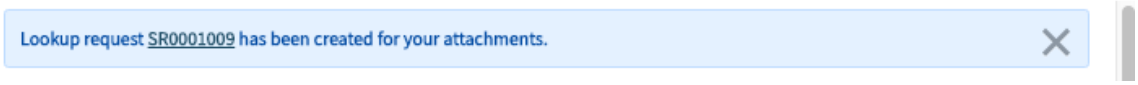
1. Crie um novo incidente de segurança ou abra um existente se você pretende anexar novos arquivos a ele.
2. Clique no ícone de clipe de papel no cabeçalho do formulário e anexe um ou mais arquivos.
3. Após concluir suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
   Depois que o registro for salvo, um **Pesquisar anexos** aparece.
4. Clique em **Pesquisar anexos** .

> **Nota:** As anotações de trabalho em **Detalhes do incidente** relate o andamento do processo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Você pode clicar no número de pesquisa no final da mensagem para exibir o registro de pesquisa. Você pode clicar no link Referência de pesquisa para exibir resultados detalhados.



Envie uma solicitação de pesquisa de IOC do Catálogo de incidentes de segurança

. Resposta a incidentes de segurança Se o plug-in estiver ativado, você pode enviar pesquisas de ameaças para arquivos, valores de hash, URLs e endereços IP do Catálogo de incidentes de segurança. As solicitações são enviadas e você pode exibir os resultados no **Minhas solicitações** módulo.

Antes de Iniciar

Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa

As pesquisas são realizadas automaticamente para o tipo de pesquisa padrão para cada origem de pesquisa listada no registro de pesquisa. Os resultados da solicitação de pesquisa estão disponíveis em **Minhas solicitações** módulo.

Procedimento

1. Navegar até **Tudo** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique em **Pesquisa de IOC** .
3. Clique em **Pesquisar arquivos, valores de hash, URLs ou endereços IP** .
4. Insira um ou mais dos seguintes:

Solicitação de pesquisa de IOC

Item a ser pesquisado	Descrição
Arquivos	Clique no ícone de clipe de papel e localize e anexe os arquivos que você deseja pesquisar. **Nota:** Por padrão, o **Tipo de pesquisa** para **Arquivo** está inativo. Os arquivos são convertidos e enviados como um valor de hash.
URLs	Em **URLs** , insira os URLs que você deseja pesquisar, separados por vírgulas. Por exemplo: www.abc.com,www.xyz.net.
Endereços IP	Em **Endereços IP** , insira os endereços IP que você deseja pesquisar, separados por vírgulas.
Valores do hash	Em **Valores de hash** insira os valores de hash que você deseja pesquisar, separados por vírgulas. **Nota:** . **Tipo de pesquisa** para **Arquivo** inativo, este valor é a ação padrão para ambos **Arquivo** e. **Valores de hash** .

5. Depois de fazer suas seleções, clique em **Enviar** .
6. Para exibir o status e/ou os resultados das pesquisas, navegue até **Autoatendimento** > **Minhas solicitações**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique no número de SR da solicitação.
   As anotações de trabalho em **Atividade** Liste as tarefas realizadas durante a pesquisa, incluindo a criação de pesquisas individuais para cada arquivo, valor de hash, URL ou endereço IP e os resultados da pesquisa.

Envie uma solicitação de verificação de vulnerabilidade de um incidente de segurança

Se o incidente de segurança tiver um ou mais itens de configuração (servidores, computadores e assim por diante), eles poderão ser verificados em busca de vulnerabilidades do Resposta a incidentes de segurança formulário.

Antes de Iniciar

. Resposta a vulnerabilidades o plug-in deve ser ativado.

Função necessária: sn_si.write

Procedimento

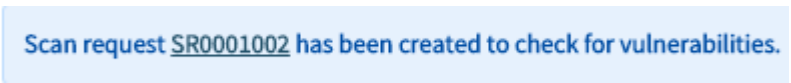
1. Crie um incidente de segurança e incluem pelo menos um recurso.
   Você também pode abrir um incidente existente que tenha itens de configuração.
2. Após concluir suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
   Depois que o registro for salvo, um **Verificar vulnerabilidades** o link relacionado é exibido.

   Nota: . **Verificar vulnerabilidades** a lista relacionada não é mostrada, você deve navegar até **Vulnerabilidade** > **Scanners**, configure pelo menos um scanner e defina seu padrão como **verdadeiro** .

3. Clique em **Verificar vulnerabilidades** .

   Nota:

   Uma mensagem aparece na parte superior do formulário de incidente de segurança, junto com um link para o registro de verificação.

4. Você pode clicar no número da solicitação de verificação para exibir o registro de verificação.
   Os detalhes do incidente mostram os resultados da verificação no registro Solicitação de verificação de segurança.

Envie uma solicitação de verificação de vulnerabilidade do catálogo Resposta de incidente de segurança

Você pode enviar verificações de vulnerabilidade para ICs e endereços IP do Resposta a incidentes de segurança catálogo. As solicitações são enviadas e você pode exibir os resultados no **Minhas solicitações** módulo.

Antes de Iniciar

Função necessária: nenhuma

Procedimento

1. Navegar até **Tudo** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique em **Verificação de vulnerabilidades** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Itens de configuração de verificação e endereços IP** .
4. Insira um ou mais dos seguintes a serem verificados.

Scanners de vulnerabilidades

Item a ser verificado	Descrição
Item de configuração	Em **Item de configuração a ser verificado** Selecione o IC a ser verificado.
Endereços IP	Em **Endereços IP a serem verificados** , insira os endereços IP, separados por vírgulas.

5. Depois de fazer suas seleções, clique em **Enviar** .
   Se um observável for encontrado, um indicador será criado, de acordo com os padrões STIXX.
6. Para exibir o status e/ou os resultados das verificações, navegue até **Autoatendimento** > **Minhas solicitações**.
7. Clique no número de SR da solicitação.
   As anotações de trabalho em **Atividades** Liste as tarefas realizadas durante a verificação, incluindo a criação de verificações individuais para cada IC ou endereço IP e os resultados das verificações.

Defina novas orquestrações sob demanda

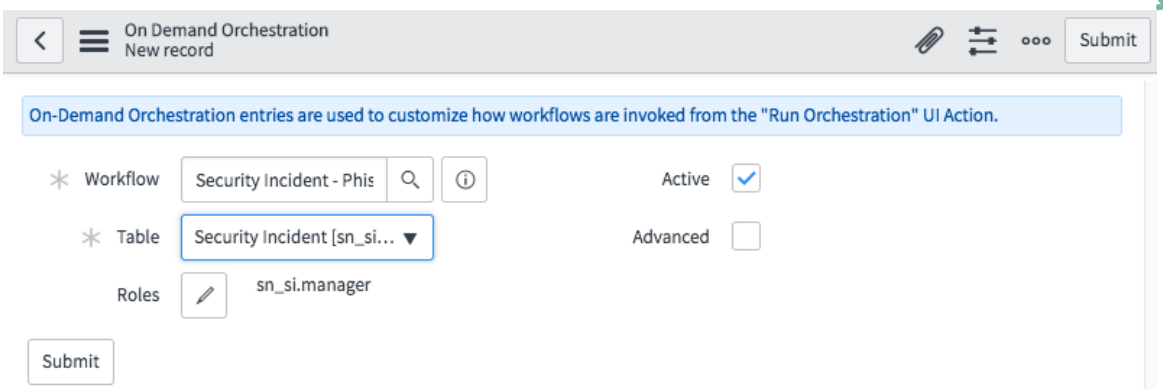
No sistema de base, você pode selecionar orquestrações sob demanda que executam fluxos de trabalho predefinidos. Você pode definir novas orquestrações sob demanda para personalizar como os fluxos de trabalho são invocados a partir do **Executar Orquestração** listas de seleção.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Orquestração sob Demanda**
2. Clique em **Nova**.



3. Preencha os campos, se for o caso.

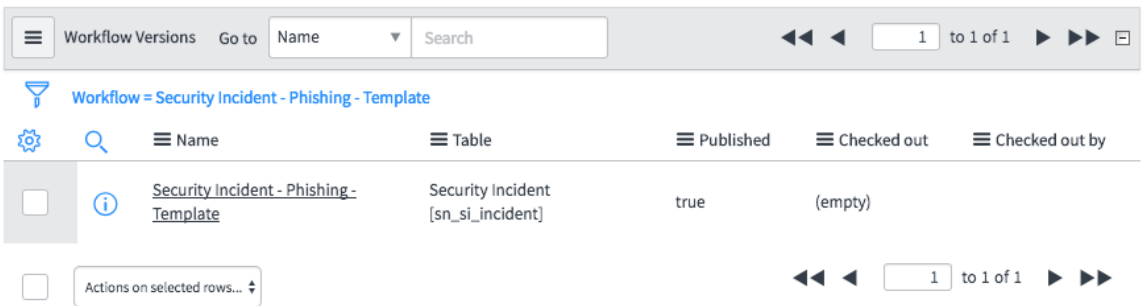
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração sob Demanda

Campo	Descrição
Fluxo de trabalho	Selecione o fluxo de trabalho a ser incluído no **Executar Orquestração** lista de seleção.
Tabela	Selecione a tabela na qual o fluxo de trabalho selecionado é executado. Se a tabela não corresponder à tabela configurada para o fluxo de trabalho selecionado, você deverá selecionar **Avançado** e modifique o. **Script de execução** para passar o registro correto para o fluxo de trabalho na execução.
Funções	Conforme necessário, selecione funções adicionais para restringir quem pode ver este fluxo de trabalho no **Executar Orquestração** lista de seleção.
Ativo	Marque esta caixa de seleção para ativar este registro de Orquestração sob demanda.
Avançado	Marque esta caixa de seleção para modificar o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho.
Script de execução	Modifique o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho. Este campo aparece apenas se a caixa de seleção **Avançado** estiver marcada.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar** .
. **Versões do fluxo de trabalho** a lista relacionada é exibida.



5. Se você precisar fazer modificações adicionais no fluxo de trabalho, será necessário fazer check-out dele.

Tópicos relacionados

Trabalhe com versões de fluxo de trabalho

Registre novas aplicações de Operações de segurança para orquestração sob demanda

No sistema de base, as aplicações de Operações de segurança são registradas automaticamente quando são ativadas. O registro permite que os fluxos de trabalho associados às aplicações estejam disponíveis para solicitações de orquestração sob

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

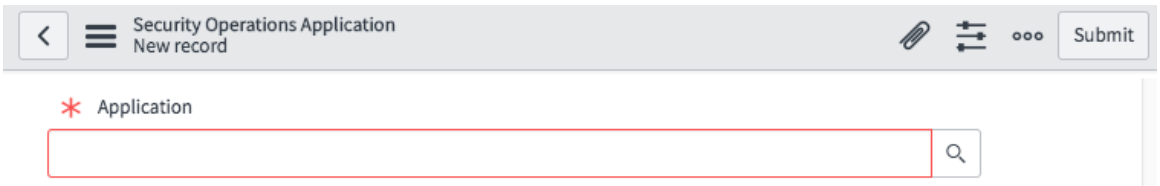
demanda. Se necessário, você pode definir novas aplicações e associar fluxos de trabalho a elas para orquestração sob demanda.

Antes de Iniciar

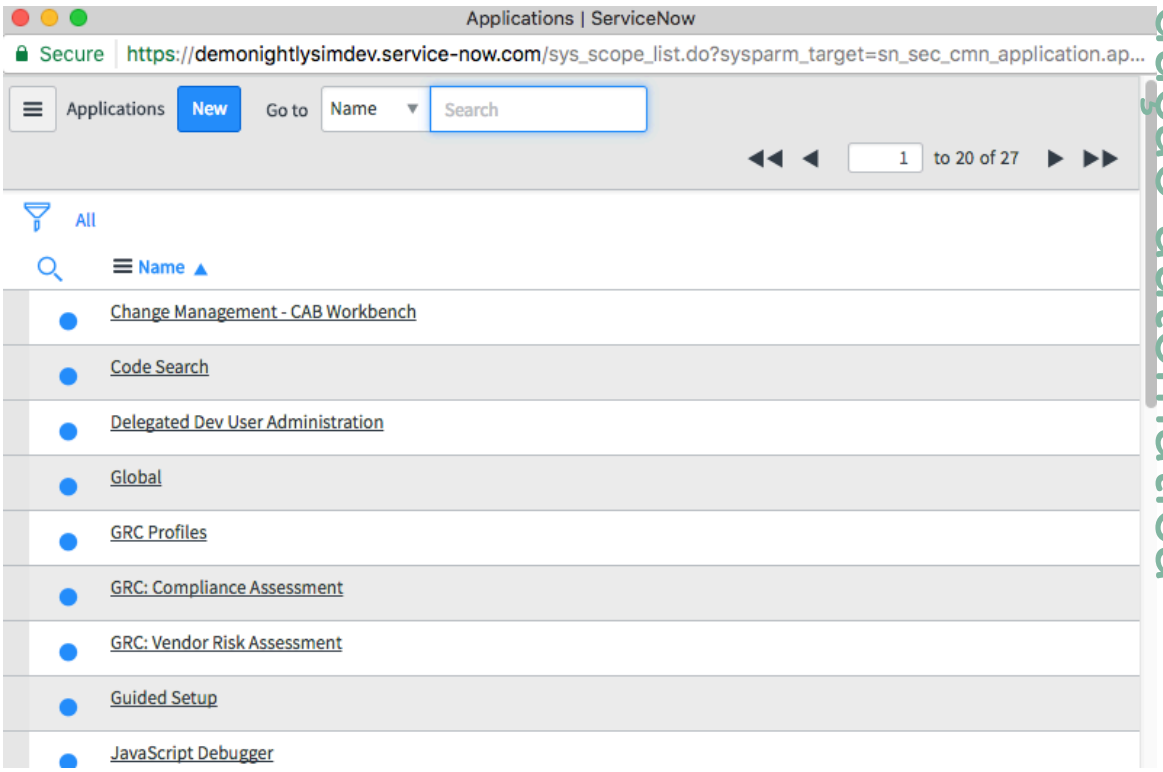
Função necessária: sn_si.write

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Registro da aplicação SecOps** e clique em **Registrar aplicação** .
   A tela da aplicação Operações de segurança é exibida.



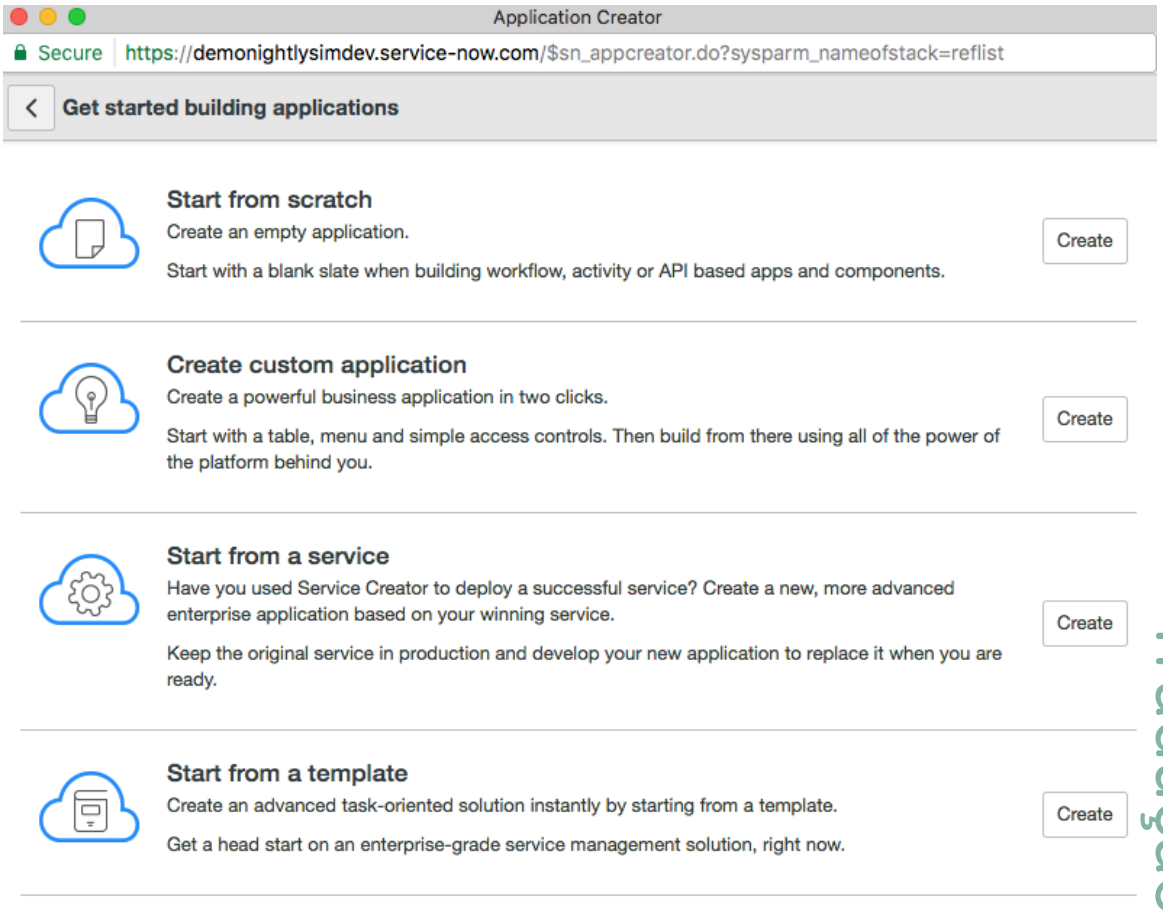
2. Em **Aplicação** , clique no ícone pesquisas (lupa).
   A tela Aplicações é exibida.



3. Clique em **Nova**.
   A tela Criador de aplicações é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: As opções exibidas dependem das aplicações que você ativou. Para obter informações detalhadas sobre como criar novas aplicações, consulte Criação de aplicações .

4. Depois que a aplicação for gerada, você poderá criar scripts para configurar a orquestração sob demanda.

Nota: Configurar a Orquestração sob demanda para novas aplicações requer conhecimento técnico avançado de script e criação de gatilhos para os scripts (regras de negócios, ação de IU, fluxos de trabalho e assim por diante). Para obter mais informações, entre em contato ServiceNow Serviços profissionais.

Adicione informações a um incidente de segurança

Depois que um incidente de segurança é criado, você pode adicionar mais detalhes para ajudar na análise, como funções de acesso e diferentes tipos de anotações.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique em **Detalhes do incidente** guia.
3. Preencha os campos, conforme necessário.

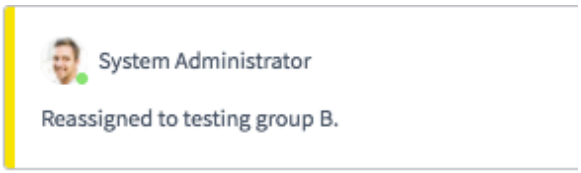
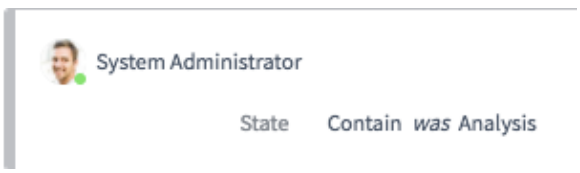
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

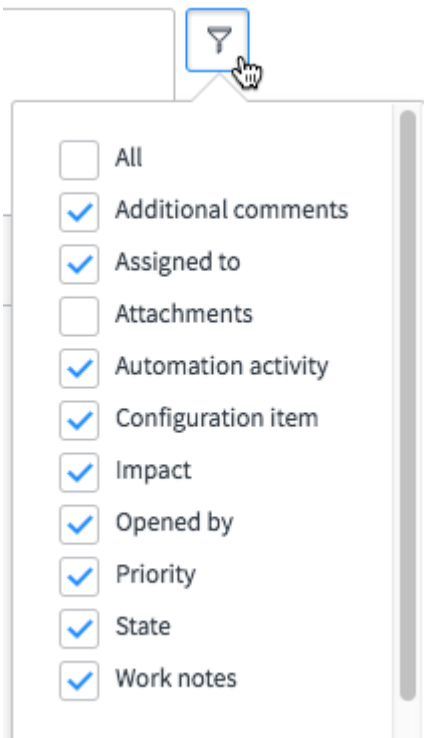
Campo	Descrição
Acesso de leitura	Fornece a um usuário com **acesso especial** acesso de leitura da função ao incidente de segurança. O usuário pode ler e escrever anotações de trabalho. **Nota:** ◦ Se um usuário for adicionado a ambos **Acesso de leitura** e. **Acesso privilegiado** e, em seguida, somente o. **Acesso privilegiado** as permissões persistem. ◦ Somente usuários com a função sn_si.admin podem modificar o acesso de leitura e o acesso privilegiado.
Participantes da lista de observação	Clique no ícone de cadeado para adicionar usuários que serão notificados quando ocorrerem mudanças no incidente de segurança. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Após concluir suas entradas, clique no ícone de cadeado para bloquear o campo.
Acesso privilegiado	Fornece a um usuário com **acesso especial** acesso de leitura e gravação da função a todos os campos do incidente de segurança, exceto **Atribuído a.** . Usuários com funções de acesso especial têm seu próprio módulo que contém todos os incidentes de segurança atribuídos a eles. Nenhum outro módulo está disponível para eles. Ninguém mais pode ver **Visível para mim** módulo. **Nota:** Somente um usuário atribuído ou alguém com uma função de segurança (por exemplo, sn_si_analyst ou sn_si.admin) pode mudar o. **Atribuído a.** campo. Se um usuário for adicionado a ambos **Acesso de leitura** e. **Acesso privilegiado** e, em seguida, somente o. **Acesso privilegiado** as permissões persistem.
Lista de anotações de trabalho	 Clique no ícone de cadeado ( ) para adicionar usuários que são notificados quando novas anotações de trabalho são adicionadas. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Após concluir suas entradas, clique no ícone de cadeado para bloquear o campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Insira uma descrição completa do incidente de segurança, junto com todas as informações que possam ajudar a encontrar a causa ou resolver o problema.
Notas de segurança	Somente funções de usuário com sn_si.admin e sn_si.analyst podem exibir ou editar as anotações seguras.
Anotações de trabalho	Digite anotações de trabalho que não estão visíveis para o cliente. As anotações de trabalho aparecem no **Atividade** área.
Atividade	Exibe informações inseridas manualmente nas anotações de trabalho e todas as atividades de tarefa atualizadas dinamicamente (ações, comentários, anotações de trabalho e assim por diante) em registros relacionados a este incidente de segurança. As anotações de trabalho aparecem com uma faixa amarela.  As anotações geradas automaticamente aparecem com uma faixa cinza. 

4. Você pode limitar os tipos de informações exibidas no **Atividade** clicando no filtro (ícone).



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: . **Atividade de automação** a caixa de seleção permite incluir qualquer aprimoramento realizado por este incidente de segurança, incluindo atividades de fluxo de trabalho, atualizações de pontuação de risco e assim por diante.

5. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Registros relacionados
   - Análise pós-incidente
   - Informações de Fechamento
6. Ao concluir suas entradas, clique em **Enviar** .

Adicione problemas, mudanças e incidentes relacionados a um incidente de segurança

Você pode adicionar registros relacionados, como problemas, mudanças e incidentes, a incidentes de segurança existentes.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique em **Registros relacionados** guia.
3. Preencha os campos, conforme necessário.

Campo	Descrição
Problema	Selecione um registro de Problema (PRB) que resolva o problema subjacente que causou a criação deste incidente de segurança. Os PRBs para este incidente são normalmente criados clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar problema** .
Primário	Selecione um registro de tarefa relacionado ao problema subjacente que causou a criação deste incidente de segurança.
Incidente de segurança primário	Selecione um registro de incidente de segurança relacionado ao problema subjacente que causou a criação deste incidente de segurança. Consulte Relacionamentos de incidentes de segurança primários e secundários.
incidente	Selecione um registro de Incidente (INC) que resolva o problema subjacente que causou a criação deste incidente de segurança. O incidente é normalmente criado clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar incidente** .
Solicitação de mudança	Selecione um registro de Solicitação de Mudança (CHG) que resolva o problema subjacente que causou a criação deste incidente de segurança. A solicitação de mudança é normalmente criada clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar mudança** .

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Detalhes do incidente
- Análise pós-incidente
- Informações de Fechamento

5. Ao concluir suas entradas, clique em **Enviar** .

Invoque um despejo de processo para um processo aprimorado no Windows

Um analista de segurança pode executar um despejo de processo em um processo específico, despejá-lo em um arquivo e publicá-lo em um site compartilhado em uma rede interna. Um analista pode exibir um processo listado de proibições, realçado em vermelho em um incidente de segurança e executar uma análise adicional.

Antes de Iniciar

Os seguintes itens são necessários:

- Um cliente que executa o Windows Vista ou superior ou um servidor que executa o Windows Server 2008 ou superior.
- O utilitário de linha de comando ProcDmp instalado, com uma variável de ambiente do sistema que aponta para o caminho do arquivo executável procdump. O nome da variável deve ser PROCDUMP. Este nome é usado em um script powershell.

Função necessária: sn_si.analyst

Procedimento

1. Navegue até o incidente de segurança com o processo aprimorado no qual você deseja invocar um procdump clicando em **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**e abra um incidente de segurança.
2. Clique em **Dados de aprimoramento** guia.
3. Clique em **Recuperar processos em execução** registro de aprimoramento.
4. Marque as caixas de seleção dos processos em execução para os quais você deseja executar um procdump, clique na lista suspensa Ações nas linhas selecionadas na parte inferior da lista e clique em **Execute Procdump** .
   Um **Fluxo de trabalho de prodump iniciado para o processo selecionado** a mensagem aparece na parte superior da lista e **Resposta do incidente de segurança - Executar procdump** o fluxo de trabalho é executado.

Exiba informações em um incidente de segurança

Você pode executar várias outras ações em um incidente de segurança existente usando os links relacionados.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Em **Links relacionados** , você pode executar as seguintes tarefas,

Opção	Descrição
Exibir runbook manual	Exiba uma lista de runbooks disponíveis para este incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Fluxo de trabalho de resposta	Exiba qualquer fluxo de trabalho associado a este incidente.
Adicionar Vários Observáveis	Adiciona uma lista de observáveis em formatos delimitados por vírgula, nova linha, guia ou barra vertical.
Adicionar ao Caso de Segurança	Adiciona o incidente de segurança a um ou mais casos de segurança. Você também pode criar um novo caso de segurança e adicionar este incidente de segurança a ele.
Obter resumos de IP do QRadar	Se uma integração do QRadar estiver disponível e contiver ICs válidos, endereços IP de origem e destino, ela acionará os fluxos de trabalho do QRadar e exibirá os resultados em anotações de trabalho.
Executar Orquestração	Escolha e execute um fluxo de trabalho de Operações de segurança.
Exibição da linha do tempo do ANS	Você pode exibir uma linha do tempo de ANS de um registro de ANS de tarefa ou de uma definição do ANS.
Mostrar todas as listas relacionadas	Exibe todas as listas relacionadas padrão e todas as listas adicionadas manualmente. **Nota:** Itens adicionados manualmente estão disponíveis somente nesta exibição.
Mostrar itens afetados	Exibe as listas de ICs, usuários e serviços diretamente afetados por este incidente
Mostrar itens relacionados	Exibe as listas de incidentes relacionados, ICs, usuários e grupos afetados por este incidente.
Mostrar IoC	Exibe as listas de observáveis, indicadores, malware, modos e métodos e solicitações de verificação de segurança associadas a este incidente.
Mostrar dados de enriquecimento	Exibe as listas de dados de aprimoramento, processos, serviços, estatísticas, pesquisas, logs de firewall e informações do usuário comprometido associadas a este incidente.
Mostrar tarefas de resposta	Exibe as listas de tarefas, SLAs, auditorias de pontuação de risco, indisponibilidades e pesquisas do Exchange associadas a este incidente.
Exibir detalhes no sistema externo	. Se este incidente de segurança foi gerado a partir de uma aplicação externa, diretamente ou por eventos, e um link para os dados de origem foi fornecido, o. **Exibir detalhes no sistema externo** A ação abre o URL. Você pode exibir e pesquisar os logs que geraram este incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

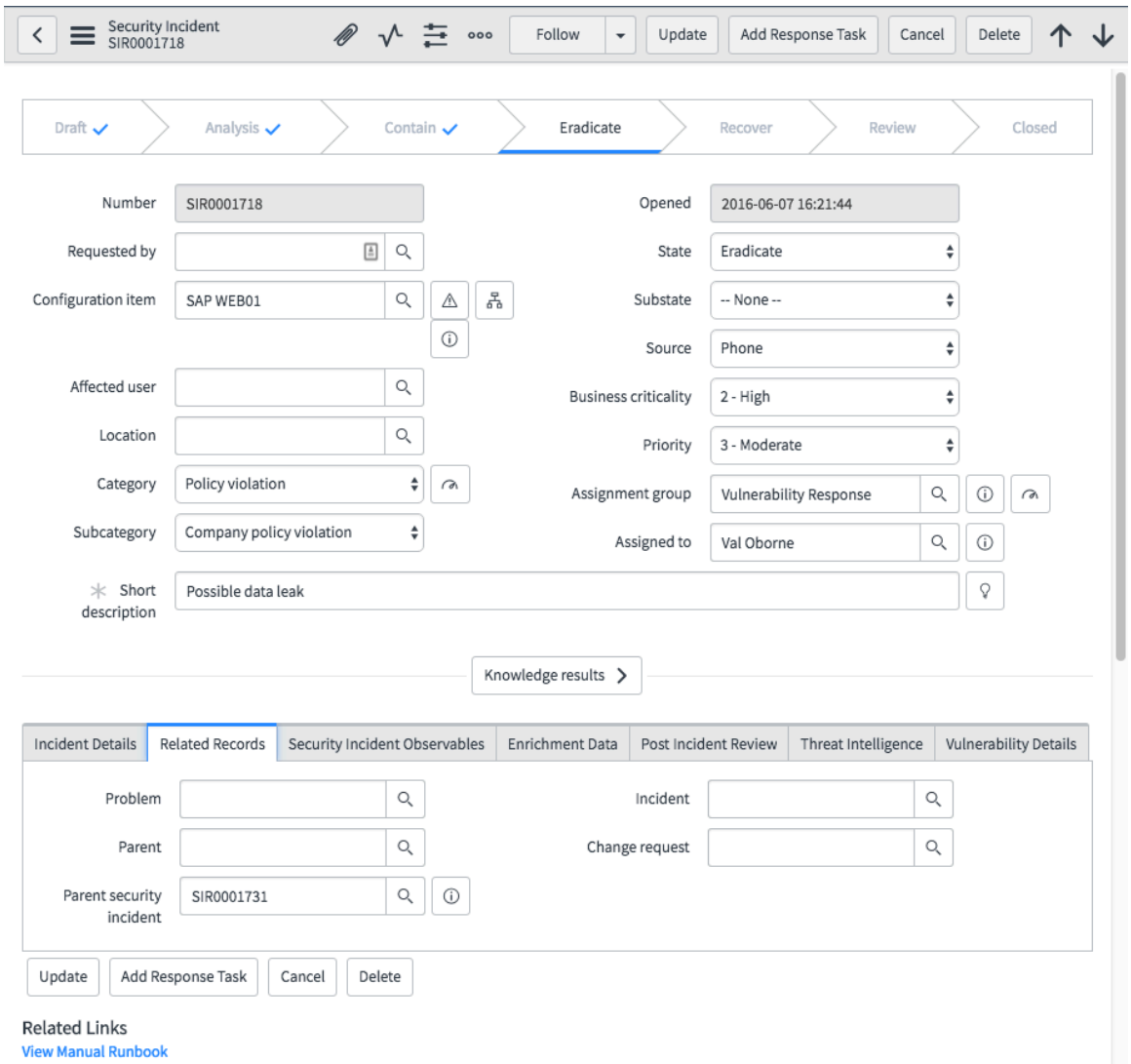
Opção	Descrição
Verificar vulnerabilidades	Se Resposta a vulnerabilidades E você selecionou pelo menos um IC afetado para o incidente de segurança, você pode enviar uma solicitação de verificação para determinar quais vulnerabilidades existem no IC.

Relacionamentos de incidentes de segurança primários e secundários

Você pode associar e rastrear o impacto de qualquer problema específico usando relacionamentos de incidente de segurança primário e secundário em Resposta a incidentes de segurança.

Usando o. **Registros relacionados** , você pode adicionar um **Incidente de segurança primário** problema para qualquer um Resposta a incidentes de segurança formulário. Automaticamente, este recurso torna o incidente secundário que aparece em **Listas relacionadas - Incidentes de segurança secundários** problema primário.

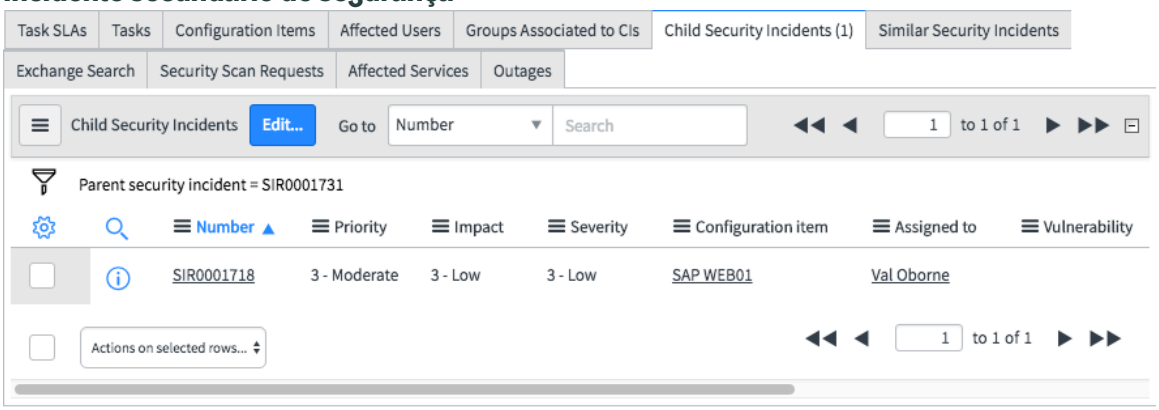
Nota: Um incidente de segurança primário existente não pode ser secundário usando o mesmo número para ambos os incidentes.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente secundário de segurança

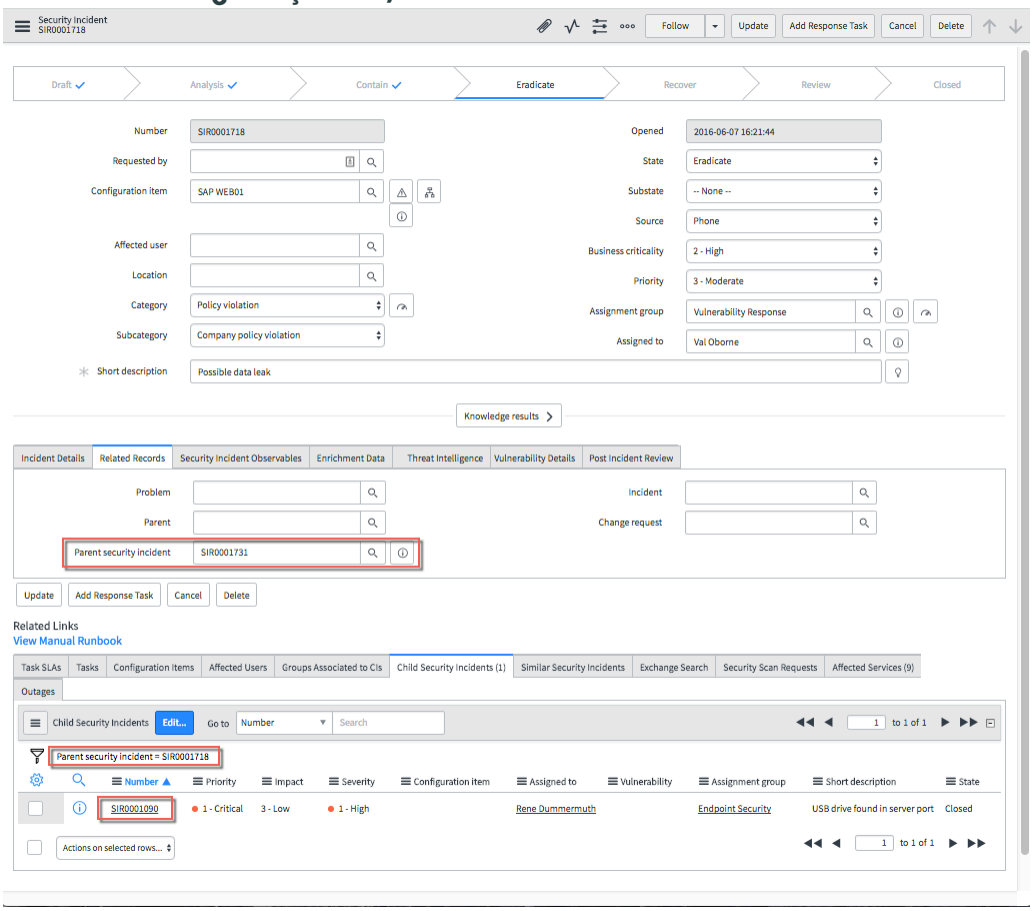


Você pode adicionar um ou mais **Incidentes de segurança secundários** para qualquer registro de incidente de segurança, bem como, usando o. **Editar** botão em **Incidentes de segurança secundários** guia. No exemplo a seguir, todos os três registros estão conectados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidentes de segurança Avós, Primários e Secundários



Observação:

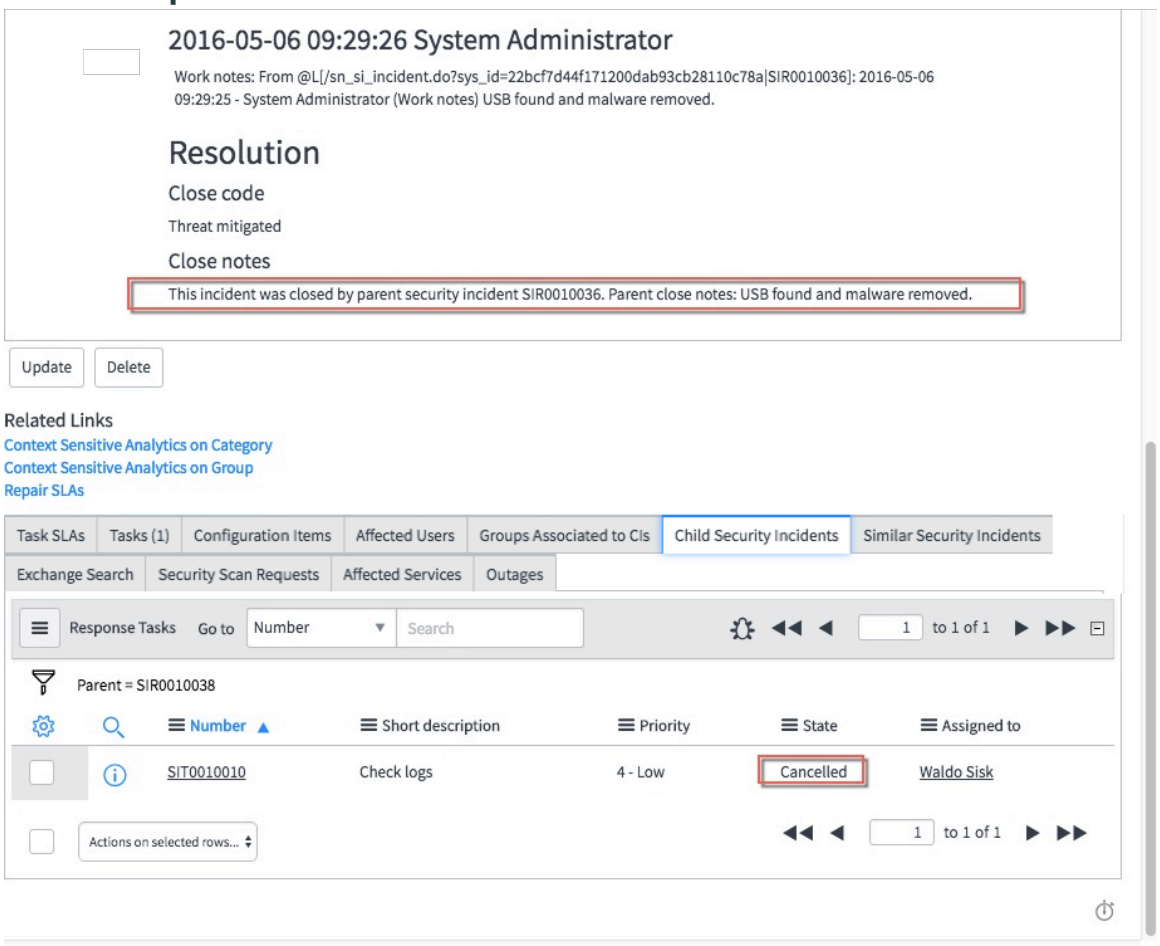
- Todas as anotações de trabalho registradas no primário são propagadas para todos os secundários ativos em **Atividades** em **Detalhes do incidente** guia.
- . **Primário** O campo é usado para associar o incidente de segurança a um registro primário, como um incidente grave, problema ou solicitação de mudança, que está fora do módulo Incidente de segurança. Para agrupar vários incidentes de segurança em um incidente de segurança principal, o. **Incidente de segurança primário** o campo é usado.

Quando um primário é encerrado ou cancelado, todos os secundários ativos também são encerrados ou cancelados. Ativo **Tarefas de resposta** os incidentes secundários são cancelados. Se não houver outros em aberto **Tarefas** , o incidente secundário está encerrado. . **Entrevista pós-incidente** registra o fechamento e as informações encontradas no **Informações de fechamento** a guia é propagada do primário para os secundários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta secundária



Exibir itens afetados para um incidente de segurança

Você pode exibir itens afetados, como ICs, usuários afetados e serviços afetados associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança cujos itens afetados você deseja exibir.
2. Clique em **Mostrar itens afetados** link relacionado.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações sobre o incidente de segurança.

Tab	Descrição
Itens de configuração	Itens de configuração (IC) afetados. Depois que os ICs afetados são identificados, você pode adicionar manualmente os recursos afetados desta lista relacionada.
Usuários afetados	Depois que os usuários afetados são identificados, você pode adicionar manualmente usuários afetados a partir desta lista relacionada.
Serviços afetados	Exiba ou adicione serviços de negócios associados ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tab	Descrição
	Nota: Se um IC afetado for adicionado após a abertura do incidente de segurança, é uma boa ideia clicar com o botão direito do mouse no cabeçalho do formulário e selecionar **Atualizar serviços afetados** .

Nota: . Integração de operações de segurança - Obter processos em execução O recurso de integração está ativo e você adiciona um IC a um incidente de segurança, o. Obter processos em execução O fluxo de trabalho é executado e recupera uma lista de processos em execução no IC.

. Integração de operações de segurança - Isolar host A capacidade de integração está ativa, você pode selecionar um ou mais ICs e restringir suas conexões do sistema a outros dispositivos. Para fazer isso, marque as caixas de seleção dos ICs e clique em **Isolar host** em **Ações nas linhas selecionadas** lista de seleção.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar** .

Exibir itens relacionados de um incidente de segurança

Você pode exibir itens relacionados, como incidentes de segurança semelhantes e secundários, usuários relacionados, grupos de vulnerabilidades e itens vulneráveis associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir itens relacionados.
2. Clique em **Mostrar itens relacionados** link relacionado.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações sobre o incidente de segurança.

Tab	Descrição
Incidentes de segurança secundários	Selecione um registro de tarefa relacionado ao problema que causou a criação deste incidente de segurança.
Incidentes de segurança semelhantes	Exiba todos os outros incidentes de segurança associados a qualquer um dos mesmos registros observáveis.
Itens de Configuração Relacionados	Exibe uma lista de incidentes de segurança que contém itens de configuração com o mesmo observável deste incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tab	Descrição
	Esta lista pode ser filtrada usando **Exclusões de IC** grupo de filtros. Quando um observável é adicionado a um incidente de segurança, esta lista é atualizada automaticamente. Por padrão, observáveis com um tipo de contexto Destino são excluídos.
Usuários relacionados	Exibe uma lista de incidentes de segurança que contém usuários com os mesmos observáveis deste incidente de segurança. Esta lista pode ser filtrada usando **Exclusão de usuário** grupo de filtros. Quando um observável é adicionado a um incidente de segurança, esta lista é atualizada automaticamente. Por padrão, observáveis com um tipo de contexto Destino são excluídos.
Grupo de filtros relacionados	Depois que os itens de configuração são identificados, qualquer IC ou grupo de filtro correspondente é adicionado automaticamente.
Grupos de vulnerabilidades	Se Resposta a vulnerabilidades estiver ativado, você pode exibir grupos de vulnerabilidade associados a este incidente de segurança.
Itens vulneráveis	Se Resposta a vulnerabilidades estiver ativado, você pode exibir itens de vulnerabilidade associados a este incidente de segurança.
Riscos	Se qualquer um dos plug-ins principais da Gestão de riscos (Gestão de políticas e conformidade, Auditoria, Gestão ou Gestão de riscos) estiver ativado, você poderá exibir ou adicionar riscos associados ao incidente de segurança. Você pode adicionar esta lista relacionada no menu de contexto do cabeçalho do formulário em **Configurar** > **Listas relacionadas**.
Eventos de item de configuração	Se Gestão de eventos ativado, você pode exibir eventos.
Alertas de item de configuração	Se Gestão de eventos ativado, você pode exibir alertas.
Casos de atendimento ao cliente	Se Atendimento ao cliente está ativado, você pode exibir Atendimento ao cliente informações do caso.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar** .

Exibir dados de aprimoramento de um incidente de segurança

Você pode exibir dados de aprimoramento, como processos em execução, serviços em execução e estatísticas de rede associadas a um incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança cujos dados de aprimoramento você deseja exibir.
2. Clique em **Mostrar Dados de Aprimoramento** link relacionado.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações sobre o incidente de segurança.

   Nota: Os detalhes dos dados brutos são armazenados em um anexo do registro de dados de aprimoramento. Se excederem o limite do campo, os detalhes exibidos serão truncados.

Tab	Descrição
Processos em execução	Armazena os registros criados pelo Resposta a incidentes de segurança **Obter processos em execução** fluxo de trabalho.
Serviços em execução	Armazena os registros criados pelo Resposta a incidentes de segurança **Obter serviços em execução** fluxo de trabalho.
Estatísticas de Rede	Armazena os registros criados pelo Resposta a incidentes de segurança **Obter estatísticas de rede** fluxo de trabalho.
Pesquisas de domínio	. Integração com WhoisXML API O plug-in está ativado, armazena os registros criados por uma pesquisa do Whois.
Logs do Firewall	Armazena dados de aprimoramento de logs de firewall, como os logs de firewall da Rede Palo Alto.
Informações do usuário comprometido	Armazena contas identificadas como sendo comprometidas por meio de um pesquisa.

   Observação: O. **Dados de aprimoramento de segurança** mostra dados brutos de aprimoramento de Resposta a incidentes de segurança fluxos de trabalho, como recuperar estatísticas de rede ou processos em execução. Esta guia pode ser exibida clicando em **Mostrar todas as listas relacionadas** link relacionado.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar** .

Exibir informações da tarefa de resposta para um incidente de segurança

Você pode exibir informações da tarefa de resposta, como ANS de tarefa, auditorias de pontuação de risco e indisponibilidades associadas a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança cujas tarefas de resposta você deseja exibir.
2. Clique em **Mostrar tarefas de resposta** link relacionado.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações sobre o incidente de segurança.

Tab	Descrição
Tarefas	Exibe tarefas já definidas para o incidente de segurança. Você pode criar manualmente uma tarefa de resposta.
Tarefas de resposta	Exibe as ações a serem executadas em resposta ao incidente de segurança.
ANS de tarefas	Exiba ou adicione ANS de tarefa ativos que foram definidos para o incidente de segurança.
Auditorias de Pontuação de Risco	Um registro de auditoria para cada instância de uma pontuação de risco que está sendo alterada.
Indisponibilidades	Exiba ou adicione manualmente novos registros de indisponibilidade associados ao incidente de segurança.
Pesquisa de E-mail	Uma lista de registros que contém critérios de pesquisa para executar consultas em um servidor de e-mail, como um Microsoft ®Exchange Server (com base na implementação instalada) e armazena os resultados recebidos. **Nota:** . Integração de operações de segurança - Recurso de pesquisa e exclusão de e-mail não está ativo, o. **Pesquisa de e-mail** o link relacionado não é exibido.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
5. Ao concluir suas entradas, clique em **Enviar** .

Exiba eventos e alertas relacionados em incidentes de segurança

Como um incidente de segurança está sendo trabalhado, você pode exibir os detalhes dos eventos. Para alertas, você pode exibir e confirmar esses alertas e criar incidentes ou incidentes de segurança a partir deles, conforme necessário.

Antes de Iniciar

Você deve ter o plug-in de suporte da Gestão de eventos de resposta a incidentes de segurança ativado.

Função necessária: si.sn_agent

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Tudo** > **Incidente de segurança** > **incidentes** > **Incidentes não atribuídos**).
2. Se os recursos afetados pelo incidente de segurança que você está exibindo tiverem recebido alertas ou eventos nas 24 horas anteriores, uma ou ambas as listas relacionadas a seguir serão exibidas.
   - Alertas de IC de incidente de segurança
   - Eventos de IC de incidente de segurança
3. Clique na lista relacionada que você deseja exibir.

Lista relacionada	Descrição
Alertas de IC de incidente de segurança	Você pode exibir detalhes de alertas recebidos nas últimas 24 horas. Você tem a opção de clicar **Confirmar** indicar que você está ciente do alerta e ele está sendo tratado. Usar **Fechar** indicar que o alerta não é importante.
Eventos de IC de incidente de segurança	Você pode exibir detalhes do evento recebido nas últimas 24 horas.

Exibir incidente de segurança para mapeamento de caso de atendimento ao cliente

Resposta a incidentes de segurança fornecido com um mapeamento de campo padrão que mapeia um incidente de segurança para um Atendimento ao cliente caso. Você pode exibir o incidente de segurança para o mapa padrão do caso CS.

Antes de Iniciar

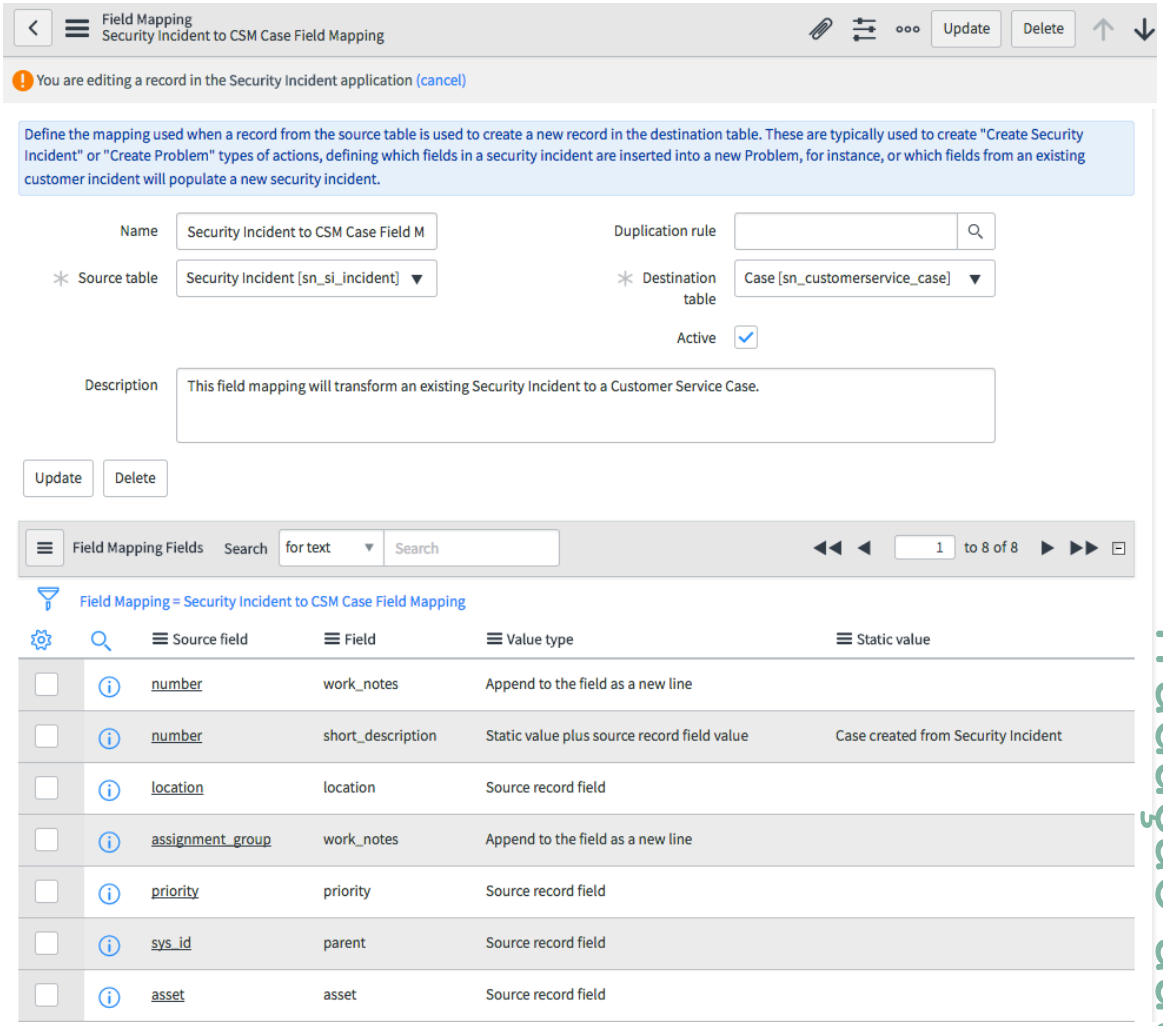
Função necessária: Sec_cmn.read

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Mapeamento de Campos**.
2. Clique em **Incidente de segurança para mapeamento de campo de caso de CSM** para exibir o mapa padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Você pode editar o mapeamento, conforme necessário.
4. Ao concluir as mudanças, clique em **Atualização** .

Exiba um runbook de Resposta de incidente de segurança

Os runbooks dão acesso a procedimentos relacionados às tarefas nas quais você está trabalhando.

Antes de Iniciar

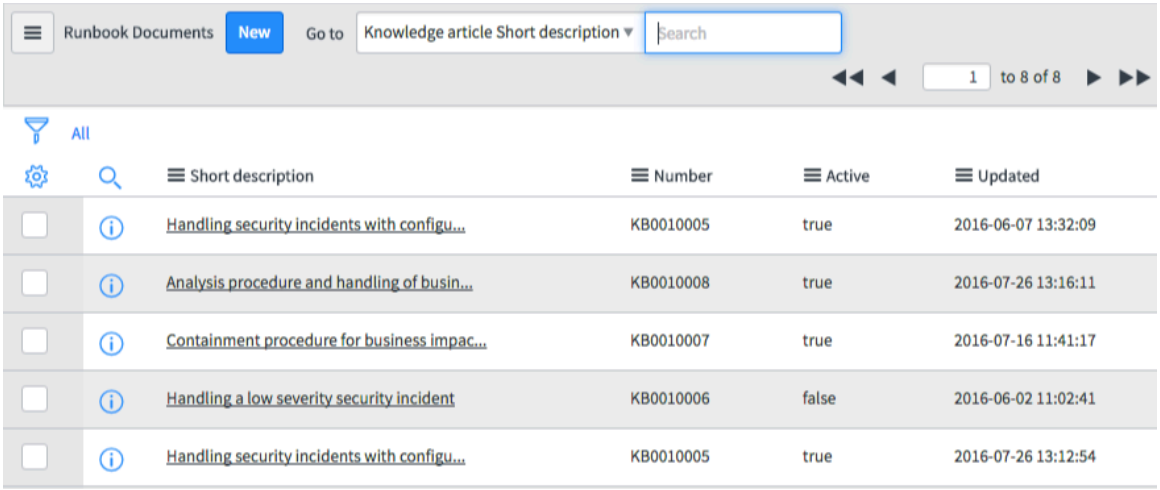
Função necessária: sn.si.knowledge_admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Runbook manual** > **Exibir documentos do runbook**.
2. Selecione um runbook na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para criar um runbook, clique em **Novo** .
   Para obter mais informações, consulte Crie um runbook .

Identifique todos os itens de configuração afetados por um incidente de segurança

Se você souber qual recurso (servidor, desktop ou outro item de configuração) está por trás de um incidente de segurança e quiser identificar recursos e serviços de negócios relacionados que podem ser afetados, poderá usar o mapa de Gestão de serviços de negócios (BSM).

Antes de Iniciar
Função necessária: administrador ou sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O mapa BSM exibe as dependências ascendentes e descendentes de um IC raiz selecionado.

Há dois métodos que você pode usar para exibir o mapa BSM de um IC:

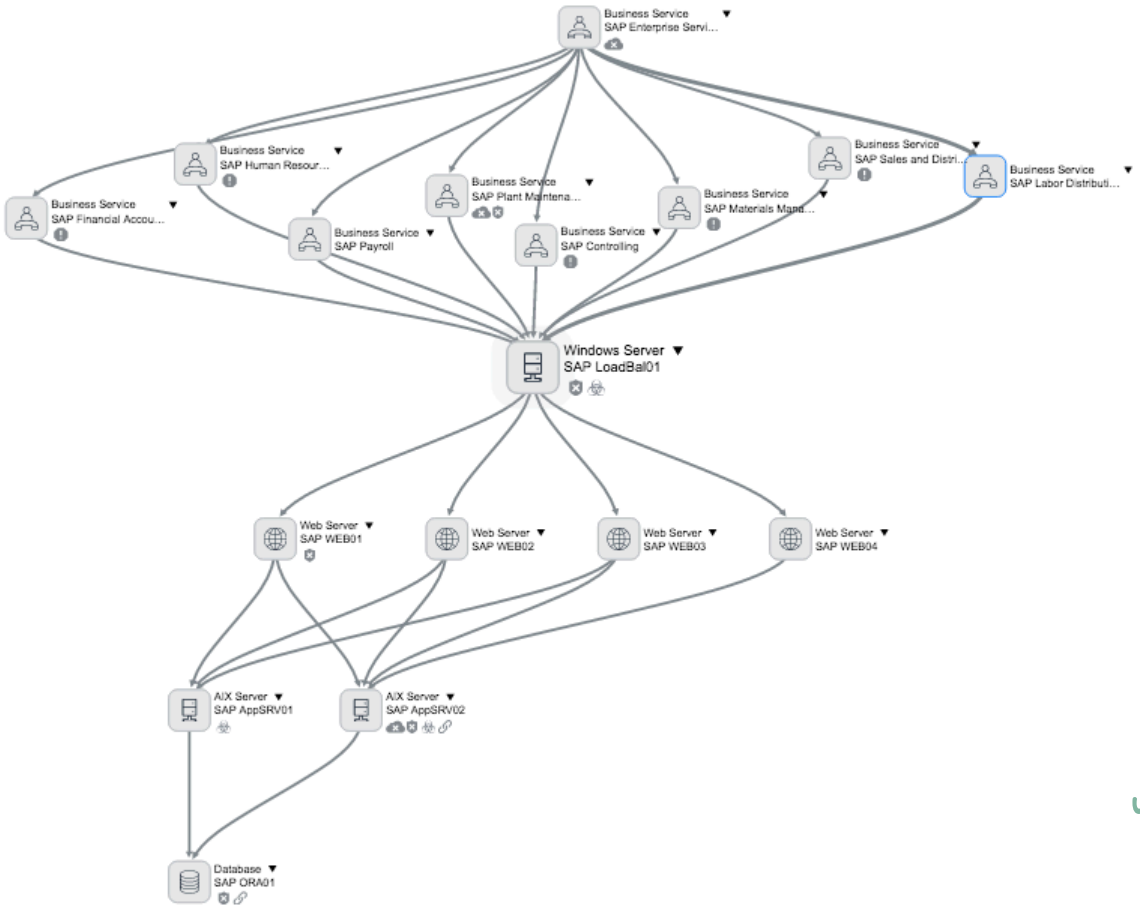
- Para exibir ICs do contexto de uma tarefa, exiba no formulário de incidente de segurança.
- Se você não quiser exibir ICs de um ponto de vista de tarefa, exiba na barra de navegação.

Procedimento

1. No formulário Incidente de segurança, preencha **Item de configuração** E clique no ícone Mapa BSM ( ).
   A tela Mapa BSM exibe o mapa do último incidente acessado na Gestão de incidentes ou do último incidente de segurança acessado na Gestão de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique nos ícones ao lado de um item de configuração para exibir diferentes tipos de detalhes sobre o recurso (servidor, desktop ou outro IC).

   Por exemplo, clique em (⚠) Para exibir alertas associados ao IC.

   Nota: Para exibir uma lista de todos os ícones disponíveis, clique em **Filtros** Acima do mapa BSM e expanda **Filtrar tipos de tarefa** .

3. Para organizar o mapa em diferentes configurações, selecione qualquer um dos formatos listados acima do mapa (**Vertical** , **Horizontal** , **Radial** ou clique em **Filtros** para filtrar o mapa para facilitar a exibição.

4. Se você abriu o mapa BSM no formulário de incidente de segurança, poderá adicionar um IC dependente ao incidente de segurança clicando com o botão direito do mouse no IC e selecionando **Adicionar ICs afetados** .

   Você também pode adicionar vários ICs de uma vez. Arraste uma caixa ao redor dos ICs que você deseja adicionar, clique com o botão direito do mouse na caixa e selecione **Adicionar ICs afetados** .

   Os ICs são adicionados à lista relacionada de ICs afetados do incidente de segurança.

Calcule a gravidade de um incidente de segurança

Você pode calcular a gravidade de um incidente de segurança usando calculadoras predefinidas.

Antes de Iniciar

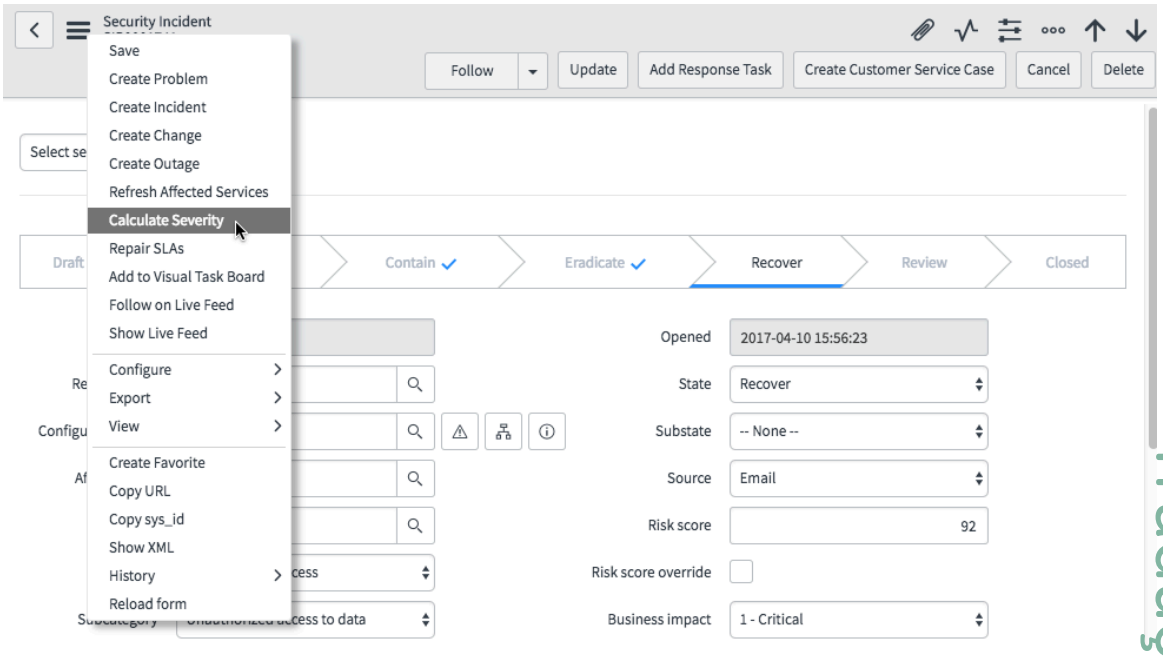
Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança para o qual você deseja calcular a gravidade.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Calcule a gravidade** :



A gravidade é calculada com base nas regras predefinidas para calculadoras de base. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.

PESQUISE e exclua e-mails de phishing

Excluir e-mails de phishing pode ajudar a reduzir a exposição a um ataque específico em uma organização. Você pode gerenciar e-mails de phishing em seu servidor de e-mail pesquisando, concedendo aprovações e excluindo-os.

Antes de Iniciar

Funções necessárias: sn_sec_cmn.cap_email_read

Você pode determinar quantos usuários foram visados por um ataque de phishing consultando um registro de e-mail associado a um incidente de segurança.

Software compatível:

- Microsoft ®Exchange Server 2010

Ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1 500 caixas de correio.

Por Que e Quando Desempenhar Esta Tarefa

Este recurso é usado pelo Integração de operações de segurança - Fluxo de pesquisa e exclusão de e-mail para executar uma consulta em seu servidor de e-mail. Dependendo dos critérios de pesquisa selecionados, a pesquisa identifica todos os e-mails em um ataque de phishing e retorna o número total de e-mails afetados ou detalhes dos e-mails afetados.

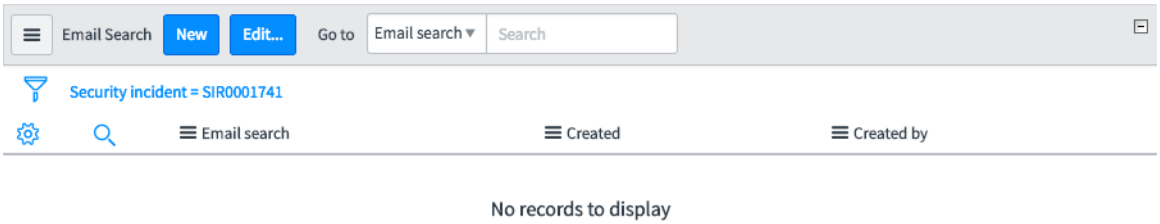
Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Escolha um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

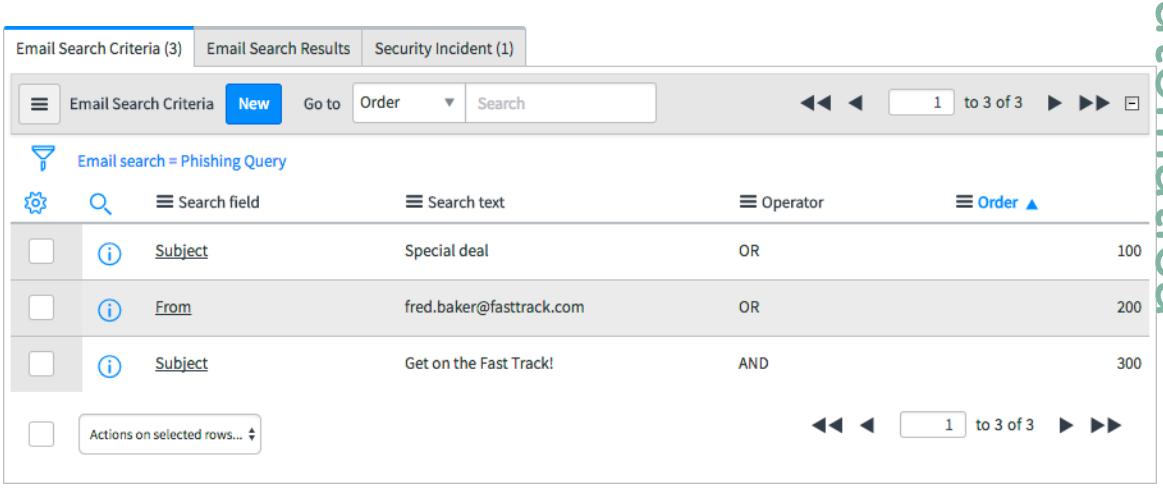
3. . **Pesquisa de e-mail** a lista relacionada não está visível, clique em **Mostrar todos os links relacionados** link relacionado.
4. Clique em **Pesquisa de e-mail** lista relacionada.



5. Clique em **Nova**.
6. Preencha os campos, se for o caso.

Campo	Descrição
Nome	Nome da consulta de pesquisa
Consultar pelo critério	Uma visualização da execução da consulta no servidor de e-mail. Gerado a partir de todos os registros de critérios de pesquisa ativos associados.
Descrição	Descreva o que a consulta de pesquisa está procurando.

7. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.



8. Clique em **Critérios de pesquisa de e-mail** e clique **Novo** .
9. Preencha ou edite os campos, conforme apropriado.

Campo	Descrição
Pesquisa de e-mail	Exibe o nome da pesquisa de e-mail. Se necessário, você pode alterá-lo.
Campo de pesquisa	Campo a ser pesquisado no servidor de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O campo de pesquisa tem as seguintes opções: **Assunto** Este critério pesquisa e-mails que contêm o texto da linha de assunto especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. **De** Este critério pesquisa e-mails que contêm o endereço de e-mail completo do remetente (por exemplo, jane.doe@abc.com) especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. **Nota:** Não é possível usar **De** e. **Destinatário** campos na mesma consulta. **Destinatário** Este critério pesquisa e-mails que contêm o endereço de e-mail completo do destinatário (por exemplo, john.doe@abc.com) especificado em **Texto de pesquisa** campo. Ele também pesquisa e-mails nos campos Para, Cc e Cco. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. **Nota:** Não é possível usar **De** e. **Destinatário** campos na mesma consulta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

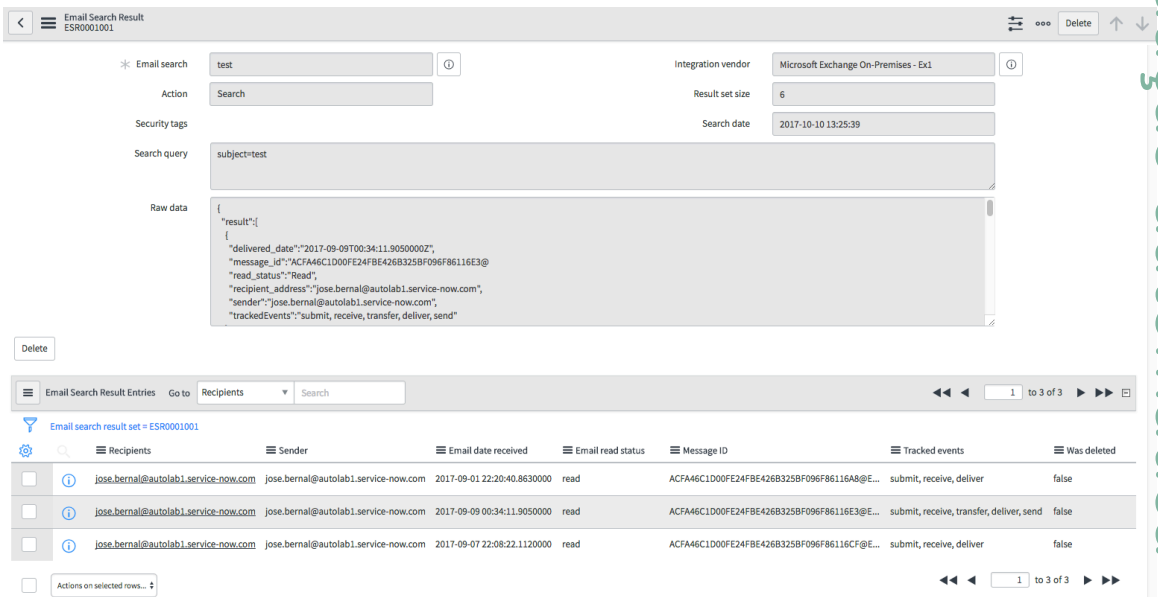
Campo	Descrição
	Corpo da mensagem Este critério pesquisa e-mails que contêm o corpo de texto especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1 500 caixas de correio. **Cc:** Este critério pesquisa e-mails que contêm o endereço de e-mail completo Cc (por exemplo: jane.doe@abc.com) especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Cco:** Este critério pesquisa e-mails que contêm o endereço de e-mail completo Cco (por exemplo: jane.doe@abc.com) especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Anexo** Este critério pesquisa e-mails que contêm o nome do arquivo de anexo ou o conteúdo do anexo especificado em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Somente anexos de texto sem formatação são compatíveis com a pesquisa do conteúdo do anexo. **Política de retenção** Este critério pesquisa e-mails que contêm números de política de retenção especificados em **Texto de pesquisa** campo. Para e-mails que atendem a esses critérios de pesquisa,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	o número total de e-mails de phishing é retornado.
Ativo	Marque esta caixa de seleção para ativar esta consulta de pesquisa de e-mail.
Operador	Os valores possíveis são AND e OR. Você pode definir como os critérios de pesquisa são combinados para serem executados no servidor de e-mail.
Ordem	A ordem na qual a consulta de pesquisa é criada a partir dos critérios de pesquisa.
Pesquisar Texto	O texto a ser pesquisado. Aspas simples, aspas duplas e dois pontos não são compatíveis.

10. Clique em **Enviar**.
11. Repita conforme necessário para definir critérios de pesquisa adicionais.
12. Você pode exibir os resultados da pesquisa clicando em **Resultados da pesquisa de e-mail** guia.

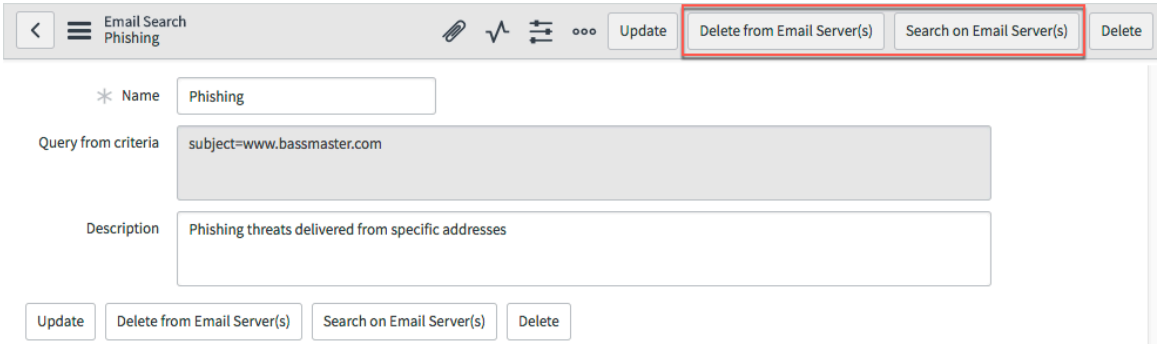


Cada linha do formulário Entradas do resultado da pesquisa de e-mail representa um e-mail separado.

13. Depois de criar um registro de critérios de pesquisa, dois botões serão exibidos no formulário Pesquisa de e-mail: **Excluir do(s) servidor(es) de e-mail** e. **Pesquisar em servidor(es) de e-mail** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



14. Para pesquisar e-mails no servidor selecionado que atendam aos critérios de pesquisa definidos, clique em **Pesquisar em servidor(es) de e-mail** .

Crie um artigo de conhecimento de incidente de segurança

Conforme você trabalha com incidentes de segurança e tarefas de resposta, os artigos de conhecimento são exibidos automaticamente para fornecer informações pertinentes sobre a tarefa que você está executando. Sua organização pode criar e manter artigos na base de conhecimento de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa

Os artigos de conhecimento compartilham informações de segurança, documentam os tipos de ameaças cibernéticas que sua organização enfrenta e fornecem respostas e respostas a essas ameaças.

Se necessário, você pode organizar artigos de conhecimento em runbooks, que criam associações entre os artigos e tarefas específicas. Por exemplo, você pode configurar um runbook com condições que fazem com que um artigo da base de conhecimento sobre phishing seja exibido ao criar um incidente de segurança para um ataque de phishing. Para obter mais informações, consulte Crie um runbook de resposta a incidentes de segurança.

Artigos de conhecimento em runbooks também podem ser associados a tarefas específicas em um playbook. Para obter mais informações, consulte Associe um artigo de conhecimento a uma tarefa do playbook.

Os benefícios dos artigos de conhecimento incluem o seguinte.

- Os funcionários têm uma fonte de informações que é fácil de pesquisar.
- As informações podem ser mantidas atualizadas, pois os artigos de conhecimento têm um ciclo de vida definido: Criar, revisar e atualizar, publicar e desativar.
- Quando você cria manualmente uma solicitação de segurança, incidente ou tarefa de resposta, uma lista de artigos relevantes é apresentada conforme você digita a descrição resumida.

Nota: É importante atribuir um gerente de conhecimento a cada base de conhecimento de incidente de segurança.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Clique no ícone Criar um artigo ( ).
3. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de conhecimento

Campo	Descrição
Número	O número da base de conhecimento gerado automaticamente.
Base de conhecimento	A base de conhecimento selecionada para este artigo.
Categoria	A categoria deste artigo.
Publicado	Quando este artigo de conhecimento foi publicado. Este valor é definido quando o artigo é criado e atualizado quando o artigo é publicado.
Válida até	Quando este artigo de conhecimento expira. Este artigo não aparecerá nos resultados de pesquisa após essa data ou se uma data não for selecionada.
Imagem	Uma imagem que aparece ao lado do artigo ao pesquisar no portal de conhecimento legado.
Fluxo de trabalho	[Somente leitura] O estado de publicação do artigo, como Rascunho ou Publicado. Quando inserir um novo artigo em um artigo existente, o estado do novo artigo é redefinido como **Rascunho** .
Origem	A tarefa para a qual este artigo de conhecimento foi criado em resposta, se houver. Este campo é definido automaticamente quando você cria o artigo de conhecimento a partir de um registro de tarefa.
Link de anexo	Caixa de seleção para baixar um arquivo anexado automaticamente quando um usuário acessa o artigo, em vez de abrir a exibição do artigo. Adicione um anexo ao artigo para usar esta opção.
Exibir anexos	Caixa de seleção para exibir anexos para usuários que exibem este artigo de conhecimento. Os anexos aparecem abaixo do texto do artigo. Adicione um ou mais anexos ao artigo para usar esta opção.
Descrição resumida	O título do artigo. Este título aparece ao navegar e pesquisar conhecimento e na parte superior do artigo.
Texto	Conteúdo do artigo. Use o editor de HTML WYSIWYG para criar conteúdo. Uma visualização do conteúdo aparece ao navegar e pesquisar conhecimento.

Nota: Se você estiver criando um artigo de conhecimento a ser associado a uma tarefa do playbook . defina **Base de conhecimento** campo para **Runbook de resposta do incidente de segurança** .

4. Clique em **Enviar** para criar o artigo.

O que Fazer Depois

Todas as etapas adicionais necessárias para publicar o artigo, como aprovações, dependem de fluxo de trabalho de publicação para a base de conhecimento.

Tópicos relacionados

Crie um runbook de resposta a incidentes de segurança

Escalar um incidente de segurança

Se existir um caminho de escalação para um incidente de segurança, o botão Escalar estará disponível no cabeçalho do incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

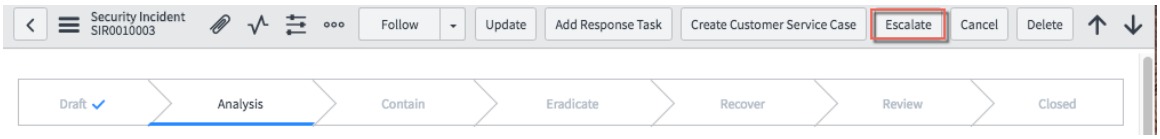
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

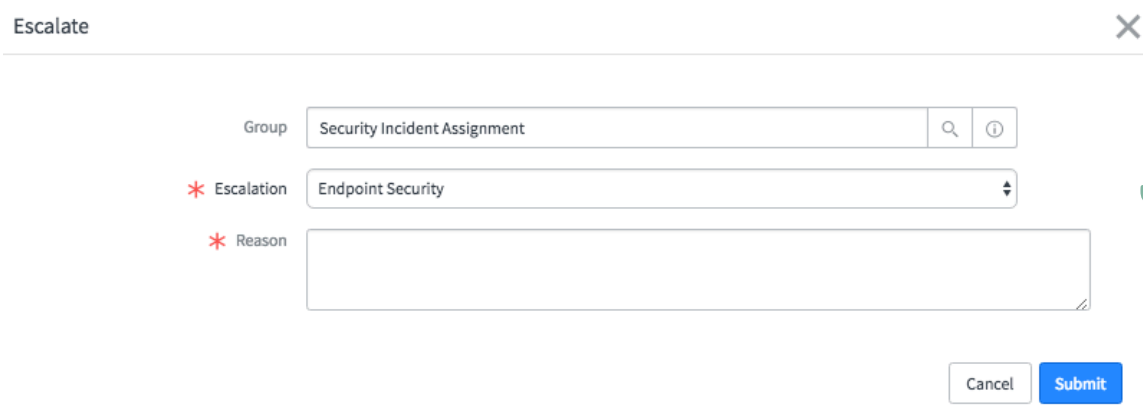
Um grupo de escalação deve ser criado para ver este botão. Para obter mais informações, consulte Crie um Operações de segurança grupo de escalação definido pelo usuário.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Abra o incidente que você deseja escalar.
3. Clique em **Escalar** botão.



4. Escolha um grupo de escalação.
5. Insira um motivo para a escalação.



6. Clique em **Enviar**.
   Atualizações **Grupo de atribuição** e. **Atribuído a.** no incidente de segurança.

Gerenciar atividades pós-incidente

Com base nos requisitos do seu negócio, uma revisão das origens e o tratamento de incidentes de segurança geralmente são necessários.

. Análise pós-incidentefuncionalidade em ServiceNow fornece muitas ferramentas para automatizar, rastrear, auditar e simplificar esse processo.

Esta seção descreve o seguinte:

- Atribuir funções de revisão pós-incidente
- Configure uma condição do gatilho de avaliação
- Execute uma revisão pós-incidente baseada em questionário
- Criar regras de atribuição de PIR
- Relatório de análise pós-incidente

Atribuir funções de revisão pós-incidente

Você pode direcionar perguntas para grupos predefinidos específicos atribuindo funções a categorias de Revisão pós-incidente (PIR).

Tradução automática

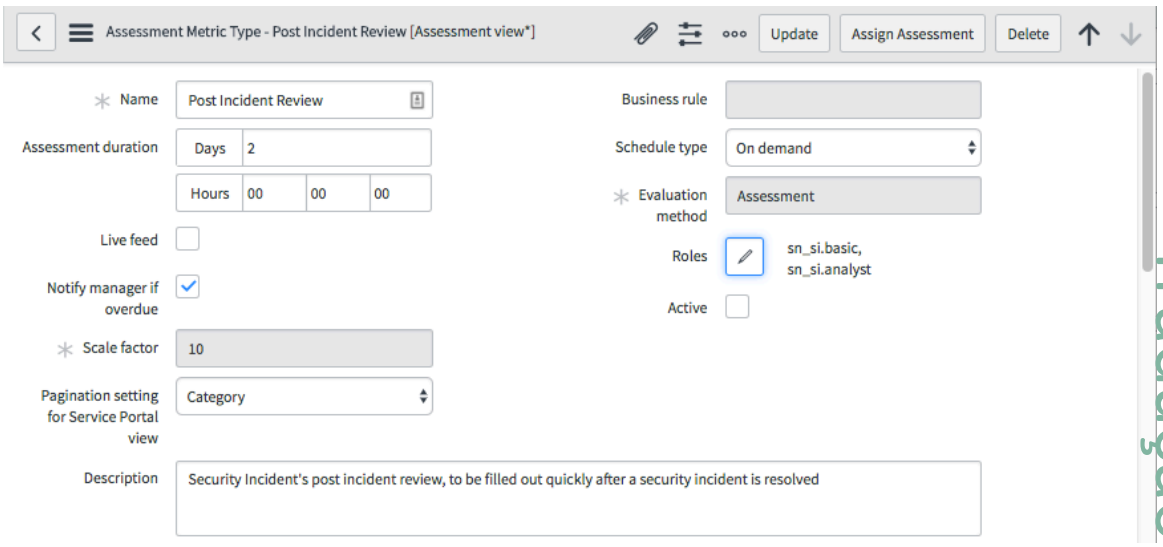
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Avaliações** > **Definição de métrica** > **Tipos**.
2. Em **Tipos** , pesquise um **Revisão pós-incidente** registro.
3. Abra o registro.
4. Atribua uma ou mais funções para esta categoria de perguntas.



5. Clique em **Atualizar**.
6. Navegar até **Administração de Usuários** > **Usuários**.
7. Escolha um usuário
8. Adicione uma ou mais funções de tipo de métrica ao registro do usuário.

> **Nota:** As funções devem corresponder às funções atribuídas na categoria Revisão pós-incidente.

Relatório de análise pós-incidente

O recurso de relatórios Revisão pós-incidente (PIR) permite configurar e baixar os relatórios de revisão pós-incidente usando a guia Revisão pós-incidente.

O administrador de segurança pode criar e configurar os modelos de relatório e mapear esses modelos para o incidente de segurança usando a configuração do relatório. Um analista de segurança pode exibir ou baixar o relatório depois que o incidente de segurança for resolvido e o status for atualizado para o estado Revisar.

Um relatório em PDF é gerado e anexado ao incidente de segurança quando o incidente é movido para o estado Encerrado após a configuração bem-sucedida.

> **Nota:** O recurso de relatórios é aplicável e compatível com Orlando Patch9.

Para personalizar seus relatórios de revisão pós-incidente, você deve fazer a configuração a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. **Modelos de relatório** : Personalize e configure os seguintes recursos do modelo de relatório para adicionar informações adicionais ao relatório:
   a. Linha do tempo
   b. Identidade visual
   c. Scripts do Modelo
2. **Configuração de Relatório**

Esta seção descreve o procedimento de configuração:

Modelos de relatório

Use#a###seção Modelos de relatório para criar modelos de relatório primários e adicionais que são aplicados##aos incidentes de segurança#para#gerar#o##relatório Revisão pós-incidente. Você pode formatar#e#configurar#o relatório com base em seus requisitos. #Os modelos também ajudam a incluir os detalhes da avaliação no modelo.

A seguir estão algumas etapas opcionais que podem ser executadas ao criar o modelo:

1. Configurando as informações de identidade visual.
2. Configuração do tamanho da página e da margem da página.
3. Adição de campos relacionados a incidentes de segurança (personalizados e padrão).
4. Usando os seguintes tokens personalizados predefinidos:
   a. *$sessionUser*retorna#o nome de usuário conectado
   b. *$date*#retorna#a data atual
   c. *$if_not_null_start & $if_not_null_end*: se esses marcadores forem usados em qualquer campo, os marcadores serão exibidos somente se o valor existir. #Por exemplo:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Incluindo os dados da lista relacionada usando os scripts de modelo. Para obter mais informações, consulte a seção abaixo em **Scripts de Modelo** .
6. Incluindo as informações da linha do tempo usando os filtros da linha do tempo. Para obter mais informações, consulte a seção abaixo em **Linha do tempo** .
7. Gerenciar e formatar o conteúdo do modelo, como anexos, tabelas e imagens.

Nota: Os recursos da barra de ferramentas do modelo de relatório aprimorado estão disponíveis somente na versão da versão Paris.

Modelos de relatório principais pontos:

1. As imagens anexadas ao modelo de relatório são exibidas no relatório Revisão pós-incidente somente quando são incluídas na##tabela sys_attachment.

   Nota: As imagens selecionadas na tabela db_image não serão exibidas no relatório de revisão pós-incidente.

2. Os vídeos não são compatíveis com o relatório de revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Os URLs no PDF não podem ser clicados. Para habilitar os URLs não clicáveis (.) é indicado como (ponto).
4. O relatório não será gerado se o tamanho do modelo de relatório exceder 50 MB.
5. A família de fontes selecionada para o conteúdo do modelo de relatório não será aplicada ao PDF se não for compatível com o gerador de PDF.

   Nota: Se a fonte correspondente não estiver lá, o gerador de PDF identificará a fonte alternativa mais próxima e gerará o PDF.

6. Se você fornecer valores de margem de página mais altos, a geração do relatório de revisão pós-incidente ocorrerá falha. Por exemplo, Margem superior e inferior > 450#e Margem esquerda e direita > 450.
7. Se um texto grande for incluído no modelo de relatório sem espaços, o texto poderá ser truncado. Visualize o texto e modifique-o de acordo.

O administrador de segurança pode visualizar o relatório usando **Visualizar relatório** Botão disponível na página Modelo de relatório.

Nota:

Selecione um Incidente de segurança para visualizar um relatório com este modelo e clique **Visualizar relatório** .

Identidade visual

Você pode adicionar o nome do modelo de identidade visual,##a imagem do cabeçalho e do rodapé, o texto do cabeçalho e do rodapé, gerar números de página e incluir o registro de identidade visual no modelo de relatório depois que ele for criado.

A seguir está um exemplo de#formato de relatório de identidade visual:

Pontos principais da identidade visual do modelo de relatório:

1. O tamanho máximo permitido para a imagem de cabeçalho e rodapé é de 5 MB. Se o tamanho exceder mais do que o limite especificado, uma mensagem de erro "O formato da imagem não pode ser reconhecido" será exibida no incidente de segurança.
2. O comprimento do texto do rodapé é limitado a 100 caracteres.
   a. Se o texto da imagem do rodapé e o conteúdo do relatório estiverem sobrepostos durante a visualização, você deverá fazer mudanças no registro de identidade visual.
   b. Se o texto do rodapé contiver um link de URL, ele poderá se sobrepor à imagem do rodapé. Visualize e corrija conforme necessário.

Linha do tempo

A configuração da linha do tempo permite criar e modificar os filtros da linha do tempo conforme#necessário. Você pode#filtrar#os tipos de atividade que devem ser incluídos no relatório, configurar se as tarefas secundárias devem ser incluídas ou excluídas no relatório e configurar se as imagens devem ser incluídas ou excluídas no relatório.

Se você quiser utilizar e preencher qualquer configuração de linha do tempo, adicione o marcador conforme mencionado abaixo: `${timeline:timeline name}`. Duas##configurações de linha do tempo de amostra#como exemplo são#fornecidas#na configuração que são usadas no##modelo de Relatório de Phishing e no modelo de Relatório Padrão. #Você pode modificar e reutilizar as configurações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Scripts do Modelo

Use os scripts do modelo para incluir os dados das listas relacionadas, carimbo de data e hora e quaisquer outros dados que não sejam diretamente identificáveis com pontos. A seguir está um exemplo:

Construa um script de modelo para exibir a lista relacionada no modelo de relatório :

1. Para preparar os dados da lista relacionada, chame o método PostIncidentReportUtils.fetchRelatedListDataForReport.
2. Para representar os dados da etapa 1 no formato e no estilo da tabela, chame o método ReportTemplateUtil.constructTablefunction.

Se você quiser utilizar e preencher qualquer script de modelo, adicione o marcador de script de modelo de marcador como *`${template_script:script name}`*.

A seguir estão alguns scripts de modelo de amostra fornecidos para configurar e modificar seus relatórios pós-incidente.

Nome do script	Descrição
formatted_current_date	Retorna a data e a hora locais atuais no formato DDMMYAYYY 00,00 AM ou PM. Por exemplo, 21 de janeiro de 2021 3:51 PM PST.
si_affected_users	Retorna os usuários afetados da lista relacionada em um formulário tabular.
si_assessments	Retorna os resultados da avaliação pós-incidente em um formulário tabular.
si_associated_phish_emails	Retorna os e-mails de phishing associados da lista relacionada em um formulário tabular.
si_associated_phish_headers	Retorna os cabeçalhos de phishing associados da lista relacionada em um formulário tabular.
si_business_criticality	Retorna o valor de criticalidade comercial codificado por cores.
si_malicious_observables	Retorna os observáveis mal-intencionados da lista relacionada em um formulário tabular.
si_observables	Retorna os observáveis da lista relacionada em um formulário tabular.
si_priority	Retorna um valor de prioridade codificado por cores.
si_response_tasks	Retorna as tarefas de resposta da lista relacionada em um formulário tabular.
si_time_to_identify	Retorna a duração gasta no estado Rascunho e Análise.
si_time_to_resolve	Retorna o tempo para resolver o incidente.

Scripts de modelo de relatório pontos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Se uma lista relacionada for adicionada com mais de 5 colunas, os dados da tabela serão truncados durante a geração do PDF. #Cada#largura mínima de coluna é definida como 124 px.
2. Se um script de modelo não puder carregar o conteúdo no modelo de relatório#devido a problemas técnicos, uma mensagem de erro será exibida no relatório, "Erro ao avaliar o script do modelo", e o administrador de segurança deverá avaliar a exatidão do script para resolver o problema.
3. si_assessments: Por padrão, todas as categorias de avaliação são adicionadas ao relatório. O administrador de segurança pode filtrar#os dados modificando o script do modelo conforme necessário. Adicione `categories: sys_id1,# sys_id2;`parâmetro para filtrar os dados.
4. Tempo de resolução e tempo para identificar scripts: Use os registros de definição que fazem parte da lista relacionada de métrica. Se os registros de definição não estiverem disponíveis#para o incidente de segurança, crie ou adicione esses registros de definição para preencher os valores dos dois campos.

Nota:

Por padrão, o administrador de segurança não tem acesso para exibir os registros de versão de#nenhuma tabela. Você deve adicionar a função de administrador para acessar os registros de versão e reverter para a versão anterior.

Configuração de Relatório

Use a seção Configuração de relatório para configurar as condições e aplicar os modelos de relatório#aos#Incidentes de segurança. Você pode adicionar um relatório primário e um ou mais modelos de relatório adicionais à mesma condição.

A seguir está um exemplo de condição fornecida para aplicar o modelo de Relatório de Phishing aos Incidentes da categoria de Phishing e#a outra#para aplicar o modelo de Relatório padrão a todos os incidentes de segurança. ##O modelo de relatório padrão será aplicado aos incidentes de segurança#se as condições não forem atendidas.

Procedimento para desativar a nova implementação

1. Desative as seguintes regras de negócios:
   a. Gerar PDF PIR
   b. Criar conhecimento no fechamento Novo
2. Ative as seguintes regras de negócio:
   a. Gerar PIR quando em Revisar e Fechar
   b. Criar conhecimento no fechamento
   c. Regen PIR no fechamento/cancelamento/exclusão]
3. Ativar a regra de IU, `Hide PIR field when empty`.
4. Vá para o layout do formulário no formulário de incidente de segurança. Em **Revisão pós-incidente** seção:
   a. Remova o seletor de relatório PIR da seção PIR
   b. Campo Relatório pós-incidente à seção PIR

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure as propriedades do relatório Revisão pós-incidente (PIR) para incidentes de segurança secundários

Você tem a opção de configurar as duas propriedades de relatório PIR a seguir para incidentes de segurança secundários:

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Nota: Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Configure as propriedades do relatório PIR para incidentes de segurança secundários

Propriedade	Uso
sn_si.generate_pir_report_for_child_si	Opção para habilitar a geração de relatórios de Revisão pós-incidente (PIR) para incidentes de segurança secundários. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local** : Navegue até Todos > Propriedades do sistema > Todas as propriedades.
sn_si.include_child_si_timeline_in_pir	Opção para incluir a linha do tempo dos incidentes de segurança secundários no relatório PIR do incidente de segurança primário. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local** : Navegue até Todos > Propriedades do sistema > Todas as propriedades.

Gerenciar relatório de revisão pós-incidente

Gerenciar relatório de revisão pós-incidente inclui as informações que foram configuradas e aplicadas pelo administrador de segurança, e os analistas de segurança podem modificar os filtros da linha do tempo no tempo de execução e baixá-los.

Antes de Iniciar
Função necessária:sn.si_analyst

Por Que e Quando Desempenhar Esta Tarefa
O analista de segurança pode selecionar um dos modelos de relatório primário ou adicional disponíveis e configurar os filtros de linha do tempo, visualizar e baixar o relatório. O analista de segurança também pode baixar diretamente o relatório com a configuração da linha do tempo que foi aplicada pela última vez.

O analista de segurança pode acessar os relatórios usando a guia Revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até o incidente de segurança no Estado de revisão.
2. Clique em **Revisão pós-incidente** guia.
3. Se o incidente de segurança estiver em **Revisão** estado:
   Modelo de relatório:
   - Por padrão, o modelo de relatório primário que foi configurado na página de configuração será aplicado ao incidente de segurança e estará disponível para download.
   - O analista pode escolher outros relatórios na lista suspensa para configurar e baixar o relatório.
4. **Configurar/Visualizar:**

   Um analista de segurança pode visualizar e modificar a configuração do modelo de relatório. Na configuração atual, o analista de segurança só pode modificar os filtros da linha do tempo.

   Caso a configuração seja modificada para o relatório primário antes que o incidente de segurança seja encerrado, o relatório de revisão pós-incidente anexado ao incidente de segurança será atualizado de acordo com as modificações feitas pelo analista de segurança. Após o fechamento, o analista poderá modificar a configuração e baixar o relatório em trânsito. No entanto, o relatório anexado seguiria a última configuração antes do fechamento.

   Para Configurar/Visualizar o relatório, execute as seguintes etapas:

   a. Selecione o modelo de relatório desejado em **Modelo de relatório** lista suspensa no **Revisão pós-incidente** guia.
   b. Clique em **Configurar/Visualizar** guia.
   c. **Atualização** ou configure os filtros da linha do tempo conforme necessário.
   d. Use **Mostrar imagens** caixa de seleção para incluir ou excluir as imagens da linha do tempo. Se desmarcado, somente os nomes das imagens serão incluídos na seção da linha do tempo.
   e. Use **Mostrar tarefas secundárias** caixa de seleção para listar todas as tarefas secundárias associadas ao incidente de segurança.
5. **Salvar** a configuração e clique em **Visualização** para visualizar e baixar o relatório.
6. Clique em **Download** para baixar diretamente o relatório.

Configure uma condição do gatilho de avaliação

Defina condições de regra e gere avaliações obrigatórias e opcionais para incidentes de segurança específicos.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para usar o recurso Condições do gatilho de avaliação pós-incidente, você deve fazer upgrade para Resposta a incidentes de segurança11,0. Antes de atualizar, você deve reverter todas as personalizações feitas para o tipo de métrica de Revisão pós-incidente e condições de gatilho. Além disso, talvez você também precise reverter as personalizações feitas para as regras de negócios específicas para a revisão pós-incidente.

- Exigir que as avaliações sejam concluídas
- Store designado

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Análise pós-incidente – Configuração de avaliações**.
2. Em **Condições do gatilho de avaliação Configurar** clique em **Configurar** .

   Nota: No formulário Configurações de avaliação e na seção Configurações de avaliações, o. **Gerar avaliações** a caixa de seleção está marcada por padrão.

   - Quando você marca a caixa de seleção, uma avaliação opcional é criada para cada incidente de segurança.
   - Quando você desmarca a caixa de seleção, as avaliações não são geradas. As regras de avaliação não são exibidas e você não pode configurar condições para os incidentes de segurança.

3. No formulário Configurações de avaliação, na seção Condições, especifique as informações necessárias.

   a. Em **Nome** especifique o nome da regra.

   b. Em **Execução** especifique o tipo de execução.

   c. Para configurar uma condição, clique no registro de regra e defina as condições no **Condição** campo.

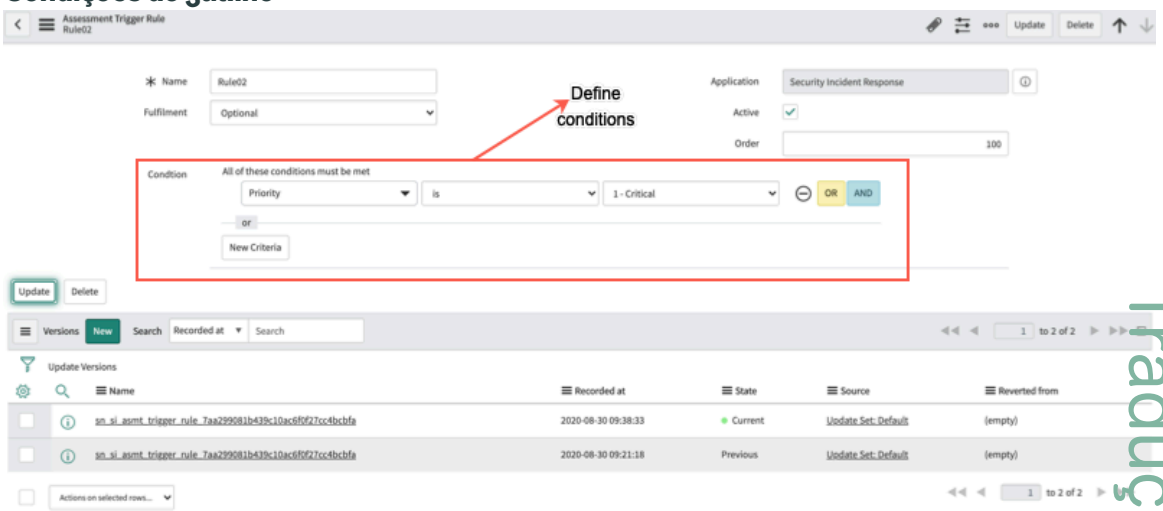
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se você criar uma regra sem definir uma condição no **Condição** , a condição é avaliada como verdadeira e a regra é aplicável a todos os incidentes de segurança.
- Você pode definir uma regra específica para tornar as avaliações obrigatórias ou opcionais, e as avaliações não são geradas para os incidentes de segurança restantes, que não correspondem às regras definidas.

Condições do gatilho



Exemplos de condições do gatilho de avaliação

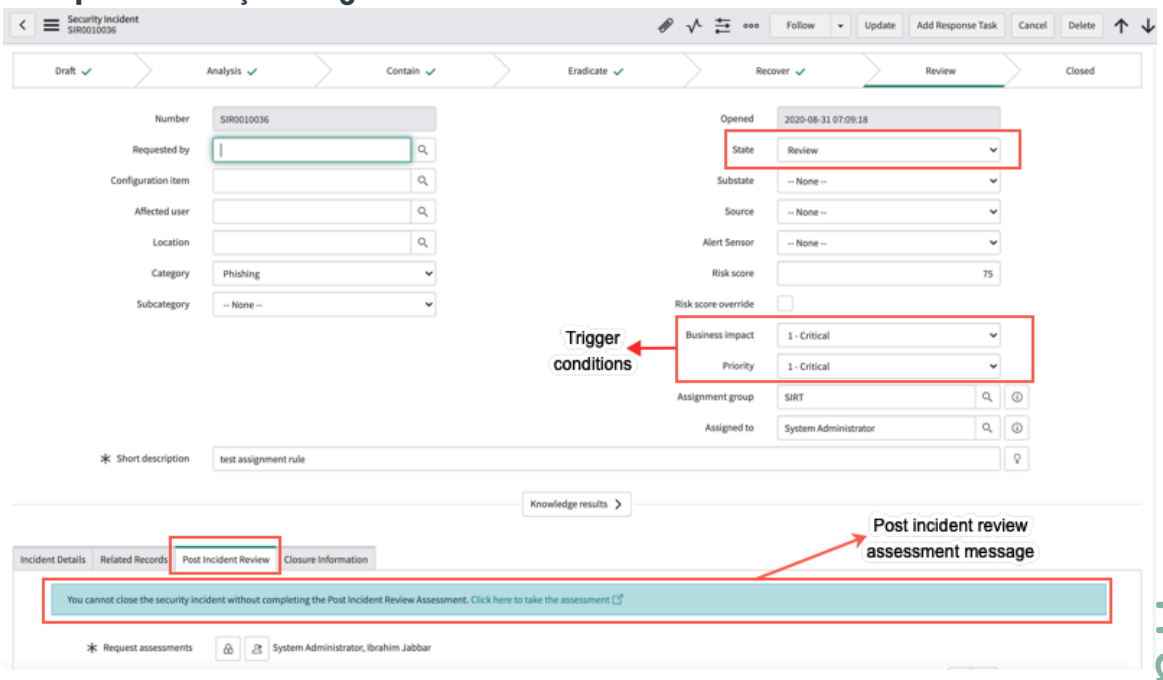
Os exemplos a seguir fornecem diferentes cenários sobre como as condições do gatilho de avaliação obrigatórias e opcionais são geradas.

- No formulário Condição do gatilho de avaliação, gere avaliações obrigatórias quando **Prioridade** e. **Impacto nos negócios** para um incidente de segurança está definido como **Crítico** em **Regra do gatilho de avaliação** página. Nesse cenário, os analistas de segurança não podem fechar o incidente até que as avaliações obrigatórias sejam concluídas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de avaliação obrigatória



- Como você pode ver, neste exemplo, se um incidente de segurança estiver em um **Revisão** estado, os analistas de segurança não podem fechar o incidente de segurança sem concluir o. **Avaliação de revisão pós-incidente** . Um link de avaliação está disponível para levar a avaliação aos analistas de segurança atribuídos (ou que solicitaram a avaliação) ao incidente.
- No formulário Condição do gatilho de avaliação, gere avaliações opcionais quando **Prioridade** e. **Impacto nos negócios** para um incidente de segurança está definido como **Alto** . Neste exemplo, se os analistas de segurança não concluírem as avaliações e fecharem o incidente de segurança, as avaliações serão canceladas automaticamente.
- Se as avaliações obrigatórias ou opcionais não corresponderem ao incidente de segurança, as avaliações não serão geradas para esses incidentes de segurança. Um analista de segurança pode fechar o incidente de segurança sem concluir a avaliação de Revisão pós-incidente.

Execute uma revisão pós-incidente baseada em questionário

Você pode decidir que uma revisão pós-incidente do incidente de segurança é garantida. Uma revisão pós-incidente descreve o que aconteceu, ajuda a determinar por que o incidente ocorreu e identifica como ele pode ser evitado ou tratado no futuro.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Nota: Qualquer usuário pode participar de um questionário de revisão pós-incidente, independentemente da função. Funções podem ser atribuídas a uma revisão.

Por Que e Quando Desempenhar Esta Tarefa

. ServiceNow Resposta a incidentes de segurança a aplicação pode automatizar a coleta de informações de revisão pós-incidente de todos os envolvidos em um incidente de segurança usando questionários. Se você decidir usar um questionário como parte de uma revisão pós-incidente, uma lista de perguntas relevantes para o incidente de segurança será enviada para a lista de participantes definida pelo usuário. Conforme cada usuário conclui o questionário, o relatório pós-incidente é gerado automaticamente. O relatório compila todas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

as informações relacionadas ao incidente de segurança, bem como todas as respostas à revisão pós-incidente.

Uma lista inicial de perguntas é fornecida com o sistema de base, mas elas são personalizáveis. Você pode criar categorias e adicionar novas perguntas a elas ou mudar perguntas individuais nas categorias existentes. Você pode fazer perguntas com base em funções. Você pode definir quando determinadas perguntas são feitas. Pode haver perguntas que você faz somente para seus servidores UNIX, por exemplo, ou somente quando há atividade criminosa. Você pode definir perguntas que são feitas dependendo da resposta para outra pergunta ou do valor em um campo no formulário. Até pode haver perguntas que são preenchidas por completo consultando o banco de dados.

Depois que o incidente de segurança é resolvido e movido para **Revisão** estado, as avaliações são geradas para todos os usuários atribuídos e usuários que são adicionados diretamente do **Solicitar avaliações** lista.

O questionário pode ser uma ferramenta útil para coletar informações sobre o tratamento do incidente de segurança de várias fontes.

Durante a revisão, você pode adicionar mais usuários à lista ou remover usuários existentes da lista, a menos que eles já tenham começado a preencher o questionário. Se você adicionar novos usuários à lista, eles receberão as perguntas quando o registro for salvo. O incidente de segurança não pode ser encerrado até que todos os questionários tenham sido concluídos. Conforme os questionários são preenchidos por cada usuário, o relatório pós-incidente é gerado automaticamente (e gerado novamente) e exibido no **Revisão pós-incidente** guia.

Para iniciar uma revisão pós-incidente:

Procedimento

1. Crie um incidente de segurança ou abra um existente navegando até **Incidente de segurança** > **incidentes** > **Atribuído a mim (ou Atribuído à equipe ou incidentes não atribuídos)**.
2. Clique em **Revisão pós-incidente** guia.
3. . **Solicitar avaliações** o padrão do campo é o indivíduo em **Atribuído a.** campo.
   Clique no ícone de cadeado para adicionar outros usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.
4. Após concluir suas entradas, clique no ícone de cadeado para bloquear o campo.

   Nota: Você também pode definir condições que, quando atendidas em um incidente de segurança, podem fazer com que usuários específicos sejam adicionados automaticamente ao **Solicitar avaliações** campo desse incidente de segurança. Por exemplo, quando um incidente de segurança **Categoria** foi alterado para **Phishing** indivíduos específicos que têm experiência em ameaças de phishing podem ser adicionados à lista de revisão pós-incidente. Para obter mais informações, consulte Criar regras de atribuição de PIR.

5. Clique em **Atualizar**.
   Quando o incidente entra em **Revisão** estado (ou imediatamente, se já estiver em **Revisão** cada um dos usuários na lista de revisão recebe uma inicial notificação por e-mail . Os lembretes são enviados conforme a data de vencimento se aproxima. Quando cada usuário acessa o questionário pelo link de e-mail ou acessando **Análise pós-incidente** > **Minhas Revisões Pendentes**, as perguntas mostradas são extraídas de todas as categorias que se encaixam neste incidente de segurança. Se novos usuários forem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adicionados à lista de revisão antes que a data de vencimento seja atingida, eles receberão notificações quando o incidente de segurança for salvo.

Conforme os usuários preenchem seus questionários, o relatório pós-incidente compila os dados e exibe o relatório no **Revisão pós-incidente** guia. Os dados do questionário são exibidos no **Descobertas** guia.

Criar categorias de questionário de revisão pós-incidente

Você pode usar as categorias de questionário que vêm com o sistema de base ou criar suas próprias categorias.

Antes de Iniciar
Função necessária: sn.si_admin

Por Que e Quando Desempenhar Esta Tarefa
Para criar uma nova categoria de perguntas:

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique em **Perguntas de revisão** .
   Uma lista de categorias é exibida, junto com sua ordem e filtros que definem em que condições as perguntas são feitas (por exemplo, somente quando a categoria de incidente de segurança é `Atividade criminosa`). Cada categoria é uma seção no questionário de revisão pós-incidente e as perguntas em cada categoria são incluídas somente quando o incidente de segurança corresponde ao filtro de condição. Por exemplo, para uma categoria de perguntas que se aplicam somente a servidores Linux, você configuraria um filtro que selecionou incidentes de segurança em que o tipo de recurso afetado era Servidor Linux. Nessa categoria, você criaria todas as perguntas necessárias quando um incidente de segurança estivesse em um servidor Linux. Você usa uma das categorias fornecidas no sistema de base ou cria uma nova categoria. Este procedimento pressupõe que você deseja criar uma nova categoria antes de definir perguntas.
3. Clique em **Novo** na lista de categorias.
4. Preencha os campos no formulário, conforme o apropriado.

Incidente de segurança

Campo	Descrição
Nome	Nome da categoria que aparece no questionário de incidente de segurança.
Tipo	A Revisão pós-incidente é o padrão.
Criar Partes Interessadas	Não usado por Resposta a incidentes de segurança.
Tabela	Este campo é atribuído automaticamente quando o formulário é enviado.
Filtrar	Insira a condição que determina quando as perguntas nesta categoria são usadas. Se um registro de incidente de segurança corresponder a este filtro, as perguntas serão incluídas em uma revisão pós-incidente desse incidente de segurança. Os filtros podem usar quaisquer dados no registro ou em outros registros vinculados a este registro. Por exemplo, o departamento do gerente do usuário solicitante.
Aplicação	Aplicação de escopo do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Peso	Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10.
Métricas totais	Número de métricas usadas pela categoria.
Descrição	Descrição do questionário.

5. Clique em **Enviar** para salvar a categoria.

Redigir perguntas de revisão pós-incidente

Você pode usar as perguntas que vêm com o sistema de base ou criar suas próprias perguntas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Os métodos para coletar informações de revisão pós-incidente podem ser na forma de perguntas ou como dados coletados automaticamente usando scripts.

As perguntas podem depender das respostas para outras perguntas. Por exemplo, você pode perguntar se todos os logs necessários estavam disponíveis. Se a resposta for Não, você fará uma pergunta de acompanhamento para determinar quais dos logs necessários não foram habilitados.

A coleta de dados com script, também chamada de métricas de script, coleta dados relacionados ao incidente de segurança por meio de scripts que você escreve. Esta ação pode ir muito além dos dados no próprio registro de incidente de segurança. Por exemplo, uma métrica de script pode coletar o tempo de indisponibilidade recente de um servidor afetado por este incidente de segurança.

Por fim, você pode misturar os dois tipos. As perguntas podem ter valores padrão obtidos de um script ou simplesmente de um campo no registro de incidente de segurança. Quando você usa um Resposta padrão de... tipo de pergunta, você pode escolher se deseja que o usuário sempre responda à pergunta, com o valor padrão fornecendo um valor inicial, ou se deseja que o usuário receba a pergunta somente se o script ou o campo ficar vazio.

Para criar uma nova pergunta:

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique na categoria para a qual você deseja criar uma nova pergunta.
3. Clique em **Métricas de avaliação** guia.
4. Clique em **Nova**.
   Você também pode clicar em uma pergunta existente para modificá-la.
5. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de métrica

Campo	Descrição
Nome	Nome da métrica (pergunta ou script). Se a métrica for uma coleta de dados com script, esse nome aparecerá no relatório pós-incidente.
Categoria	A categoria à qual a métrica pertence. O sistema preencherá automaticamente essa categoria se você criar uma métrica a partir do formulário Categoria de métrica. **Nota:** Você não poderá mudar a categoria se o campo **Depende de** estiver definido ou se outra métrica depender dessa métrica
Método	Indica o tipo de métrica, da seguinte forma: ○ *Assessment*: Uma pergunta que não tem valor padrão. Vários tipos de dados podem ser definidos no **Tipo de dados** . **Tipo de campo** , como caixas de seleção, listas de seleção, entrada de texto. ○ *Script*: Métrica com script. Obtenha valores gravando um script personalizado. . *Script*o método é compatível com **Duração** , **Número** e **Percentual** tipos de dados. ○ *Default answer from field*Uma pergunta em que a resposta padrão vem de um campo selecionado no incidente de segurança. Selecionar esta opção adiciona dois campos ao **Geral** guia: ▪ *Default answer*: Selecione o campo no incidente de segurança que contém a resposta padrão para a pergunta. Por exemplo, para a pergunta: "Quem relatou inicialmente este incidente?", o. **Solicitado por** o campo seria uma opção provável. ▪ *Ask question*Especifica quando fazer a pergunta: Sempre ou somente se **Resposta padrão** o campo está vazio. Usando o exemplo acima, a pergunta seria feita se **Solicitado por** o campo está vazio. ○ *Default answer from script*Uma pergunta em que a resposta padrão vem de um script. A resposta pode ser um número, cadeia de caracteres ou porcentagem. . **Geral** adiciona um campo: *Ask question*: Como especifica quando fazer a pergunta: Sempre ou somente se o script não fornecer uma resposta padrão. O script é definido na guia **Tipo de campo**. **Nota:** Se você selecionar um **Tipo de dados** incompatível com o selecionado **Método** , o sistema muda automaticamente o. **Método** para um valor compatível.
Peso	[Obrigatório] Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10. Esse campo ficará visível e será obrigatório somente se o **Tipo de dados** for **Data**, **Data/Hora** ou **Cadeia de caracteres**. Esses tipos de dados não são incluídos nos cálculos de resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	[Obrigatório] Valor numérico que determina a ordem da pergunta de métrica em questionários de avaliação, em relação a outras perguntas de métrica na mesma categoria. A métrica com o menor valor de ordem aparece como a primeira pergunta na seção de categoria. Por padrão, a ordem é 100. **Nota:** Não importa qual valor de ordem você usa para métricas com o método de script, já que eles não aparecem em questionários.
Ativo	Caixa de seleção que determina se esta métrica é usada. Se a caixa de seleção não estiver marcada, será como se o registro de métrica não existisse.
Obrigatório(a)	Marque a caixa que torna a pergunta de métrica obrigatória (selecionada) ou opcional (desmarcada) em questionários de avaliação. Os usuários não podem enviar questionários até que eles forneçam respostas válidas a todas as perguntas obrigatórias, que são indicadas por um indicador de status de campo vermelho. Este campo ficará visível somente se **Depende de** o campo está vazio e o tipo de dados não é **Caixa de seleção** .

6. Clique em **Geral** e preencha os campos, conforme apropriado.

Guia Geral

Campo	Descrição
Pergunta	Texto a ser usado como pergunta nos questionários de revisão de incidentes de segurança. Insira uma pergunta clara e direta que seja fácil de responder, como **Como contemos o incidente**
Descrição	Informações sobre a métrica e o que ela avalia. . *Method*. **Avaliação** incluir detalhes que ajudam os usuários a entender como responder à pergunta. Esse texto aparece como uma dica quando um usuário aponta para o texto da pergunta no questionário.
Depende de e exibido quando	Selecione uma pergunta em **Depende de** campo do qual a pergunta atual depende. Por exemplo, a pergunta "Quais logs adicionais foram necessários?" Depende da pergunta "Todos os logs necessários estavam disponíveis?" Em seguida, use **Exibido quando** campo para identificar quando você deseja que a pergunta dependente apareça nos questionários. Por exemplo, se você quiser que a pergunta dependente seja feita somente quando o usuário responder **Não** "Todos os logs necessários estavam disponíveis?" pergunta, selecione **Não** em **Exibido quando** campo. **Nota:** O sistema evita a criação de dependências recursivas entre métricas. Por exemplo, se a Métrica A depender da Métrica B, a Métrica B não poderá depender da Métrica A.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Tipo de campo** e preencha os campos, conforme apropriado.

Guia Tipo de campo

Campo	Descrição
Tipo de dados	O tipo de dados da resposta esperada da qual a lista de tipos disponíveis depende para o método selecionado. Se o método for **Avaliação**, o tipo de dados determinará como os usuários responderão à pergunta correspondente nos questionários. Se o método for **Script**, o tipo de dados determinará como o sistema calculará os resultados da avaliação. **Nota:** Se outra pergunta depender dessa métrica, você não poderá mudar o tipo de dados.
Respostas aleatórias	Caixa de seleção que determina se as opções de resposta para esta pergunta de métrica devem ser apresentadas em ordem aleatória sempre que um usuário abrir um questionário de avaliação que contém a pergunta. A preferência de resposta pode ser influenciada pela ordem na qual as opções de resposta aparecem. Isso pode resultar em resultados tendenciosos. As opções de resposta de aleatoriedade podem ajudar a evitar essa tendência. Este campo ficará visível somente se você selecionar **Escala Likert** ou **Opção** em **Tipo de dados** campo.
Plug-in dependente	[Obrigatório se *Method*. **Script** .] Plug-in que contém as tabelas consultadas no script. O sistema executará o script de métrica somente se o plug-in estiver ativo. Os valores padrão disponíveis são **Gestão de ativos**, **CMDB**, **Core**, **Gestão de custos**, **Compras** e **Software Asset Management**. Este campo ficará visível somente se *Method*. **Script** . **Nota:** ◦ Se o valor padrão Core for usado, o script será sempre executado. ◦ Se você for um administrador, poderá adicionar mais opções de plug-ins ao campo.
Definição de escala	Configuração que determina se valores numéricos menores ou maiores são iguais a uma boa pontuação nos cálculos de resultados da avaliação. Selecione **Baixo** se valores numéricos menores forem melhores, como para uma métrica que mede o número de defeitos de um fornecedor. Selecione **Alto** se valores numéricos maiores forem melhores, como para uma métrica que mede a satisfação do usuário em uma escala de um a cinco. O valor padrão é **Alto**. Este campo é visível e obrigatório, a menos que *Data type*. **Data** , **Data/Hora** ou **Cadeia de caracteres** . Os resultados para esses tipos de dados não são incluídos nos cálculos de resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Mín	O valor numérico mais baixo a ser usado como uma opção de resposta em avaliações ou como um valor com escala em uma métrica com script. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert** este campo é somente leitura e é definido automaticamente com base na menor definição de métrica *Value*.
Máx	Maior valor numérico a ser usado como opção de resposta ou valor com escala. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert** este campo é somente leitura e é definido automaticamente com base na maior definição de métrica *Value*.
Script	Script que obtém as informações do sistema desejadas. O script tem uma variável de entrada, definida com o ID do incidente de segurança (primário) e três variáveis de saída possíveis definidas pelo script, string_result, scaled_result e actual_result. Quando o tipo de dados é Cadeia de caracteres, somente string_result é necessário. Este campo fica visível e obrigatório quando *Method*. **Script** ou o valor padrão vem de um script.
Modelo	Um conjunto predefinido de respostas comuns a serem usadas para a pergunta. Por exemplo, um modelo de frequência provavelmente começaria com um valor de "Nunca" e subiria até o valor superior de "Sempre". Este campo ficará visível e obrigatório somente se *Data type*. **Modelo** . **Nota:** Se outra métrica depender dessa métrica, você não poderá mudar o modelo.

8. **Opcional:** Ao concluir suas entradas, clique em **Atualização** .

Criar regras de atribuição de PIR

Além de adicionar manualmente a lista de avaliação de revisão pós-incidente de usuários para um incidente de segurança, você pode definir regras de atribuição para adicionar usuários automaticamente à lista.

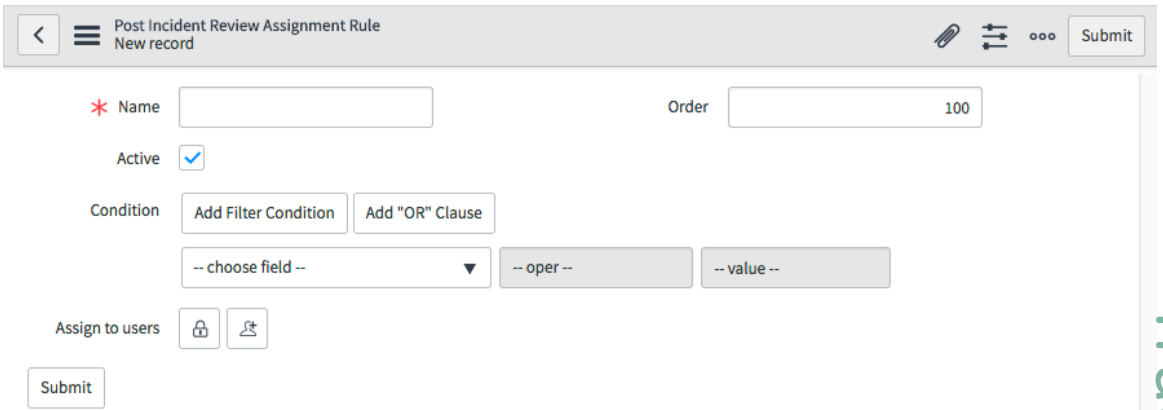
Antes de Iniciar
Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Análise pós-incidente – Configuração de avaliações**.
2. Detalhar até **Regras de atribuição de usuário** seção.
3. Clique em **Configurar**.
4. Clique em **Nova**.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta regra de atribuição.
Ativo	Marque esta caixa de seleção para ativar a regra.
Ordem	Insira um valor numérico para especificar onde, na lista de regras de atribuição, esta regra deve aparecer. Números mais baixos aparecem na parte superior da lista. **Nota:** Somente a primeira regra de atribuição correspondente é executada e somente os usuários definidos nessa regra são adicionados à lista de avaliação.
Condição	Use o construtor de condições definir as condições que devem ser atendidas no incidente de segurança para que esta regra seja executada. Para obter mais informações, consulte o exemplo abaixo.
Atribuir a usuários	Clique no ícone de cadeado para adicionar usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.

6. Clique em **Enviar**.

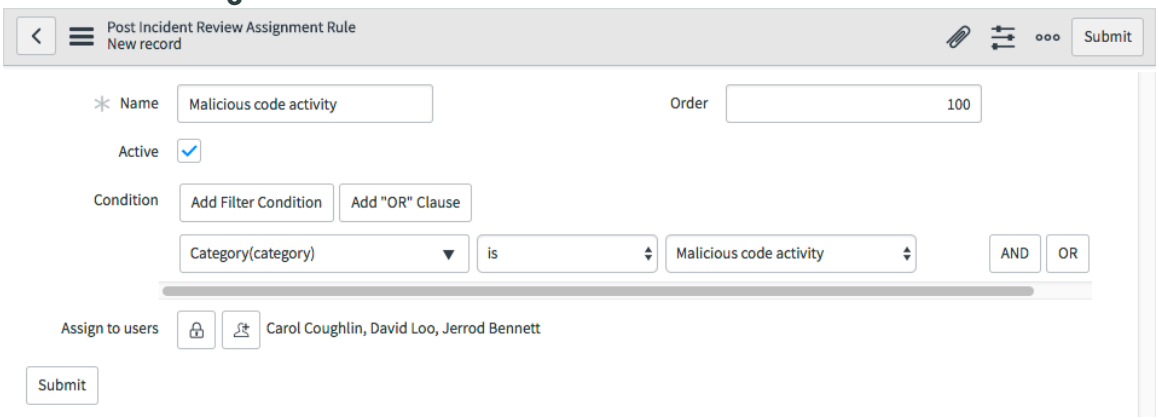
Example: Atividade de código malicioso

Na regra de atribuição de revisão pós-incidente mostrada aqui, quando um incidente de segurança com **Categoria** campo definido como **Atividade de código mal-intencionado** transições para **Revisão** estado, os três usuários identificados (que são especialistas em lidar com atividades de código mal-intencionado) são adicionados à lista de usuários que receberão o questionário de revisão pós-incidente para este incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de código malicioso



Fechar incidentes de segurança

Quando um incidente de segurança faz a transição para o estado Revisão, é possível fechá-lo e inserir um código de fechamento apropriado. Códigos de fechamento podem ser pesquisados posteriormente para facilitar a localização.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Nota: Em versões anteriores de Resposta a incidentes de segurança, os usuários podem fechar incidentes de segurança ou solicitações como spam. Em Istanbul versão, a opção de spam não está mais disponível. Incidentes ou solicitações de segurança de spam podem ser cancelados ou excluídos, conforme apropriado.

Procedimento

1. Se o incidente de segurança que você deseja fechar ainda não estiver aberto, navegue até **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**e localize o incidente de segurança que você deseja fechar.

   Nota: Se houver algum avaliações de revisão pós-incidente que não foram concluídos para este incidente de segurança, o incidente de segurança não pode ser encerrado. Retornar a **Incidente de segurança** > **Análise pós-incidente** > **Todas as revisões incompletas**localize as revisões que estão incompletas e peça aos revisores para concluir suas revisões ou cancelar as avaliações restantes.

2. Clique em **Informações de fechamento** e preencha os campos, conforme apropriado.

Incidente de segurança

Campo	Descrição
Criar artigo de conhecimento	Selecione este campo para criar automaticamente um rascunho de artigo da base de conhecimento que contém o conteúdo da revisão pós-incidente.
Código de fechamento	Selecione o código de fechamento que melhor descreve o motivo pelo qual você está fechando este incidente de segurança. ○ Investigação concluída ○ Ameaça mitigada ○ Vulnerabilidade corrigida

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Vulnerabilidade inválida ○ Não resolvido ○ Falso positivo
Encerrado por	Exibe o usuário que fechou o incidente de segurança após a atualização do registro.
Encerrado	Exibe a data e a hora do fechamento após a atualização do registro.
Anotações de encerramento	Insira anotações adicionais que descrevam o resultado do fechamento deste incidente de segurança.

3. Clique em **Atualizar**.
4. O usuário atribuído pode alterar manualmente o. **Estado** . **Encerrado** .
   Quando um incidente primário é encerrado, todas as tarefas de resposta pertencentes ao incidente secundário são canceladas. Se não houver outros tipos de tarefas, o incidente secundário também será encerrado.

Adicione informações de fechamento a um incidente de segurança

Quando um incidente de segurança está no estado Revisão ou Encerrado, você pode inserir informações de fechamento.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ele ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique em **Registros relacionados** guia.
3. Preencha os campos, conforme necessário.

Campo	Descrição
Criar artigo de conhecimento	Marque esta caixa de seleção para gerar um artigo de conhecimento usando o conteúdo do relatório pós-incidente.
Código de fechamento	Selecione o código de fechamento que melhor descreve o motivo do fechamento do incidente de segurança.
Encerrado por	[Somente leitura] Exibe o usuário que fechou o incidente de segurança.
Encerrado	[Somente leitura] Exibe a data e a hora em que o incidente de segurança foi encerrado.
Anotações de encerramento	Como o incidente de segurança foi encerrado, incluindo lições aprendidas, resolução e assim por diante.

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Detalhes do incidente
   - Análise pós-incidente
5. Ao concluir suas entradas, clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restringir o acesso a incidentes de segurança

Gerencie o acesso dos incidentes de segurança que contêm informações confidenciais. Você pode impor restrições de incidentes de segurança para determinar quem pode acessar um determinado incidente e limitar o acesso somente a usuários ou grupos específicos.

Antes de Iniciar

Função necessária: sn_si.admin

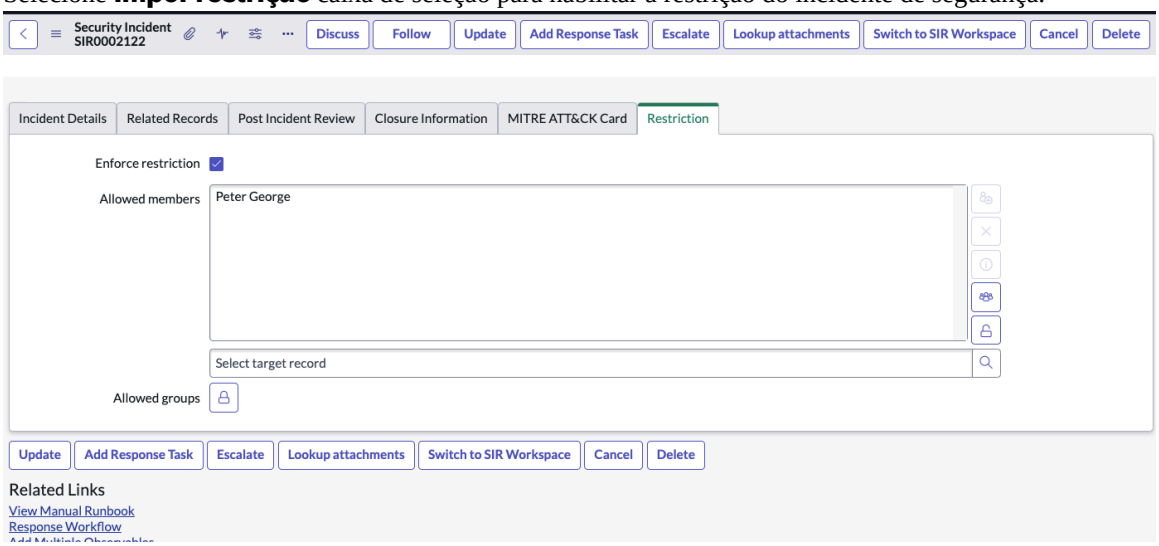
Por Que e Quando Desempenhar Esta Tarefa

As restrições de incidentes de segurança permitem ocultar incidentes de segurança críticos de serem acessados por outros usuários em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança que um usuário pode acessar. Você pode impor uma restrição de incidente de segurança habilitando o. **Impor restrição** e marque os usuários ou grupos que têm permissão para acessar o incidente de segurança específico.

Depois de impor a restrição a incidentes de segurança específicos e limitar o acesso a determinados usuários ou grupos, todos os outros usuários restantes em sua organização não poderão acessar esses incidentes de segurança, mesmo que pesquisem um incidente de segurança restrito específico.

Procedimento

1. Abra um incidente de segurança que você deseja restringir.
2. Se você estiver usando a IU clássica, execute o seguinte:
   a. Clique em **Restrição** guia.
   b. Selecione **Impor restrição** caixa de seleção para habilitar a restrição do incidente de segurança.



   c. No campo Membros permitidos, clique em ícone para selecionar os usuários que podem acessar o incidente de segurança.
   d. Selecione ícone para adicionar a si mesmo como o usuário permitido.
   e. Selecione ícone para adicionar ou remover usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. No campo Grupos permitidos, clique em ícone para selecionar os grupos que podem acessar o incidente de segurança.

g. Selecione ícone para adicionar ou remover grupos.

> **Nota:** Após **Impor restrição** se a caixa de seleção estiver habilitada para o incidente de segurança, somente sn_si.admin e membros ou grupos permitidos terão acesso ao incidente de segurança.

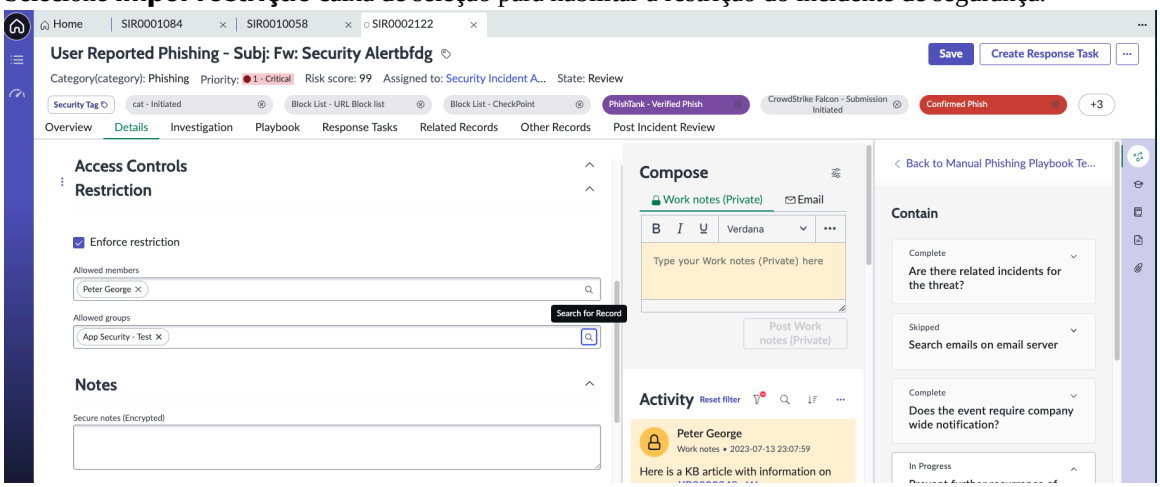
h. Clique em **Atualizar**.

3. Se você estiver usando o Espaço SIR, execute o seguinte:

a. No incidente de segurança, clique em **Detalhes** guia.

b. Role para baixo e clique em **Restrição** seção.

c. Selecione **Impor restrição** caixa de seleção para habilitar a restrição do incidente de segurança.



d. No campo Membros permitidos, selecione os usuários que podem acessar o incidente de segurança usando a opção Pesquisar.

e. No campo Grupos permitidos, selecione os grupos que podem acessar o incidente de segurança usando a opção Pesquisar.

> **Nota:** Após **Impor restrição** se a caixa de seleção estiver habilitada para o incidente de segurança, somente sn_si.admin e membros ou grupos permitidos terão acesso ao incidente de segurança.

f. Clique em **Salvar**.

Gerencie ameaças à segurança usando Espaço do analista de segurança

Resposta a incidentes de segurança inclui uma nova interface do usuário chamada Espaço do analista de segurança que apresenta ferramentas avançadas para ajudar na análise, incluindo o playbook, a exibição de verificação e guias para trabalhar em vários incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criadas especificamente para analistas de segurança, as poderosas ferramentas do Espaço do analista de segurança permite que você analise o volume cada vez maior de dados associados a incidentes de segurança. E as ações automatizadas reduzem significativamente o tempo de investigação do incidente de segurança, o que pode ser a diferença entre interromper um ataque e sofrer uma violação.

Antes de usar o. Espaço do analista de segurança

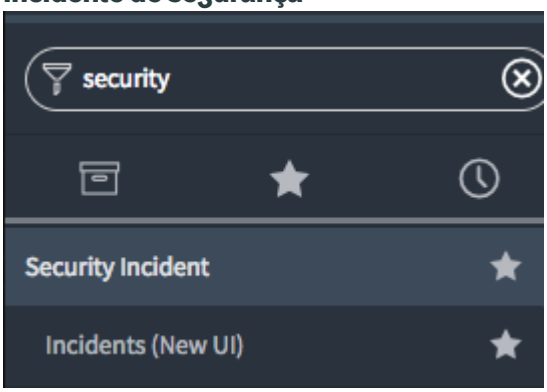
Antes de começar a usar Espaço do analista de segurança, Você deve garantir que sua instância tenha pelo menos London Patch 3 instalado, que você tenha as funções corretas definidas e que tenha Baixado a aplicação de IU de Resposta de incidente de segurança do ServiceNow Store.

Nota: Se sua instância estiver executando uma versão anterior à London Patch 3, você deverá solicitar o plug-in de IU de Resposta de incidentes de segurança por meio do sistema de Atendimento ao cliente HI.

Como acessar o Espaço do analista de segurança

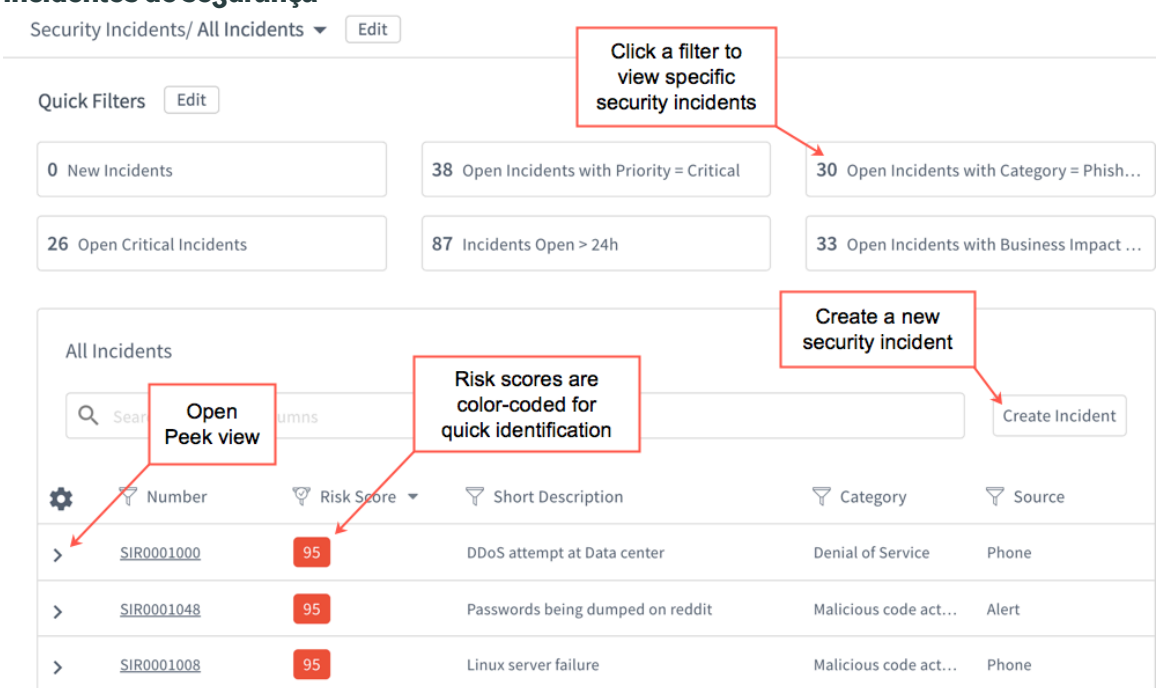
Para acessar este novo espaço, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.

Incidente de segurança



O espaço é aberto em uma guia separada do navegador.

Incidentes de segurança



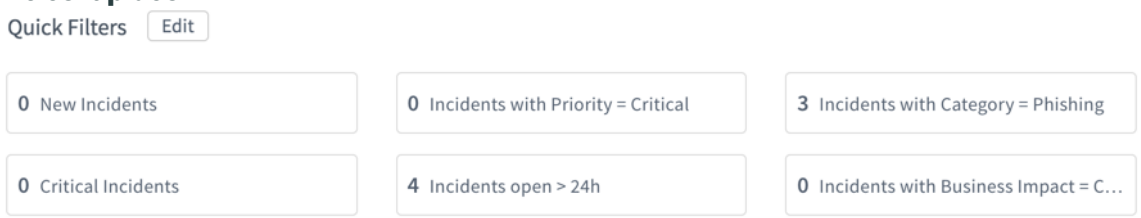
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Localize os incidentes de segurança que você deseja analisar com Filtros rápidos

. Espaço do analista de segurança o fornece várias ferramentas para filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Os Filtros rápidos permitem selecionar um subconjunto dos incidentes de segurança com base nos critérios no filtro.

Filtros rápidos



Basta clicar no filtro rápido que você deseja usar.

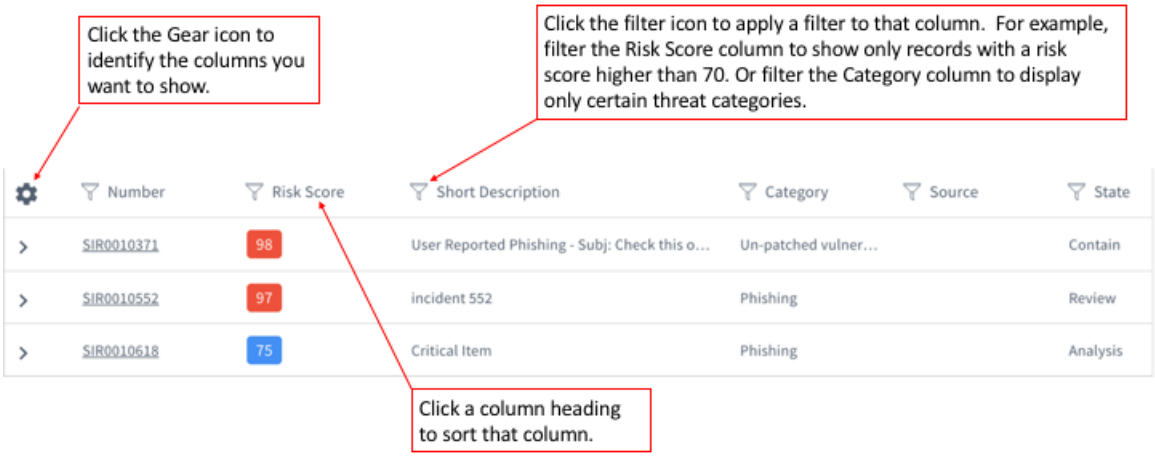
Nota: Você pode clicar em um **Editar** botão para identificar quais filtros rápidos você deseja exibir na tela de lista. No mínimo um filtro deve ser selecionado, até no máximo seis.

Você pode definir filtros rápidos adicionais, bem como filtros primários para Espaço do analista de segurança, usando o ambiente clássico. Para obter mais informações, consulte Configurar filtros primário e secundário para Espaço do analista de segurança.

Personalize a lista de incidentes de segurança

Como acontece com todas as listas em sua instância, o Espaço do analista de segurança fornece ferramentas para personalizar a lista e classificar as informações exibidas para atender às suas necessidades de análise.

Personalize a lista de incidentes de segurança



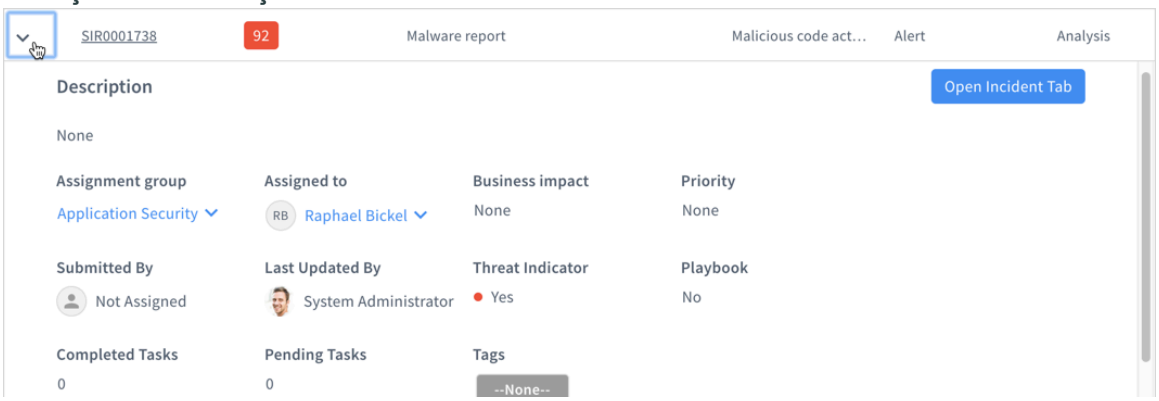
Poupe tempo com a exibição de verificação

Antes de abrir um registro de incidente de segurança, você pode economizar tempo usando a exibição de verificação. Este recurso permite localizar rapidamente artefatos de segurança vitais sem precisar recarregar a página inteira. Basta clicar em **>** ícone à esquerda de um número de incidente de segurança para dar uma olhada.

Tradução automática

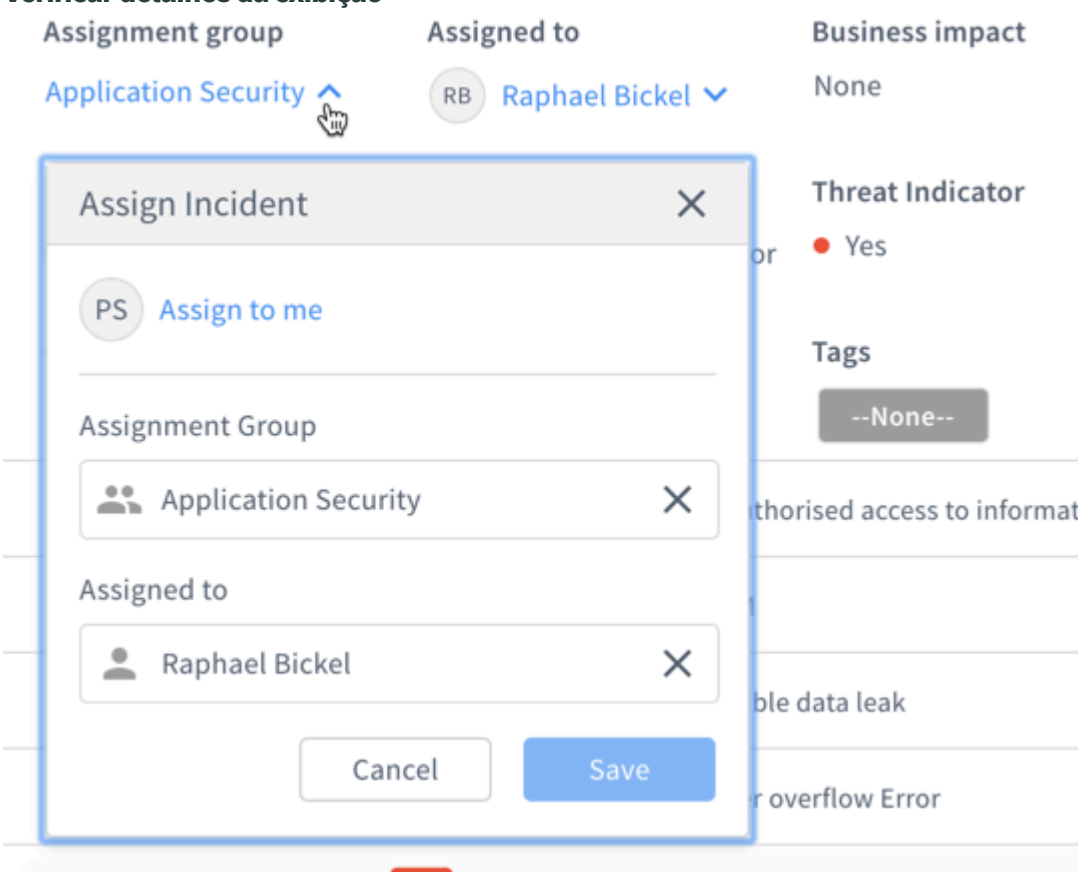
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de verificação



A exibição Peek fornece um snapshot de informações vitais em uma única exibição. Esta exibição pode economizar um tempo valioso quando você está trabalhando com vários incidentes. Você pode clicar nas setas para baixo em determinados campos para fazer atualizações dinâmicas, como atribuir um grupo de atribuição ou um analista específico.

Verificar detalhes da exibição



Execute ações rápidas em um incidente de segurança

Depois de selecionar e abrir um incidente de segurança específico, você pode executar ações de economia de tempo no registro.

Tradução automática

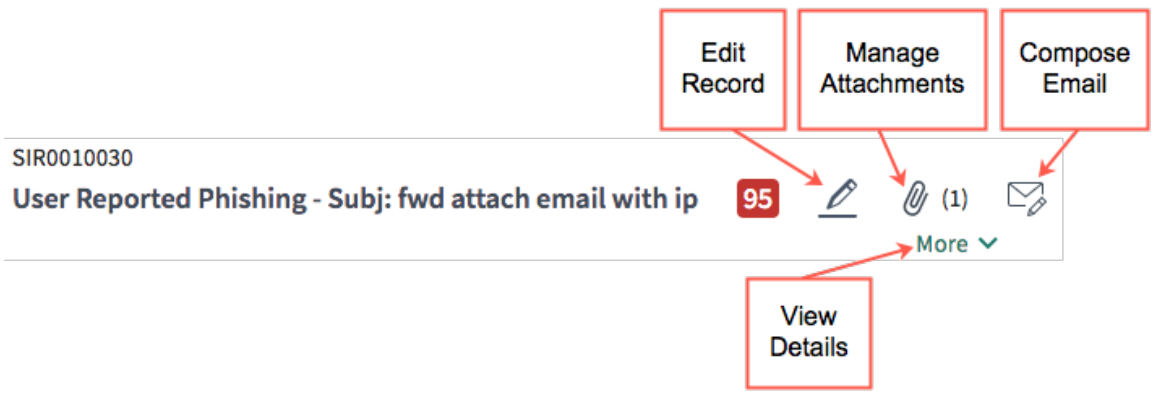
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o incidente de segurança estiver aberto, clique em **Editar registro** ícone para fazer mudanças rápidas em qualquer um de seus campos. Se o registro estiver fechado, você poderá mudar somente seu marcador.
- Clique em **Gerenciar anexos** para anexar arquivos ao incidente de segurança. Você também pode baixar ou remover arquivos anexados e editar a criptografia aplicada aos anexos.
- Clique em **Compor e-mail** para enviar um e-mail rápido para um colega. Os e-mails podem ser de formato livre ou você pode enviar e-mails predefinidos selecionados em uma lista de modelos. E-mails enviados e respostas recebidas são capturados na Linha do tempo do incidente.

> **Nota:** Você pode criar modelos personalizados que contenham conteúdo reutilizável para e-mails e notificações por e-mail. As variáveis podem ser usadas para inserir informações específicas do incidente ou alerta de segurança, como linha de assunto, prioridade ou categoria de ameaça. Use a tabela Incidente de segurança [sn_si_incident] para e-mails e notificações por e-mail relacionadas a. Resposta a incidentes de segurança. Para obter mais informações, consulte Modelos de e-mail

- Clique em **Mais** para exibir um snapshot rápido do incidente de segurança, como a descrição, o impacto nos negócios e a prioridade. Você também pode clicar na seta para baixo em **Grupo de atribuição** e. **Atribuído a.** campos para fazer mudanças dinâmicas nesses campos.

Grupo de atribuição



Trabalhe com vários incidentes de segurança

A interface com guias permite que você mantenha vários incidentes de segurança abertos simultaneamente para que você possa alternar entre eles com um único clique. Isso pode economizar tempo e permitir que você veja o panorama geral quando ameaças de várias fontes são identificadas.

Trabalhe com vários incidentes de segurança



Exiba informações de análise nas guias de incidentes de segurança

Quando você abre um registro de incidente de segurança, três guias são mostradas:

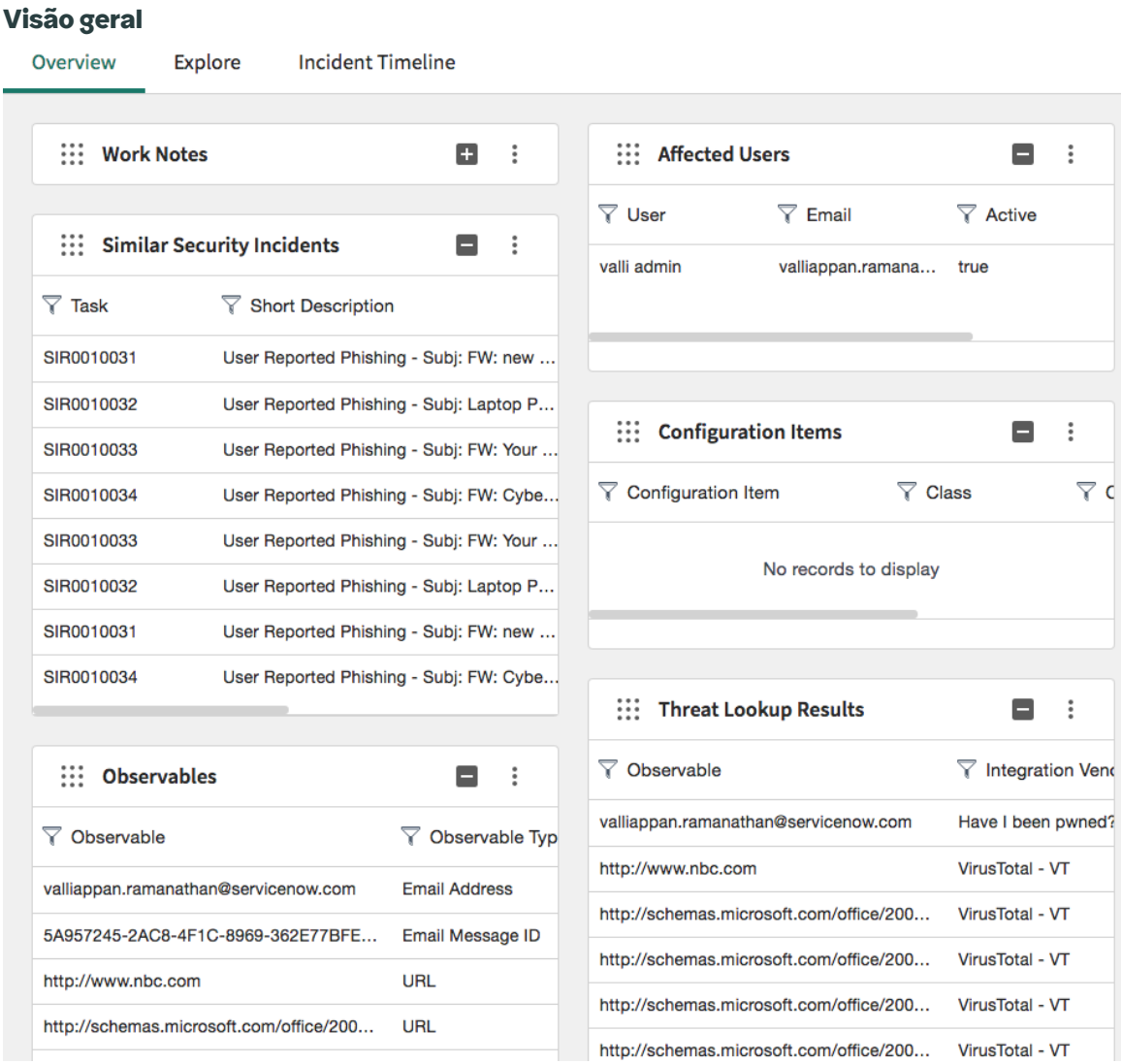
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Visão geral
- Explorar
- Linha do tempo do incidente

Guia "Visão geral"

Use **Visão geral** para exibir informações em um incidente de segurança em um único local. Não há necessidade de abrir outra aplicação ou console.

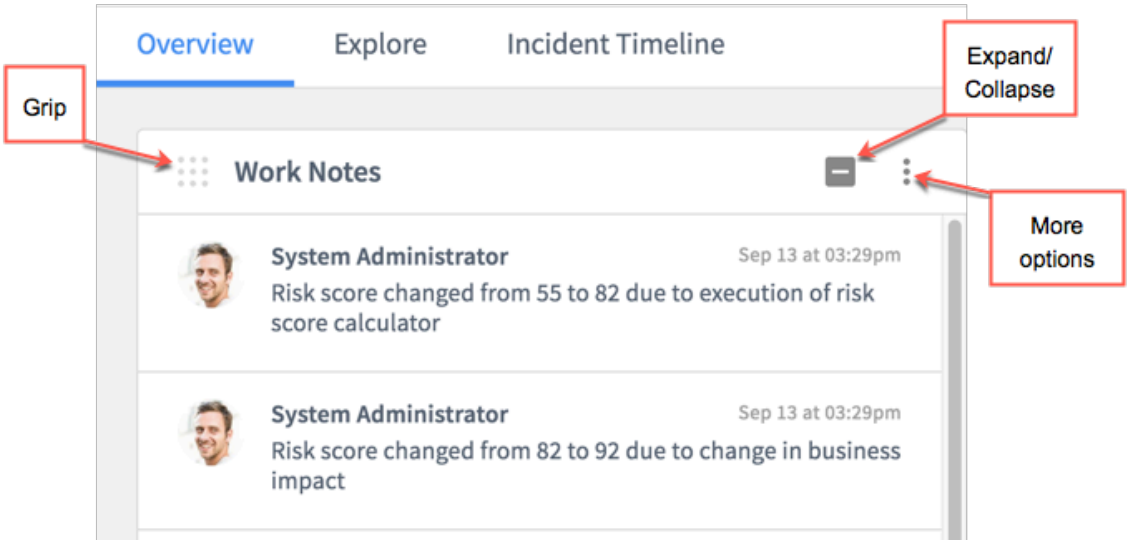


Os blocos que são exibidos no **Visão geral** as guias são personalizáveis. Você pode recolhê-los e expandi-los conforme necessário e movê-los arrastando **Alça** ícone. Clique em **Mais opções** ícone para excluir um bloco ou mudar o texto do título.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

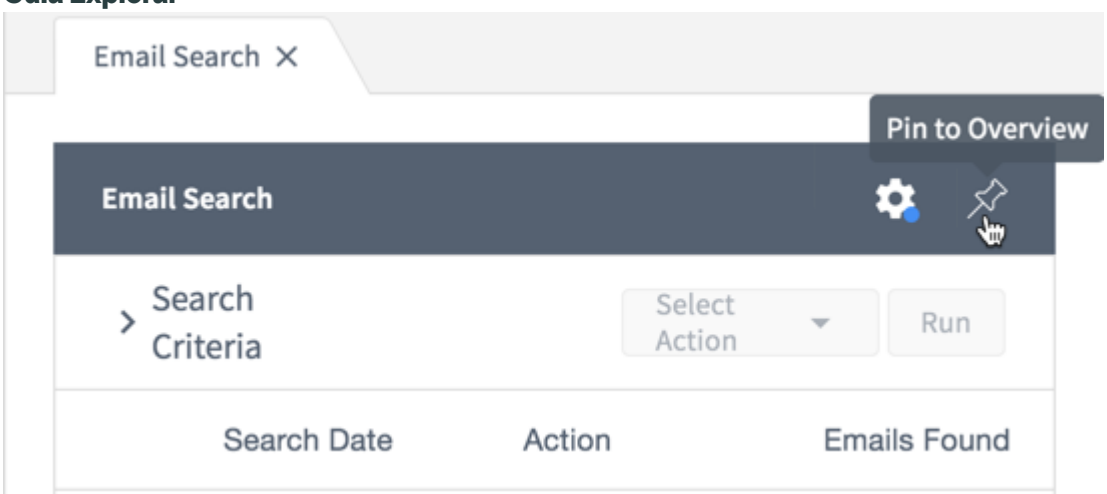
Guia "Visão geral"



Guia Explorar

Configure os blocos exibidos no **Visão geral** usando **Explorar** guia. Basta selecionar os blocos que você deseja exibir no painel esquerdo e clicar em **Fixar** ícone. Os blocos fixados aparecem automaticamente em **Visão geral** guia.

Guia Explorar



O painel esquerdo do **Explorar** inclui uma ampla variedade de informações que você pode exibir no **Visão geral** guia. Por exemplo, expanda **Observáveis** para exibir essas listas relacionadas.

- Observáveis
- Resultados da Pesquisa de ameaças
- Resultados da verificação de segurança
- Pesquisas de domínio
- Aprimoramento de Observável

Listas relacionadas adicionais estão disponíveis em **Usuários** , **Itens de configuração** e **Incidentes** .

Tradução automática

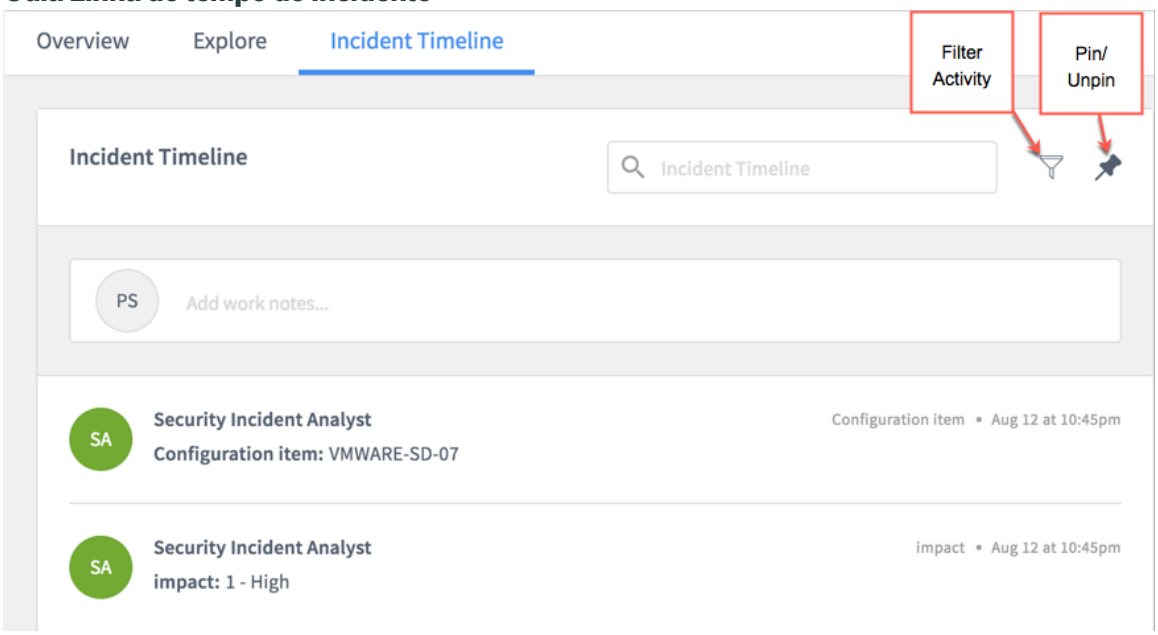
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Linha do tempo do incidente

Use **Linha do tempo do incidente** durante sua investigação para fins de acompanhamento. Sempre que uma ação é executada em um incidente de segurança, o sistema a registra na Linha do tempo do incidente.

- Você também pode adicionar anotações de trabalho manualmente à linha do tempo digitando-as em **Adicionar anotações de trabalho** e clicando **Publicar** .
- Você pode pesquisar uma atividade de linha do tempo específica usando a caixa Pesquisar.
- . **Atividade de filtro** o ícone permite exibir somente os tipos de atividade da linha do tempo que você deseja ver (por exemplo, somente incidentes criados por um analista específico).
- Você pode adicionar ou remover a Linha do tempo do incidente do **Visão geral** usando **Fixar/Desfixar** ícone.

Guia Linha do tempo do incidente



Lide com incidentes de segurança usando o Playbook

Resolva determinados tipos de ameaças à segurança de maneira passo a passo usando os playbooks de analista de segurança integrados. Por exemplo, um analista pode usar o playbook para resolver ataques de phishing e ameaças causados por atividades de código mal-intencionado. Para obter mais informações, consulte Resolva ameaças à segurança com o playbook.

Resolva ameaças à segurança com o playbook

Use o Playbook para resolver determinados tipos de ameaças à segurança de maneira passo a passo. Por exemplo, você pode resolver ataques de phishing e ameaças causados por atividade de código mal-intencionado usando playbooks.

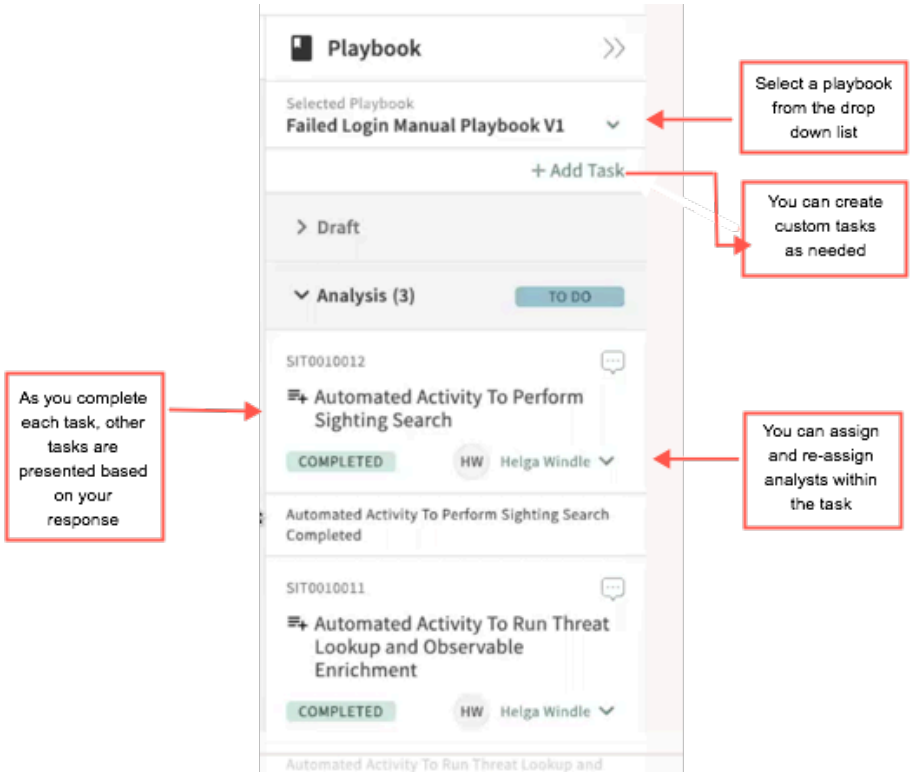
Antes de Iniciar
Função necessária: sn_si.admin ou admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Cada grupo de tarefas (Análise, Conter e assim por diante) orienta você por uma série de perguntas e outras atividades para resolver a ameaça.

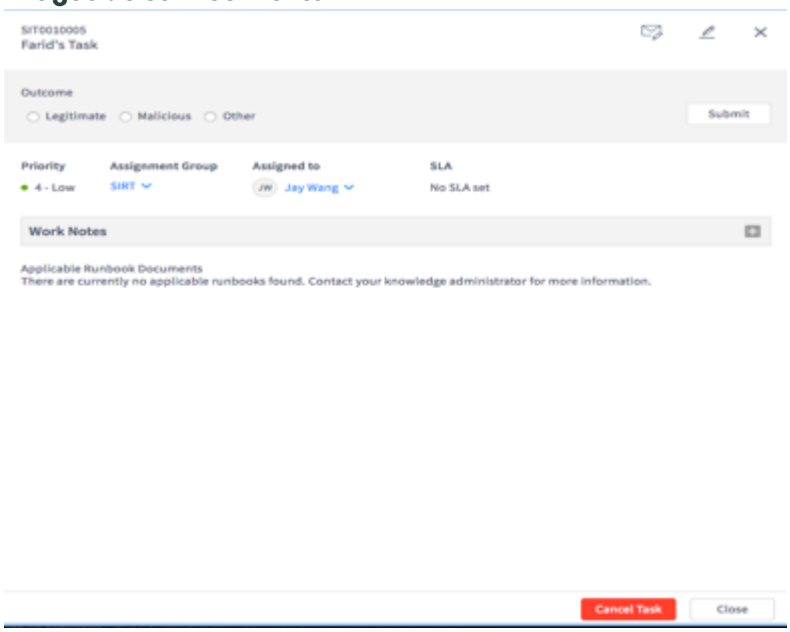
Playbook



Ao trabalhar em cada tarefa, insira anotações de trabalho para ajudar a analisar ataques semelhantes no futuro. Depois que uma ameaça é identificada, você também pode usar as informações no playbook para colocar a ameaça em quarentena, isolar ativos afetados de forma semelhante e remover malware.

Os artigos de conhecimento, incluídos em cada tarefa, fornecem dicas e outras informações para ajudá-lo a executar as etapas necessárias.

Artigos de conhecimento



Tradução automática

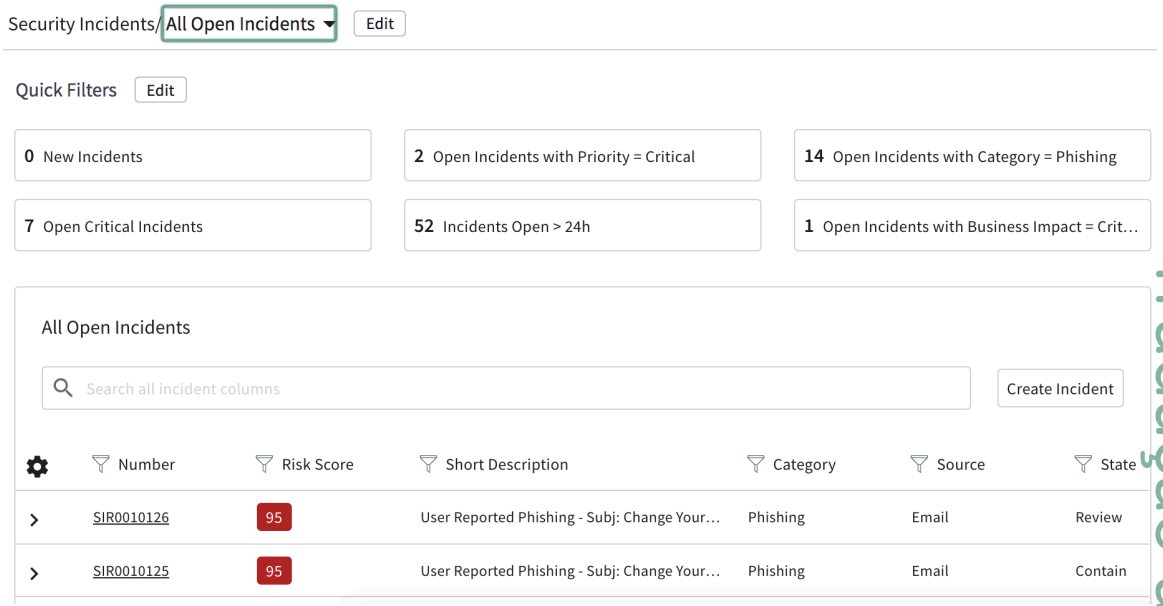
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O sistema de base inclui artigos de conhecimento para cada uma das tarefas do playbook. No entanto, você pode escreva seus próprios artigos de conhecimento e. associe-os a tarefas do playbook .

Nota: Para obter um exemplo de como usar o playbook para analisar e resolver uma ameaça específica, consulte Resolver ataques de phishing relatados pelo usuário com o playbook.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Incidentes (Nova IU)**.
   A tela Incidentes de segurança mostra os incidentes de segurança que foram atribuídos a você.



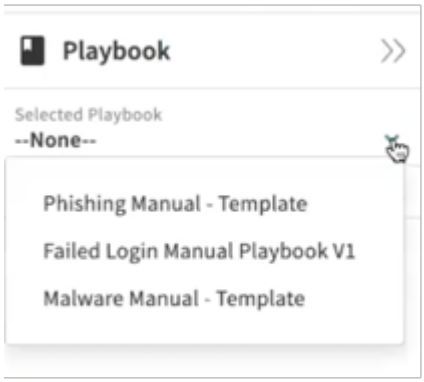
2. Você pode clicar em **Atribuído a mim** lista de seleção para selecionar um filtro diferente, como todos os incidentes em aberto ou todos os incidentes não atribuídos.
   Como alternativa, você pode clicar em um dos Filtros Rápidos para exibir incidentes de segurança de um tipo específico, como Somente Incidentes Críticos.
3. Clique no incidente de segurança que você deseja analisar.

   Priorizar incidentes de segurança com alto pontuações de risco .

4. Se o painel do playbook na borda direita da tela estiver fechado, clique no ícone do playbook ( ) para abri-lo.
   Se nenhum playbook for atribuído ao incidente de segurança, você poderá selecionar um playbook na lista de seleção do Playbook selecionado, conforme mostrado abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você também pode atribuir um playbook diferente ao incidente de segurança. Para incluir um playbook na lista de seleção do Playbook selecionado ou para mudar o playbook para um incidente de segurança, consulte Habilitar playbooks para seleção de analista para obter detalhes.

O playbook específico para o tipo de ameaça à segurança é aberto. É dividido em categorias de tarefas semelhantes. Por exemplo, você usa as tarefas no **Análise** grupo para determinar a validade e o escopo da ameaça. . **Conter** o grupo inclui tarefas para isolar a ameaça para um usuário ou ativo específico. As tarefas no **Erradicar** o grupo orienta você durante o processo de remoção do malware ou recriação da imagem do host.

5. Clique no primeiro grupo (**Análise** e clique na primeira tarefa no playbook.
6. Siga os prompts na tarefa.
   - Algumas tarefas fazem uma pergunta, como "O e-mail faz parte da campanha?" Execute a análise necessária para responder à pergunta e selecione **Sim** ou **Não** .
   - Se você tiver artigos de conhecimento definidos e associados a tarefas do playbook , os artigos aparecem quando você começa a trabalhar em uma tarefa.
   - Algumas tarefas são transitórias. Eles simplesmente instruem você a executar uma ação, como adicionar observáveis a um incidente de segurança. Depois de concluir a ação, clique em **Marcar como concluído** .

   À medida que você conclui as tarefas, as tarefas subsequentes são apresentadas a você com base nas escolhas feitas. Grupos esmaecidos (como **Recuperar** , **Revisão** e assim por diante) pode ser ativado por suas escolhas.
7. Continue trabalhando em cada tarefa apresentada a você até concluir todas as tarefas para resolver a ameaça e fechar o incidente de segurança.

Tópicos relacionados

Adicione uma tarefa personalizada ao playbook

Resolver ataques de phishing relatados pelo usuário com o playbook

O playbook de phishing orienta você nas tarefas necessárias para analisar e resolver um ataque de phishing relatado por um dos funcionários da sua empresa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

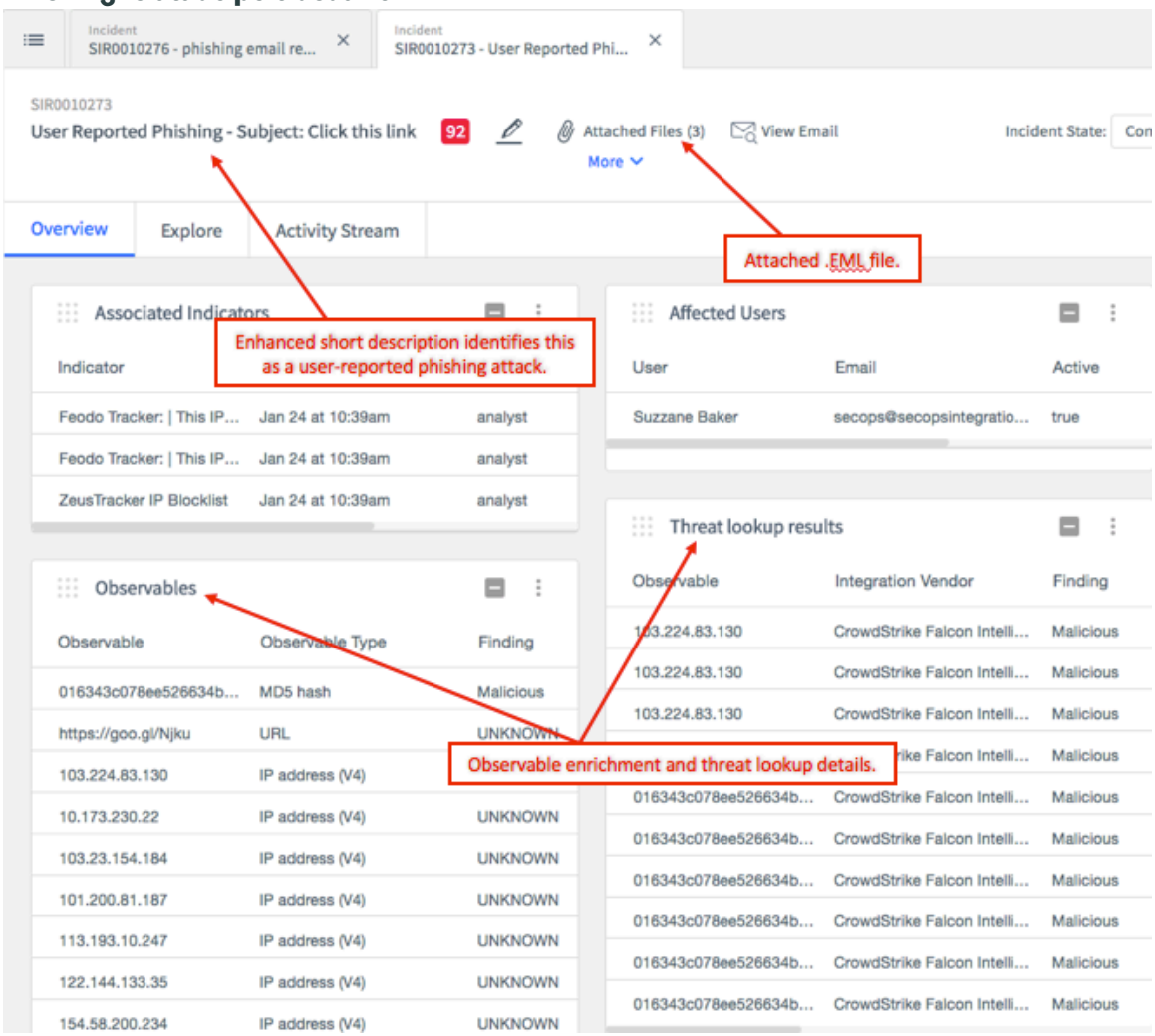
Como os incidentes de segurança são criados a partir de ataques de phishing relatados pelo usuário

Durante a configuração da Resposta do incidente de segurança, o administrador do sistema cria uma série de regras de correspondência de e-mail que pode identificar e-mails que contêm sinais de um ataque de phishing. Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .eml para o endereço de e-mail de phishing definido pela sua organização.

Quando o e-mail é recebido no endereço de e-mail de phishing, o anexo .eml é analisado e suas informações são comparadas com as regras de correspondência de e-mail. Se uma correspondência for encontrada, um incidente de segurança contendo as seguintes informações será criado:

- A descrição resumida inclui phishing relatado pelo usuário, seguido pelo assunto real do e-mail de origem.
- O arquivo .eml é anexado ao incidente de segurança.
- Se o .eml contiver observáveis, eles serão analisados e as pesquisas de aprimoramento e ameaça serão realizadas automaticamente.

Phishing relatado pelo usuário

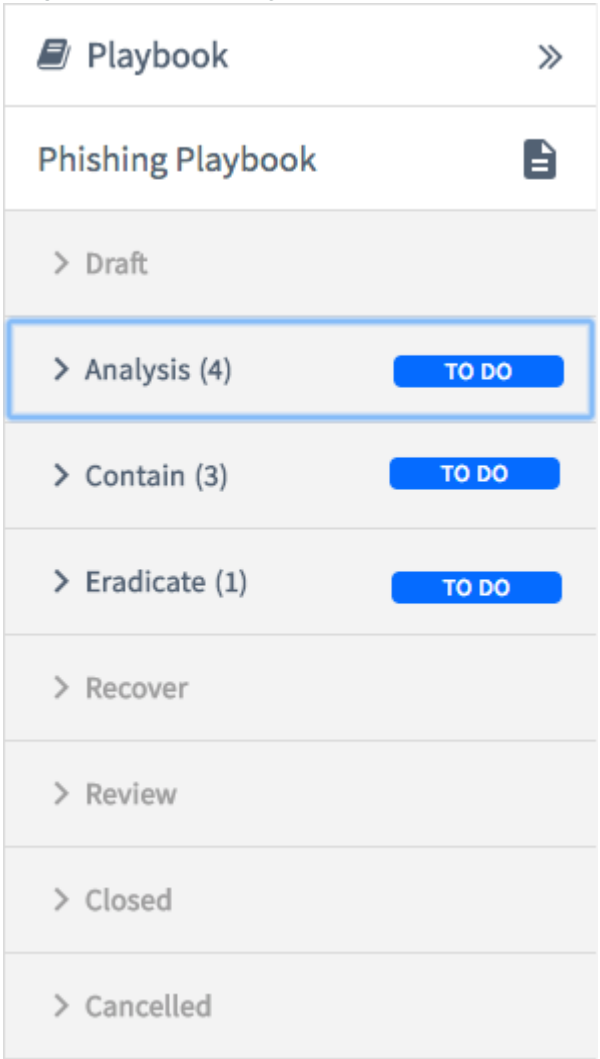


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando um incidente de segurança da categoria de phishing é aberto, o Playbook de Phishing fica disponível automaticamente. Basta clicar no ícone do playbook ( ) para abrir o playbook.

Playbook de phishing



O playbook de phishing contém tarefas para ajudar você a analisar, conter e erradicar uma ameaça de phishing. As tarefas são organizadas em estados (por exemplo, **Análise** , **Conter** e assim por diante). Quando todas as tarefas de um estado forem concluídas, o playbook orientará você para o próximo estado.

Analisando detalhes do incidente de segurança

Quando o incidente de segurança está no estado Análise, você recebe tarefas para executar a investigação básica do incidente, incluindo:

- Determinar a validade do incidente.
- Estudar o impacto da ameaça potencial.
- Coordenar uma resposta eficaz ao incidente.

Ao trabalhar nas tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Familiarize-se com os artigos de conhecimento.
- Abra o anexo de e-mail e examine-o em busca de sinais de elementos de phishing comuns.
- Revise os resultados da pesquisa de ameaças.

Que contém o incidente de segurança

Quando o incidente de segurança está em **Conter** estado, você receberá tarefas para revisar os detalhes do e-mail. Para garantir que as ameaças não entrem em sua organização, atualize as defesas de rede, na forma de assinaturas e regras do Sistema de defesa contra invasão (IDS) e do Sistema de prevenção de invasão (IPS).

Ao trabalhar nas tarefas:

- Tome ações para limitar os impactos da ameaça, como isolar os dispositivos afetados.
- Examine os observáveis anexados ao e-mail.
- Determine se algum conteúdo de e-mail está associado a uma ameaça conhecida, incluindo:
  - URL
  - Remetente do e-mail
  - URL de phishing
  - Endereço IP do servidor SMTP do remetente

Erradicar o malware

Depois de implantar assinaturas e regras atualizadas em sua solução antivírus, use as tarefas em **Erradicar** estado para determinar se o malware está presente e manipulá-lo adequadamente.

Conforme você trabalha nas tarefas:

- Verifique os endpoints dos dispositivos afetados quanto à presença de malware.
- Remova qualquer malware encontrado.
- Como último recurso, limpe e recrie a imagem dos dispositivos host.

Revisando o incidente de segurança

Se você determinou que um ataque de phishing foi um alarme falso ao executar as tarefas de análise, o incidente de segurança será movido para **Revisão** e você precisa notificar seus usuários para que eles saibam que é seguro abrir o anexo de e-mail.

Fechando o incidente de segurança

Quando todas as tarefas no playbook forem concluídas, o incidente de segurança será movido para **Encerrado** estado. Você deve inserir comentários de encerramento antes que o incidente possa ser encerrado.

Cancelando um incidente de segurança

Quando um incidente de segurança está em **Revisão** e você informou com sucesso aos usuários que o e-mail não é uma ameaça, o. **Cancelado** o estado se torna ativo e você pode cancelar o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A tarefa de recuperação não é usada no playbook de Phishing.

Associe um artigo de conhecimento a uma tarefa do playbook

Ao analisar ameaças à segurança usando Resposta a incidentes de segurança playbook, você pode exibir artigos de conhecimento para cada tarefa, se definido pela sua organização. Se os artigos de conhecimento não estiverem presentes, você poderá criá-los e associá-los a tarefas do playbook.

Antes de Iniciar

Como você usa o playbook em Resposta a incidentes de segurança anote o texto associado a cada tarefa. Por exemplo, a primeira tarefa na categoria Phishing é **O alerta foi enviado pelo funcionário?** Esta é a descrição resumida da tarefa e você precisa deste texto (exatamente como ele aparece no playbook) para associar um artigo de conhecimento à tarefa.

Função necessária: sn_sir.knowledge_admin e sn_si.admin ou admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Crie e publique um artigo de conhecimento para uma tarefa específica do playbook.
3. Navegar até **Incidente de segurança** > **Runbook manual** > **Criar novo runbook**.
4. Crie um runbook, preenchendo as seguintes informações:

Campo	Descrição
Artigo de conhecimento	Selecione o artigo de conhecimento publicado que você deseja associar à tarefa do playbook.
Tabela	Selecione Resposta a incidentes de segurança Tarefa [sn_si_task].
Condição	Defina o construtor de condições como: ○ **Opção:** Selecione **Descrição resumida** . ○ **Operador:** Selecione **.** . ○ **Valor de entrada:** Insira a descrição resumida da tarefa, exatamente como ela aparece no playbook.

5. Clique em **Enviar**.
   Na próxima vez que você executar o playbook e selecionar esta tarefa, o artigo de conhecimento associado será exibido.

Tópicos relacionados

Crie um artigo de conhecimento de incidente de segurança

Crie um runbook de resposta a incidentes de segurança

Adicione uma tarefa personalizada ao playbook

. Espaço do analista de segurança o sistema de base inclui uma série de tarefas para cada categoria de ameaça. Você pode criar tarefas personalizadas que atendam às necessidades exclusivas do seu sistema ou clientes.

Tradução automática

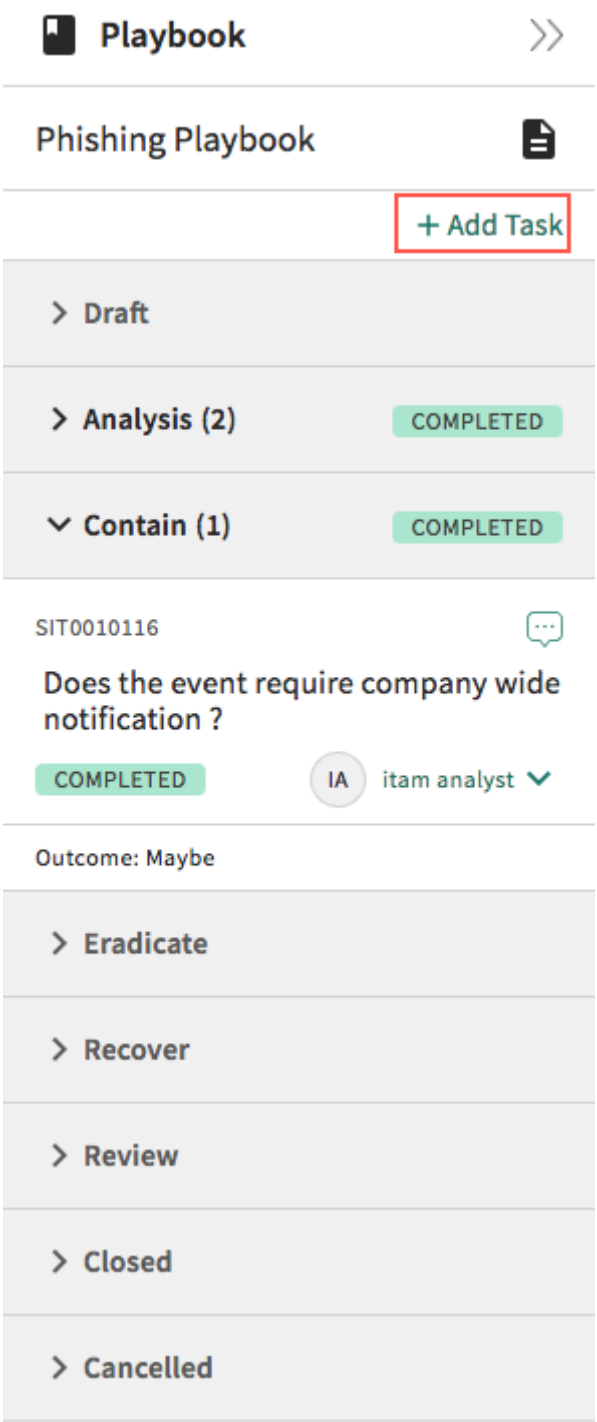
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.basic ou security_admin

Procedimento

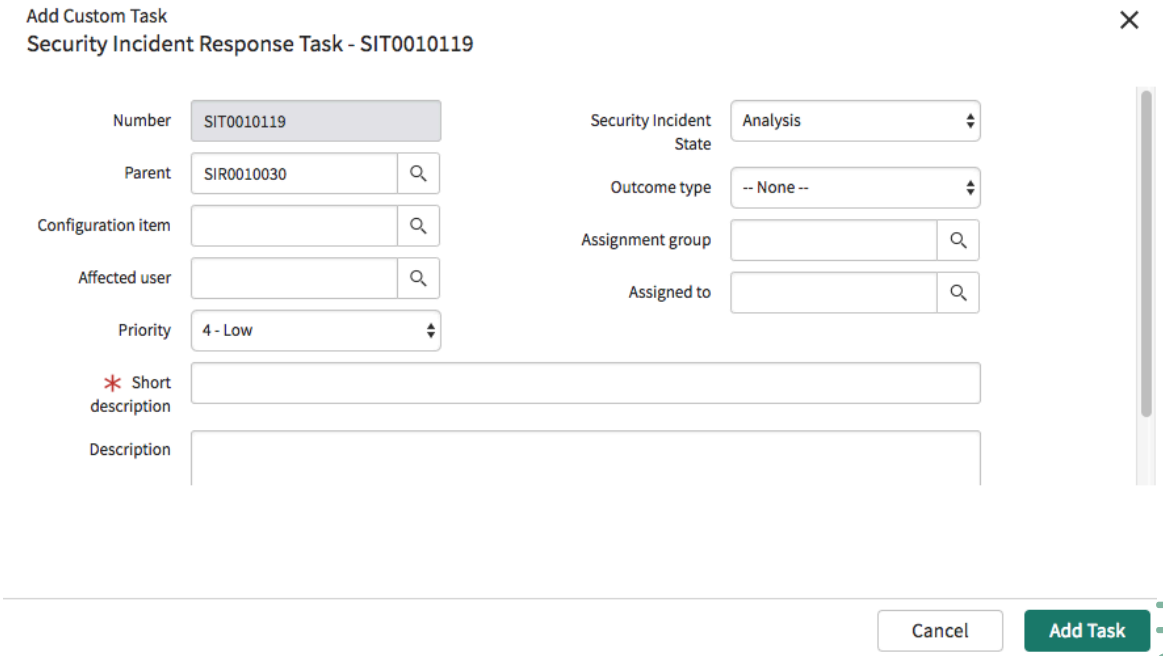
1. Com o playbook aberto, clique em **Adicionar tarefa** .



A tela Adicionar tarefa personalizada é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Preencha os campos, conforme necessário.

Campo	Descrição
Número	[Somente leitura] O número da tarefa de incidente de segurança gerado automaticamente.
Primário	O número do incidente de segurança relacionado.
Item de configuração	O item de configuração afetado pelo problema de segurança, se houver.
Usuário afetado	O usuário afetado pelo problema de segurança, se houver.
Prioridade	Selecione a prioridade usada para determinar quando esta tarefa deve ser executada.
Estado do Incidente de segurança	O estado atual da tarefa de resposta de segurança. Você pode selecionar um estado futuro, se necessário.
Tipo de resultado	Se você tiver a função sn_si.basic, selecione **Sim/Não** como o tipo de resultado. Se você tiver a função security_admin, poderá criar um tipo de resultado personalizado com vários valores de saída personalizados. Por exemplo, você pode definir uma tarefa com valores dependentes com base na categoria de ameaça. Para obter mais informações, consulte Listas de seleção
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído será selecionado.
Atribuição a	O indivíduo atribuído para executar a tarefa.
Descrição resumida	Uma descrição da tarefa do playbook de Incidente de segurança.
Descrição	Insira uma descrição para a tarefa selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Ao concluir suas entradas, clique em **Adicionar tarefa** .
   A tarefa é inserida no playbook após a tarefa atual.

Detecta pesquisas sobre ataques de phishing e malware relatados pelo usuário

Execute pesquisas de vistas em e-mails ou observáveis para determinar com que frequência determinados tipos de ataques, como ataques de phishing ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada um avistamento. As pesquisas de vistas de observáveis devem ser configuradas para seus armazenamentos de log ou gestão de eventos e informações de segurança (SIEM).

Como usar o recurso de pesquisa de detecções para localizar usuários com phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Assista a este vídeo de três minutos para saber como usar o recurso de pesquisa de avistamentos para localizar usuários com phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Os seguintes termos são usados para descrever ataques de phishing relatados pelo usuário:

- Usuário com phishing: Um usuário que recebeu um e-mail de phishing.
- Usuário vítima: Um usuário que interagiu com o URL de phishing, normalmente clicando em um link no e-mail de phishing. Potencialmente, esta ação expõe credenciais ao invasor.

Ao começar a analisar um incidente de phishing, você pode Execute uma pesquisa de vistas de e-mail ou Execute uma pesquisa de vistas observáveis identificar outros usuários em sua organização que são afetados pelo mesmo ataque de phishing. PESQUISE seus armazenamentos de logs para identificar usuários vítimas e com phishing. Depois de identificar a lista de usuários afetados, crie incidentes de segurança secundários para executar procedimentos abrangentes de resposta a incidentes usando as ferramentas disponíveis em Resposta a incidentes de segurança.

Nota: Você também pode usar a seguinte abordagem para executar uma pesquisa de vistas:

- Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes** e clique em um incidente de segurança.
- Clique em **Mostrar IOC** Em Links relacionados. Uma lista de observáveis é exibida.
- Selecione um observável na lista e no **Ações** , selecione uma das seguintes opções:
  - Executar pesquisa de detecções de tráfego na web
  - Executar pesquisa de detecções de tráfego de e-mails
- Especifique o intervalo de tempo e clique em **Pesquisa** para executar uma pesquisa de vistas.

Configurações de pesquisa de vistas salvas

Configure pesquisas de vistas e crie configurações salvas para SIEMs ou outros armazenamentos de log para instâncias de observáveis para determinar a presença de observáveis mal-intencionados em seu ambiente.

Nota: Pesquisas salvas e consultas no local são compatíveis somente com a Integração Splunk.

Tópicos relacionados

Criar registros de configuração de pesquisa de vistas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execute uma pesquisa de vistas de e-mail para ataques de phishing relatados pelo usuário

PESQUISE usuários que receberam e-mails de phishing com base em observáveis, como assunto do e-mail, nome do remetente ou ID da mensagem. Você pode conter e erradicar esses e-mails de phishing da sua organização.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

PESQUISE os logs de tráfego de e-mail do Splunk para coletar a lista de destinatários de um e-mail suspeito. A pesquisa pode ser realizada usando o remetente do e-mail, o ID da mensagem de e-mail ou o assunto do e-mail associado a um incidente de segurança como critérios.

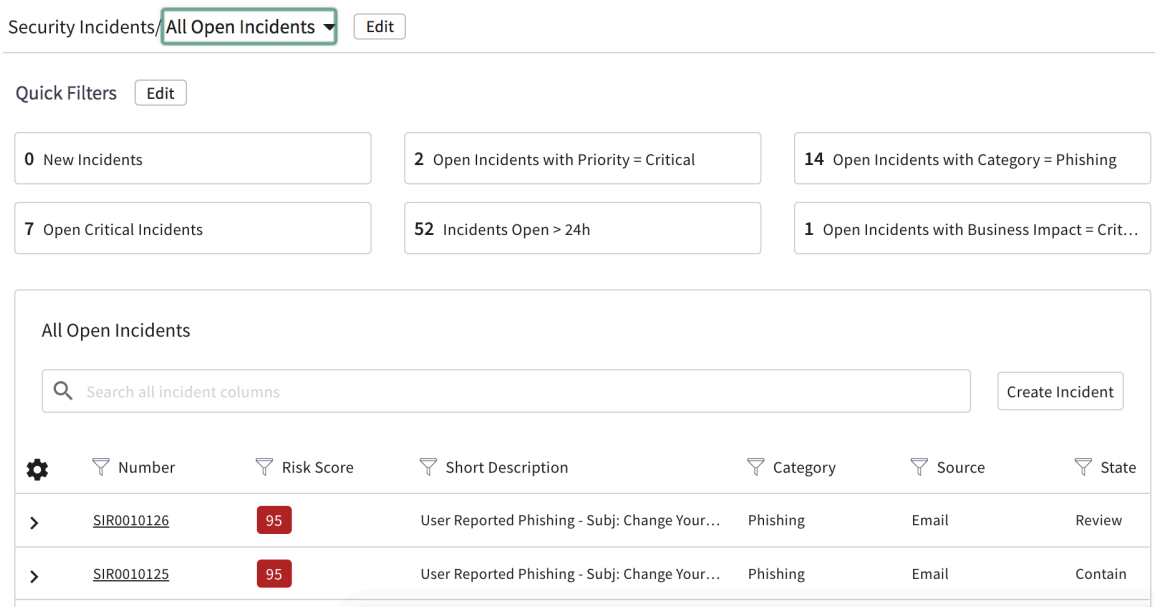
Nota:

- Esta implementação da pesquisa de vistas para observáveis baseados em e-mail foi testada somente com o armazenamento de logs do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com CIM (Common Information Model, Modelo de informações comuns) para que a consulta de pesquisa de vistas retorne resultados precisos.

Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Em **Incidentes de segurança** , selecione um dos filtros, como todos **incidentes em aberto** , **todos os incidentes atribuídos a você** ou **todos os incidentes** .

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos** .

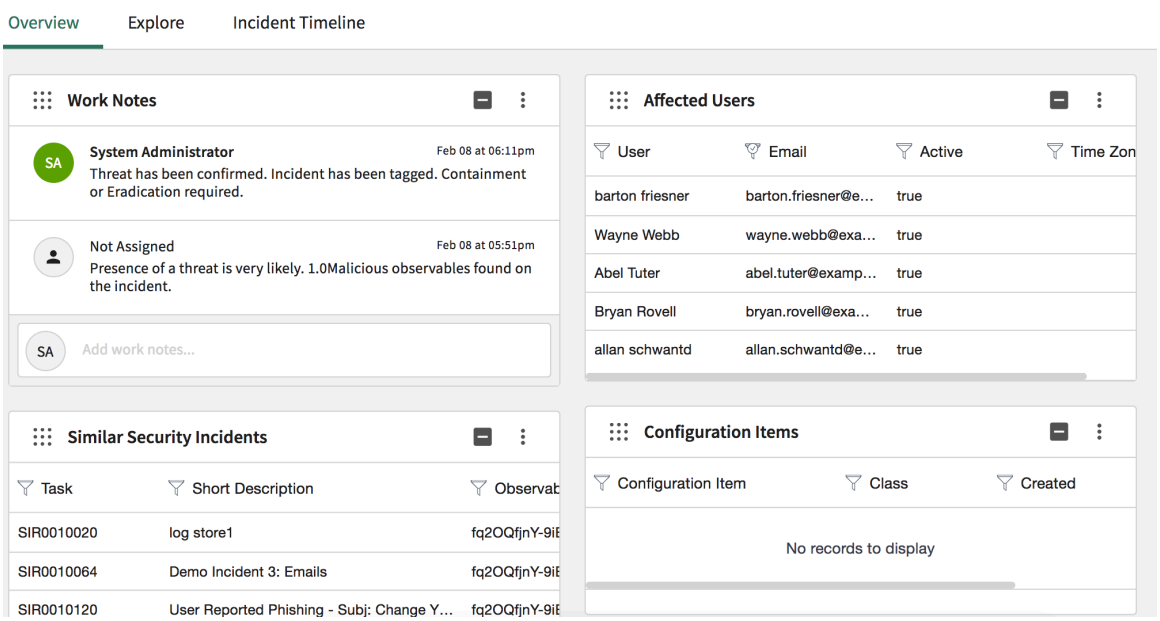


3. Clique no incidente de segurança que você deseja analisar.

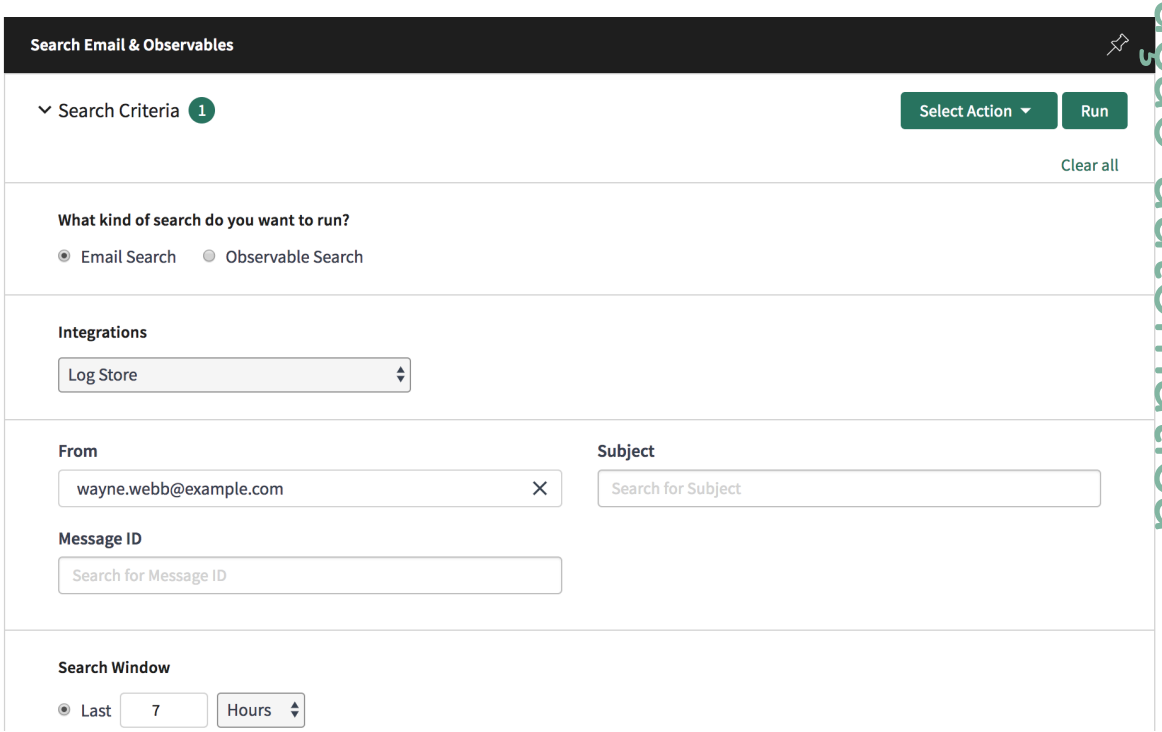
   A guia Visão geral fornece uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Explorar** guia.
5. Em **Dados do incidente** , navegue até **Investigação** > **Pesquisar e-mail e observáveis**.



6. Expanda a seção Critérios de pesquisa.
7. Selecione **Pesquisa de e-mail** como o tipo de pesquisa que você deseja executar e especifique o restante dos critérios de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Critérios de pesquisa

Campo	Descrição
Integrações	Tipo de integrações. Selecione **Armazenamento de logs** da lista. **Nota:** Este recurso é compatível somente com o armazenamento de logs do Splunk.
De	Endereço de e-mail completo do remetente (por exemplo, jane.doe@example.com).
ID da Mensagem	ID da mensagem de e-mail do armazenamento de logs.
Assunto	Assunto do e-mail de phishing.
Janela de pesquisa	Janela de tempo para a pesquisa (por exemplo, as últimas 24 horas).

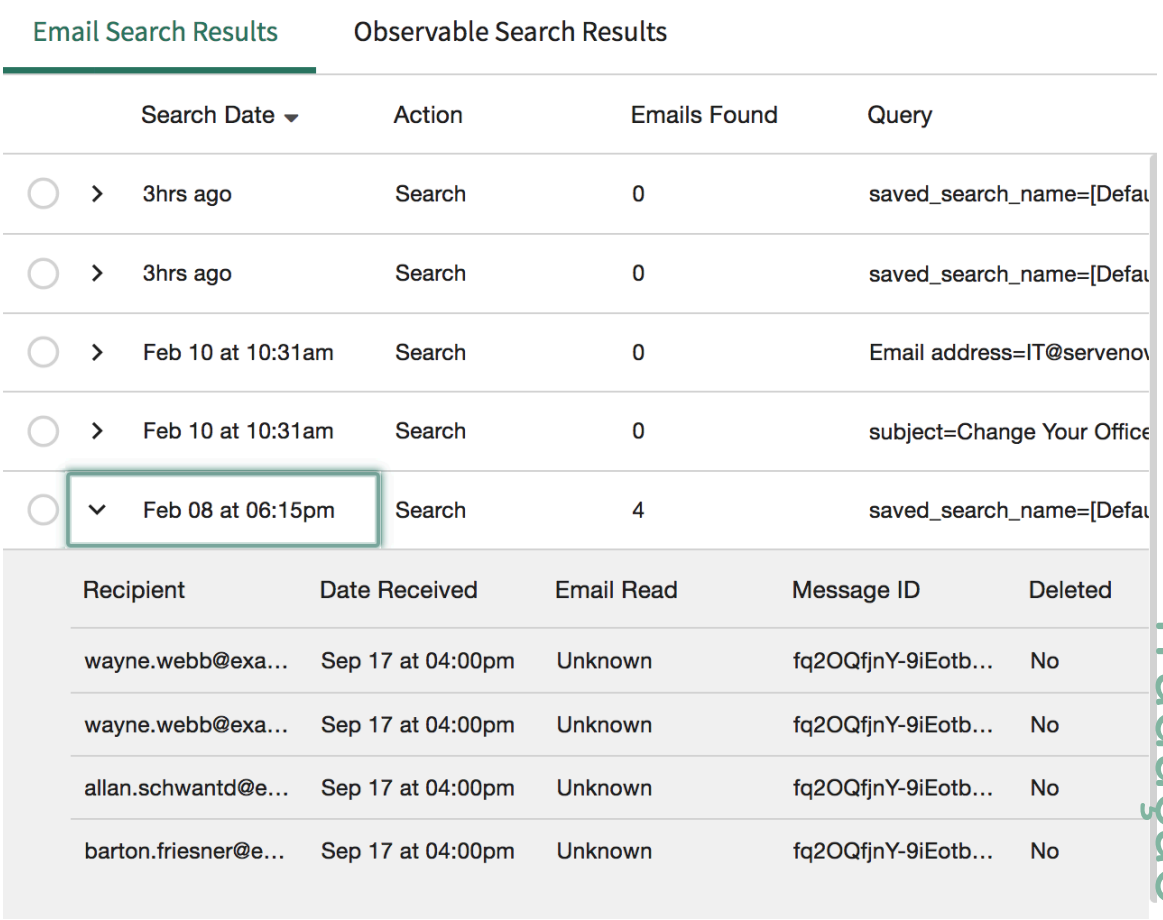
8. Em **Selecione Ação** , selecione **Pesquisa** e clique em **Executar** .

   O armazenamento de logs do Splunk é pesquisado usando os critérios inseridos, e os usuários visados pelo ataque de phishing são mostrados no **Resultados da pesquisa de e-mail** guia. O número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o destinatário e o ID da mensagem, são exibidos.

9. Para exibir a lista de usuários que receberam o e-mail de phishing, clique em **>** Símbolo na coluna Data de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Para exibir uma lista de usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

A coluna Usuário com phishing identifica os destinatários do e-mail.

Nota: A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

11. Para investigar melhor os usuários que são alvos do ataque de phishing, siga estas etapas:

a. Marque as caixas de seleção ao lado dos nomes de usuário.

b. Na lista, selecione **Criar incidente de segurança secundário** e clique em **Executar** .
Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique em **Explorar** e navegue até **incidentes** > **Incidentes de segurança secundários**.

Resultado
A lista de usuários com phishing é exibida.

Execute uma pesquisa de avistamentos observáveis para ataques de phishing e malware relatados pelo usuário

Execute pesquisas de vistas em observáveis para descobrir quantos usuários visitaram um site malicioso ou suspeito em um período específico.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode executar uma pesquisa de tráfego de rede em observáveis, como o URL, o host de destino ou o endereço IP de destino associado a um incidente de segurança.

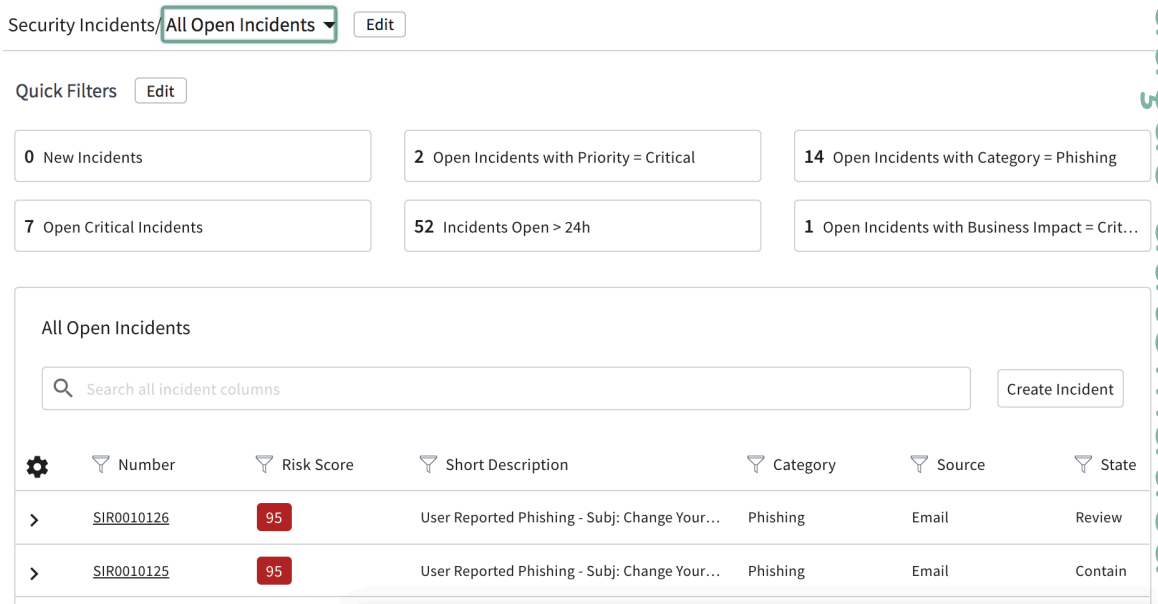
Nota:

- Esta implementação da pesquisa de vistas para observáveis foi testada somente com o armazenamento de logs do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com CIM (Common Information Model, Modelo de informações comuns) para que a consulta de pesquisa de vistas retorne resultados precisos.

Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Em **Incidentes de segurança** , selecione um filtro diferente, como todos **Incidentes atribuídos a mim** , **Todos os incidentes em aberto** ou **Todos os incidentes** .

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos** .

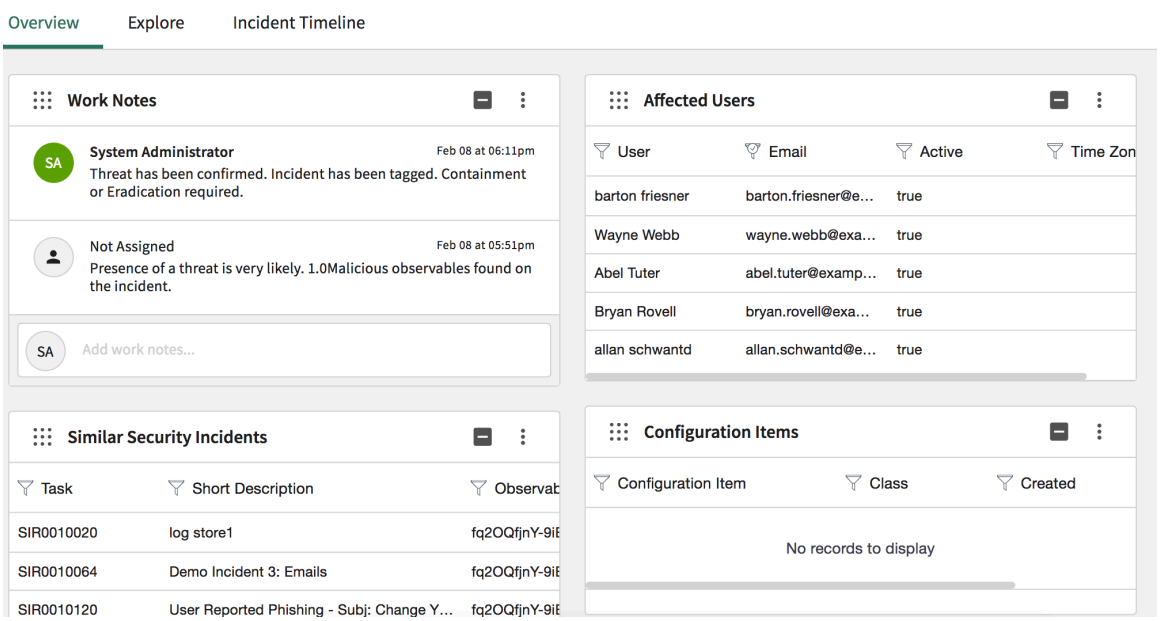


3. Clique no incidente de segurança que você deseja analisar.

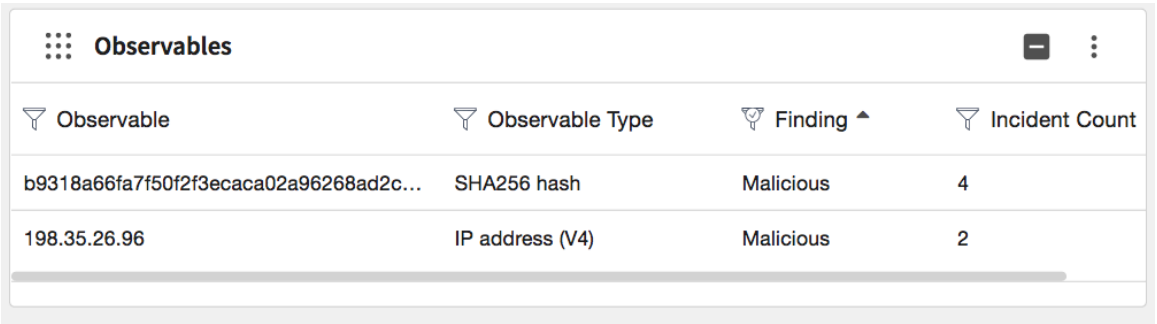
   Você pode ver uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



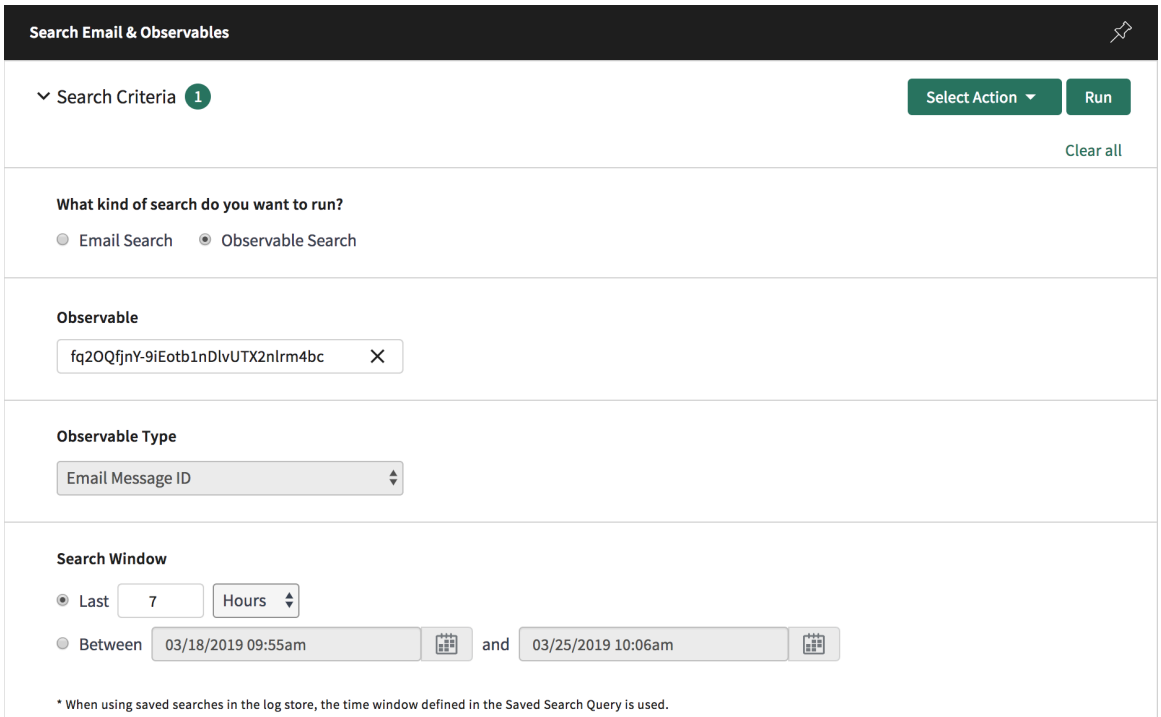
Na seção Observáveis, observe que a coluna Observável mostra o endereço de e-mail, o assunto e o URL. Observe também que a coluna Descoberta mostra que o URL foi verificado automaticamente quando o e-mail de phishing foi enviado e determinado como um URL mal-intencionado conhecido. A coluna Contagem de incidentes mostra os outros incidentes que compartilham o mesmo observável. Esses artefatos indicam que você provavelmente está pronto para prosseguir para os procedimentos de contenção desse ataque de phishing, incluindo a determinação de quantos usuários na organização foram afetados.



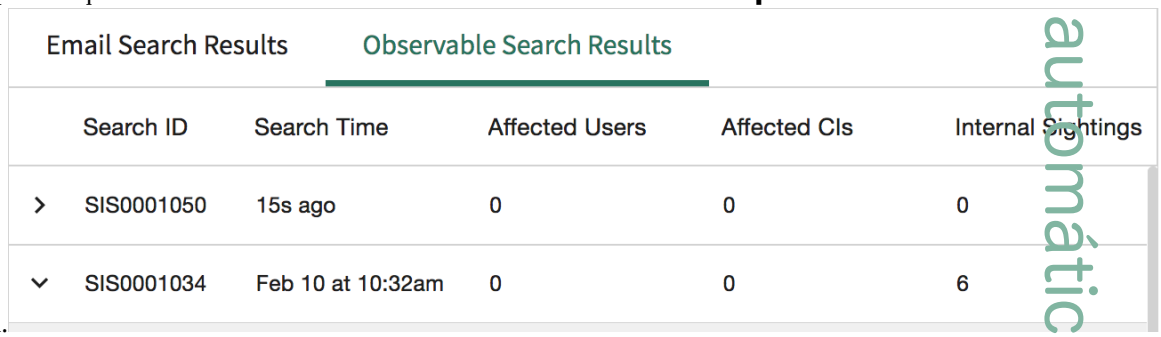
4. Navegar até **Explorar** > **Investigação** > **Pesquisar e-mail e observáveis**.
5. Expanda a seção Critérios de pesquisa e clique em **Pesquisa de observável** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Insira o observável que você está procurando e uma janela de tempo para a pesquisa (por exemplo, últimas 24 horas).
7. Em **Selecione Ação** , selecione **Pesquisa** .
   O armazenamento de logs do Splunk é pesquisado usando os critérios inseridos e os principais usuários visados pelo ataque mal-intencionado são mostrados no **Resultados da Pesquisa** **observável**guia.



8. Para exibir os usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

   A coluna Usuário com phishing identifica os destinatários do e-mail de phishing e a coluna Interação do usuário identifica os usuários que clicaram em um URL de phishing ou interagiram com um endereço de e-mail suspeito. A coluna Interação do usuário é definida como verdadeira ou falsa, dependendo se o usuário clicou no link mal-intencionado ou no IP.

   Nota: A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

9. Para investigar melhor os usuários que clicaram no e-mail de phishing e potencialmente comprometer suas credenciais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Nas colunas Usuário com phishing e Interação do usuário, marque as caixas de seleção ao lado dos nomes de usuário exibidos **verdadeiro** .

b. Clique em **Criar incidente de segurança secundário** e clique em **Executar** .
Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique em **Explorar** e navegue até **incidentes** > **Incidentes de segurança secundários**.

Resultado
A lista de usuários com phishing é exibida.

Criar registros de configuração de pesquisa de vistas

Crie vários registros de configuração de pesquisa de vistas e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar
Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a Integração Splunk.

Por Que e Quando Desempenhar Esta Tarefa
Você também pode criar registros de configuração de pesquisa de vistas para invocar pesquisas salvas No armazenamento de logs do Splunk Enterprise.

Nota: As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com CIM (Common Information Model, Modelo de informações comuns) do Splunk.

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinam vários registros de evento.
- Pesquisas eficientes e eficazes.
- Use entradas com parâmetros na pesquisa salva do Splunk.

O sistema de base inclui as configurações de amostra mostradas nesta imagem:

Configurações de pesquisa salvas

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração no local são consultas de exemplo e podem ser substituídas por parâmetros apropriados para seu ambiente. Crie configurações de pesquisa salvas adicionais conforme necessário. Quando você define uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à configuração salva definida em sua instância do Splunk. Se o nome e os parâmetros não

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de vistas.

Nota: Em sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique em **Permissões** Link para navegar até a página Permissões. Selecione **Todos os aplicativos** botão de opção e habilite **Permissão de leitura** opção para **Todos** . Isso mudará o valor da coluna Compartilhamento de Privado para App para sua consulta de pesquisa salva. Se isso não estiver definido, a consulta de pesquisa salva poderá não retornar resultados.

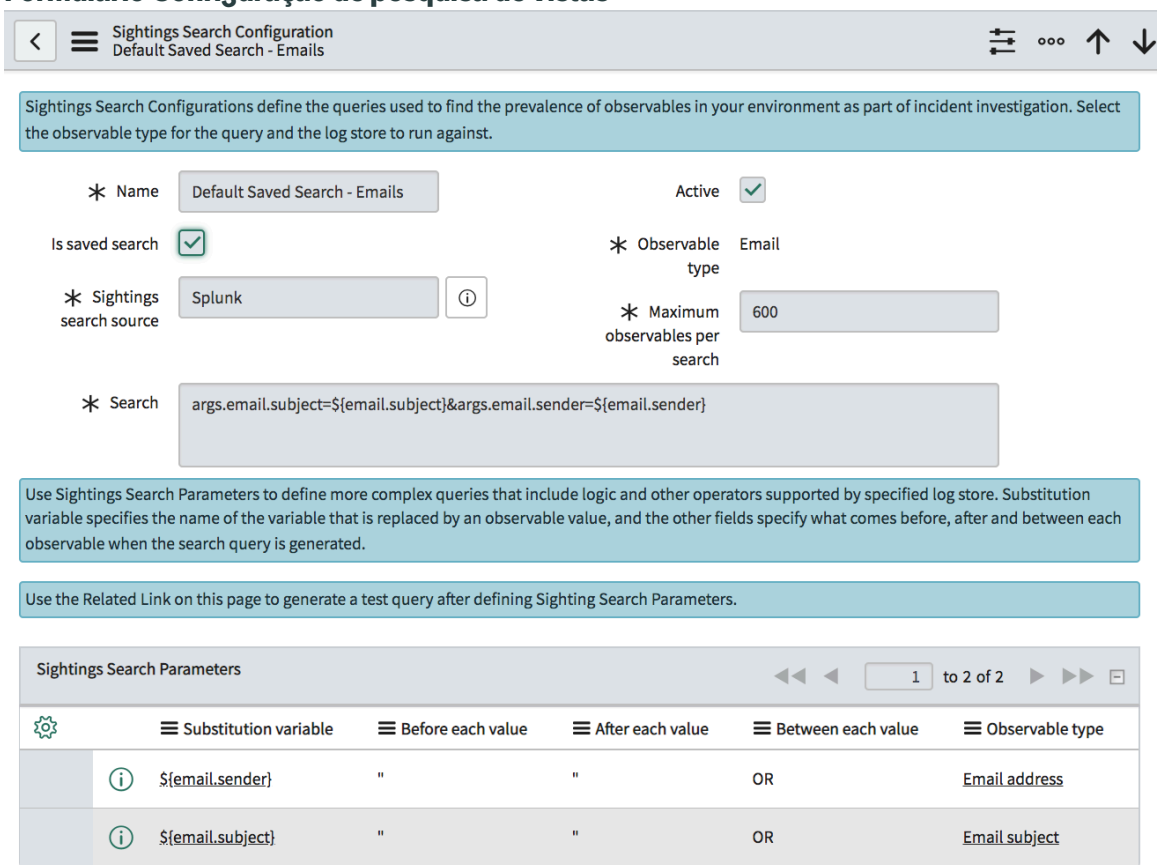
Para verificar se a configuração de pesquisa salva corresponde à configuração definida em sua instância do Splunk:

1. Navegar até **Configurações** > **Pesquisas, Relatórios e Alertas**.
2. Mudança **Contexto da aplicação** . **Todos** .

   Uma lista de relatórios de pesquisa é exibida.
3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de vistas contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Formulário Configuração de pesquisa de vistas



Em sua instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - E-mails e os mesmos parâmetros de pesquisa para o endereço de e-mail e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem os mesmos, a pesquisa de vistas não gerará um resultado preciso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Operações de segurança** > **Integrações** > **Configuração da Pesquisa de detecções** e criar um novo registro (consulte a tabela para obter descrições dos campos).

Formulário Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome da configuração.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de vistas. Selecione o armazenamento de logs do Splunk como a origem.
Ativo	Opção para o status da pesquisa salva. Somente configurações de pesquisa ativas podem ser usadas para executar uma pesquisa de vistas.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `(observável)` , Mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com o armazenamento de logs do Splunk.

2. Clique em **Enviar**.

Resultado
Você criou um registro de configuração de pesquisa de vistas.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de vistas** e especificam uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Recursos do Playbook

A Resposta a incidentes de segurança fornece um conjunto avançado de recursos de playbook que inclui uma biblioteca abrangente de playbooks, subfluxos e ações. Você pode criar ou configurar playbooks de forma rápida e fácil sem escrever código complicado. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo.

Os recursos do Playbook incluem o seguinte:

Resposta a incidentes de segurança playbooks	Ações do playbook de resposta a incidentes de segurança
Os playbooks fornecidos com o sistema de base são projetados para acelerar o processo de investigação de incidentes de segurança automatizando tarefas complexas e mundanas.	Ações complexas que são críticas para criar playbooks estão disponíveis como **Bibliotecas de ação** . Essas Bibliotecas de ação permitem que os administradores de segurança criem playbooks sem escrever nenhum código complicado. Consulte Ações do playbook de resposta a incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança playbooks	Ações do playbook de resposta a incidentes de segurança
Os playbooks são altamente configuráveis e criados usando a tecnologia Flow Designer da ServiceNow. Para configurar, copie o playbook fornecido com o sistema de base e modifique-o usando a interface gráfica simples de arrastar e soltar. Consulte Resposta a incidentes de segurança playbooks.	

Ativar um Resposta a incidentes de segurança fluxo

Os administradores de segurança e designers de fluxo podem usar Resposta a incidentes de segurança fluxos para automatizar o processo de resolução de incidentes de segurança na organização.

Antes de Iniciar

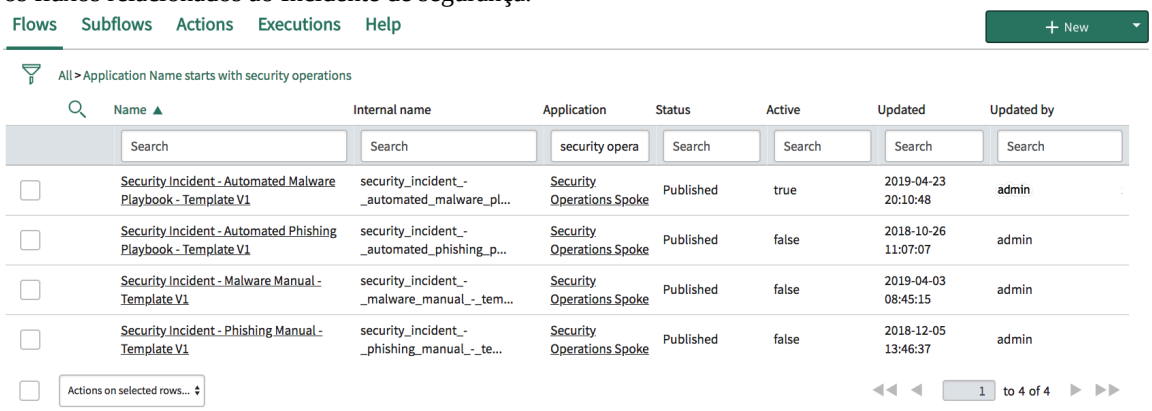
Função necessária: sn_si.admin, action_designer e flow_designer

Por Que e Quando Desempenhar Esta Tarefa

Os fluxos fornecidos com o sistema de base estão em um estado inativo. Ative esses fluxos antes de usá-los.

Procedimento

1. Baixe e instale . Operações de segurança Aplicação Spoke.
   Esta aplicação Spoke fornece ações de operações de segurança que você pode usar durante a definição Resposta a incidentes de segurança fluxos.
2. Navegar até **Flow Designer** > **Designer** e pesquise Operações de segurança Aplicação Spoke para exibir os fluxos relacionados ao Incidente de segurança.

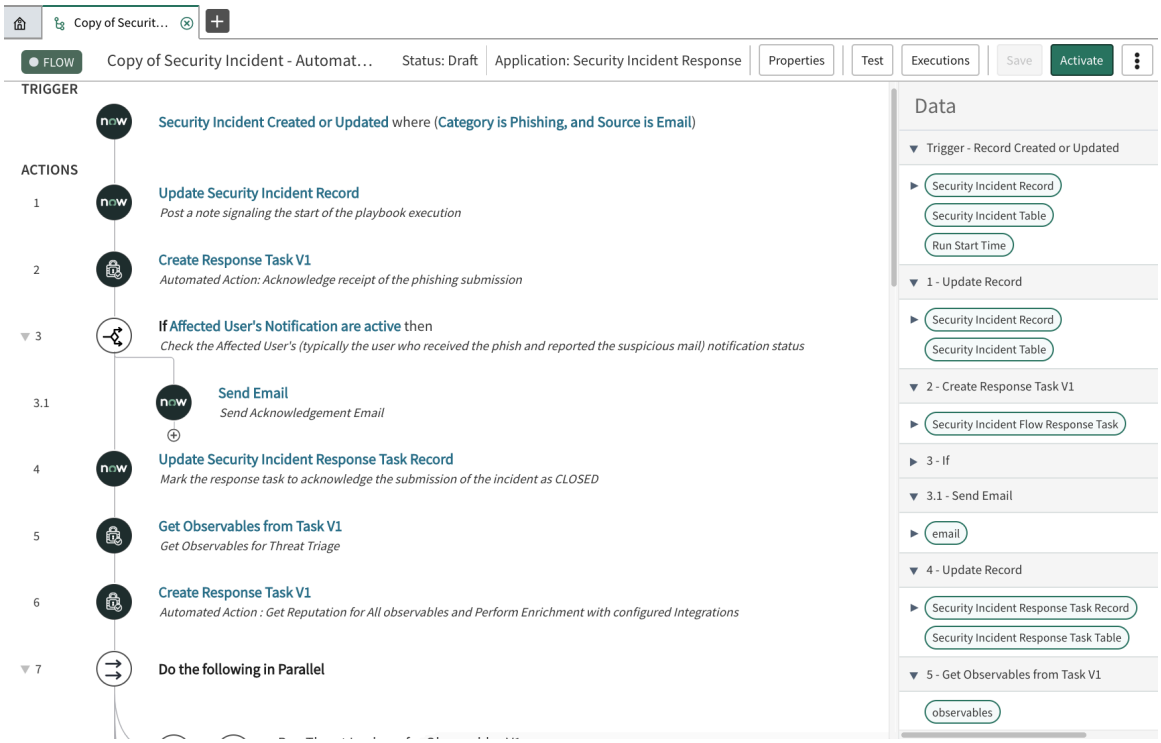


Observe que os fluxos têm um status Publicado e estão inativos.

3. Por exemplo, se você quiser ativar o fluxo do Playbook de malware automatizado, clique em **Incidente de segurança - Playbook de phishing automatizado - Modelo V1** link para exibir o fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Não é possível editar os fluxos fornecidos com o sistema de base, pois eles são fluxos somente leitura. Você pode usar esses fluxos como estão ou fazer uma cópia e modificá-los conforme necessário.

4. Clique em **Ativar** para ativar o fluxo.

Resultado

O fluxo do Playbook de Phishing automatizado está ativo e pronto para uso.

Resposta a incidentes de segurança playbooks

Você pode invocar o fluxo do playbook de incidentes de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados pelo Flow Designer existentes, ele continuará funcionando e as atividades continuarão sendo renderizadas como tarefas de resposta.

Resposta a incidentes de segurança O oferece suporte a dois tipos de playbooks:

- Playbooks baseados em processos
- Playbooks baseados em fluxo

Além dos playbooks listados, também há subfluxos no spoke de Operações de segurança que podem ser chamados no playbook de fluxos. Ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Ative um fluxo de Resposta a incidentes de segurança .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbooks baseados em processos

O componente do playbook funciona somente para playbooks integrados Workflow Studio e não para fluxos. No entanto, os playbooks baseados em fluxo existentes continuarão funcionando e as atividades continuarão sendo renderizadas como tarefas de resposta.

Resposta a incidentes de segurança fornece os seguintes playbooks com o sistema de base.

Playbook para phishing manual

O Playbook de Phishing Manual fornece orientação passo a passo para seus analistas sobre como eles podem resolver manualmente tipos específicos de ameaças à segurança em suas atividades de phishing.

Visão geral

O modelo Playbook de Phishing Manual foi projetado para executar as tarefas de resposta de phishing manualmente e inclui uma sequência de ações que inclui condições de gatilho. Você pode usar os modelos DE PAD para executar as etapas no playbook de resposta a phishing e resolver esses incidentes com eficiência.

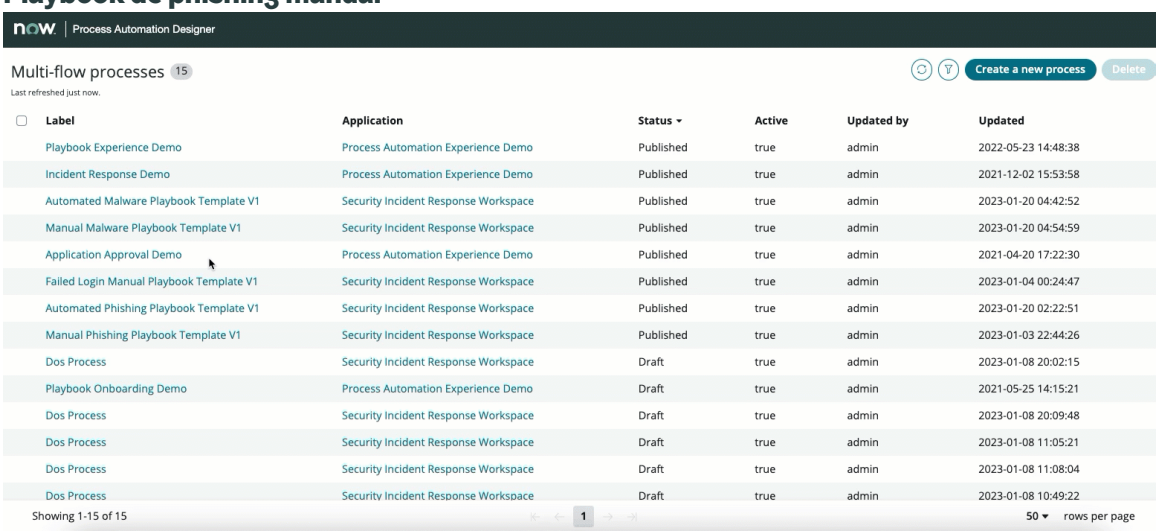
Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Playbook de Phishing manual no Designer de automação de processos (PAD) e executar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Playbook de phishing manual



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

continua concluindo tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar playbooks para Phishing manual Workflow Studio

Use estas etapas para criar playbooks para phishing manual no Workflow Studio.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

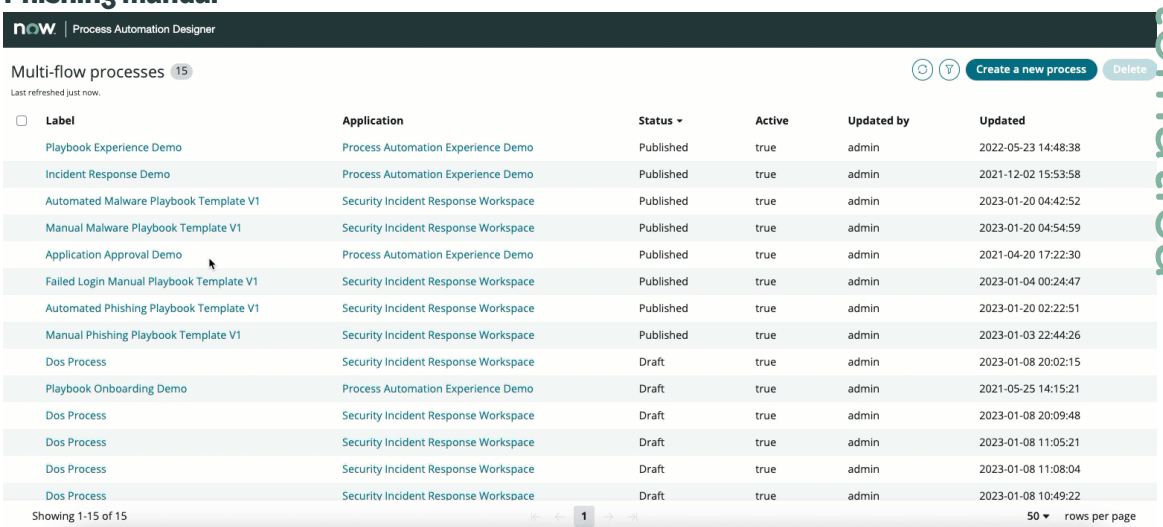
Procedimento

1. Clique **Tudo** > **Designer de automação de processos** > > **Novo(a)** e selecione **Playbook** .

   Por exemplo, Modelo de Playbook de Phishing Manual V1.

2. Insira um nome para o playbook, a descrição e a aplicação para a qual o playbook está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando seu playbook deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando seu playbook deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Phishing manual



7. Clique em **Vá para o Designer** .
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova fase** .
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
   . **Condição de execução** e. **Indicar quando começar** os campos indicam quando a fase seria executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Clique em **Salve e feche** .

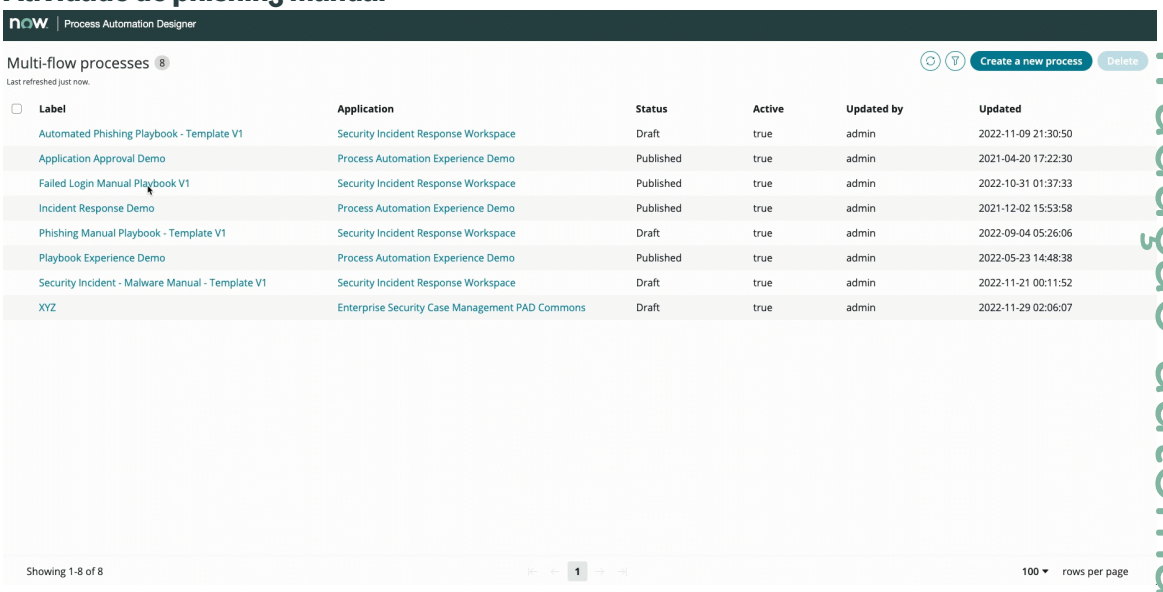
11. Para adicionar outra fase, clique em **Adicione outra fase** .
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** a fase começa imediatamente e não tem condição de execução. **Conter** a fase começa após a conclusão da fase anterior e tem uma condição de execução baseada no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.

12. Clique em **Adicione outra atividade** Em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.

    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.

13. Clique em **Crie uma nova atividade** .
    Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Atividade de phishing manual



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade.

15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.

16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Adicionar atividades paralelas

. **Quando começar** o campo está definido como **Com anterior** , em seguida, as atividades paralelas podem ser iniciadas.

Para passar de uma fase para a próxima fase

Se nenhuma condição de execução for definida, as fases e atividades serão executadas sequencialmente.

Você pode usar a condição de execução para ignorar atividades ou fases. Neste exemplo, **A fase Conter começa quando o resultado de "O e-mail tem indicadores de ameaça?" Sim** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para passar de uma fase para outra fase, você pode usar a plataforma fornecida **Definição de atividade - Atualizar registro** . Isso atualizará o campo de estado do incidente de segurança e retomará a execução do playbook para a próxima fase.

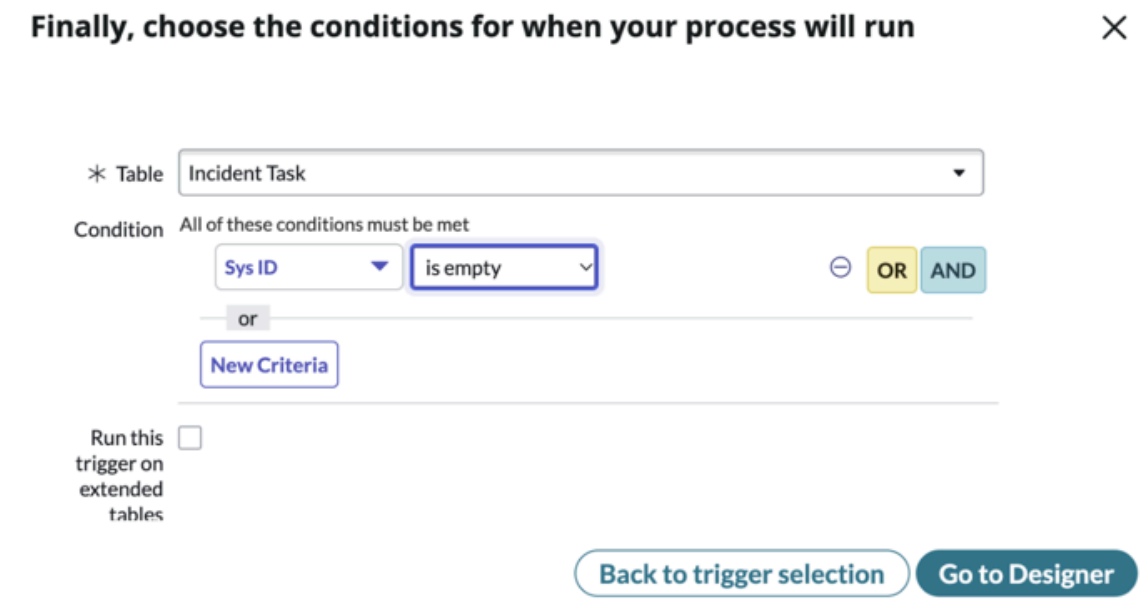
No entanto, o desafio com esta definição de atividade é que, se dissermos que o playbook está na fase Análise e se o usuário tiver atualizado manualmente o estado para dizer revisão, a atividade Atualizar registro mudará novamente o estado para Conter para continuar a execução do playbook. Isso substituirá a mudança manual feita.

Para superar isso, no sistema de base, uma definição de atividade chamada **Atualizar estado da tarefa** fornecido. Esta atividade não substituirá o estado do incidente de segurança se o estado atual do estado da segurança estiver à frente da fase no playbook.

Crie uma definição de processo com condição de gatilho fictícia

Uma definição de processo sempre requer uma condição de gatilho. Mas, se você não tiver certeza de quando o processo deve ser acionado, ainda poderá criar uma definição de processo com uma condição de gatilho fictícia. Defina a condição do gatilho como **sys_id está vazio** . Esta condição nunca será atendida.

Condições do processo



Tradução automática

Usando o playbook de Phishing manual

Use estas etapas para saber como você pode usar o playbook de Phishing manual no Espaço do analista DO SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

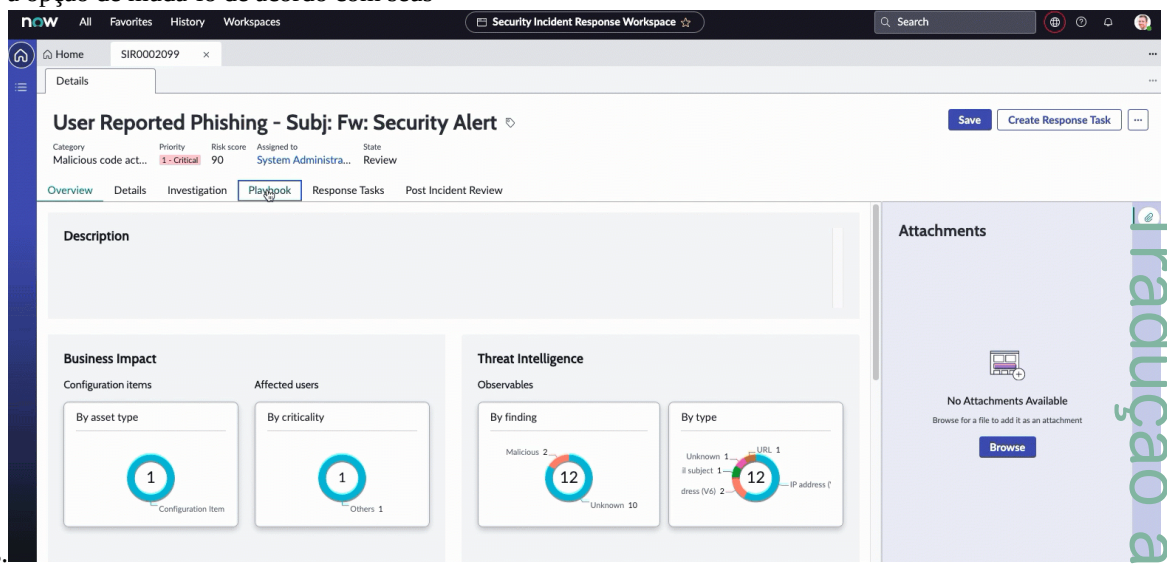
1. No espaço SIR, abra um incidente de segurança.
2. Clique em **Playbook** guia.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

Nota: Se você não vir nenhum playbook listado, será necessário acessar o PAD e habilitar que eles o vejam no **Playbook** guia.

3. Clique em **Playbook de Phishing Manual** .
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.
   Você tem a opção de mudá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de mudá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Resumo do Playbook do espaço

A seguir descreve o resumo do processo.

- Entenda o playbook legado baseado em fluxo.
- Liste as possíveis atividades, fases após a análise do fluxo. Procure as etapas em que a Orquestração verdadeira pode ser criada.
- Pegue cada atividade e verifique se a definição de atividade fornecida pelo sistema de base pode atender ao caso de uso ou não.
- Liste os casos de uso de atividade que precisam que novas definições de atividade sejam implementadas. Classificá-los - Interativo, não interativo ou automatizado. Para criar uma definição de atividade:
  - Crie um subfluxo ou uma ação para o caso de uso.
  - Decida se os dados associados devem ser capturados na tabela de dados de fluxo ou em uma tabela personalizada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se estiver usando a tabela de dados de fluxo, crie a definição de dados de fluxo em **sys_flow_data_definition** . Ao criar um registro de dados de fluxo no subfluxo, selecione a definição de dados de fluxo criada.
- Crie um **definição de atividade** .
- Mapeie o plano de automação.
- Preencha **Experiência de atividade** propriedades.
- Crie uma ação em Ações do Playbook. Deve haver uma ação de atividade existente para atribuí-la à definição de atividade.
- Para substituir a experiência de cartão padrão com base no tipo de experiência selecionado, adicione a substituição do playbook usando o conceito de IU de atividade.

- Algumas atividades podem ser feitas para lidar com automáticas e interativas usando o sinalizador Aguardar entrada do usuário no subfluxo. Esta entrada pode ser passada durante a configuração da atividade na definição do processo.
- Depois de ter todas as definições de atividade necessárias para o seu processo, comece a criar a definição do processo usando Workflow Studio.

Playbook para phishing automatizado

O playbook de phishing automatizado fornece orientação passo a passo para seus analistas sobre como eles podem resolver tipos específicos de ameaças à segurança em suas atividades de phishing automatizado.

Visão geral

O modelo de playbook de phishing automatizado foi projetado para automatizar as tarefas de resposta de phishing e contém uma sequência de ações que inclui condições de gatilho. Você pode usar os modelos de playbook em Workflow Studio automatizar as etapas no playbook de resposta a phishing e resolver esses incidentes com eficiência. Este modelo de playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar.

Neste playbook, não haverá interação do usuário quando a categoria de um incidente de segurança estiver definida como phishing. Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Playbook de Phishing automatizado em Workflow Studio e este playbook executa automaticamente todas as tarefas, como análise, conter, erradicar e revisar.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

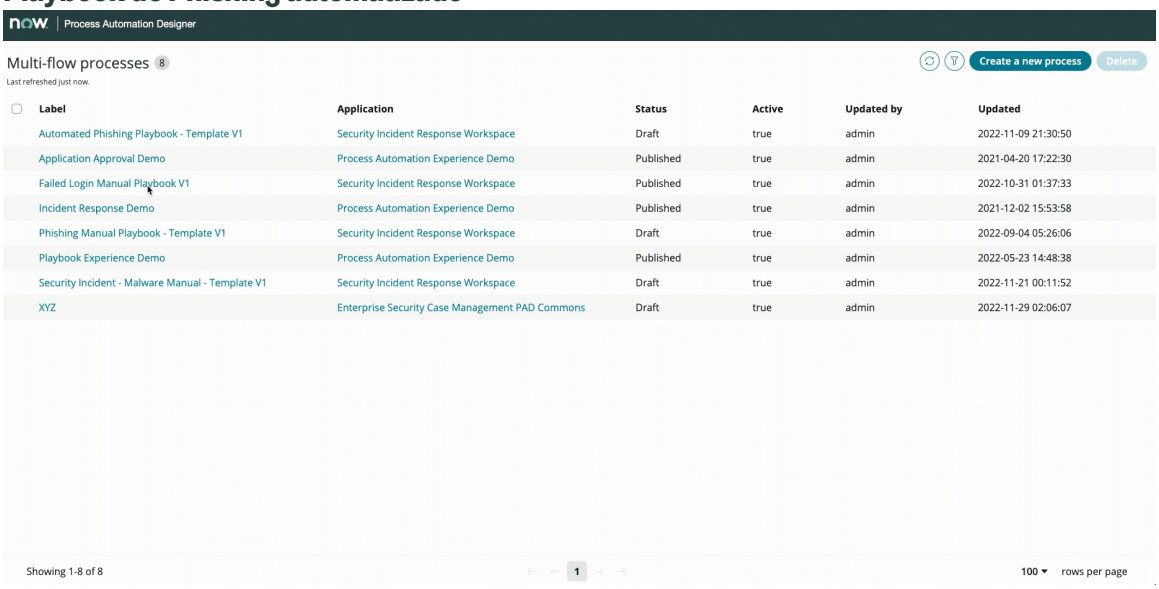
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de Phishing automatizado



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você continua concluindo tarefas e fases. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Crie processos para phishing automatizado no PAD

Use estas etapas para criar processos para phishing automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clique **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

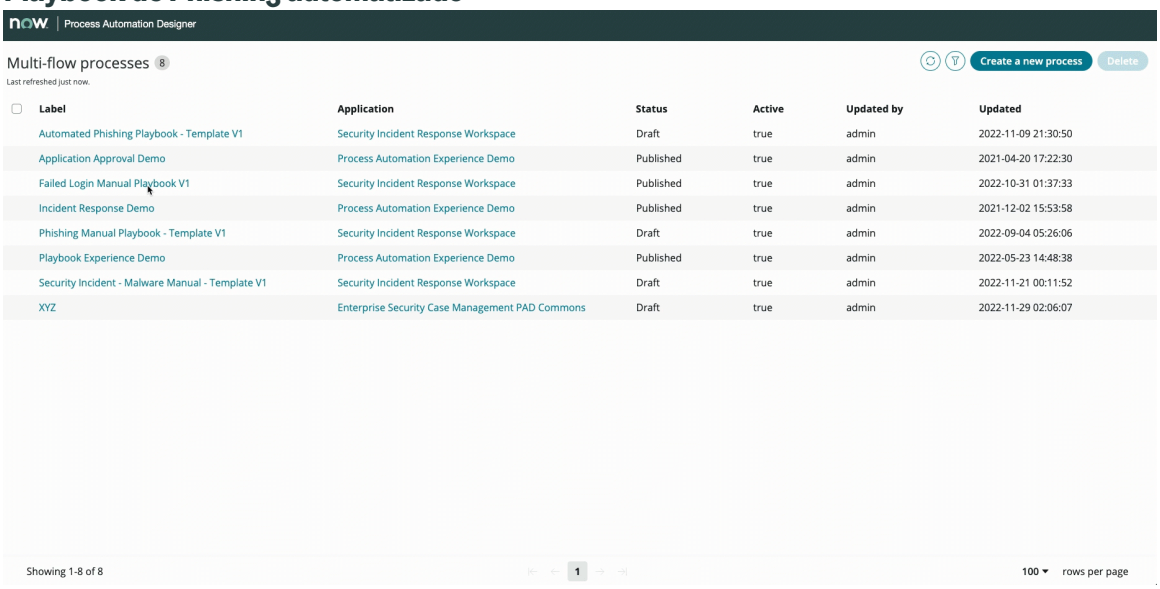
   Por exemplo, Modelo de Playbook de Phishing Automatizado V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de Phishing automatizado

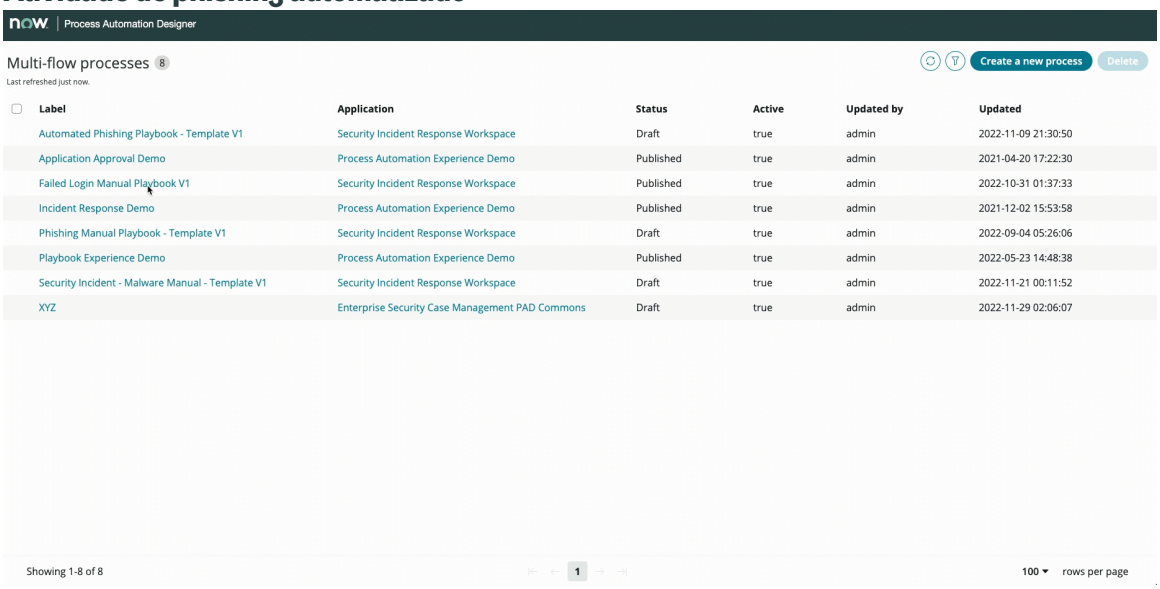


7. Clique em **Vá para o Designer** .
   A página Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova fase** .
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
   . **Condição de execução** e. **Indicar quando começar** os campos indicam quando a fase seria executada.
10. Clique em **Salve e feche** .
11. Para adicionar outra fase, clique em **Adicione outra fase** .
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** a fase começa imediatamente e não tem condição de execução. **Conter** a fase começa após a conclusão da fase anterior e tem uma condição de execução baseada no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique em **Adicione outra atividade de processo** Em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique em **Crie uma nova atividade** .
    Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de phishing automatizado



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Usando o playbook de phishing automatizado

Use estas etapas para saber como você pode usar o playbook de Phishing automatizado no Espaço do analista DO SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique em **Playbook** guia.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

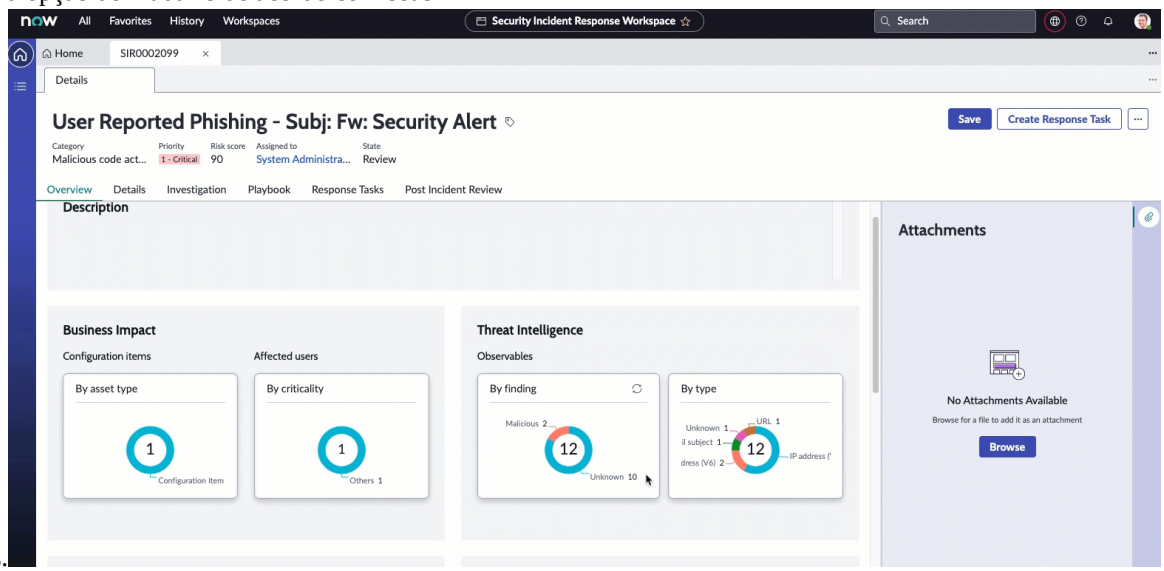
   Nota: Se você não vir nenhum playbook listado, será necessário acessar o PAD e habilitar que eles o vejam no **Playbook** guia.

3. Clique em **Playbook de Phishing automatizado** .
   Para phishing automatizado, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de mudá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de mudá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para malware manual

O playbook de Malware manual fornece orientação passo a passo sobre como os analistas podem resolver alertas de malware manualmente com mais eficiência.

O modelo Playbook de Malware Manual foi projetado para executar manualmente as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de playbook em Workflow Studio Para executar as etapas no playbook de Malware manual e resolver esses alertas com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se o malware for criado ou atualizado. Você precisa ativar o Playbook de Malware Manual em Workflow Studio e criar todas as tarefas, como análise, conter, erradicar e revisar.

A seguir estão as fases da definição do processo e correspondem ao estado de alerta de malware:

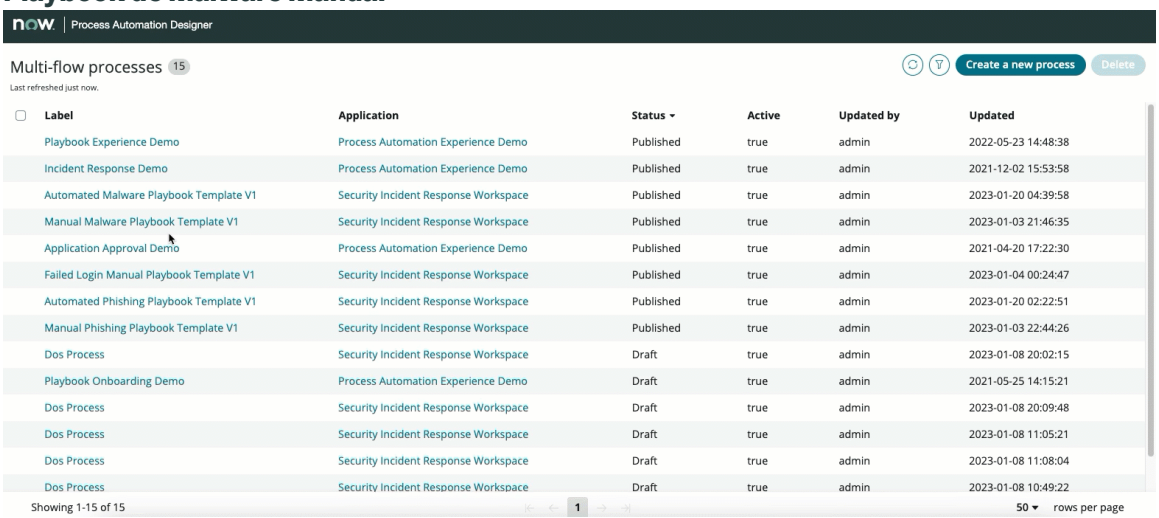
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de Malware Manual



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você continua concluindo tarefas e fases. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Crie processos para Malware manual no PAD

Use estas etapas para criar processos para malware manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clique **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

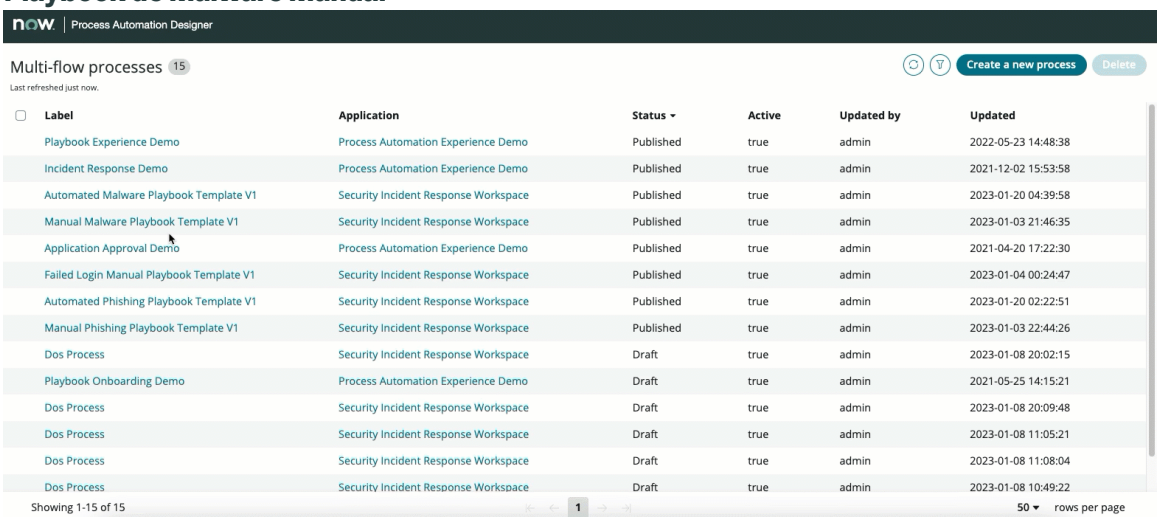
   Por exemplo, Modelo de Playbook de Malware Manual V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de Malware Manual

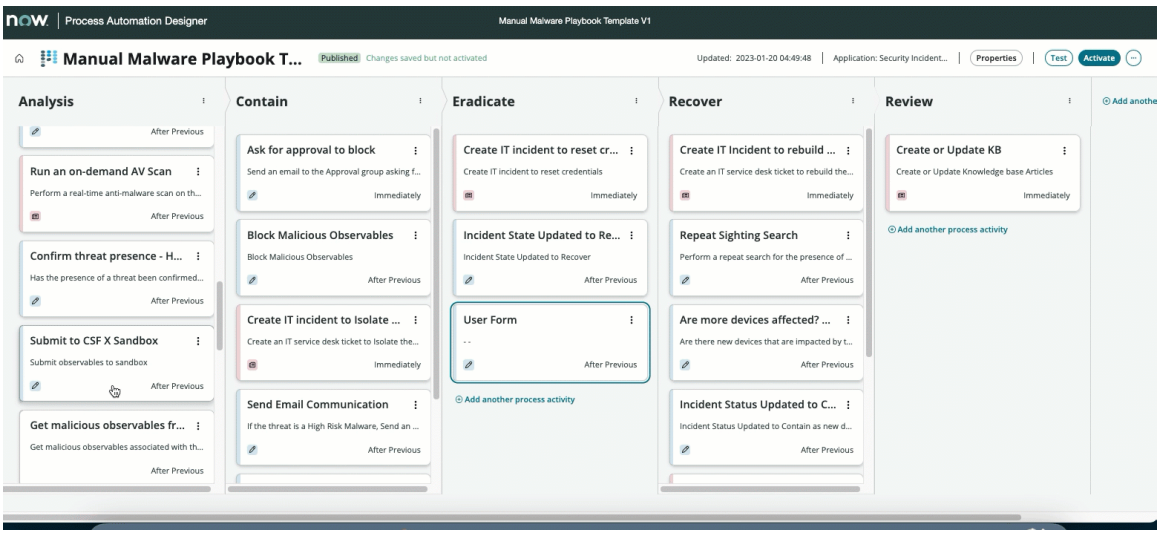


7. Clique em **Vá para o Designer** .
   A página Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova fase** .
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
   . **Condição de execução** e. **Indicar quando começar** os campos indicam quando a fase seria executada.
10. Clique em **Salve e feche** .
11. Para adicionar outra fase, clique em **Adicione outra fase** .
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** a fase começa imediatamente e não tem condição de execução. **Conter** a fase começa após a conclusão da fase anterior e tem uma condição de execução baseada no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique em **Adicione outra atividade de processo** Em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique em **Crie uma nova atividade** .
    Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade manual de malware



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Uso do playbook de Malware manual

Use estas etapas para saber como você pode usar o playbook de Malware manual no Espaço de analistas DO SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique em **Playbook** guia.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

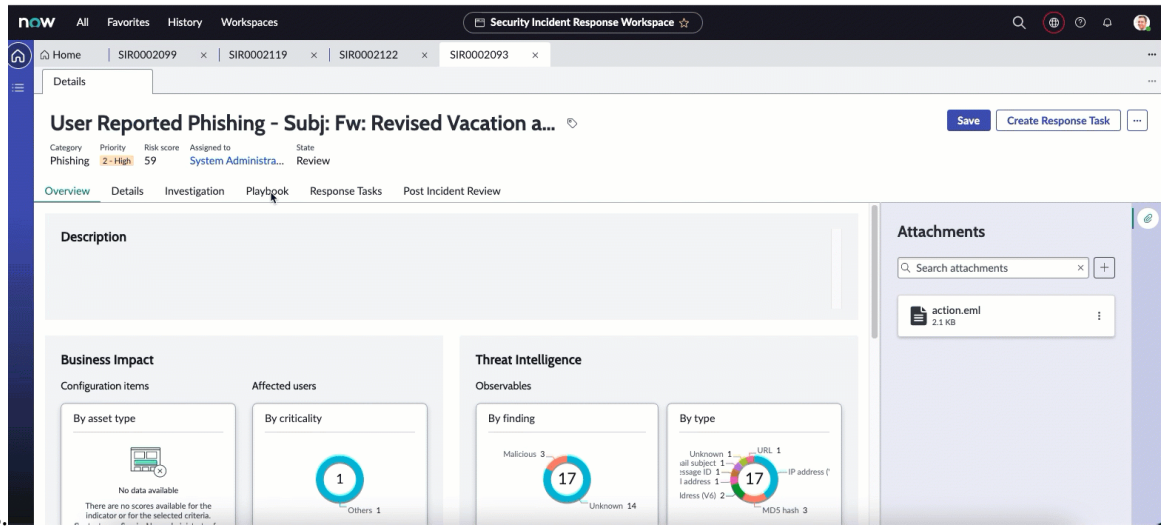
   Nota: Se você não vir nenhum playbook listado, será necessário acessar o PAD e habilitar que eles o vejam no **Playbook** guia.

3. Clique em **Playbook de Malware Manual** .
   Para malware manual, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de mudá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de mudá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para malware automatizado

O Playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajuda os analistas a resolver alertas de malware com mais eficiência.

O modelo Playbook de Malware automatizado foi projetado para automatizar as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de playbook em Workflow Studio Automatizar as etapas no playbook de Malware automatizado e resolver esses alertas com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o playbook de Malware automatizado em Workflow Studio e este playbook executa automaticamente todas as tarefas, como análise, conter, erradicar e revisar.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

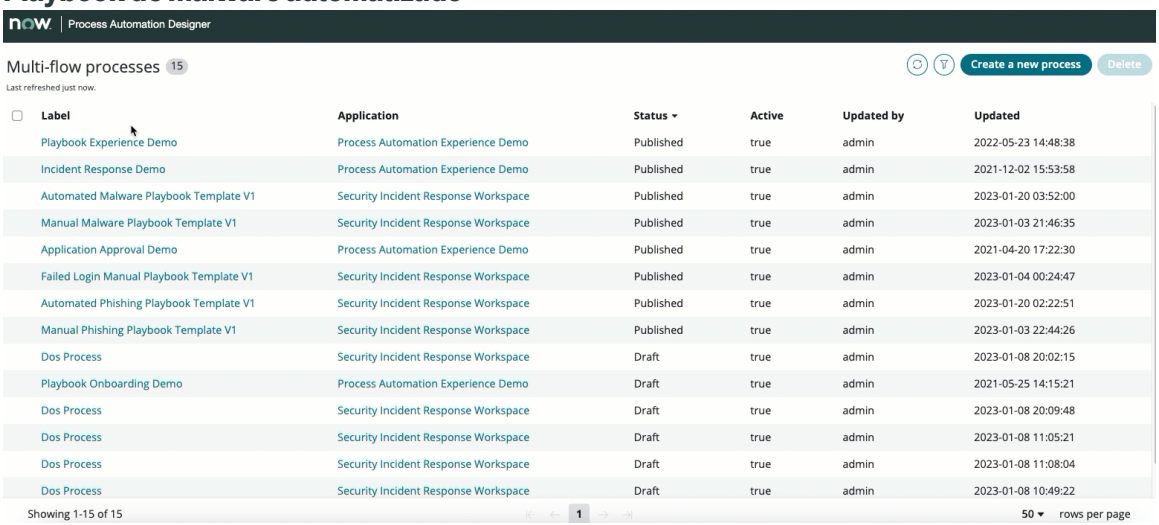
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você continua concluindo tarefas e fases. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Processos de criação de Malware automatizado no PAD

Use estas etapas para criar processos para malware automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clique **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

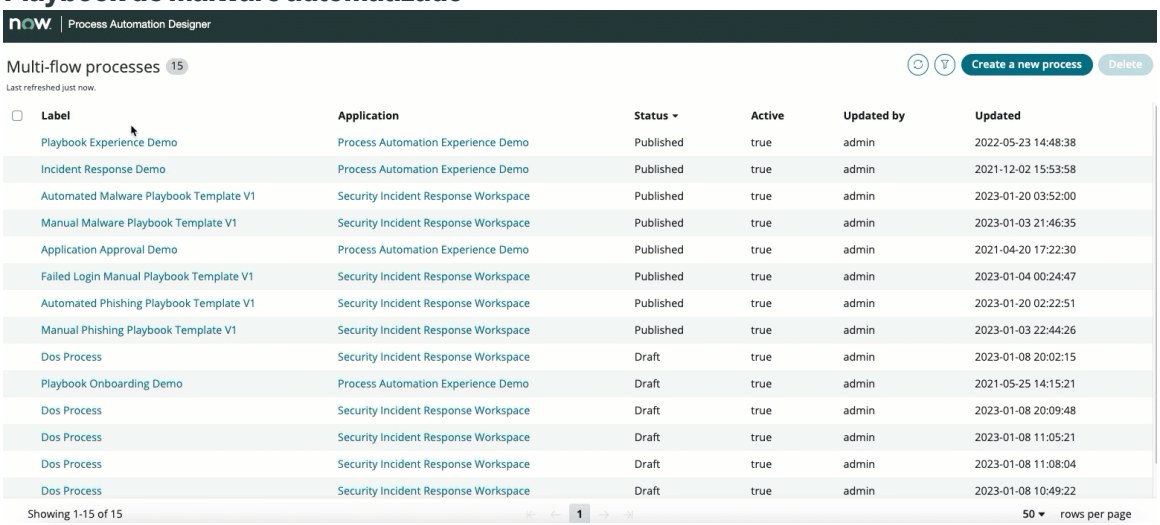
   Por exemplo, Modelo de Playbook de Malware Automatizado V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado

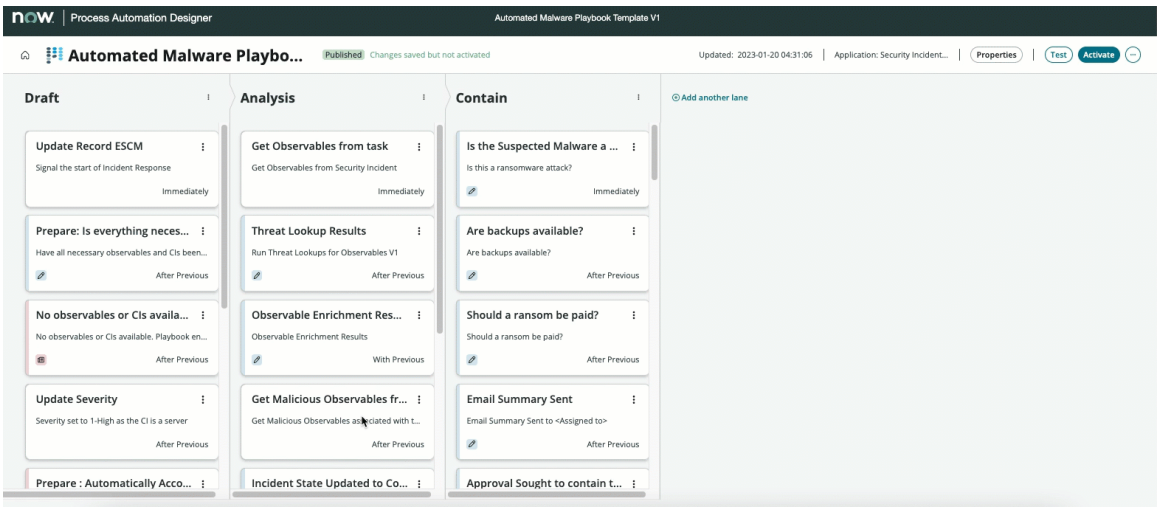


7. Clique em **Vá para o Designer** .
   A página Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova fase** .
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
   . **Condição de execução** e. **Indicar quando começar** os campos indicam quando a fase seria executada.
10. Clique em **Salve e feche** .
11. Para adicionar outra fase, clique em **Adicione outra fase** .
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** a fase começa imediatamente e não tem condição de execução. **Conter** a fase começa após a conclusão da fase anterior e tem uma condição de execução baseada no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique em **Adicione outra atividade de processo** Em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique em **Crie uma nova atividade** .
    Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de malware automatizada



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Uso do Playbook de Malware automatizado

Use estas etapas para saber como você pode usar o playbook de Malware automatizado no Espaço de analistas DO SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique em **Playbook** guia.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

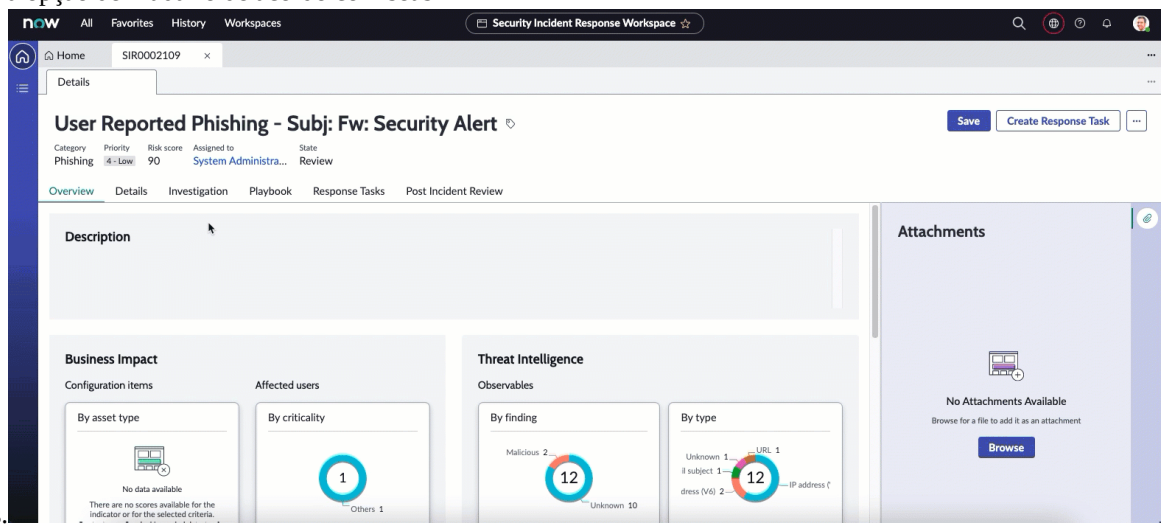
   Nota: Se você não vir nenhum playbook listado, será necessário acessar o PAD e habilitar que eles o vejam no **Playbook** guia.

3. Clique em **Playbook automatizado de malware** .
   Para malware automatizado, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de mudá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de modificá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para falha de login manual

O playbook Manual de login com falha fornece orientação e ajuda a otimizar a investigação de incidentes de segurança de login com falha.

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado. Essas tentativas de login malsucedidas podem ser falsos positivos ou tentativas feitas por invasores para obter acesso às contas de e-mail do usuário.

Você pode usar os modelos de playbook em Workflow Studio Para executar as etapas no playbook Falha de login e resolver incidentes de segurança de login com falha com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a incidentes de segurança de login com falha. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança de login com falha for criado ou atualizado. Você precisa ativar o Playbook Manual de Login com Falha em Workflow Studio e criar todas as tarefas, como análise, conter, erradicar e revisar.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

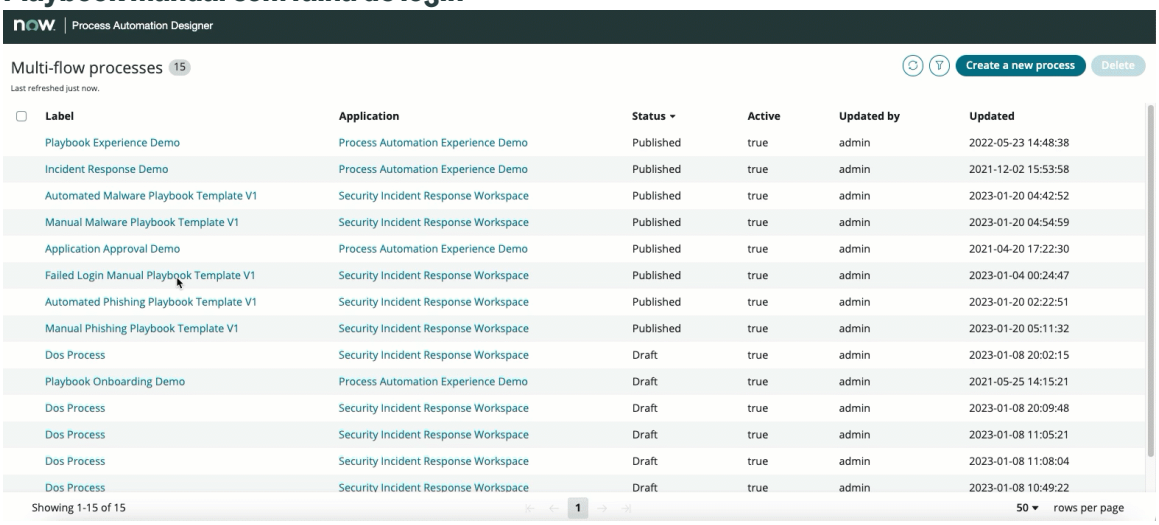
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual com falha de login



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você continua concluindo tarefas e fases. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para Falha de login manual no PAD

Use estas etapas para criar processos para Login manual com falha no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clique **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

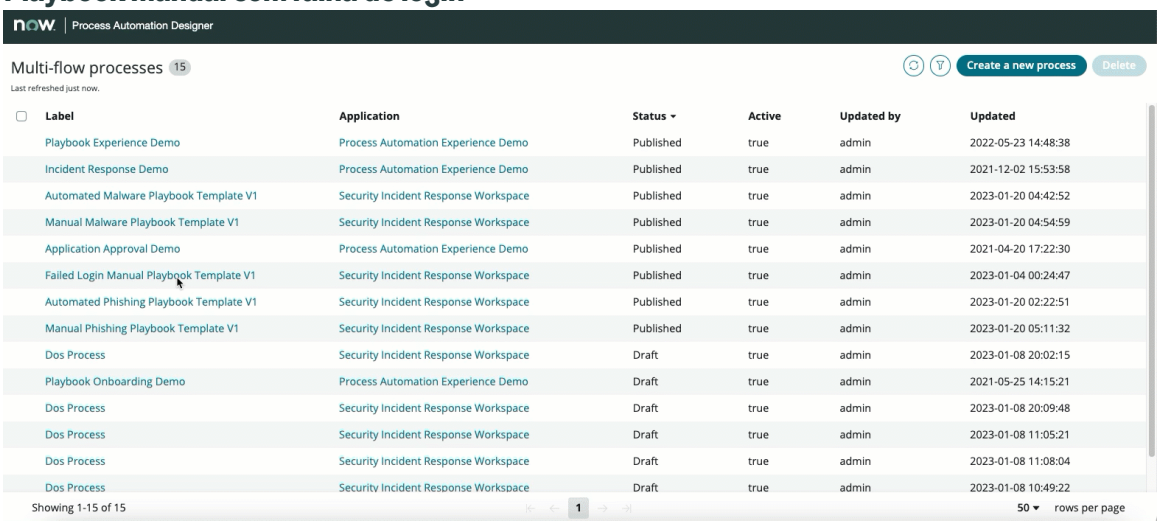
   Por exemplo, Falha no login Manual Playbook - Modelo V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual com falha de login

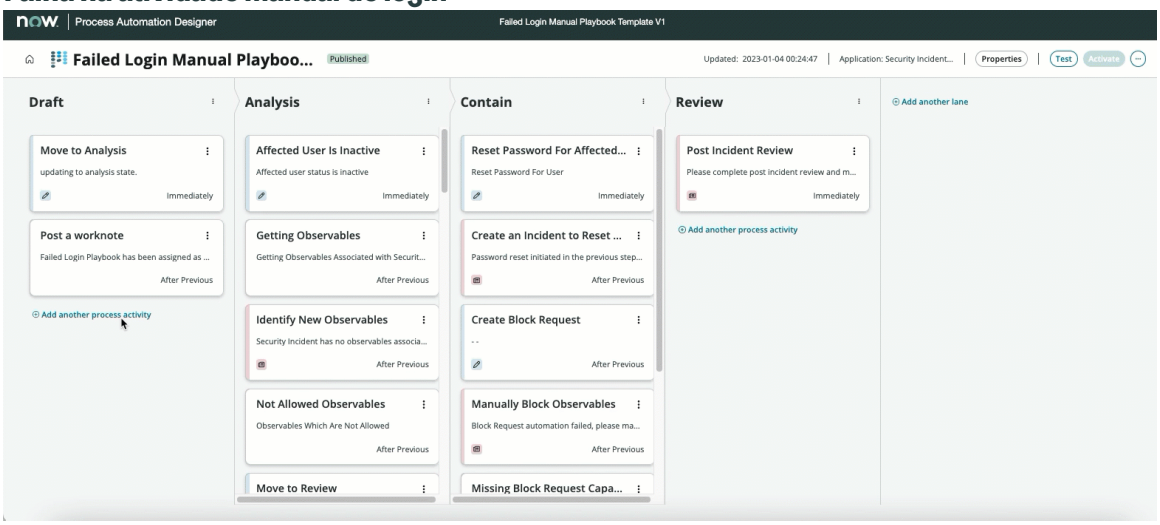


7. Clique em **Vá para o Designer** .
   A página Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova fase** .
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
   . **Condição de execução** e. **Indicar quando começar** os campos indicam quando a fase seria executada.
10. Clique em **Salve e feche** .
11. Para adicionar outra fase, clique em **Adicione outra fase** .
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** a fase começa imediatamente e não tem condição de execução. **Conter** a fase começa após a conclusão da fase anterior e tem uma condição de execução baseada no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique em **Adicione outra atividade de processo** Em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique em **Crie uma nova atividade** .
    Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falha na atividade manual de login



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Usando o playbook Manual de Login com Falha

Use estas etapas para saber como você pode usar o playbook Manual de login com falha no Espaço de analista DO SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique em **Playbook** guia.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

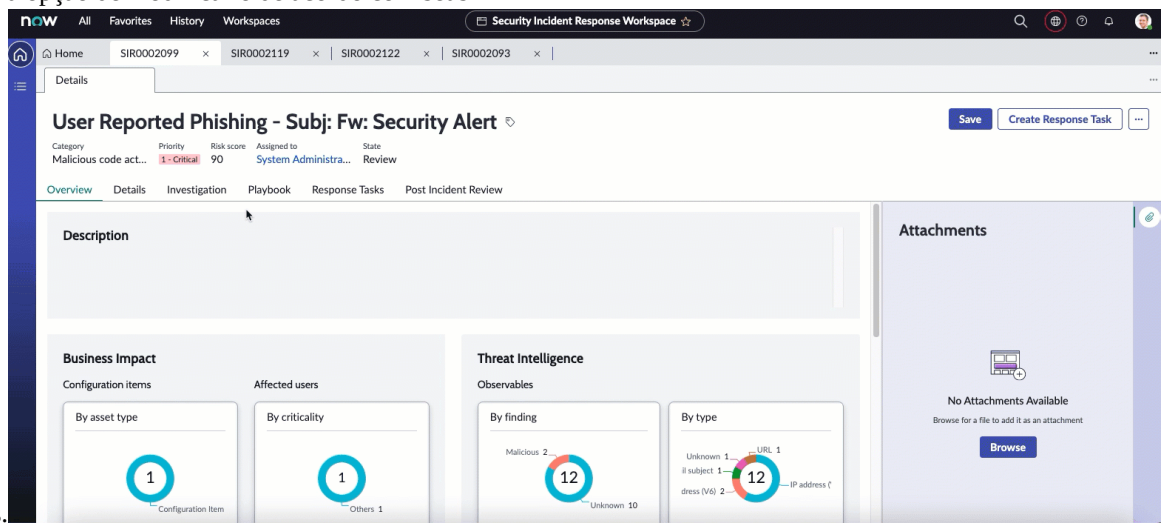
   Nota: Se você não vir nenhum playbook listado, será necessário acessar o PAD e habilitar que eles o vejam no **Playbook** guia.

3. Clique em **Playbook manual com falha de login** .
   Para Login manual com falha, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de modificá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de mudá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbooks baseados em fluxo

Usando o Flow Designer, os administradores de segurança e os autores de design de fluxo podem fazer a transição mais facilmente de playbooks manuais ou não documentados para playbooks automatizados e repetíveis. O recurso de arrastar e soltar fornece flexibilidade na movimentação de objetos, verificações de condição, ramificação paralela, tabelas de decisão e muito mais.

Resposta a incidentes de segurança fornece os seguintes playbooks com o sistema de base.

Além dos playbooks listados, também há subfluxos no spoke de Operações de segurança que podem ser chamados no playbook de fluxos. Ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Ative um fluxo de Resposta a incidentes de segurança .

Playbook para phishing automatizado

O playbook de phishing automatizado ajuda a resolver determinados tipos de ameaças à segurança de maneira passo a passo. Com os modelos do Flow Designer, você pode automatizar as etapas no playbook de resposta a phishing e resolver incidentes de forma rápida e eficiente.

Você pode usar modelos criados com o Flow Designer para automatizar as tarefas no Playbook de resposta a phishing para analisar e resolver ataques de phishing em sua organização.

O playbook de resposta a phishing inclui os seguintes fluxos e subfluxos:

- Incidente de segurança - Modelo de resposta automatizada a phishing: Este modelo foi projetado para automatizar as tarefas de resposta a phishing e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de phishing: Este modelo é o fluxo de trabalho de resposta de phishing manual existente. Defina a categoria como Phishing para ativar o fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar para facilitar a leitura. Para acessar esses fluxos, você deve instalar o. Spoke de Operações de segurança .

Nota: Ative esses modelos antes de usá-los. Consulte Ative um fluxo de Resposta a incidentes de segurança para obter detalhes.

- Executar pesquisas de ameaças para observáveis: Executa pesquisas de ameaças de observáveis selecionados.
- Enriquecer observáveis: Permite enriquecer observáveis com informações adicionais de várias fontes.
- Avaliar o impacto do e-mail de phishing: Permite avaliar o impacto do e-mail de phishing. Quando você recebe um e-mail no endereço de e-mail de phishing, esse subfluxo analisa o anexo .eml e compara as informações com as regras de correspondência de e-mail.
- Erradicar e-mails de phishing: Permite excluir ou erradicar e-mails de phishing para ajudar a reduzir a exposição a um ataque específico.
- Executar pesquisa de vistas em observáveis: Determina a prevalência de uma ameaça ao longo do tempo ou testa os esforços de correção ou erradicação.
- Criar solicitações de bloco: Bloqueia a comunicação com observáveis associados ao incidente.

Esses subfluxos representam um conjunto de operações reutilizáveis que você pode usar em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Execute o fluxo do playbook de resposta automatizada a phishing

Usando o Flow Designer, você pode definir e automatizar tarefas no playbook para analisar e resolver ataques de phishing contra sua organização.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Solicitação de bloqueio (Operações de segurança Palo Alto Networks NGFW Integration)
  - Aprimoramento de Observável
  - Pesquisa de detecção
  - Pesquisa de ameaças
  - Microsoft Office Exchange

Por Que e Quando Desempenhar Esta Tarefa

Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .eml para o endereço de e-mail de phishing definido pela sua organização. Usando as tarefas definidas no fluxo do playbook automatizado de phishing, você pode fazer a triagem, analisar, conter e erradicar uma ameaça de phishing. Essas tarefas podem ser invocadas como parte de diferentes estados de incidente (por exemplo, Análise, Conter e assim por diante). Quando um incidente de segurança de phishing é criado, o fluxo de phishing automatizado pode ser acionado automaticamente. Usando o Flow Designer, você pode exibir os detalhes das várias ações de resposta a incidentes conforme elas são invocadas.

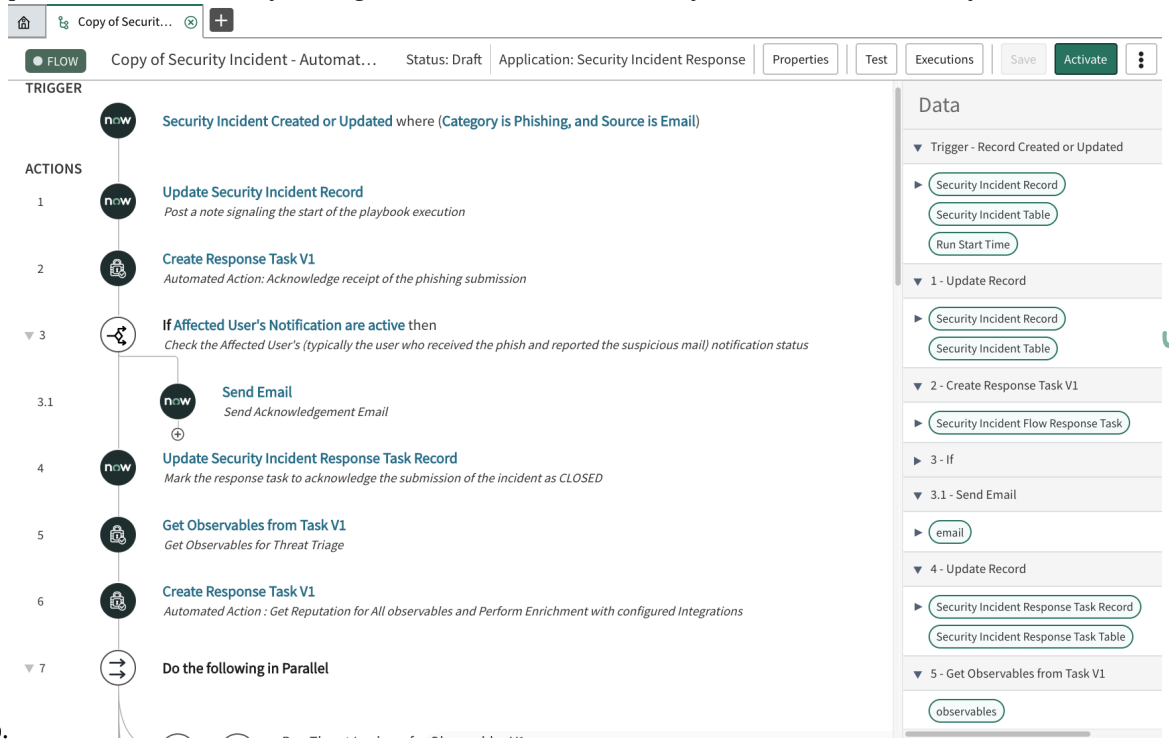
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O fluxo do playbook Incidente de segurança - Modelo de resposta automatizada a phishing V1 é Somente leitura. Você pode fazer uma cópia do fluxo e fazer mudanças conforme necessário.

As etapas a seguir descrevem como fazer uma cópia do modelo de playbook de phishing e orientam você por algumas das tarefas no fluxo.

Procedimento

1. Navegar até **Tudo** > **Flow Designer** > **Designer** para exibir os fluxos disponíveis com Operações de segurança Spoke.
2. Clique em **Incidente de segurança - Modelo de resposta automatizada a phishing VI** link.
3. Na página Fluxo, clique no ícone Mais , faça uma cópia do fluxo e abra-o para seu uso.
   Você pode modificar as condições do gatilho, adicionar ou remover ações e fazer outras mudanças no fluxo.



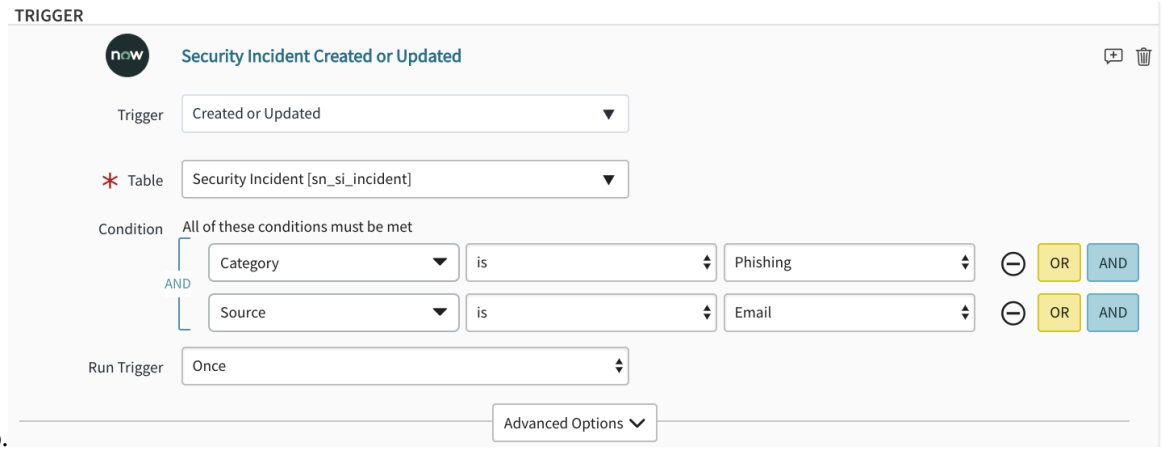
Esta imagem mostra as condições do gatilho e as etapas que o fluxo executa. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

4. Clique em **Gatilho** ícone.

Tradução automática

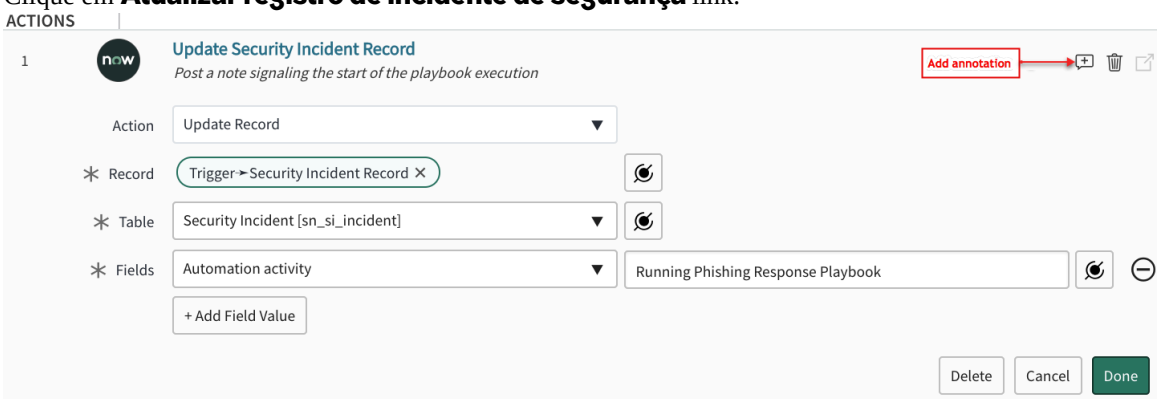
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na primeira etapa, você define ou define o gatilho para o fluxo. Especifique as condições do gatilho e a frequência com que você deseja que o gatilho.



Quando as condições definidas no fluxo (Categoria é Phishing e Origem é E-mail) são atendidas no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. Clique em **Atualizar registro de incidente de segurança** link.



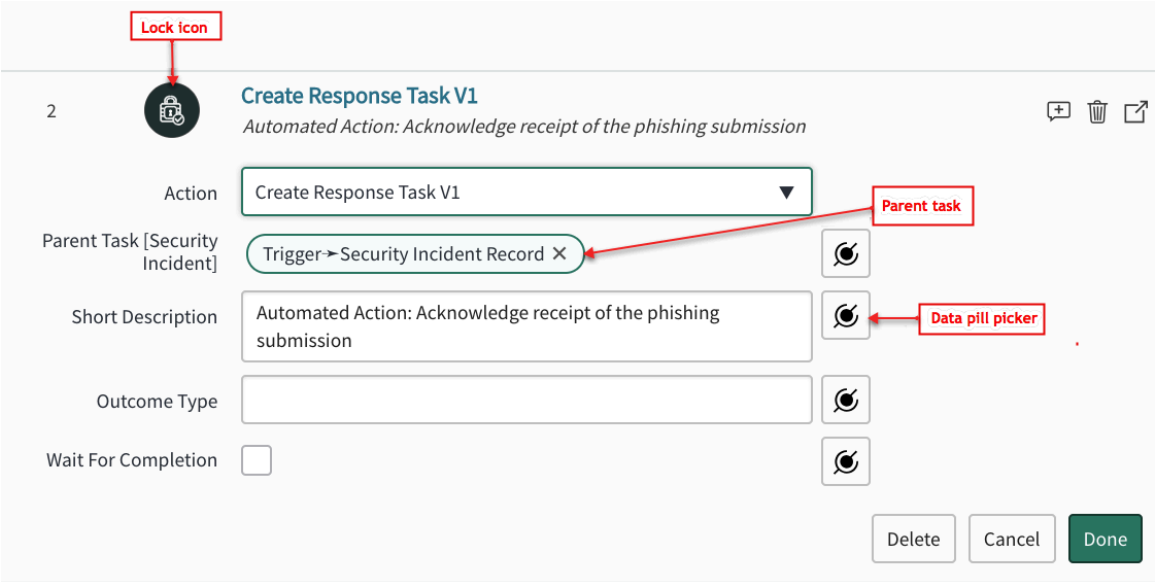
Atualizar registro de incidente de segurança é a primeira etapa no fluxo. Clique no ícone de anotação para adicionar uma anotação ao analista de segurança indicando que ocorreu um incidente de phishing e que o fluxo automatizado do playbook de phishing começou a ser executado.

6. Prossiga com a etapa 2 no fluxo e clique em **Criar tarefa de resposta** link.

Nesta etapa, o fluxo cria uma tarefa de resposta automatizada para confirmar o recebimento para o remetente do incidente ou do usuário afetado.

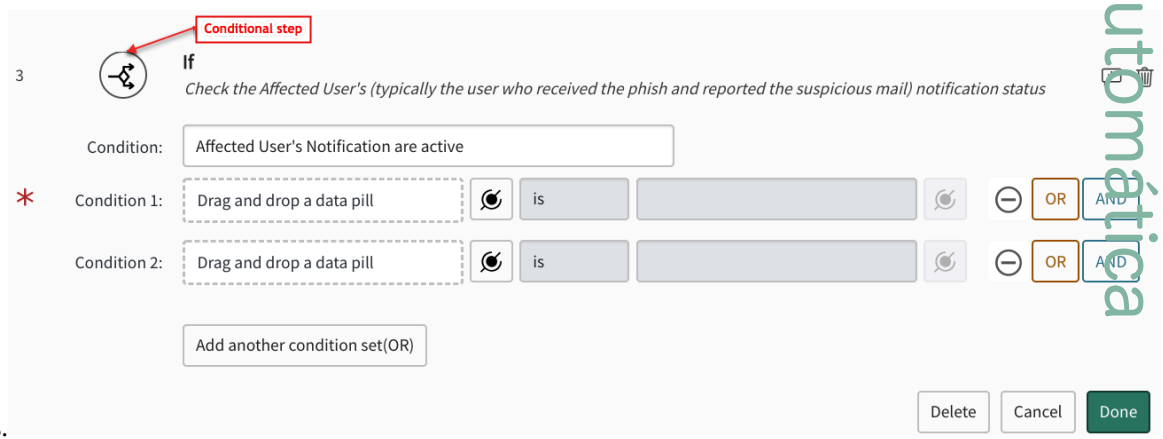
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Observe **Tarefa primária [Incidente de segurança]** o campo faz referência ao registro primário associado a esta etapa. Você pode escolher qualquer registro de referência usando o ícone do seletor de cápsula de dados ou arraste o item de referência relevante do painel direito. Observe o ícone de cadeado . O ícone de cadeado indica que a etapa não requer nenhuma intervenção do usuário.

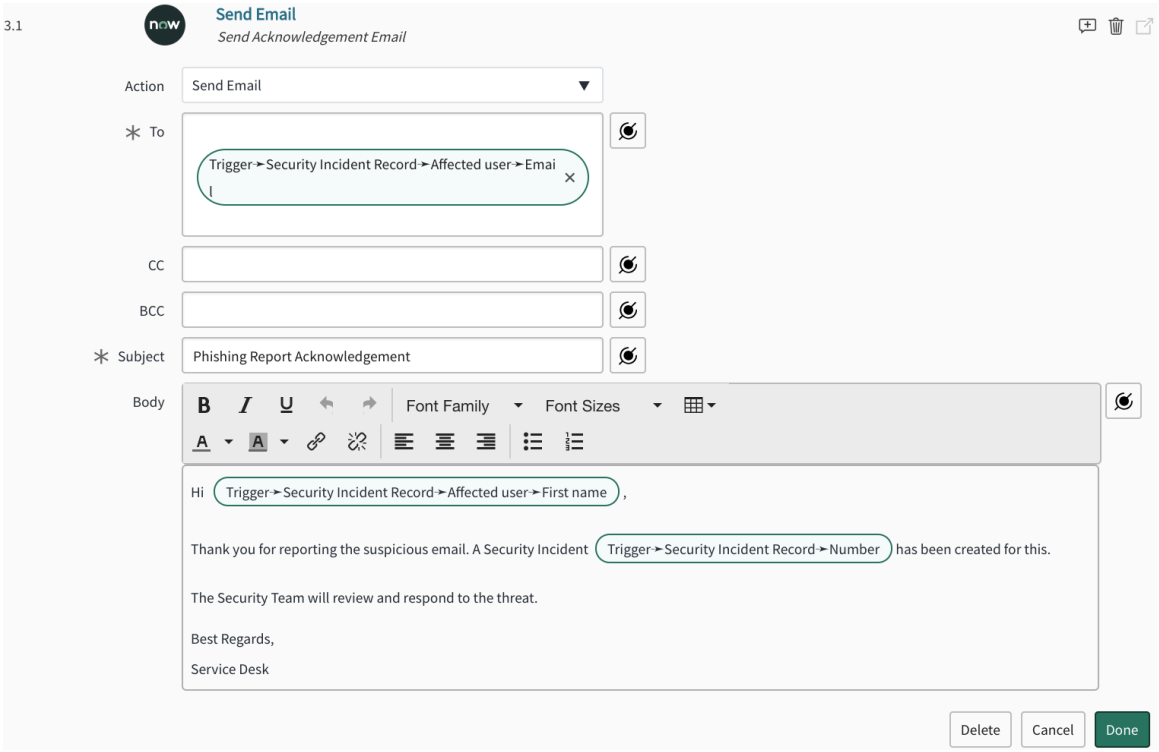
7. Na etapa 3, o fluxo coleta detalhes adicionais do usuário afetado (normalmente o usuário que enviou o incidente) para garantir que ele possa enviar uma notificação com sucesso.
Você pode especificar condições para verificar se o status do usuário afetado é Ativo e se o usuário pode receber notificações.



Observe o ícone de etapa condicional na etapa 3. O fluxo executa a próxima etapa (3,1) somente se as condições especificadas forem atendidas.

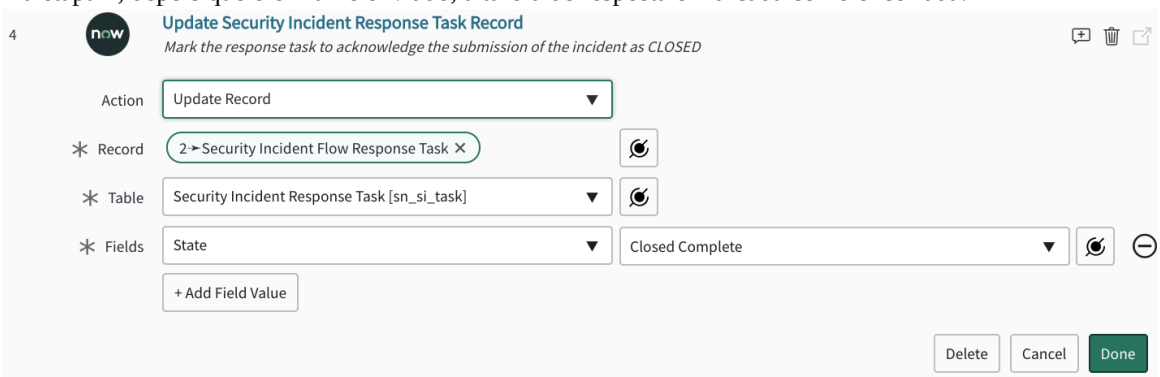
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

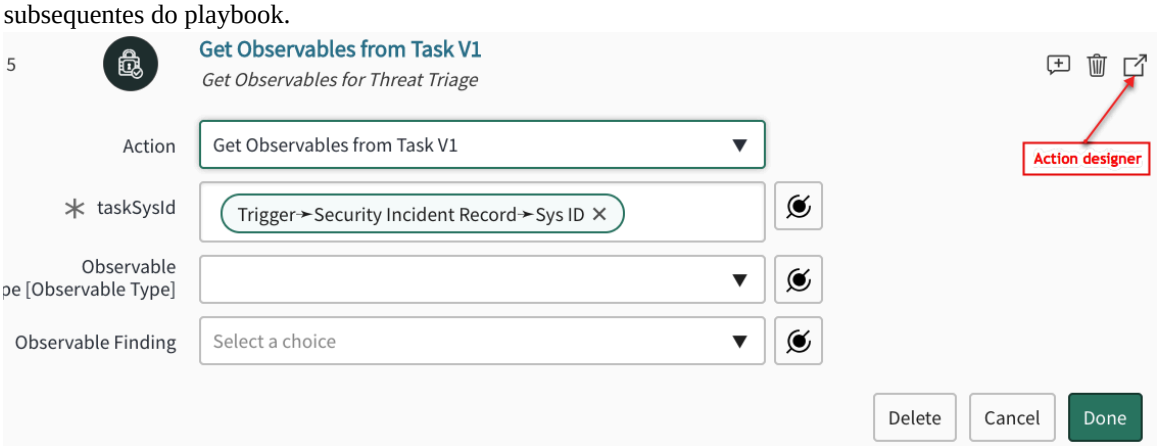


Quando as condições definidas na etapa 3 forem atendidas com sucesso, o e-mail será enviado.

8. Na etapa 4, depois que o e-mail é enviado, a tarefa de resposta é marcada como encerrada.



9. Na etapa 5, todos os observáveis envolvidos no incidente (como assunto do e-mail, endereço de e-mail do qual o e-mail de phishing foi enviado, URL de phishing) ou observáveis pertencentes a uma categoria selecionada (hash, arquivo ou domínio) são coletados para executar ações automatizadas adicionais nas etapas subsequentes do playbook.



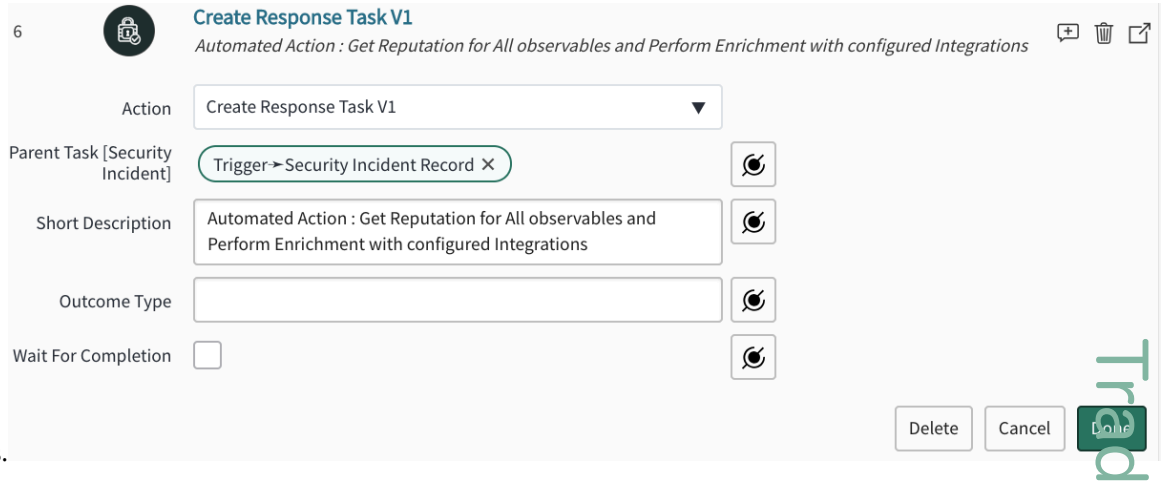
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

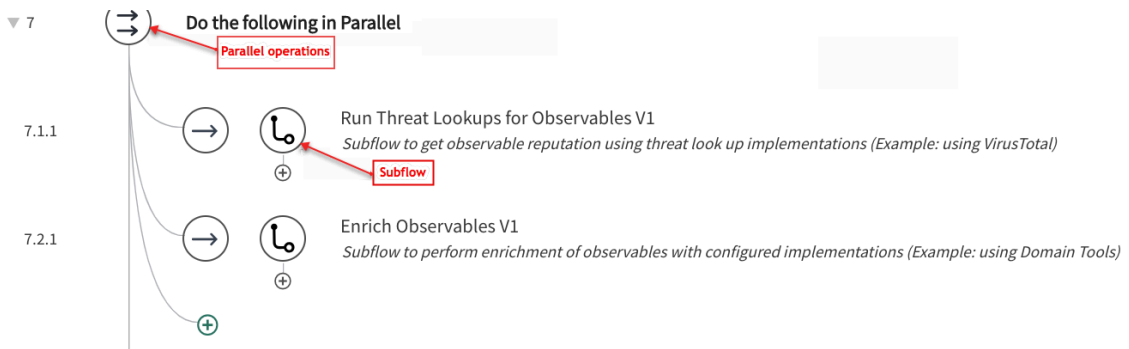
Clique no ícone do designer de ação para ver uma exibição detalhada da ação.

Para exibir o. Designer de ações expanda uma etapa no fluxo e clique no ícone do designer de ação.

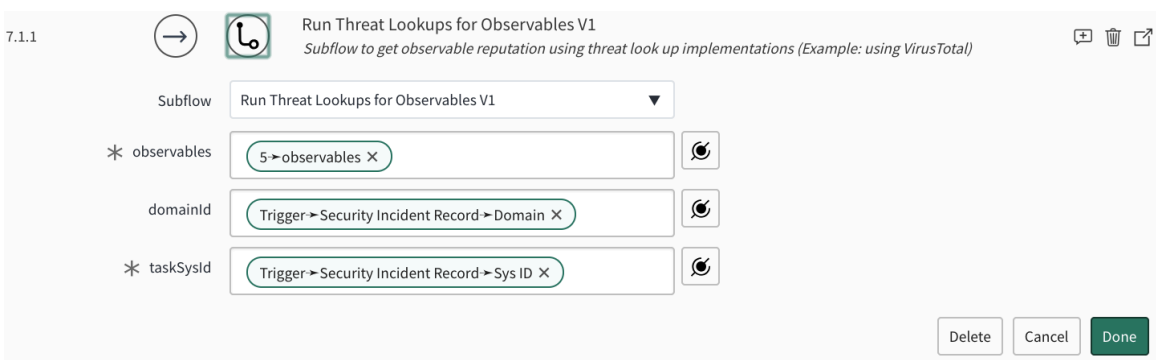
10. Na etapa 6, uma tarefa de resposta automatizada é criada. Esta tarefa captura o início do processo de obter a reputação de todos os observáveis e executar o aprimoramento com integrações configuradas.



11. Na etapa 7, dois subfluxos são chamados:
    - Executar pesquisas de ameaças para observáveis: Este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
    - Enriquecer observáveis: Este subfluxo é usado para realizar o aprimoramento de observáveis com implementações configuradas.



Observe os ícones desta tarefa. Ícone de operações paralelas indica que as tarefas serão realizadas em paralelo e o ícone de subfluxo indica que a tarefa que está sendo executada é um subfluxo, conforme mostrado abaixo:

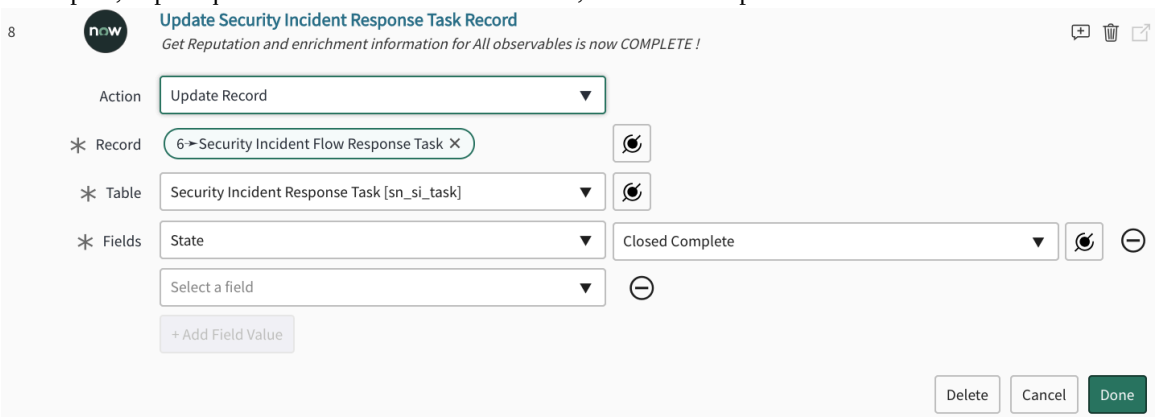


Tradução automática

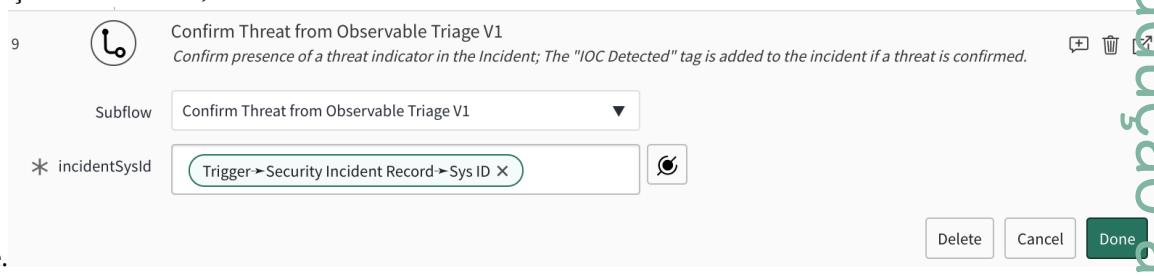
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observe o número 5 no campo Observáveis. Isso indica que a pesquisa de ameaças será executada em observáveis recuperados na etapa 5. Este subfluxo, por sua vez, chama fluxos de trabalho e ações existentes, conforme mostrado em Designer de subfluxo .

12. Na etapa 8, depois que os subfluxos forem concluídos, a tarefa de resposta será marcada como encerrada.

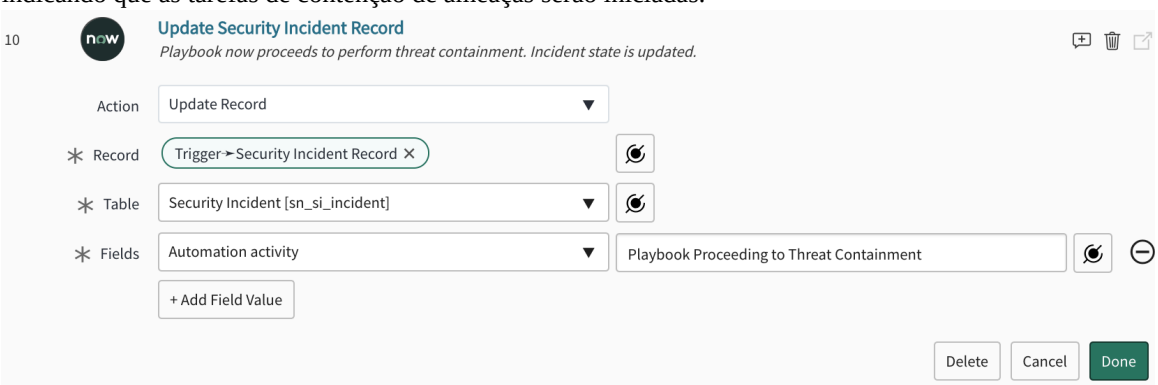


13. Na etapa 9, o subfluxo Confirmar ameaça da triagem observável é chamado.
Este subfluxo é usado para confirmar a presença de um indicador de ameaça no incidente.
Se a ameaça for confirmada, um sinalizador "IOC detectado" será adicionado ao



incidente.

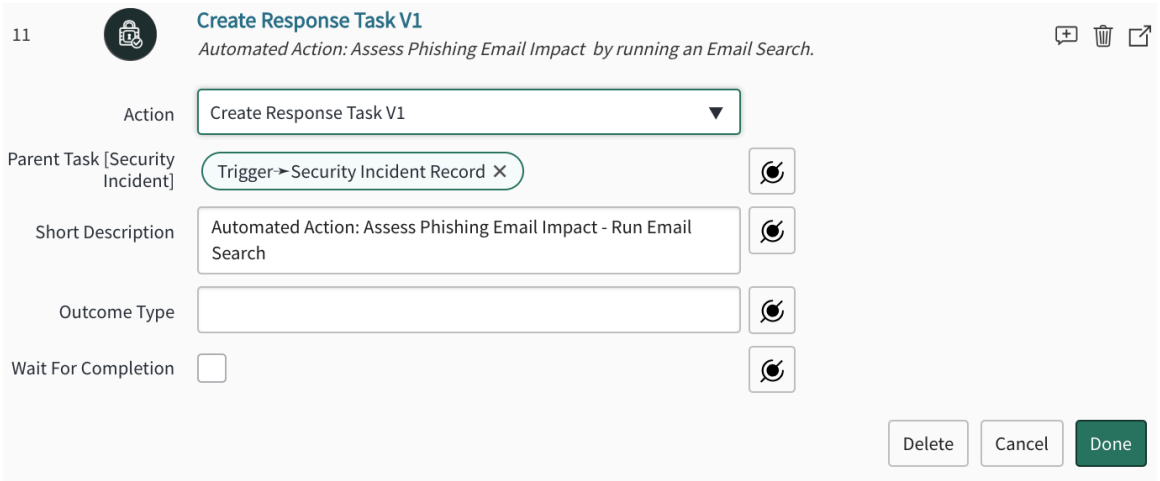
14. Quando a ameaça é confirmada, na etapa 10, você atualiza o incidente de segurança e adiciona uma anotação indicando que as tarefas de contenção de ameaças serão iniciadas.



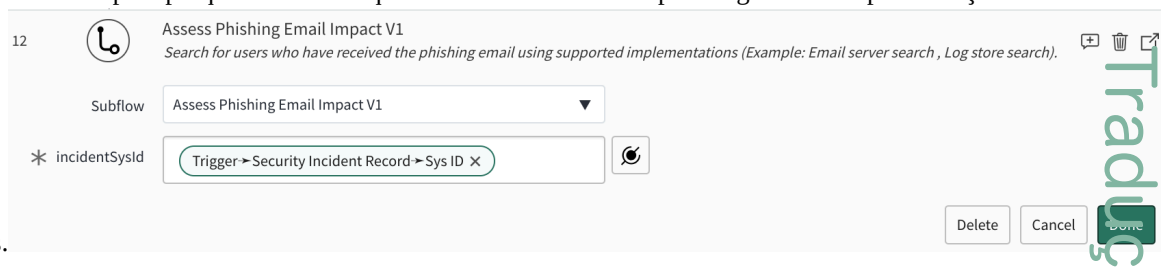
15. A etapa 11 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa usada para avaliar o impacto dos e-mails de phishing.

Tradução automática

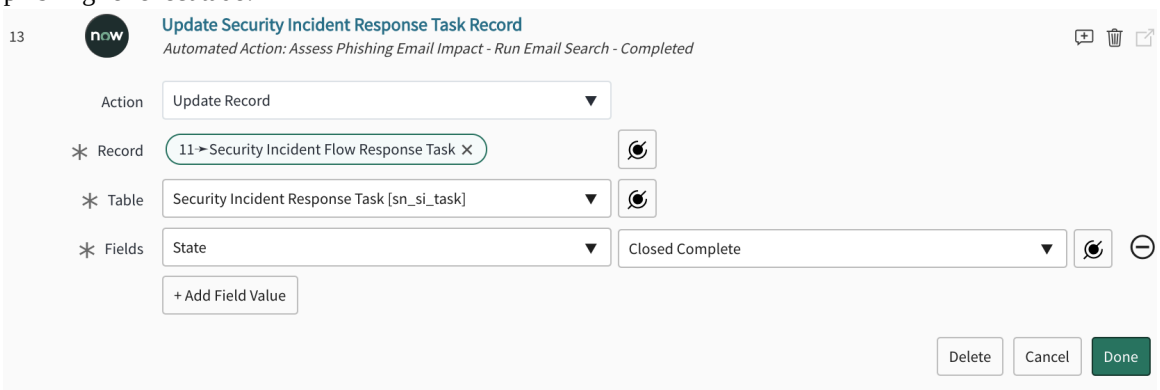
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



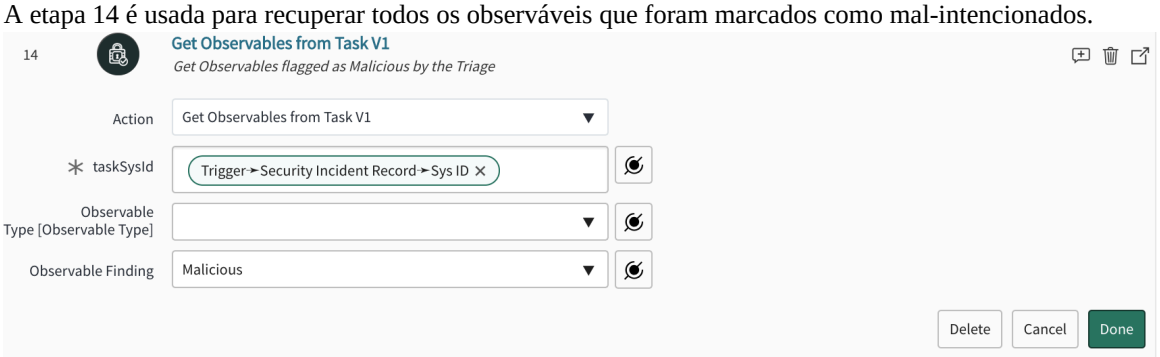
16. Na etapa 12, o subfluxo Avaliar impacto de e-mail de phishing é chamado.
Este subfluxo é usado para pesquisar usuários que receberam o e-mail de phishing usando implementações compatíveis.



17. Na etapa 13, a tarefa é marcada como Encerrada para indicar que o subfluxo Avaliar impacto de e-mail de phishing foi executado.



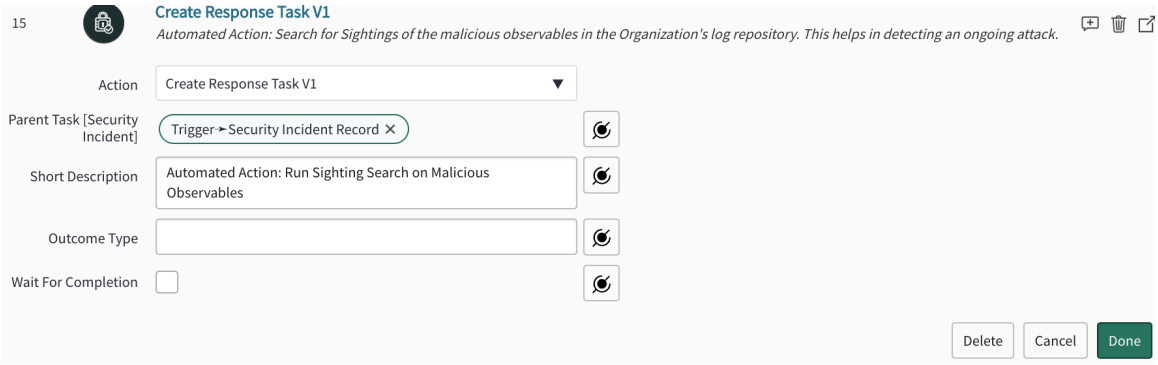
18. A etapa 14 é usada para recuperar todos os observáveis que foram marcados como mal-intencionados.



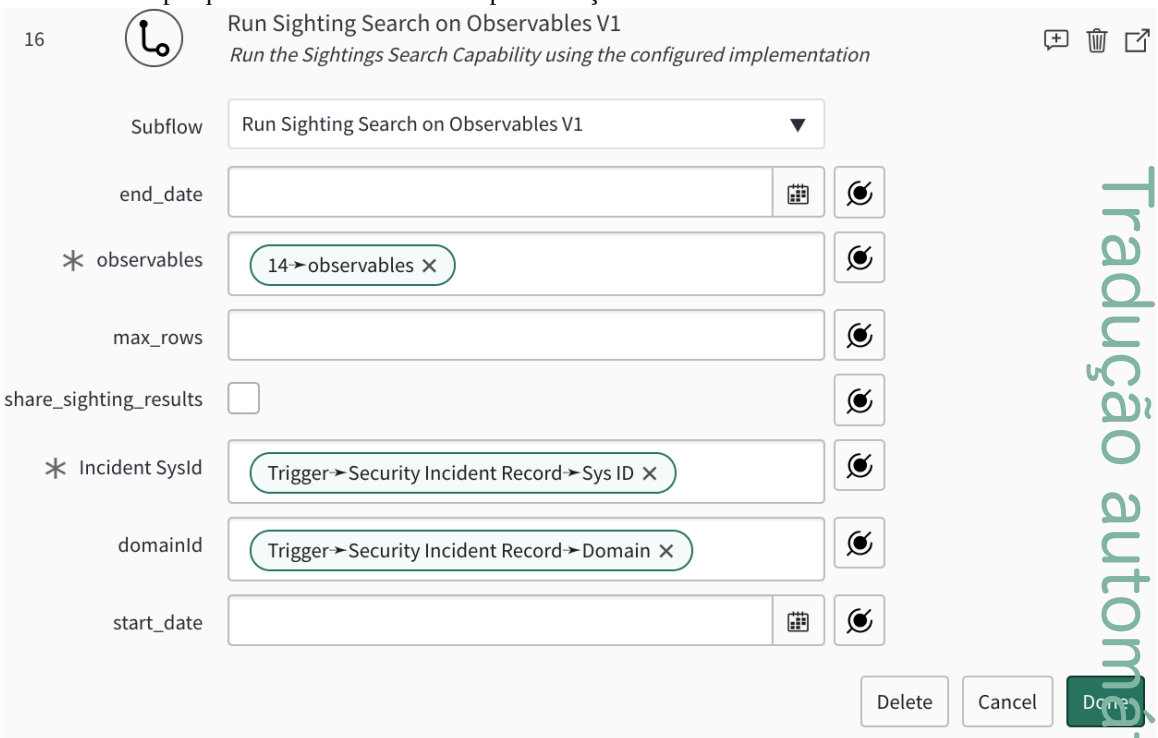
19. A etapa 15 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa de pesquisa de detecção de observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

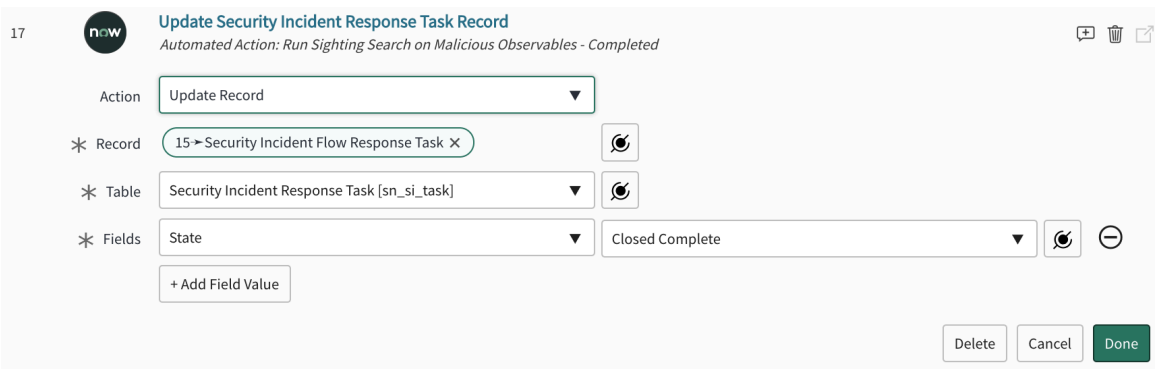


20. Na etapa 16, o subfluxo Executar pesquisa de vistas em observáveis é chamado. Este subfluxo executa uma pesquisa de vistas usando a implementação



configurada.

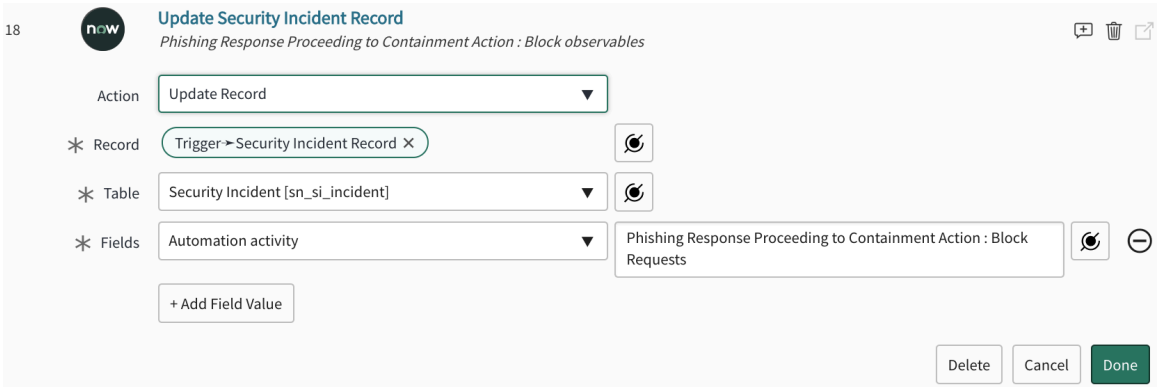
21. Na etapa 17, a tarefa é marcada como Encerrada para indicar que o subfluxo Executar pesquisa de vistas em observáveis foi concluído.



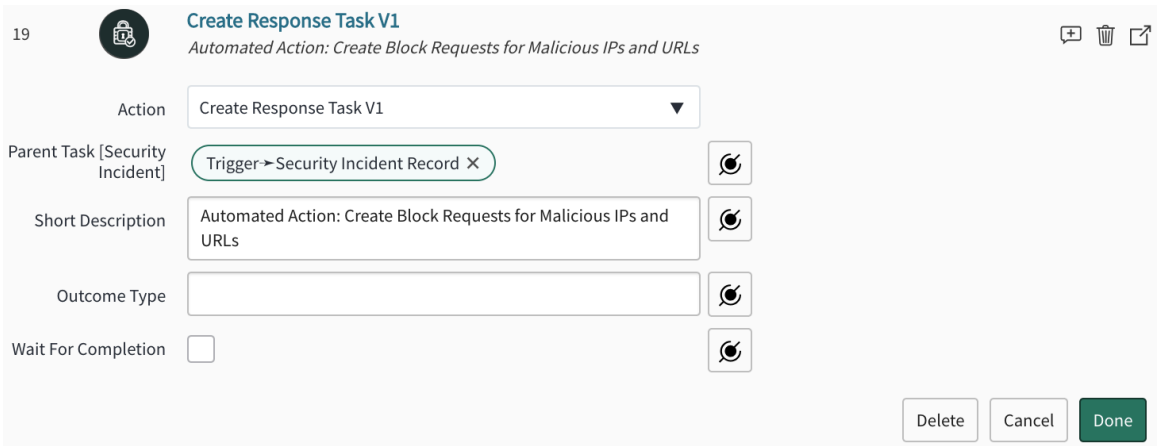
22. Depois de identificar os observáveis mal-intencionados, na etapa 18, atualize o registro do incidente de segurança para indicar que as ações de contenção serão iniciadas.

Tradução automática

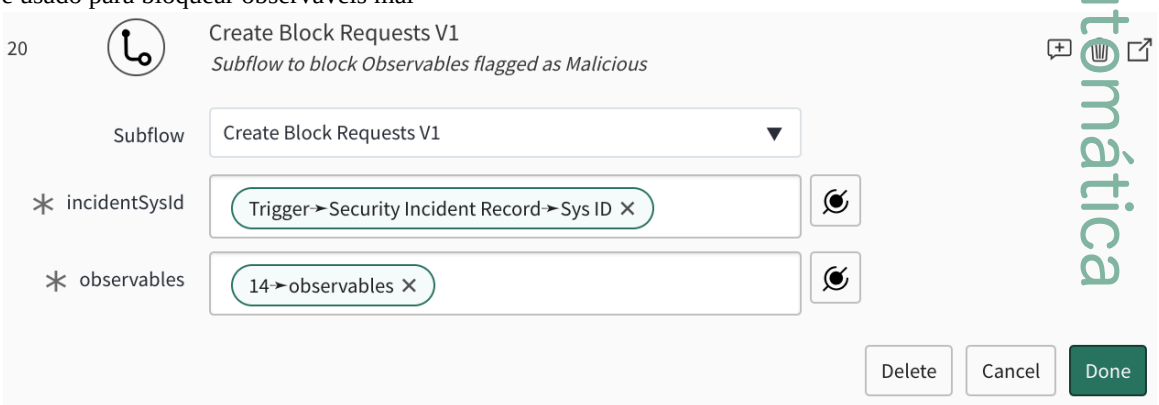
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



23. A etapa 19 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa de solicitações de bloco.

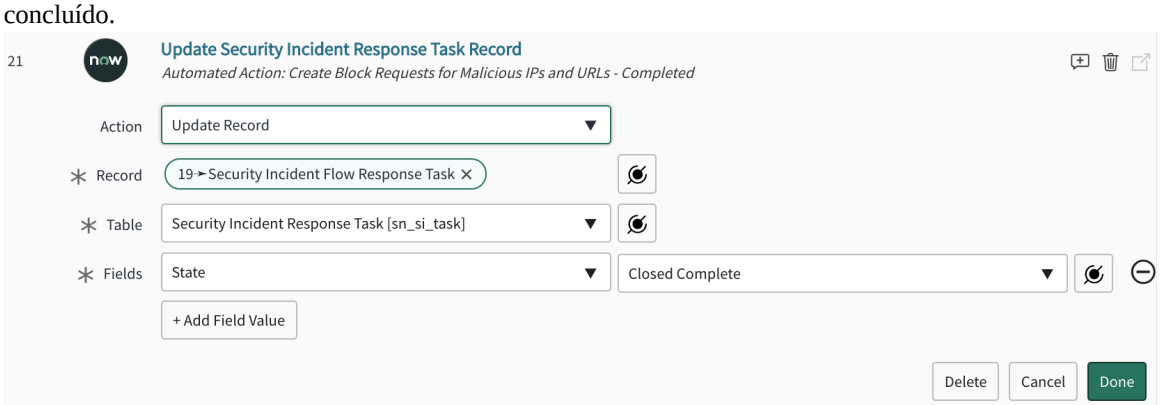


24. Na etapa 20, o subfluxo Criar solicitações de bloco é chamado. Este subfluxo é usado para bloquear observáveis mal-



intencionados.

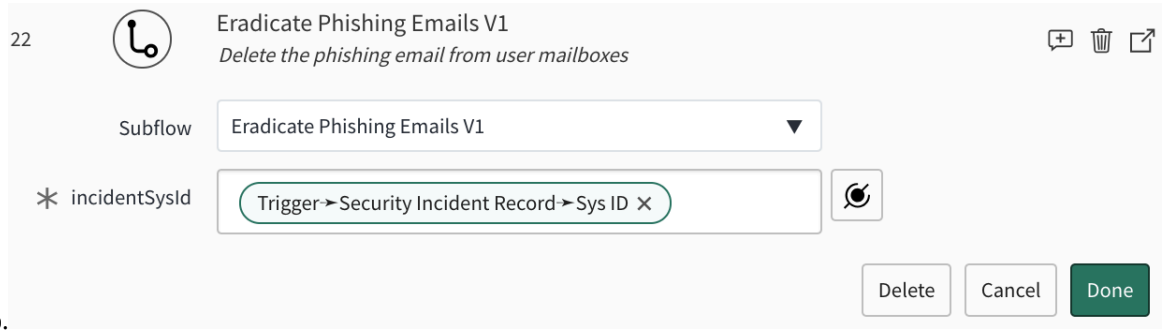
25. Na etapa 21, a tarefa é marcada como Encerrada para indicar que o subfluxo Criar solicitações de bloco foi concluído.



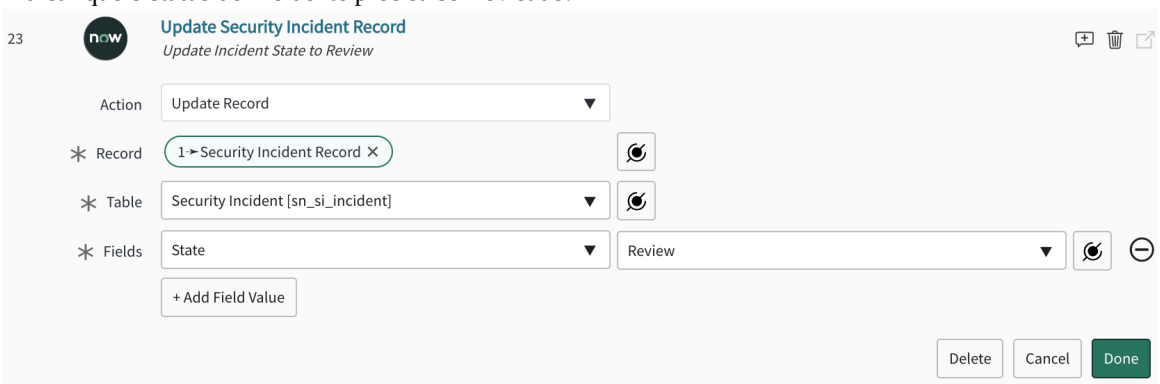
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

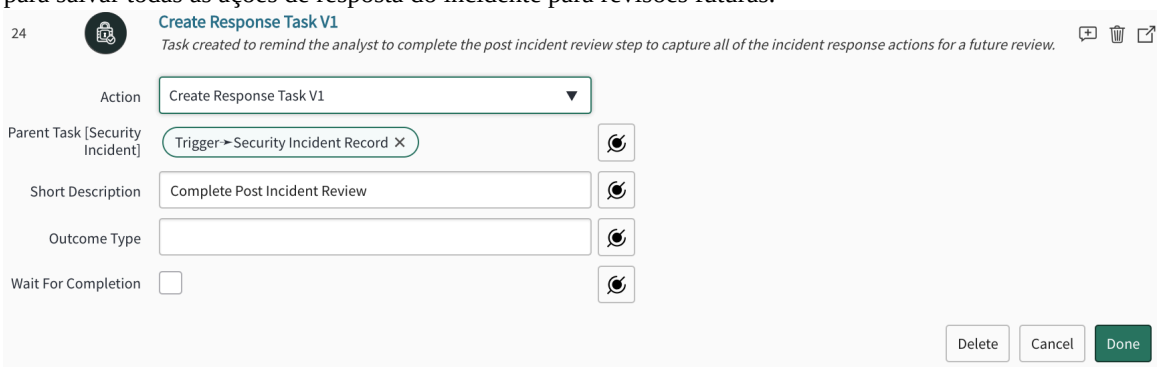
26. Na etapa 22, o subfluxo Erradicar e-mails de phishing é chamado.
Este subfluxo é usado para excluir e-mails de phishing das caixas de correio do usuário.



27. Após a exclusão dos e-mails de phishing, na etapa 23, você atualiza o registro do incidente de segurança para indicar que o status do incidente precisa ser revisado.



28. Na última etapa, o fluxo cria uma tarefa de resposta automatizada.
Esta tarefa é usada para enviar um lembrete ao analista de segurança para salvar todas as ações de resposta do incidente para revisões futuras.



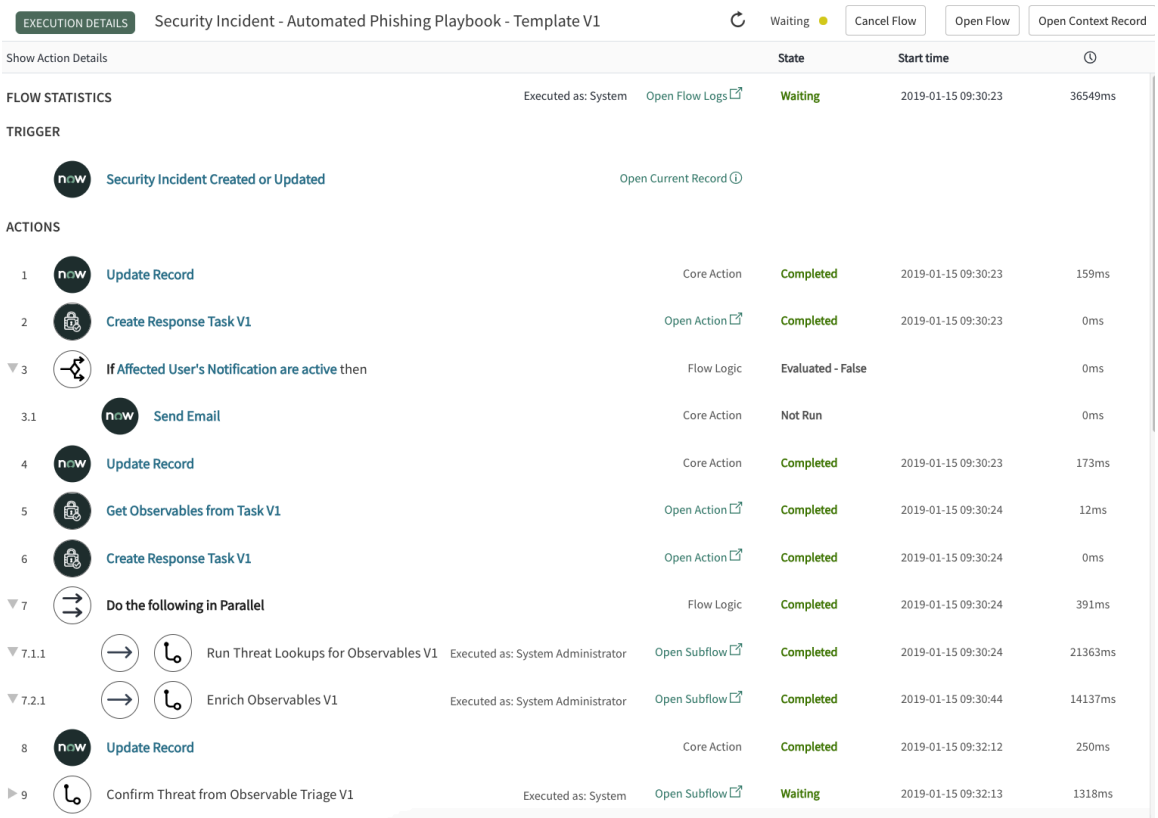
O que Fazer Depois

Você pode clicar em **Teste** para simular as ações no fluxo antes de publicá-lo. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo e executá-lo.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



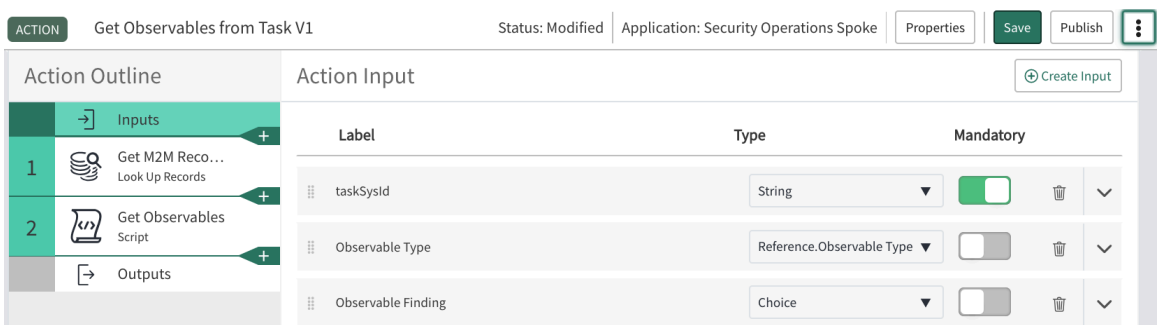
Exibir o designer de ação de fluxo do playbook de resposta de phishing automatizado

Você pode detalhar o Designer de ação para exibir informações detalhadas sobre as ações que estão sendo executadas para uma etapa específica no fluxo do playbook de resposta automatizada de phishing.

Esta página descreve a página Designer de ação da etapa Obter observáveis da tarefa. Selecione uma tarefa no painel Descrição da ação para exibir os detalhes.

Ação de entrada

Esta seção mostra detalhes sobre como a ação foi criada, incluindo o ID do incidente, o tipo de observável (hash ou IP) e descoberta observável (somente e-mails mal-intencionados).

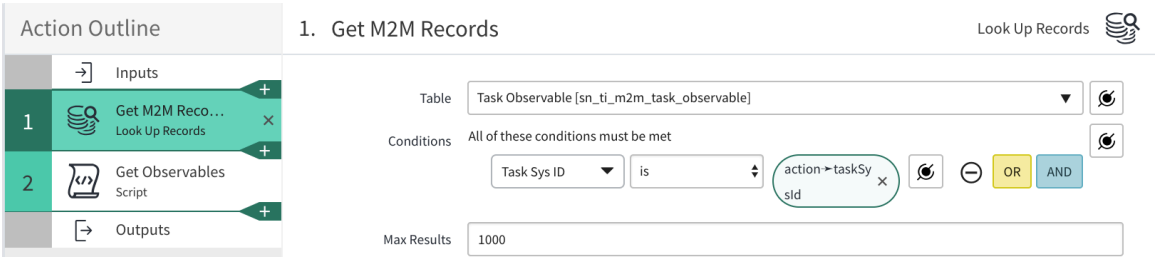


Obter registros M2M

Esta seção mostra as condições que foram definidas para pesquisar observáveis em uma tabela especificada.

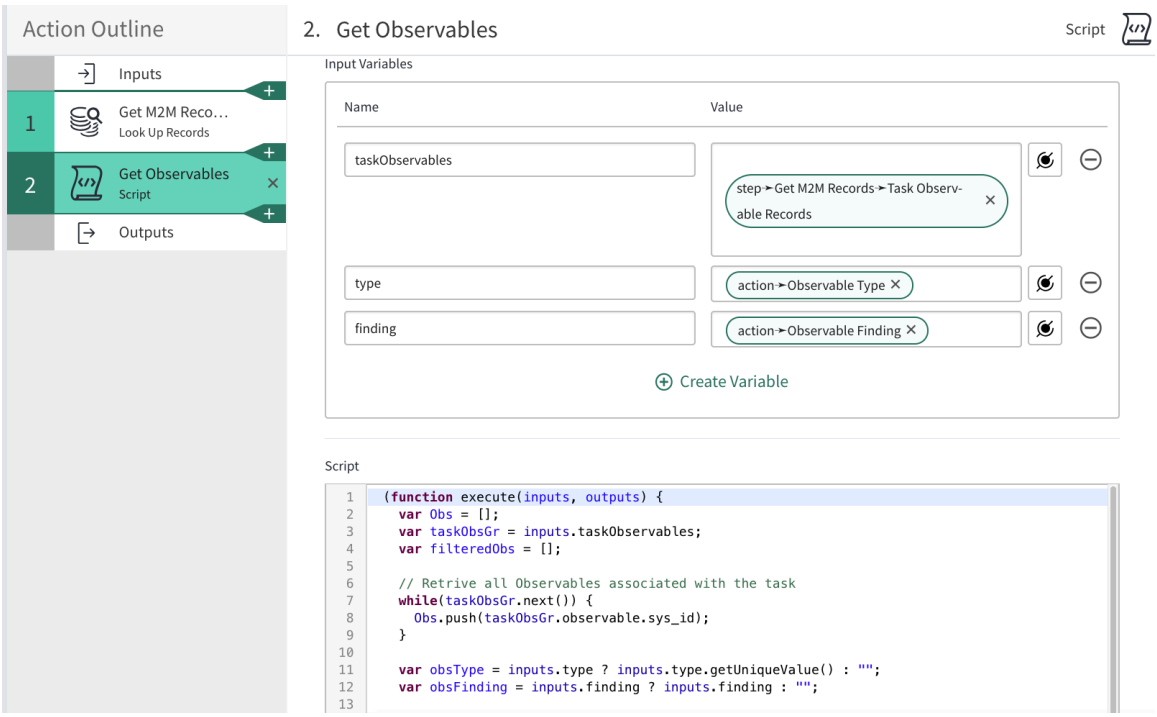
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Obter observáveis

Esta seção mostra o script usado para recuperar observáveis com base nas condições de filtro especificadas. Por fim, os observáveis que atendem a esses critérios e a contagem são exibidos.



Nota: Todas as ações definidas neste fluxo são reutilizáveis e podem ser modificadas de acordo com seus requisitos.

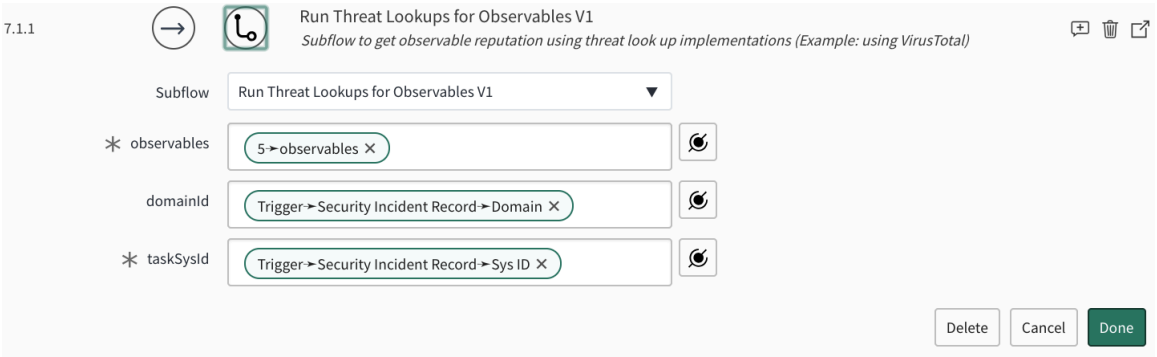
Exiba o designer de subfluxo do playbook de resposta automatizada de phishing

Você pode detalhar o Designer de subfluxo para exibir informações detalhadas sobre o subfluxo que está sendo executado como parte do fluxo do playbook de resposta automatizada de phishing.

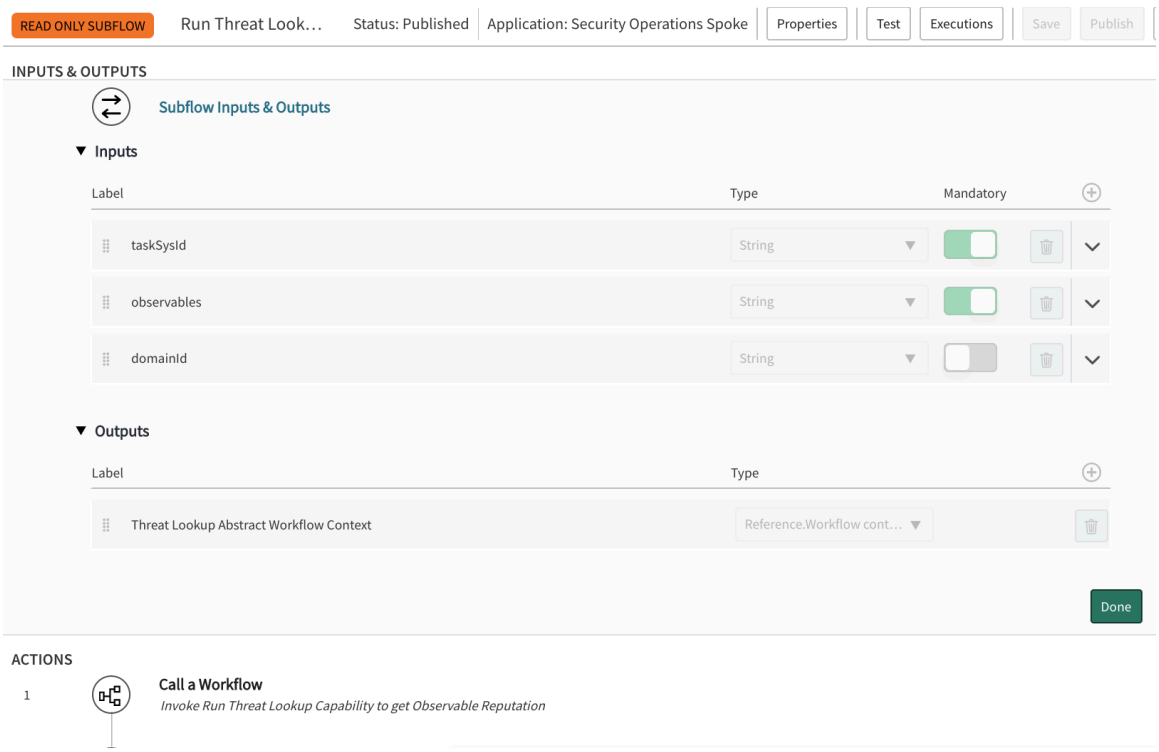
Você pode iniciar o Designer de subfluxo para exibir detalhes adicionais de um subfluxo. A página do Designer de subfluxo do subfluxo Executar pesquisas de ameaças para observáveis é mostrada aqui. Selecione Na imagem abaixo para exibir o Designer de subfluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Na página Designer de subfluxo, você pode ver as entradas e saídas desse subfluxo e as ações de fluxo de trabalho subjacentes que estão sendo executadas.



Nota: Este subfluxo é somente leitura e não pode ser editado. Você pode adicionar ou excluir subfluxos à etapa, mas não pode modificar o subfluxo.

Playbook para malware automatizado

O Playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajuda você a resolver alertas de malware de forma rápida e eficiente.

Use o fluxo do playbook de malware para automatizar as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. O modelo de fluxo inclui condições de gatilho, uma sequência de ações e subfluxos anotados para facilitar a leitura.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que são anotados para facilitar a leitura. Para acessar esses fluxos, você deve instalar o Spoke de Operações de segurança E Operações de segurança Palo Alto Networks - Wildfire do ServiceNow Store.

Nota: Você deve ativar esses modelos antes de usá-los.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os seguintes fluxos e subfluxos estão incluídos:

- Incidente de segurança - Modelo de Playbook de malware automatizado: Este modelo foi projetado para automatizar as respostas a alertas de malware e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de malware: Este modelo é o fluxo de trabalho de resposta manual de malware existente que é ativado quando a categoria é definida como Atividade de código mal-intencionado.

Subfluxos

- Confirmar ameaça do observável: Verifica se os observáveis são mal-intencionados e precisam ser resolvidos.
- Definir gravidade do incidente: Define um status de gravidade para o incidente.
- Playbook de ransomware: Determina se é um ataque de ransomware.

Esses subfluxos representam um conjunto de operações reutilizáveis que podem ser usadas em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Execute o fluxo automatizado do playbook de malware

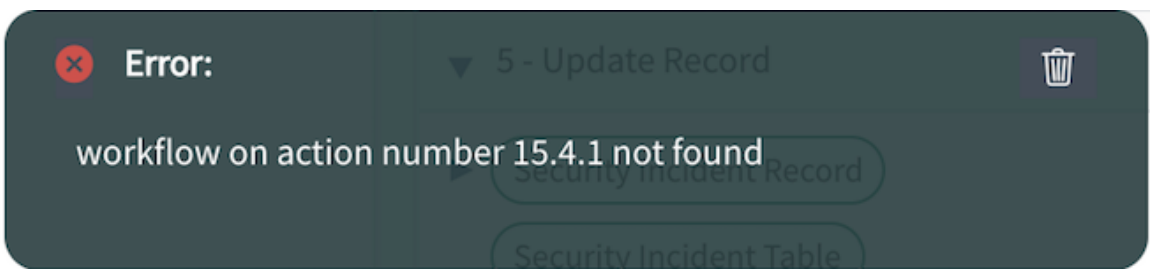
Use este fluxo para automatizar tarefas no playbook para analisar e resolver ataques de malware contra sua organização.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Palo Alto Networks incêndio florestal para Operações de segurança
  - Pesquisa de vistas (Splunk)
  - Solicitações de bloqueio
  - Pesquisa de ameaças
  - Aprimorar observáveis

  Verifique se essas integrações estão funcionando corretamente antes de você ativar Incidente de segurança - Modelo Playbook de malware automatizado.

- Aplicativo Wildfire da Palo Alto Networks: Para acessar o fluxo do playbook automatizado de malware, você deve instalar o aplicativo Security Operations Spoke e Security Operations Palo Alto Networks - Wildfire do ServiceNow Store. Se o aplicativo Security Operations Palo Alto Networks Wildfire não estiver instalado, você verá um erro "Fluxo de trabalho na ação número 15.4.1 não encontrado", conforme mostrado abaixo:



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você não quiser instalar este aplicativo, exclua as etapas **15,2, 15,3 e 15,4** do fluxo do playbook de malware automatizado.

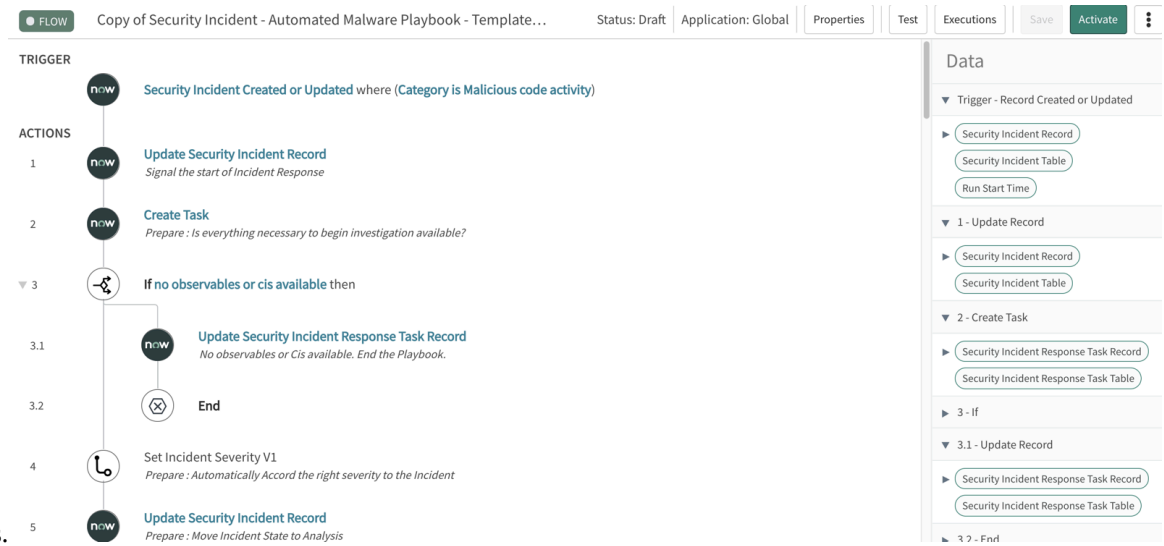
- Certifique-se de que as seguintes condições foram atendidas:
  - O incidente de segurança foi atribuído a um analista de segurança que pertence ao grupo de aprovação apropriado.
  - O analista de segurança que lida com o incidente deve ter um endereço de e-mail válido.
  - Os itens de configuração e observáveis necessários foram adicionados ao incidente de segurança.
- Para **Etapa 21 (Solicitar aprovação)** , Mude o Grupo de **Atribuição de incidente de segurança** ao seu grupo preferencial.
- A etapa 21 do fluxo é uma etapa de aprovação de tarefa obrigatória em que uma solicitação de aprovação é enviada ao administrador. Para aprovar a solicitação, o administrador deve navegar até a página Aprovações de tarefa e definir o campo Estado como **Aprovado** . Se a tarefa não for aprovada, o designer de fluxo não poderá prosseguir e o processo será encerrado.

Por Que e Quando Desempenhar Esta Tarefa

Quando uma atividade de código mal-intencionado é detectada na rede, um incidente de segurança é criado e o fluxo do playbook de malware automatizado é iniciado. Você pode usar as tarefas definidas no fluxo do playbook automatizado de malware para fazer a triagem, analisar, conter e erradicar a ameaça.

Procedimento

1. Navegar até **Tudo** > **Flow Designer** > **Designer** Para exibir os fluxos disponíveis com o spoke de Operações de segurança.
2. Clique em **Incidente de segurança - Modelo de Playbook de malware automatizado VI** link.
3. Na página Fluxo, clique no ícone Mais , faça uma cópia do fluxo e abra-o para seu uso.
   Agora você pode fazer mudanças em seu fluxo, como modificar condições ou ações do gatilho ou adicionar e remover ações.

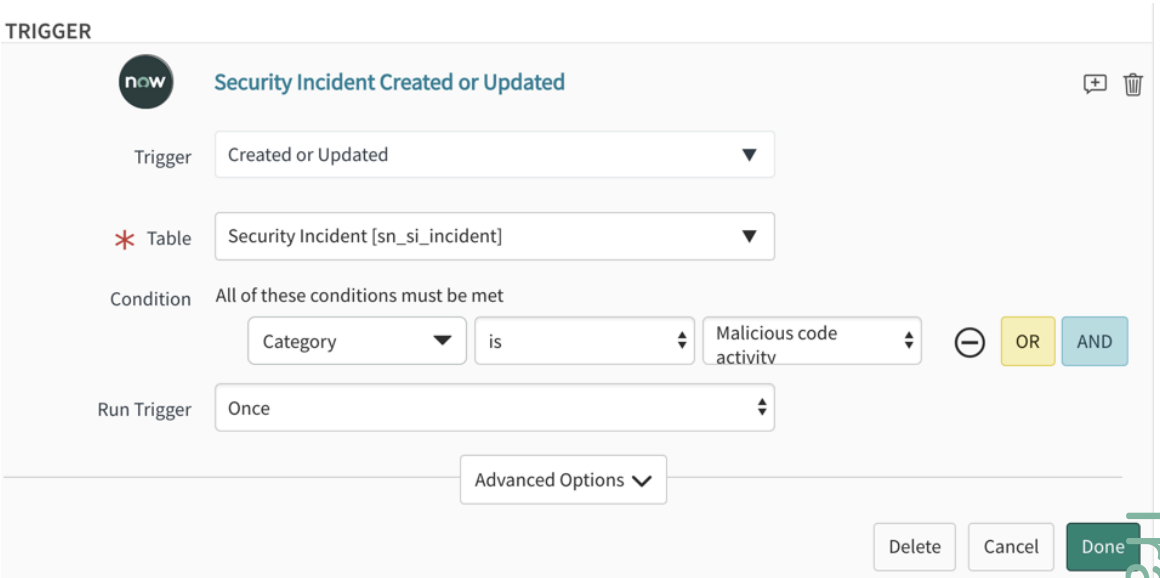


Mostra o gatilho e as etapas que serão executadas com o fluxo. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

Tradução automática

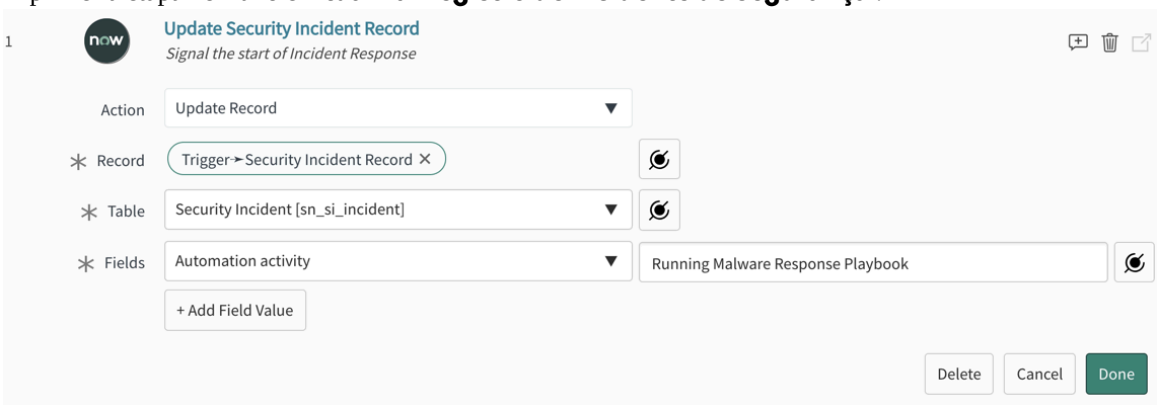
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Gatilho** ícone.
   Na primeira etapa, você define ou define o gatilho para o fluxo. Especifique as condições para o gatilho e a tarefa a serem executados quando as condições forem atendidas.



   Quando a condição definida no fluxo (Categoria é atividade Código mal-intencionado) é atendida no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. A primeira etapa no fluxo é **Atualizar registro de incidente de segurança** .



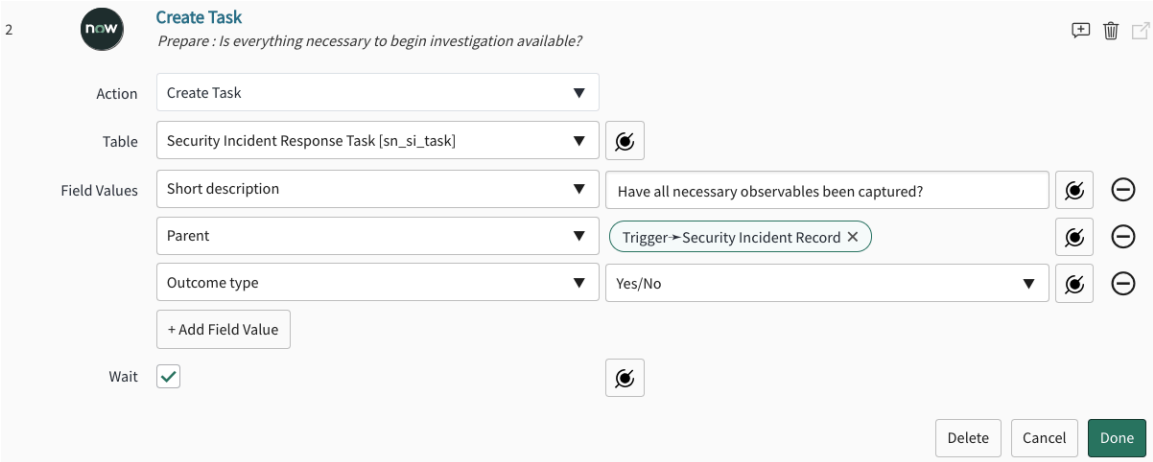
   Clique no link e clique no ícone de anotação para adicionar uma anotação ao analista de segurança indicando que houve alguma atividade de código mal-intencionado e que o fluxo do playbook de resposta automatizada de malware começou a ser executado.

6. Prossiga com a etapa 2 no fluxo e clique em **Criar tarefa** link.

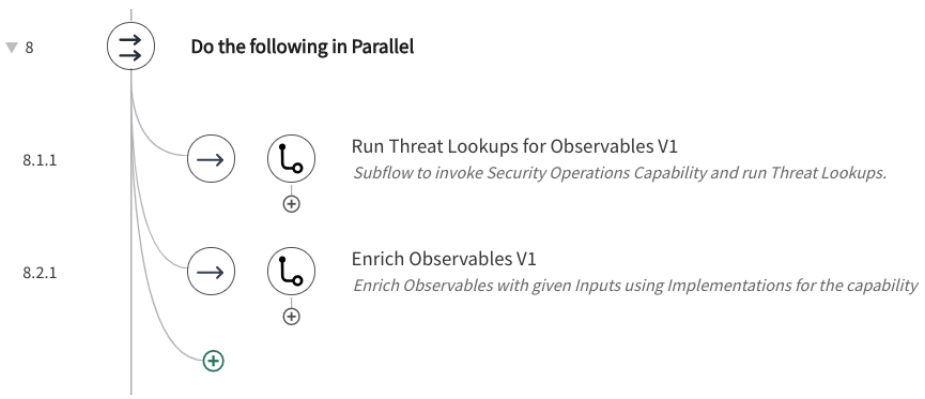
   Nesta etapa, uma tarefa de resposta automatizada é criada para verificar se todos os observáveis necessários foram capturados e se a investigação pode começar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



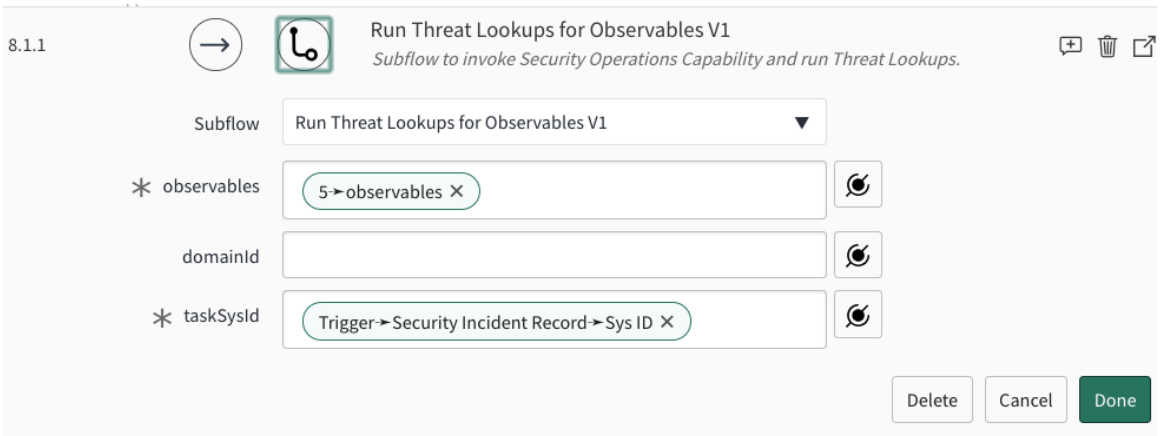
7. Se o tipo de resultado for **Não** Indica que não há observáveis e ICs disponíveis para iniciar a investigação. Atualize o registro do incidente de segurança para indicar que o playbook não pode prosseguir.
8. Se o tipo de resultado for **Sim** , O subfluxo Definir severidade do incidente atribui automaticamente a severidade correta ao incidente de segurança.
9. Na próxima etapa, o registro de incidente de segurança é atualizado.
10. Na próxima etapa, todos os observáveis envolvidos no incidente ou em uma categoria selecionada são coletados para executar ações automatizadas adicionais nas etapas subsequentes do playbook.
11. Na próxima etapa, uma tarefa de resposta automatizada é criada.
    Esta tarefa captura o início do processo de obter a reputação de todos os observáveis e executar o aprimoramento com integrações configuradas.
12. Na etapa 8, dois subfluxos são chamados:
    - Executar pesquisas de ameaças para observáveis: Este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
    - Enriquecer observáveis: Este subfluxo é usado para realizar o aprimoramento de observáveis com implementações configuradas.



Observe os ícones desta tarefa. Ícone de operações paralelas indica que as tarefas serão realizadas em paralelo e o ícone de subfluxo indica que a tarefa que está sendo executada é um subfluxo, conforme mostrado abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Observe o número 5 no campo Observáveis. Isso indica que a pesquisa de ameaças será executada em observáveis recuperados na etapa 5. Este subfluxo, por sua vez, chama fluxos de trabalho e ações existentes.

13. Na próxima etapa, a ação Executar a pesquisa de registros é executada.
Esta ação é usada para pesquisar registros de contexto de fluxo de trabalho em que os fluxos de trabalho primários podem ser um dos seguintes.
    - Contexto de fluxo de trabalho abstrato de Pesquisa de ameaças
    - Contexto de Fluxo de Trabalho Abstrato de Aprimoramento de Observável
14. Na próxima etapa, os resultados de reputação e aprimoramento são revisados para cada 8 registros.
15. Continue revisando as próximas etapas:
    a. Atualizar registro de incidente de segurança: Atualiza o registro de incidente de segurança para indicar que as atividades de pesquisa e aprimoramento de reputação foram concluídas.
    b. Obter observáveis da tarefa: Recupera todos os observáveis mal-intencionados associados ao incidente de segurança.
    c. Criar tarefa: Verifica e confirma se as execuções de triagem automatizada foram bem-sucedidas.
16. Se houver observáveis que foram sinalizados como mal-intencionados:
    a. Atualizar registro de incidente de segurança: Publique uma anotação de trabalho indicando que uma ameaça foi detectada.
    b. Criar consulta de entrada a partir de observáveis: Se mais de dez observáveis tiverem sido sinalizados como mal-intencionados, o subfluxo Pesquisa de vistas em observáveis (no Splunk ou Carbon Black) será executado.
17. Se os observáveis não forem sinalizados como mal-intencionados, o fluxo continuará com as seguintes etapas:
    a. Atualizar registro de incidente de segurança: Publique uma anotação de trabalho indicando que nenhuma ameaça foi detectada
    b. Obter observáveis da tarefa: Identifica todos os IDs de hash SHA256 do incidente.
    c. Pesquisar registros observáveis: Pesquisa registros que atendem a estes critérios.
18. Continue revisando as próximas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para cada observável mal-intencionado, o. **Palo Alto Networks de operações de segurança - Obtenha aprimoramento de dados Wildfire** o fluxo de trabalho é executado.

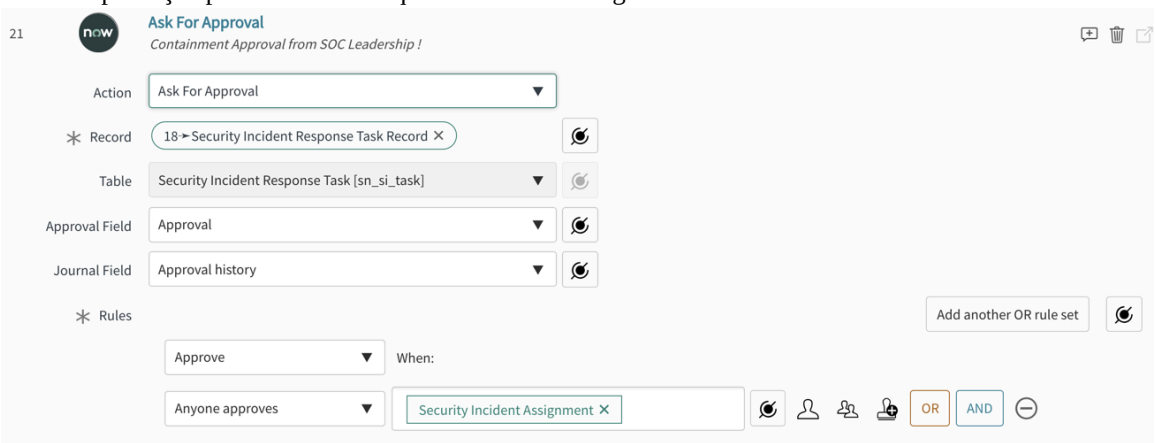
b. Revisa os resultados da investigação para ver se eles são satisfatórios.
Uma tarefa de resposta é criada para verificar se o malware suspeito é um ataque de ransomware. Em caso afirmativo, o subfluxo do Playbook do ransomware será executado.

c. Na próxima etapa, um e-mail é enviado com um resumo da análise e uma solicitação de aprovação para iniciar os procedimentos de contenção.

d. Uma tarefa é criada para capturar detalhes da aprovação solicitada.

e. A próxima etapa é atualizar o registro de incidente de segurança.
Publique uma anotação de trabalho informando ao analista de segurança que a solicitação de aprovação foi feita.

f. Solicita aprovação para conter os ataques de malware do gerente do SOC.



Nota: Quando uma solicitação de aprovação for gerada pelo fluxo, a anotação de trabalho será atualizada com a seguinte mensagem:

Uma solicitação de aprovação foi feita para o <task id> prosseguir com contenção.
Para aprovar esta tarefa, como gerente de SOC, siga estas etapas manualmente:

- Navegue até a página Aprovações de tarefa.
- Você verá a lista de aprovações. Clique no <task id> que será aprovado.
- Estado para **Aprovar** E Salve o <task id> atualizado.

g. Na próxima etapa, o registro de incidente de segurança é atualizado para rastrear o status de aprovação.

h. Em seguida, uma tarefa é criada para iniciar procedimentos de contenção.

i. O subfluxo Executar solicitações de bloco para observáveis mal-intencionados é executado e um registro de incidente é criado com uma solicitação para recriar o dispositivo infectado e seus ativos.

j. Em seguida, uma tarefa é criada para executar a pesquisa de vistas para confirmar se o ambiente é seguro.
A pesquisa de avistamentos é repetida até que nenhuma vista seja encontrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

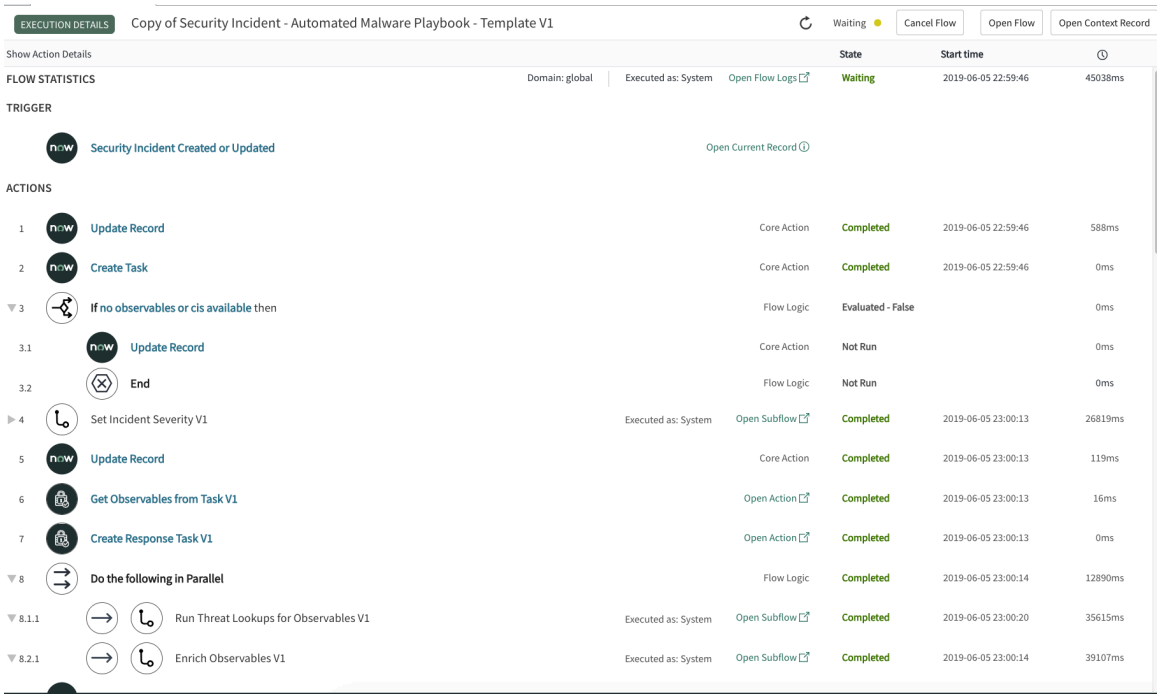
k. Em seguida, uma tarefa é criada para indicar que o registro de incidente de segurança está pronto para revisão.

l. Por fim, o registro é atualizado e movido para a fase Revisão.

O que Fazer Depois

Você pode clicar em **Teste** simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.



Playbook para falha de login manual

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado.

Essas tentativas de login malsucedidas podem ser falsos positivos ou tentativas feitas por invasores para obter acesso às contas de e-mail do usuário. Nesses cenários, o playbook Manual de login com falha pode fornecer orientação e ajudar a otimizar a investigação de incidentes de segurança de login com falha.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

Spoke: Instalar o spoke de operações de segurança (sn_sec_spoke)

Capacidades-chave

O playbook de login com falha abrange os seguintes recursos para investigar incidentes de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Verifica se o usuário afetado é um usuário ativo/inativo
2. Observáveis da lista de filtros permitidos
3. Enriquece os observáveis
4. Executa pesquisa automatizada de ameaças.
5. Envia e-mail automatizado ao usuário para confirmar a falha na tentativa de login.
6. Atribui tarefas ao analista para investigar o acesso do usuário
7. Identifica observáveis mal-intencionados e bloqueia IPs e URLs.
8. Redefine a senha do usuário.
9. Atualiza o status do incidente de segurança
10. Atribui tarefas a um analista de segurança para lidar com a revisão pós-incidente.

Capacidades necessárias

- Pesquisa de ameaças (total de vírus, análise híbrida)
- Aprimoramento observável (Whois, ReverseWhois)
- Pesquisa de vistas (Splunk, QRadar)
- Bloqueio de observável (ponto de verificação, Palo Alto)

Para obter mais informações, consulte ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças de segurança passo a passo, consulte Resolva ameaças à segurança com o playbook.

Uso do playbook de login com falha com recursos do Flow Designer

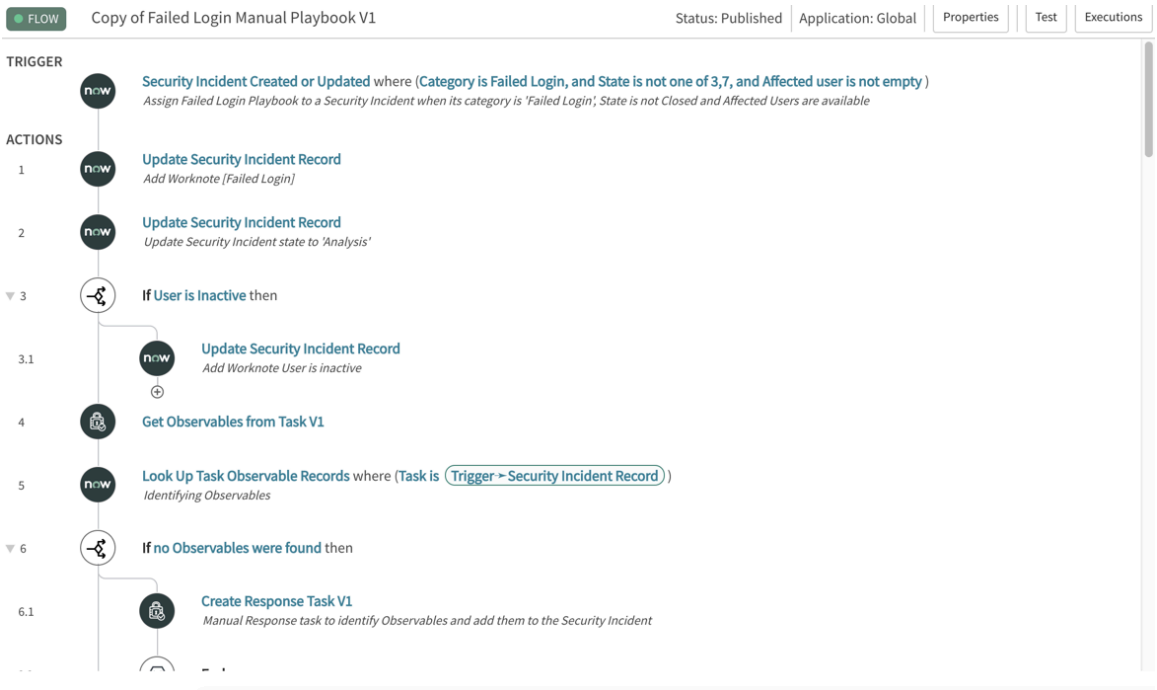
Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** e clique em **Login com falha** playbook.
3. Faça uma cópia dos seguintes fluxos para copiar o Playbook de login com falha e fazer as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
   - Playbook V1 manual com falha de login
   - Falha no login - Analisar a resposta do usuário e atualizar a tarefa de resposta V1
4. Faça as modificações necessárias de acordo com sua exigência. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
5. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative os fluxos copiados depois de fazer modificações de acordo com seus requisitos.

A imagem a seguir mostra uma cópia do playbook Manual de login com falha. Revise as etapas abaixo para entender as várias ações no playbook.

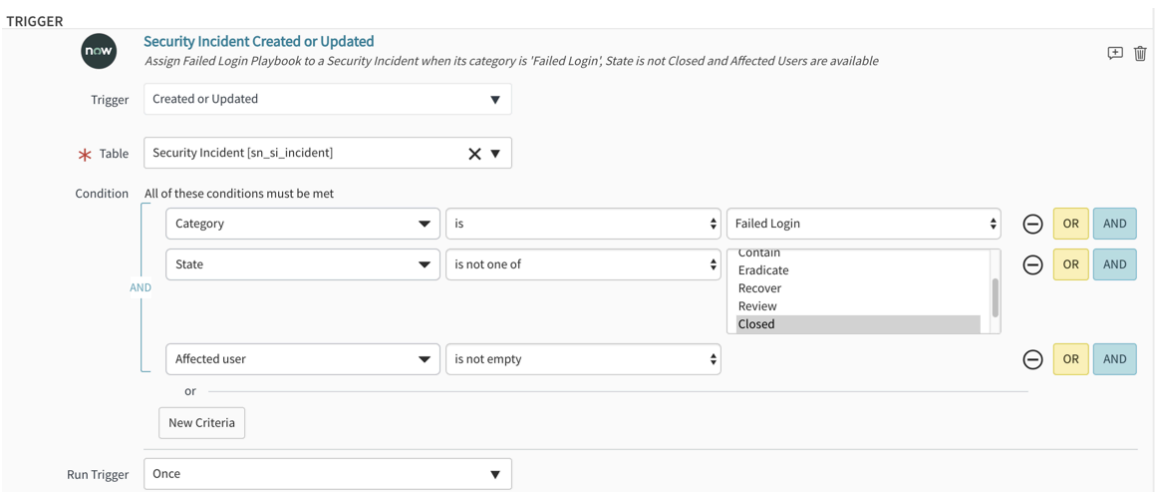
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- A categoria é Falha no login
- Tem um ou mais usuários afetados
- O incidente de segurança não foi encerrado ou cancelado

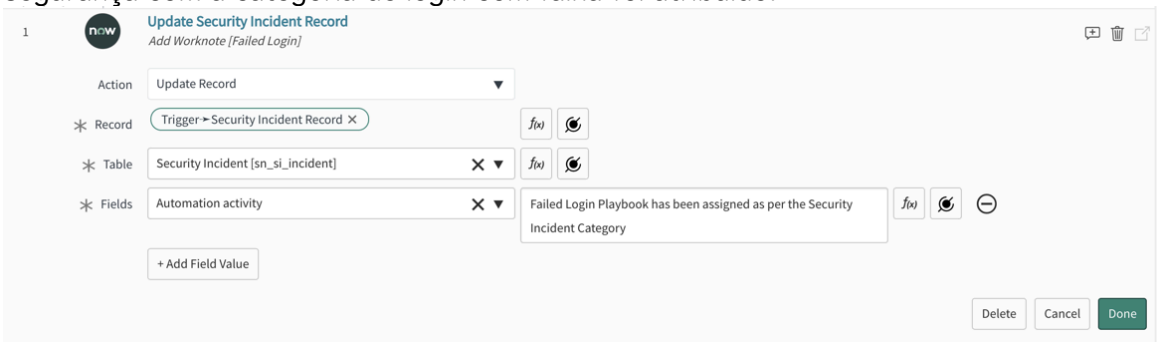


As etapas a seguir orientam você pelas ações, tarefas e subfluxos que estão disponíveis no playbook Manual de login com falha.

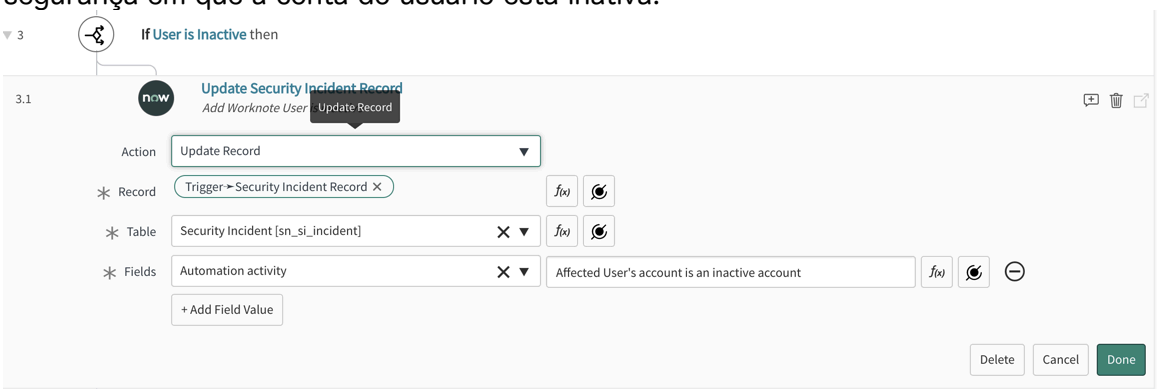
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Quando o playbook começa a ser executado, na Etapa 1, o playbook é atualizado automaticamente com uma anotação de trabalho mostrando que o incidente de segurança com a categoria de login com falha foi atribuído.



2. Na Etapa 2, o playbook é atualizado e movido para o estado Análise.
3. Na Etapa 3, o playbook verifica se o usuário afetado é um usuário ativo ou inativo. Se o usuário estiver inativo, uma anotação de trabalho será adicionada ao incidente de segurança em que a conta do usuário está inativa.



Nota: Na etapa 3 do fluxo, o fluxo verifica usuários inativos no `sn_si_incident` tabela disponível em ServiceNow. Esta etapa é fornecida como uma diretriz e deve ser modificada para o seu ambiente específico. Se você quiser usar essa funcionalidade, recomendamos que você tenha uma integração do Active Directory configurada em seu ambiente. Você pode verificar com sua integração do Active Directory para encontrar o status do usuário e, dependendo da resposta, você pode projetar as próximas etapas para seu playbook.

Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para que o analista de segurança trabalhe com a equipe DE TI para bloquear o usuário e prosseguir com o restante das etapas no playbook.

4. Na Etapa 4, os observáveis do incidente de segurança são recuperados.
5. Na Etapa 5, os observáveis são identificados.
6. Se nenhum observável for encontrado, uma tarefa de resposta manual será criada na Etapa 6 e o fluxo será encerrado.

Tradução automática

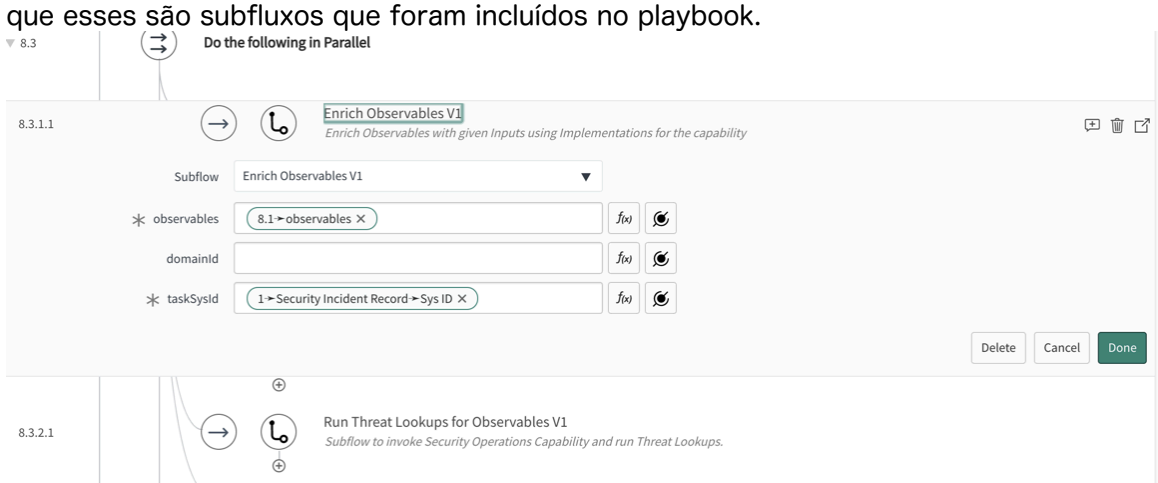
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Se observáveis forem encontrados na Etapa 7, a lista de observáveis que não são permitidos será identificada.
8. Se pelo menos um dos observáveis da lista não for permitido, as seguintes etapas serão executadas:
   a. As etapas 8,1 e 8,2 são executadas. Os observáveis são recuperados e uma tarefa de resposta automatizada é iniciada.

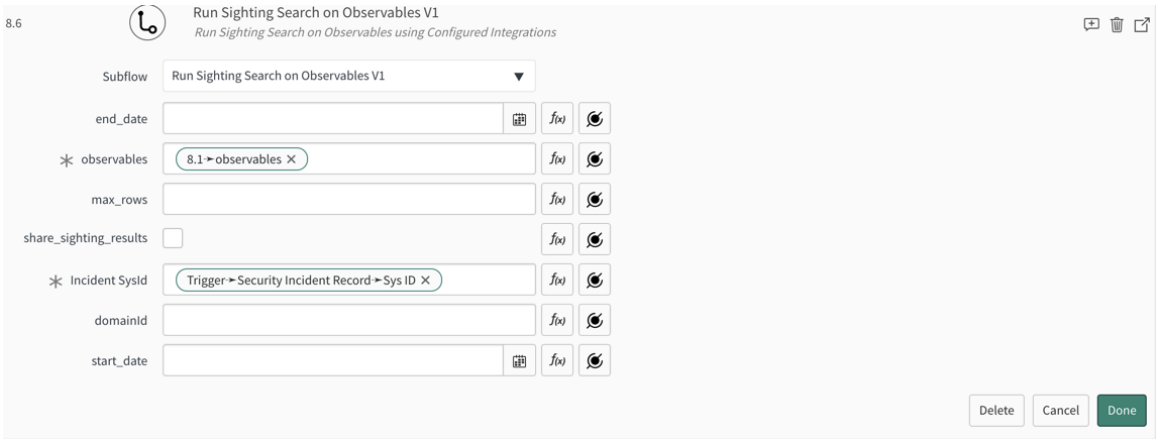


   b. Depois que a tarefa automatizada é criada, a Etapa 8,3 (8.3.1.1 e 8,3.2,1) é executada e as integrações Enrich observables e Pesquisa de ameaças são executadas. Observe que esses são subfluxos que foram incluídos no playbook.



   c. Na Etapa 8,4, depois que as integrações foram concluídas, o registro de incidente de segurança é atualizado.
   d. Na Etapa 8,5, uma nova tarefa de resposta é criada para indicar a próxima tarefa automatizada que ocorrerá.
   e. Na Etapa 8,6, a integração da Pesquisa de vistas será executada nos observáveis.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Após a conclusão do subfluxo de Pesquisa de vistas, na Etapa 8,7, o incidente de segurança é atualizado.

g. Na Etapa 8,8, os observáveis são verificados para ver se são mal-intencionados.

h. Se os observáveis não forem mal-intencionados e a conta do usuário estiver ativa, um e-mail automatizado será enviado ao usuário para reconfirmar as tentativas de login malsucedidas. Uma tarefa de resposta manual é criada para identificar os observáveis e adicioná-los ao incidente de segurança. O playbook termina nesta fase.

i. Se os observáveis forem mal-intencionados, três tarefas de resposta serão criadas:

  i. Um e-mail automatizado é enviado ao usuário para confirmar **(Sim ou Não)** tentativas de login malsucedidas. Se o usuário responder Sim:

    1. O status do incidente de segurança é atualizado para **Conter** .

    2. Um e-mail automatizado é enviado ao usuário para redefinir a senha.

    3. O subfluxo Redefinir senha é iniciado e um e-mail é enviado ao usuário quando a tarefa é concluída.

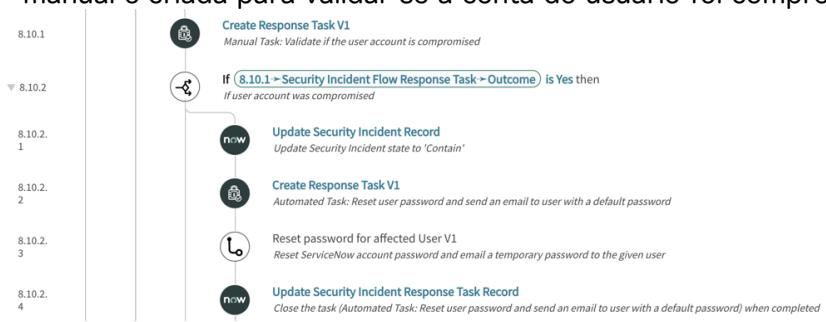
> **Nota:** A etapa Redefinir senha é fornecida como uma diretriz. As etapas no fluxo redefinem a senha da conta do usuário no sistema ServiceNow. Mas o processo para redefinir a senha pode ser diferente dependendo do seu ambiente. Você pode verificar com sua integração do Active Directory para redefinir a senha dos usuários automaticamente. Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para que o analista de segurança trabalhe com a respectiva equipe de TI para redefinir a senha dos usuários e prosseguir com o restante das etapas no playbook, após concluir a respectiva tarefa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ii. Se o usuário responder Não, um e-mail automatizado será enviado ao usuário para reconfirmar a resposta. O analista de segurança precisa executar manualmente as ações apropriadas.

iii. Se o usuário não responder ao e-mail automatizado, o analista de segurança deverá atualizar o incidente de segurança manualmente e fornecer uma resposta. Uma tarefa manual é criada para validar se a conta do usuário foi comprometida.



9. Na Etapa 8.10.3, o estado do incidente de segurança é atualizado.

10. Na Etapa 8.10.4, uma tarefa automatizada é criada para verificar se a implementação do recurso Criar solicitações de bloqueio para IPs e URLs mal-intencionados está disponível. Se a implementação de capacidade estiver disponível, o subfluxo Criar solicitações de bloco será executado. Se isso não estiver disponível, o incidente de segurança será atualizado e uma anotação de trabalho será publicada para indicar que a implementação da capacidade não está disponível.

11. Na Etapa 9, o incidente de segurança é atualizado e o estado é definido como **Revisão** .

12. Na Etapa 10, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para Automação de incidentes de segurança secundários

Os incidentes de segurança duplicados são categorizados como incidentes de segurança secundários e são acumulados nos incidentes de segurança primários.

O playbook de Automação de incidentes de segurança secundário ajuda a reduzir o tempo necessário para investigar e fechar incidentes de segurança duplicados. Este playbook acumula automaticamente artefatos exclusivos específicos do incidente de segurança secundário (observáveis, usuários afetados, ICs) para o incidente de segurança primário.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

Spoke: Instalar o spoke de operações de segurança (sn_sec_spoke)

Capacidades-chave

O playbook de automação secundária abrange os seguintes recursos:

1. Move o incidente de segurança para **Análise** fase.

2. Elimina duplicatas e adiciona (acumula) os usuários e ICs afetados ao incidente de segurança primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adiciona observáveis do incidente secundário ao incidente de segurança primário.
4. Fecha ou cancela o incidente de segurança secundário quando o incidente de segurança primário é encerrado.

Capacidades necessárias

Para obter mais informações, consulte ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças de segurança passo a passo, consulte Resolva ameaças à segurança com o playbook.

Compreensão mais profunda do playbook de Automação de incidentes de segurança secundários com recursos do Flow Designer

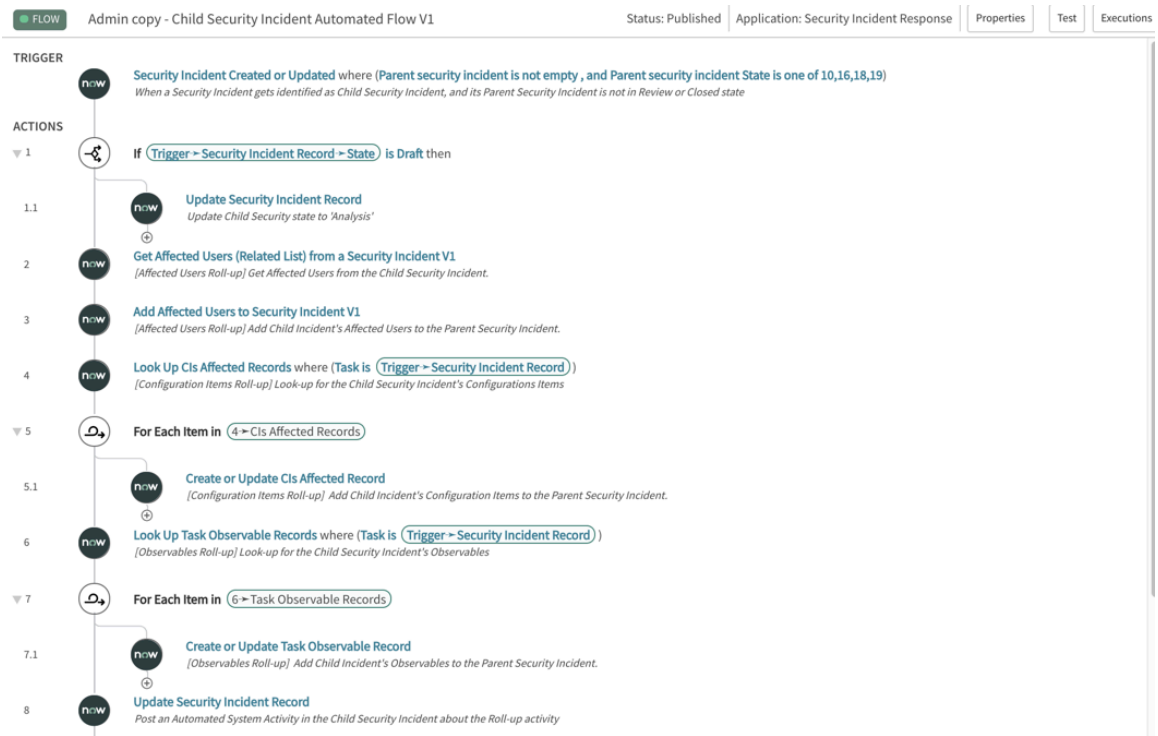
Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** E clique no playbook Login com falha.
3. Faça uma cópia do playbook Automação de incidentes de segurança secundários e faça as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
4. Faça as modificações necessárias de acordo com sua exigência. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
5. Ative o playbook.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative o fluxo copiado depois de fazer modificações de acordo com seus requisitos.

A imagem a seguir mostra uma cópia do playbook Automação de incidentes de segurança secundários. Revise as etapas abaixo para entender as várias ações no playbook.

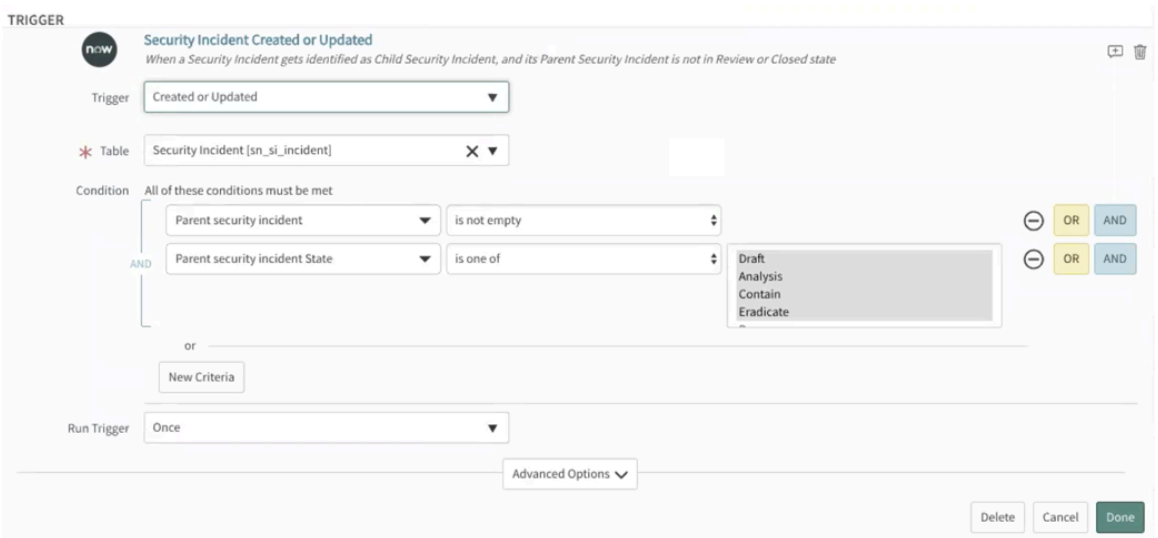
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este playbook é acionado quando:

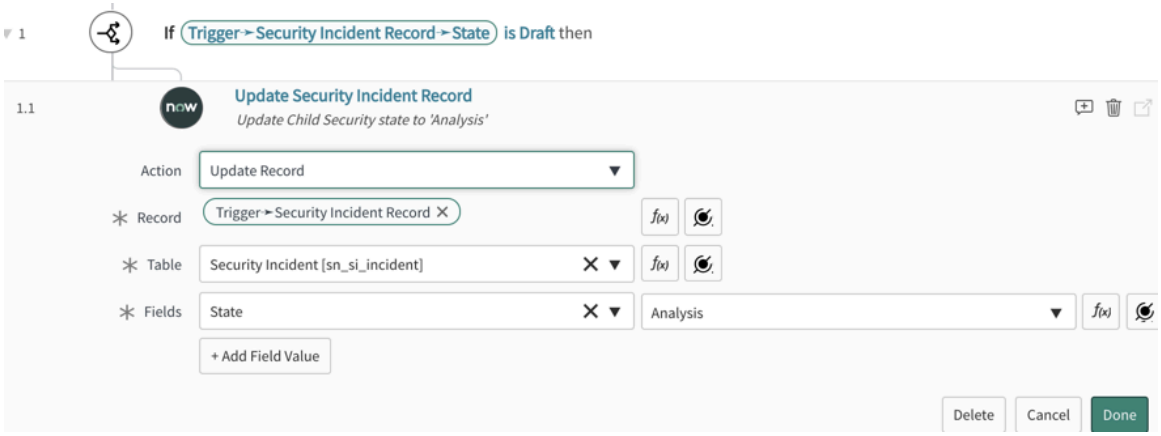
- O campo de incidente de segurança primário não está vazio.
- O incidente de segurança primário está no estado Rascunho, Análise, Conter ou Erradicar.



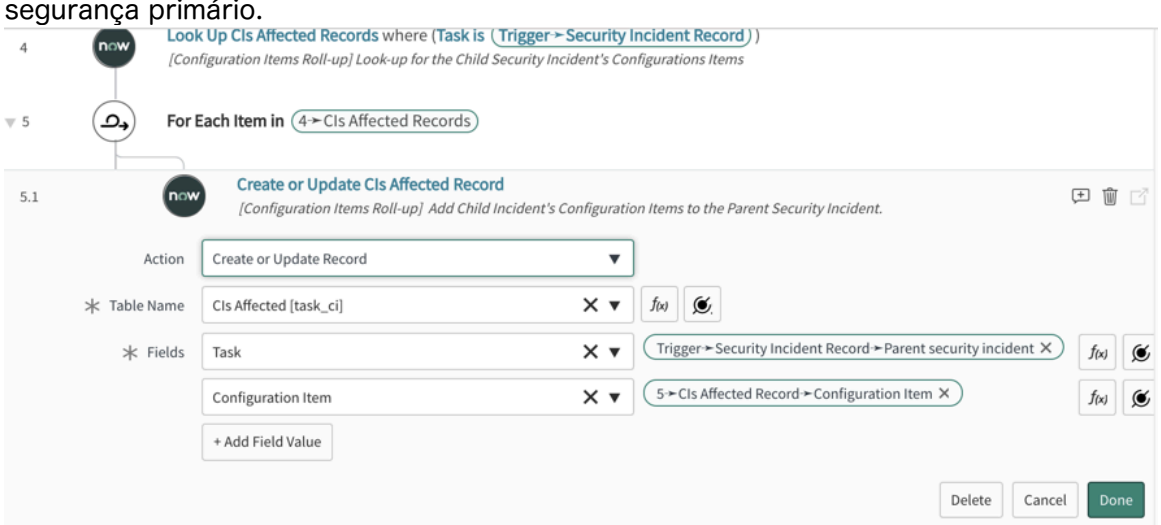
As etapas a seguir orientam você pelas ações e tarefas que estão disponíveis no playbook Automação de incidentes de segurança secundários.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

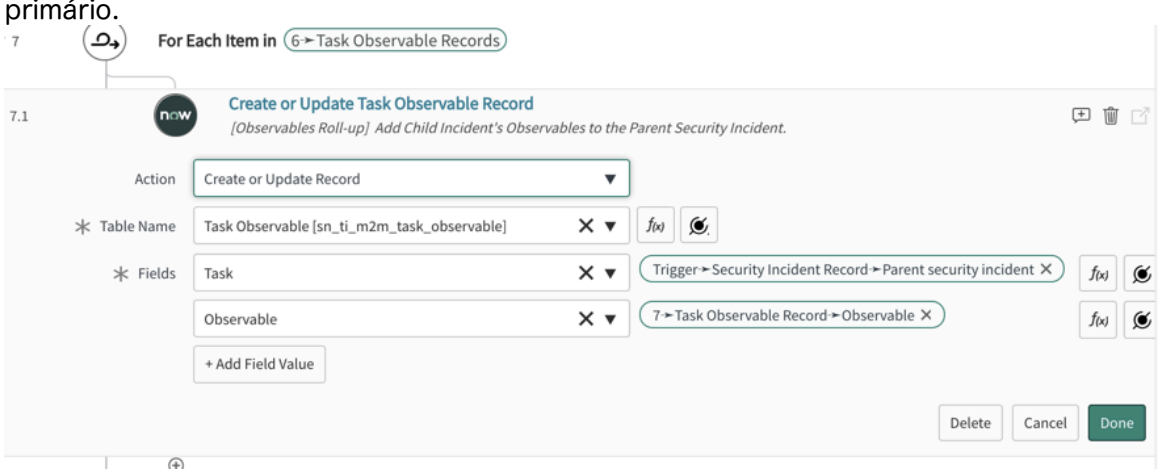
1. Quando o playbook começa a ser executado, na Etapa 1, se o incidente de segurança estiver no estado Rascunho, ele será atualizado e definido como o estado Análise.



2. Nas etapas 2 e 3, os usuários afetados pelo incidente de segurança são recuperados e acumulados no incidente de segurança primário. Todos os usuários duplicados são eliminados.
3. Nas etapas 4 e 5, os itens de configuração associados ao incidente de segurança secundário são recuperados e ICs exclusivos são acumulados para o incidente de segurança primário.



4. Nas etapas 6 e 7, observáveis associados ao incidente de segurança secundário são recuperados e observáveis exclusivos são acumulados para o incidente de segurança primário.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Nas etapas 8 e 9, anotações de trabalho automatizadas são publicadas nos incidentes de segurança primários e secundários, indicando que os usuários afetados, os itens de configuração e os observáveis foram acumulados do incidente de segurança secundário para o primário.

Playbook para Office 365 - Arquivo mal-intencionado detectado

Este playbook fornece etapas de correção sistemáticas para investigar arquivos mal-intencionados detectados no Office 365.

Quando arquivos mal-intencionados são detectados no Office 365, você pode usar o playbook 365 - Arquivo mal-intencionado detectado no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos mal-intencionados.

Configure o playbook Arquivo malicioso do Office detectado

Use as etapas a seguir para configurar o playbook Arquivo malicioso detectado do Office.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Office 365 - Arquivo mal-intencionado detectado** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook Office 365 - Arquivo mal-intencionado detectado e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique em  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

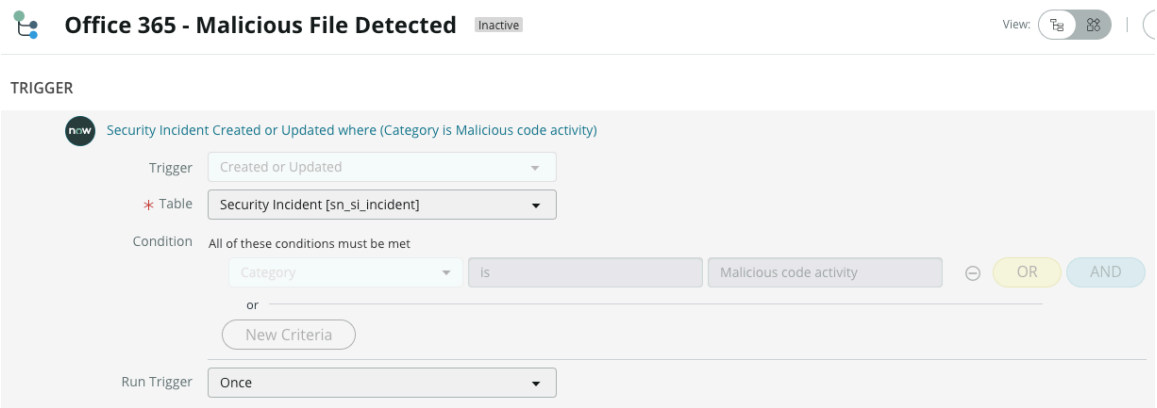


4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Atividade de código mal-intencionado** .



Use o playbook Arquivo mal-intencionado detectado do Office 365

Use este playbook para investigar arquivos mal-intencionados detectados no Office 365. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Arquivo mal-intencionado detectado do Office 365.

Antes de Iniciar

Função necessária:

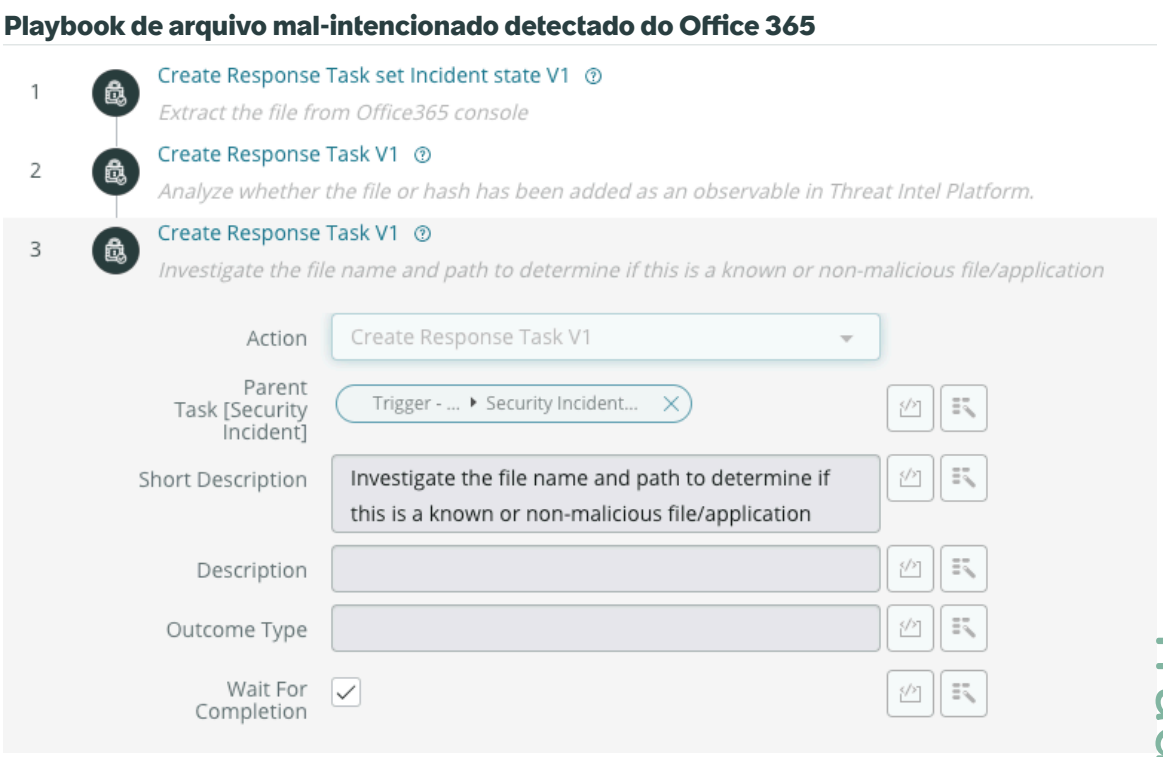
- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa extrair o arquivo mal-intencionado do console do Office 365.
2. Na Ação 2, você precisa analisar se o arquivo ou hash foi adicionado como observável na Plataforma Intel de ameaças.
3. Na Ação 3, você precisa investigar o nome e o caminho do arquivo para determinar se ele é um arquivo/aplicação conhecido ou não malicioso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na Ação 4, você precisa enviar o arquivo para a Sandbox para analisar os resultados.
5. Na Ação 5, com base na investigação feita até o momento, você precisa verificar se o arquivo ou hash é malicioso ou não.
   Se o arquivo ou hash não for mal-intencionado, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
6. Na Ação 6, se o arquivo ou hash for malicioso, as ações 7 e 8 serão executadas.
7. Na Ação 7, você precisa entrar em contato com o usuário final para obter uma justificativa comercial válida sobre o motivo pelo qual ele tem um arquivo mal-intencionado no dispositivo.
   Se o arquivo ou hash for mal-intencionado, você poderá usar o Modelo de e-mail preexistente no playbook para enviar e-mail ao usuário final solicitando esclarecimentos.
8. Na Ação 8, você precisa verificar se o usuário final forneceu uma justificativa comercial válida ou não.
   Se o usuário final fornecer uma justificativa comercial válida, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
9. Na Ação 9, se o usuário não forneceu uma justificativa comercial válida, as ações 10, 11 e 12 serão executadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Na Ação 10, como não havia justificativa comercial válida, você pode encaminhar o arquivo mal-intencionado ou hash para a Equipe da Intel de ameaças para revisão.
11. Na Ação 11, você precisa executar o script do scanner de Bytes de malware para verificar se o arquivo ou hash é malicioso.
12. Na Ação 12, você precisa executar uma Análise Forense para verificar se o arquivo ou hash é malicioso.
13. Na Ação 13, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de repetição

Este playbook ajuda a determinar se a resposta do incidente foi fornecida em um relatório de phishing exato ou semelhante no passado e funciona automaticamente no novo relatório de forma semelhante.

O playbook de detecção de repetição verifica se o incidente de phishing relatado recentemente se assemelha a um incidente passado. Quando a detecção de repetição é identificada, o incidente de segurança correspondente e os detalhes da resolução são fornecidos ao analista, que pode usá-lo no incidente recém-relatado, resultando em uma correção rápida do incidente de segurança.

Configure o playbook de detecção de repetição

Use as etapas a seguir para configurar o playbook de detecção de repetição.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (`sn_sec_spoke`). Você tem uma opção para modificar as seguintes propriedades do sistema:

- `sn_sec_spoke.similarphish.earlyterminationscore`
- `sn_sec_spoke.similarphish.lookbackdays`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- `sn_sec_spoke.similarphish.maxcomparissize`
- `sn_sec_spoke.similarphish.minmatchscore`

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Detecção de repetição** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique em  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

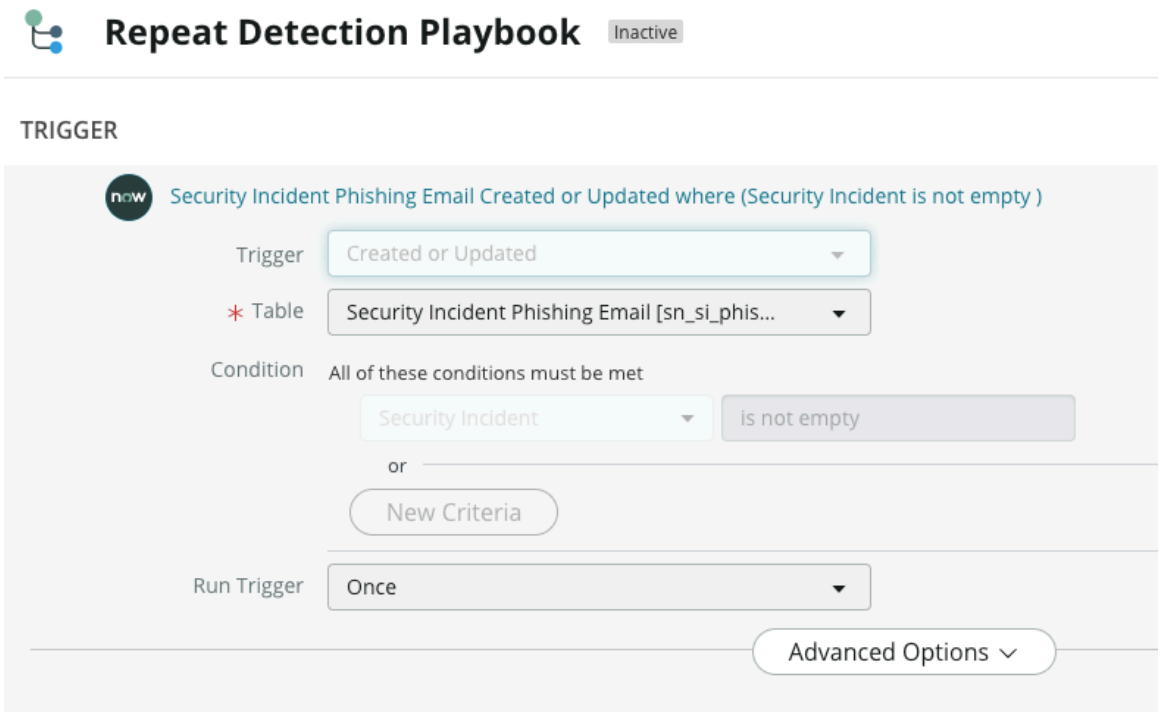


4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado quando **Incidente de segurança não está vazio** .



Use o playbook de detecção de repetição

Use este playbook para investigar se a resposta do incidente foi fornecida em um relatório de phishing exato ou semelhante no passado e funciona automaticamente no novo relatório de forma semelhante. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de repetição.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

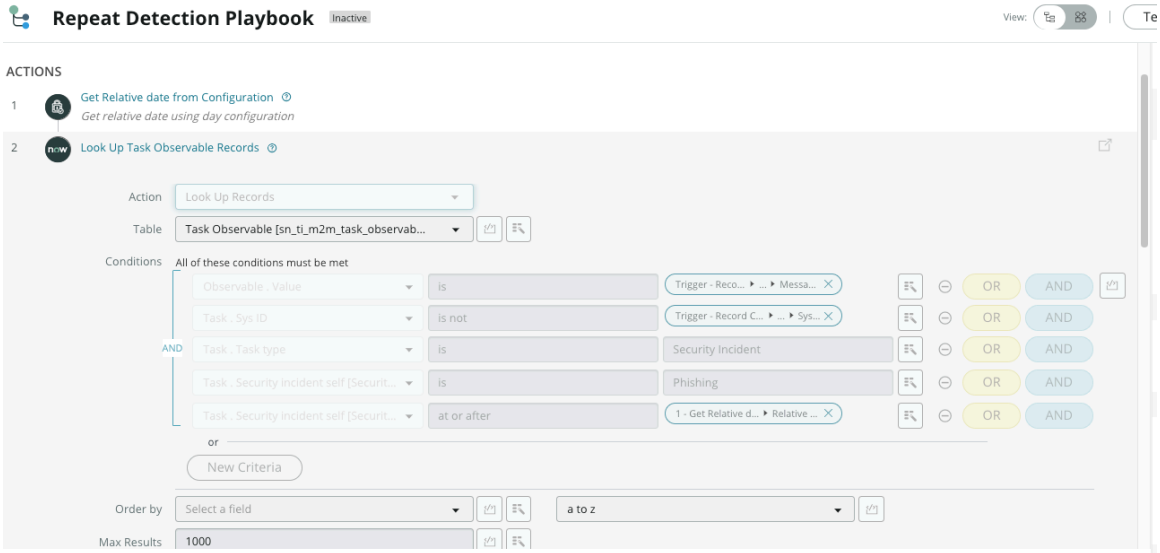
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, o playbook recupera a data relativa do incidente de segurança usando a configuração do dia.
2. Na Ação 2, o playbook pesquisa os registros do Observável de tarefa na tabela `sn_ti_m2m_task_observable` Que correspondem ao incidente com base no ID da mensagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

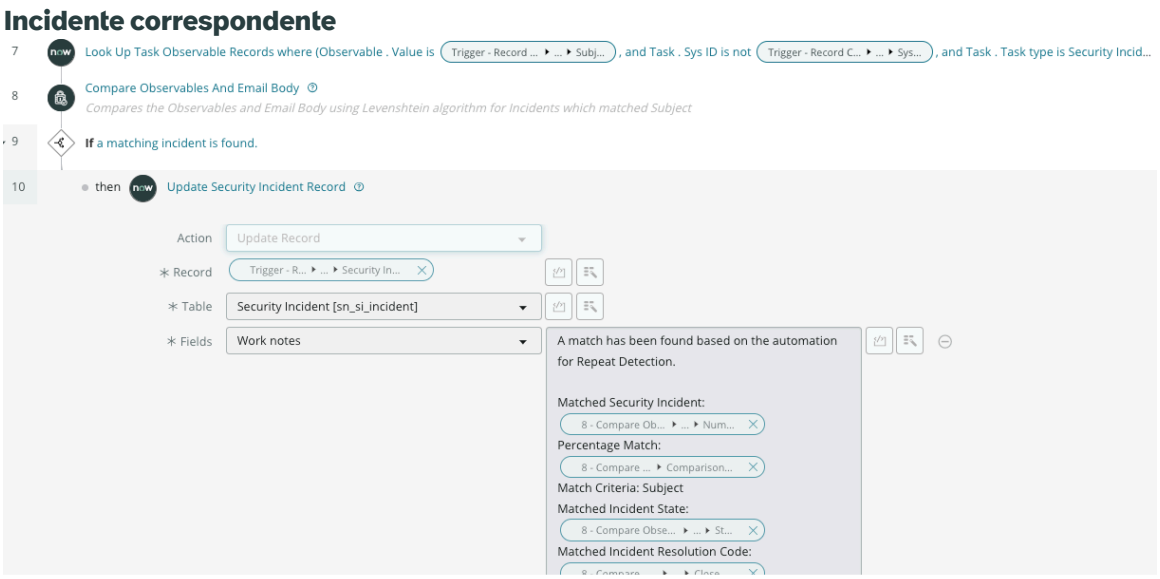
Playbook de detecção de repetição



3. Na Ação 3, o playbook compara os observáveis de tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que corresponderam ao ID da mensagem.
4. Na Ação 4, com base na investigação feita até o momento, o playbook verifica se o incidente correspondente foi encontrado com base no ID da mensagem ou não.
   Na Ação 5, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho em que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 6, o fluxo termina.
5. Se o incidente correspondente não for encontrado, na Ação 7, o playbook pesquisará os registros do Observável de tarefa na tabela `sn_ti_m2m_task_observable` Que correspondem ao incidente com base no assunto.
6. Na Ação 8, o playbook compara os Observáveis de tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao assunto.
7. Na Ação 9, o playbook verifica se o incidente correspondente foi encontrado ou não.
   Na Ação 10, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho em que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 11, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Na Ação 12, o playbook pesquisa os registros do Observável de tarefa na tabela `sn_ti_m2m_task_observable` Que correspondem ao incidente com base no endereço.
9. Na Ação 13, o playbook compara os observáveis de tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao endereço.
10. Na Ação 14, o playbook verifica se o incidente correspondente foi encontrado com base no endereço ou não. Na Ação 15, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho em que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 16, o fluxo termina.

Playbook para e-mails falsificados (usando o mesmo nome de exibição)

Este playbook fornece etapas de correção sistemáticas para investigar e-mails falsificados, que são acionados quando nomes falsificados de e-mails são enviados para os funcionários da organização.

Configure o playbook de e-mails falsificados

Use as etapas a seguir para configurar o playbook de e-mails falsificados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

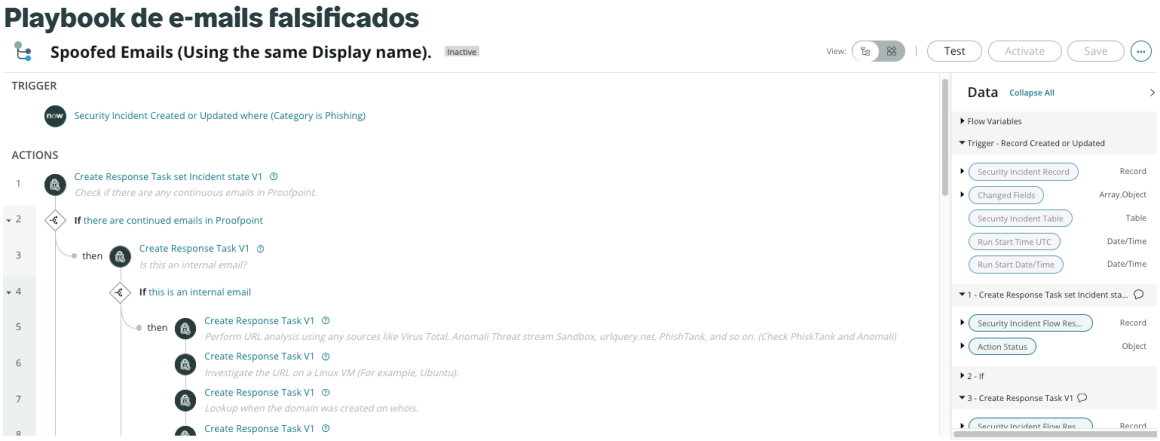
Certifique-se de ter instalado o spoke do Security Operations (`sn_sec_spoke`).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **E-mails falsificados (usando o mesmo nome de exibição)** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias.

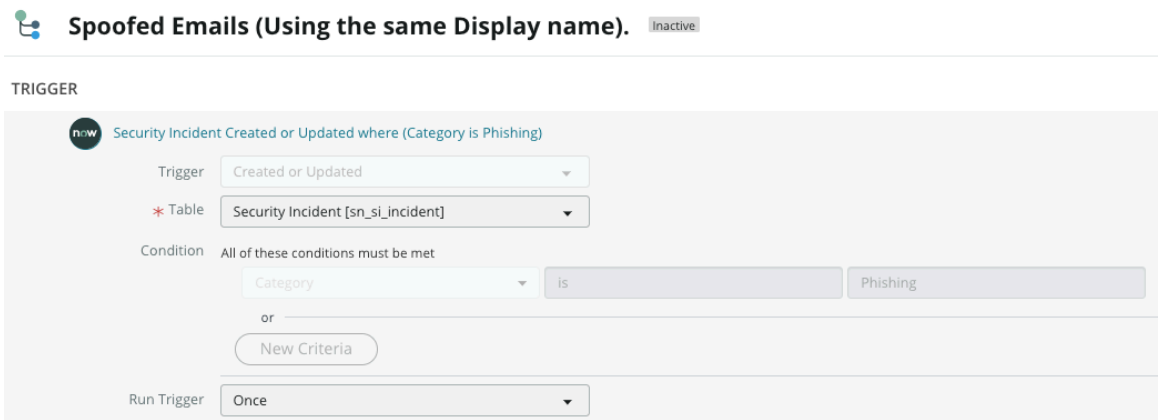
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar uma cópia do fluxo do playbook, clique em  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Phishing** .



Use o playbook de E-mails falsificados (usando o mesmo nome de exibição)

Use este playbook para investigar e-mails falsificados, que são acionados quando nomes falsificados de e-mails são enviados para os funcionários da organização. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de e-mails falsificados (usando o mesmo nome de exibição).

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

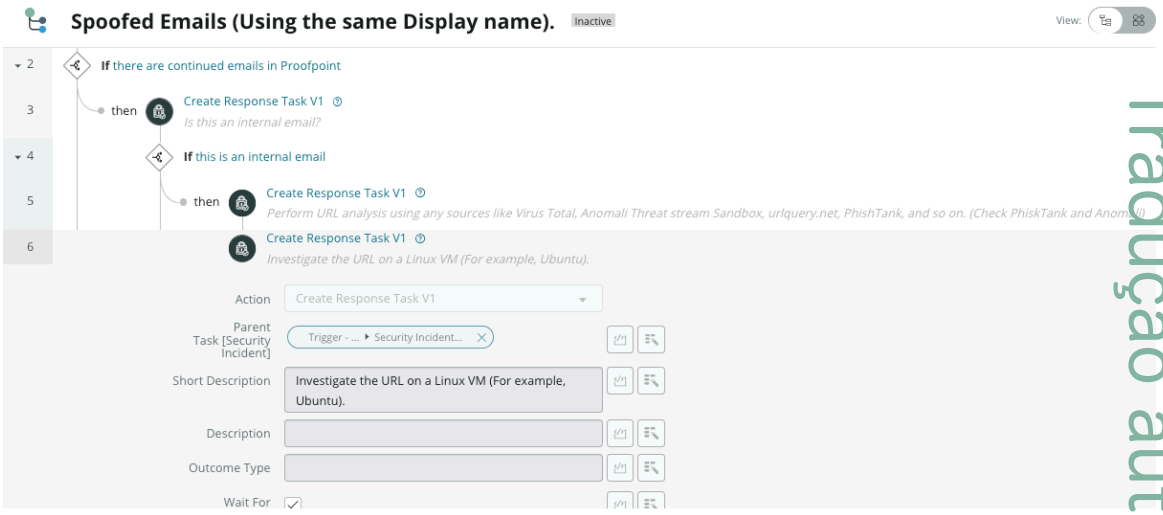
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se há e-mails falsificados contínuos no Proofpoint.
2. Na Ação 2, se houver e-mails contínuos no Proofpoint, verifique se este é um e-mail falsificado interno ou não.
3. Na Ação 3, se este for um e-mail falsificado interno, execute as seguintes ações:

   a. Na Ação 5, você precisa executar a análise de URL usando fontes como Total de vírus, Área restrita de fluxo de ameaças Anomali, urlquery.net, PhishTank (por exemplo, verifique PhiskTank e Anomali).

   b. Na Ação 6, você precisa investigar o URL em uma VM Linux (por exemplo, Ubuntu).

Playbook de e-mails falsificados (usando o mesmo nome de exibição)



   c. Na Ação 7, você precisa pesquisar quando o domínio foi criado no WHOIS.
   Procure domínios registrados recentemente (na última semana) que sejam suspeitos e tenham uma alta probabilidade de ataques de phishing.

   d. Na Ação 8, com base na investigação feita até o momento, você precisa verificar se este e-mail contém um anexo ou link mal-intencionado.
   Se este e-mail não contiver um anexo ou link mal-intencionado, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na Ação 9, se o e-mail contiver anexos ou links maliciosos, execute as ações a seguir.

i. Na Ação 10, você precisa entrar em contato com o usuário afetado para verificar se as credenciais estão comprometidas. Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário afetado.

ii. Na Ação 11, você precisa verificar se as credenciais estão comprometidas com base na resposta do e-mail. Se as credenciais não foram comprometidas, o fluxo será encerrado.

1. Na Ação 12, se as credenciais estiverem comprometidas, na Ação 13, você precisará verificar se usuários adicionais foram afetados. Se nenhum usuário adicional for afetado, o fluxo será encerrado.

2. Na Ação 14, se usuários adicionais forem afetados, execute as seguintes ações:

a. Na Ação 15, você precisa pesquisar e excluir e-mails usando o Microsoft Exchange Online.

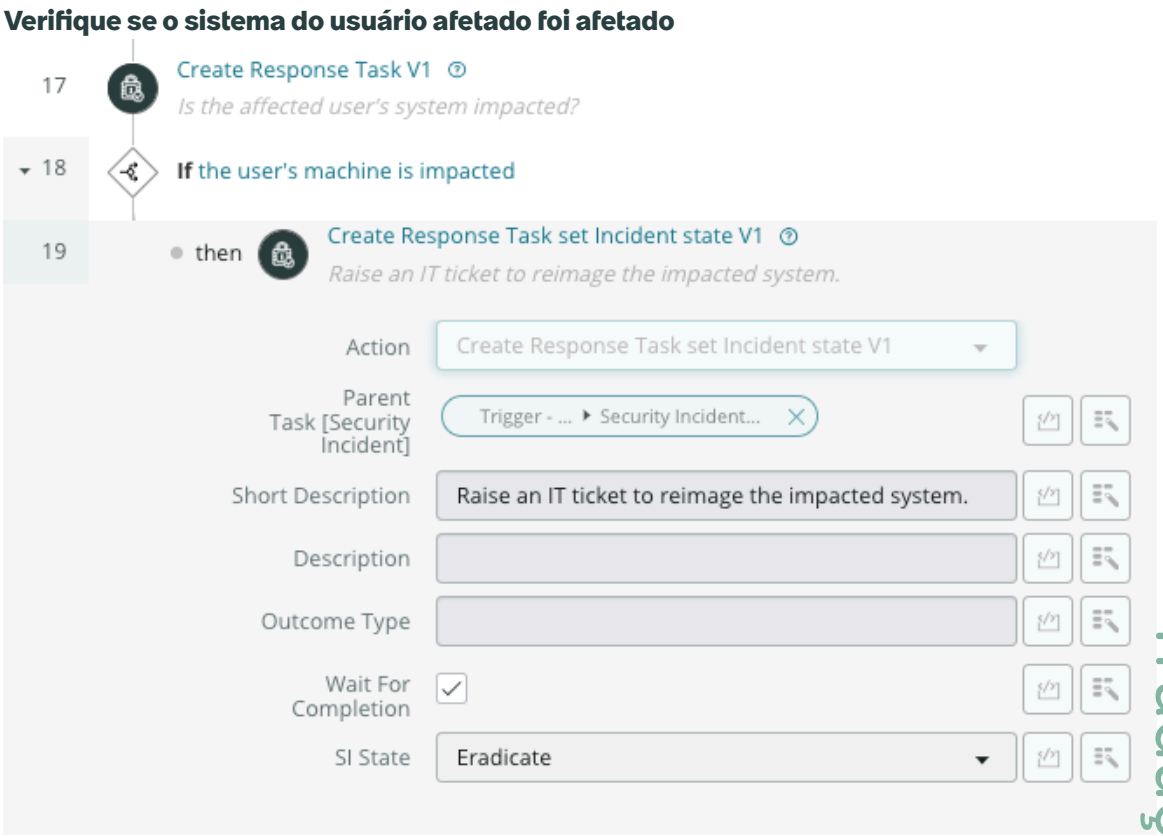
b. Na Ação 16, você precisa bloquear o remetente e os arquivos ou anexos maliciosos no Office 365 e no Proofpoint.

4. Na Ação 17, se este não for um e-mail falsificado interno, você precisará verificar se o sistema do usuário afetado foi afetado.

5. Na Ação 18, se o sistema do usuário for afetado, na Ação 19, gere um tíquete DE TI para recriar a imagem do sistema afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na Ação 20, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de endpoint

Este playbook fornece etapas de correção sistemáticas para investigar alertas de malware acionados em um host ou endpoint (por exemplo, uma detecção de arquivo mal-intencionado).

Quando os alertas do CrowdStrike são acionados em um host ou endpoint, você pode usar o playbook de detecção de endpoint no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos maliciosos.

Configure o playbook de detecção de endpoint

Use as etapas a seguir para configurar o playbook de detecção de endpoint.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

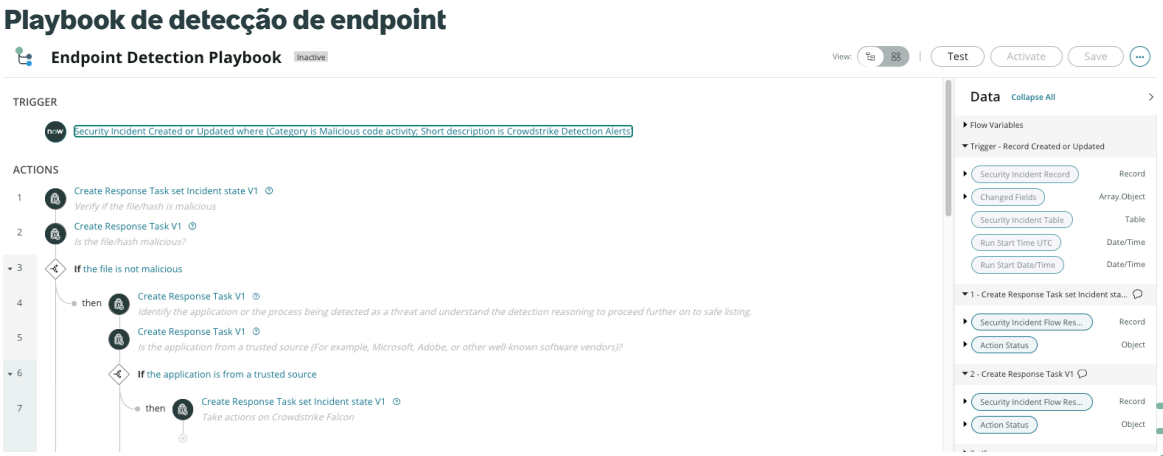
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Detecção de endpoint** playbook.

Tradução automática

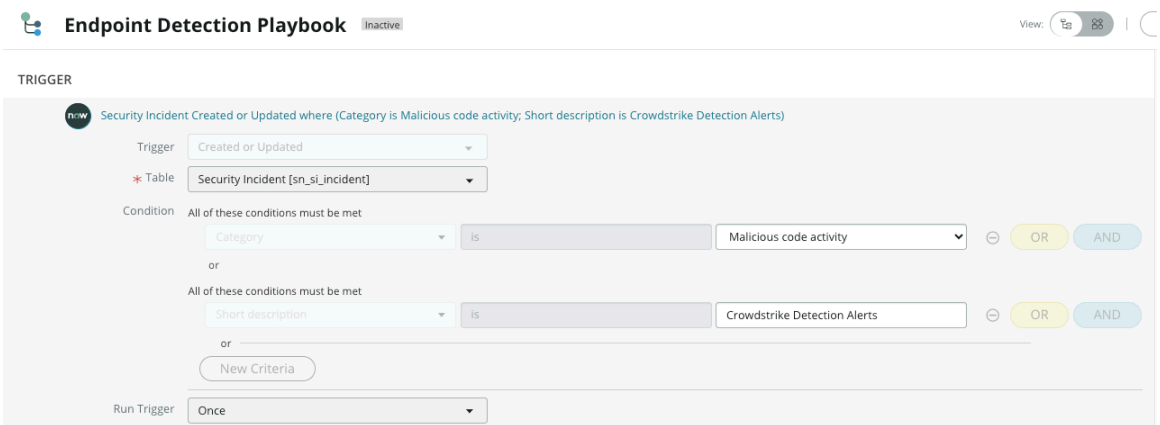
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. **Opcional:** Você pode criar uma cópia do fluxo do playbook de detecção de endpoint e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique em ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:
   - **Categoria** . **Atividade de código mal-intencionado** .
   - **Descrição resumida** . **Alertas de detecção do CrowdStrike** .



Use o playbook de detecção de endpoint

Use este playbook para investigar alertas de malware acionados em um host ou endpoint. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de endpoint.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se o arquivo ou hash é mal-intencionado analisando os resultados da pesquisa de ameaças no SIR e coletando informações do VirusTotal, Wildfire, ThreatCrowd etc.
2. Na Ação 2, você precisa verificar se o arquivo ou hash é malicioso ou não.
3. Na Ação 3, se o arquivo ou hash for mal-intencionado, execute as seguintes ações:

   a. Na Ação 4, você precisa identificar a aplicação ou o processo que está sendo detectado como uma ameaça e coletar informações sobre o raciocínio de detecção para prosseguir para a listagem segura.

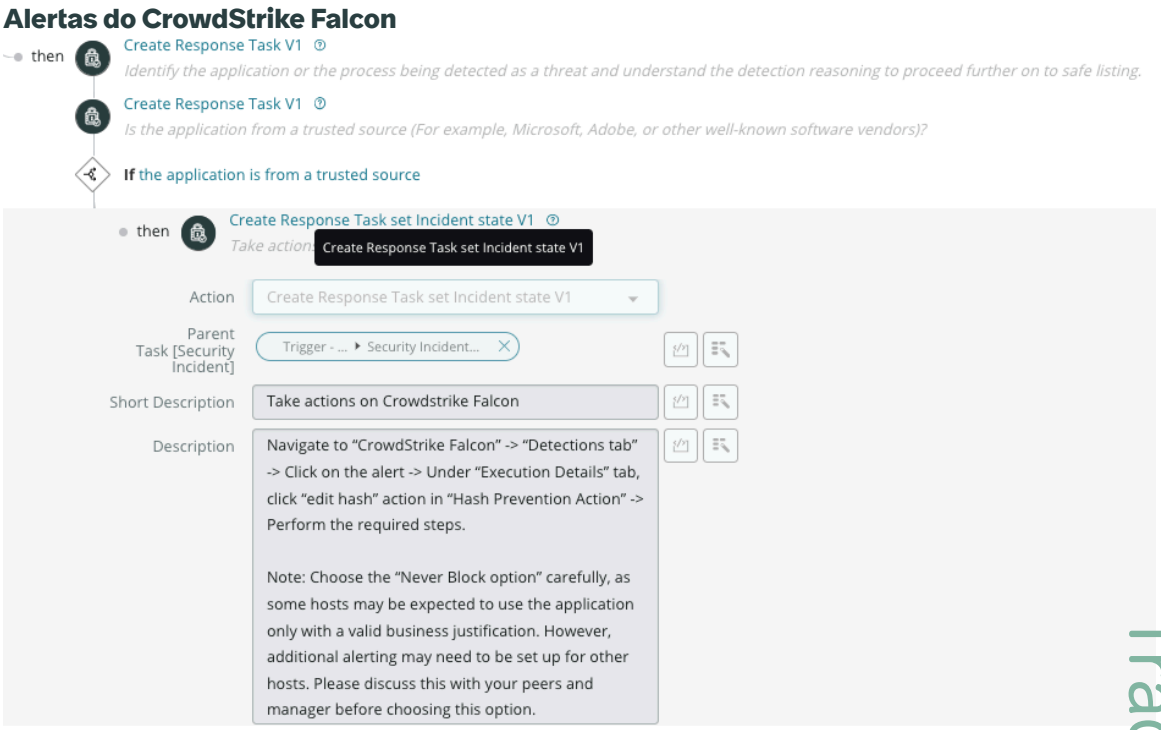


   b. Na Ação 5, você precisa verificar se a aplicação é de uma fonte confiável (por exemplo, Microsoft, Adobe ou outros fornecedores de software conhecidos).

   c. Na Ação 6, se a aplicação for de uma fonte confiável, você precisará executar uma ação nos alertas do CrowdStrike Falcon.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Na Ação 7, execute as seguintes ações:

i. Navegar até **CrowdStrike Falcon** > **Detecções** guia.

ii. Clique no alerta do CrowdStrike Falcon.

iii. Na guia Detalhes da execução, clique em **Editar hash** Ação na Ação de prevenção de hash.

iv. Execute as etapas necessárias.

> **Nota:** Escolha **Nunca bloquear** opção com cuidado, pois somente determinados hosts podem ter permissão para usar a aplicação com uma justificativa comercial válida. No entanto, alertas adicionais podem precisar ser configurados para outros hosts.

e. Na Ação 8, se a aplicação não for de uma fonte confiável, você precisará escolher se deseja renunciar o arquivo ou a aplicação do dispositivo localmente.
Na Ação 10, se você quiser renunciar o arquivo ou a aplicação do dispositivo localmente, execute as seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Em Ação 11, navegue até **Arquivos em quarentena** e filtre o endpoint pesquisando o nome do dispositivo.

ii. Selecione o arquivo que precisa ser dispensado localmente e clique em **Versão** .

Nota:

- O arquivo ainda é executado neste endpoint específico. No entanto, a detecção e a quarentena continuam acontecendo em todos os outros hosts.
- Para liberar em massa o arquivo de quarentena em vários hosts, selecione o nome e o status do arquivo apropriados. Clique em **Selecione** e selecione **Versão** .

Na Ação 12, se você não quiser renunciar o arquivo ou a aplicação do dispositivo localmente, poderá redirecionar o usuário para o Suporte DE TI para solicitar a instalação das aplicações aprovadas.

4. Na Ação 14, se o arquivo ou hash não for mal-intencionado, execute as seguintes ações:

a. Na Ação 15, você precisa determinar se o arquivo/hash é de alto risco ou baixo risco com base na função do usuário (departamento ou posição que lida com informações confidenciais), no tipo de aplicação (ransomware, rootkit etc.) e no impacto da aplicação (quantos usuários foram afetados).

b. Na Ação 16, se o arquivo for de alto risco, execute as seguintes ações:

i. Na Ação 17, revise os resultados com a Equipe de inteligência contra ameaças.

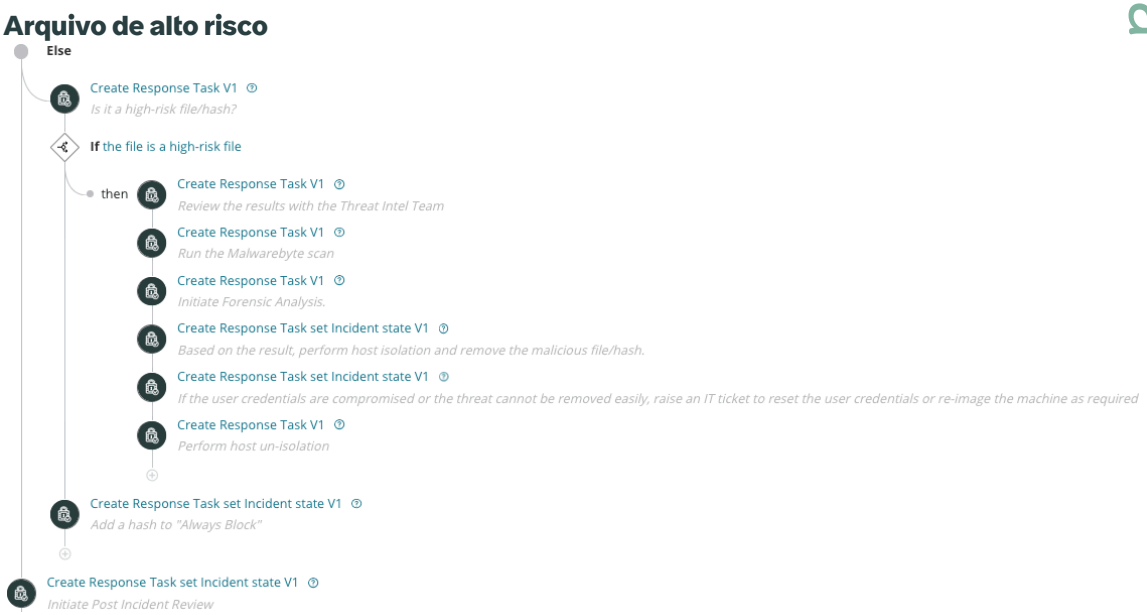
ii. Na Ação 18, execute a verificação de bytes de malware no arquivo.

iii. Na Ação 19, inicie a Análise Forense.

iv. Na Ação 20, com base no resultado da Análise Forense, execute o isolamento do host e remova o arquivo/hash mal-intencionado.

v. Na Ação 21, se as credenciais do usuário estiverem comprometidas ou a ameaça não puder ser removida facilmente, gere um tíquete DE TI para redefinir as credenciais do usuário ou recriar a imagem da máquina conforme necessário.

vi. Em Ação 22, execute o desisolamento do host.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na Ação 23, se o arquivo não for de alto risco, execute as seguintes ações:

i. Navegar até **CrowdStrike Falcon** > **Configurações** guia.

ii. Na guia Configurações, navegue até **Hashes de prevenção** > > **Carregar hash** > **Adicione o hash**.

iii. Escolha o SO necessário e selecione **Bloquear sempre** .

5. Na Ação 24, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para possível spray de senha

Este playbook fornece etapas de correção sistemáticas para investigar alertas de pulverização de senha acionados por vários logins com falha (muitas falhas de autenticação de mais de um endereço IP para o mesmo usuário).

Configure o playbook de spray de senha possível

Use as etapas a seguir para configurar o playbook de spray de senha possível.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

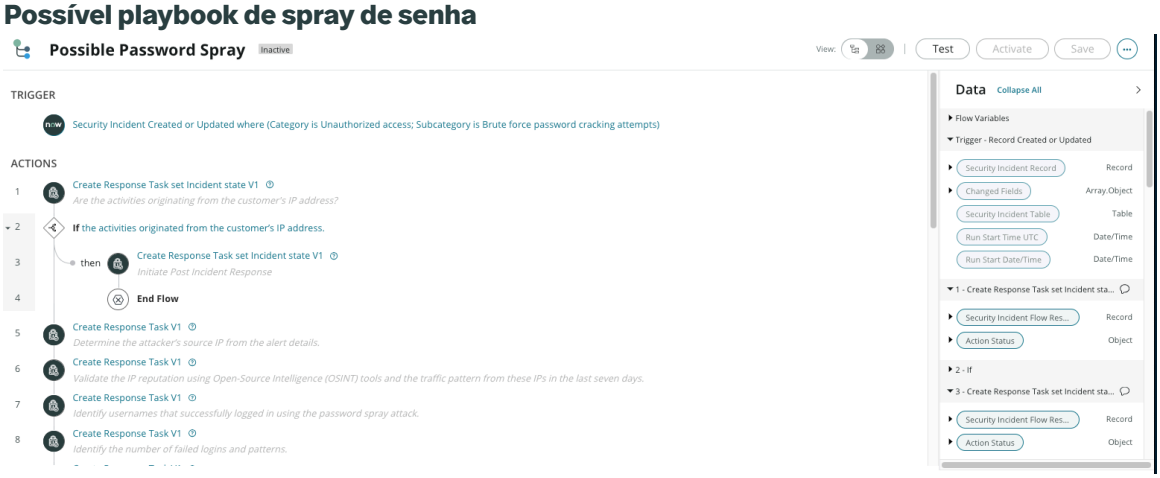
1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Tudo** > **Flow Designer** e selecione **Possível spray de senha** playbook.

3. **Opcional:** Você pode criar uma cópia do possível fluxo do playbook Spray de senha e fazer as modificações necessárias.

Para criar uma cópia do fluxo do playbook, clique em  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

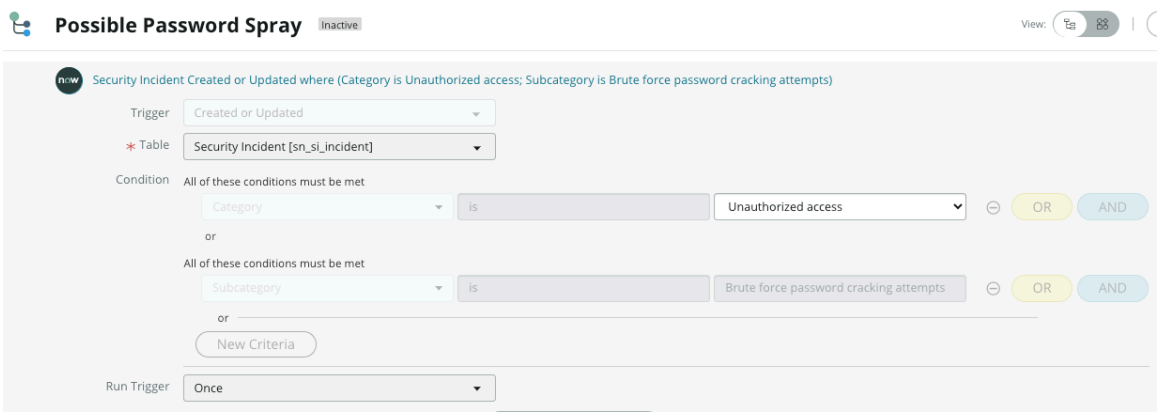
Possível playbook de spray de senha



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:
   - **Categoria** . **Acesso não autorizado** .
   - **Subcategoria** . **Tentativas de quebra de senha por força bruta** .



Possível playbook de spray de senha

Use este playbook para investigar alertas de spray de senha acionados por vários logins com falha (muitas falhas de autenticação de mais de um endereço IP para o mesmo usuário). As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de pulverização de senha possível.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

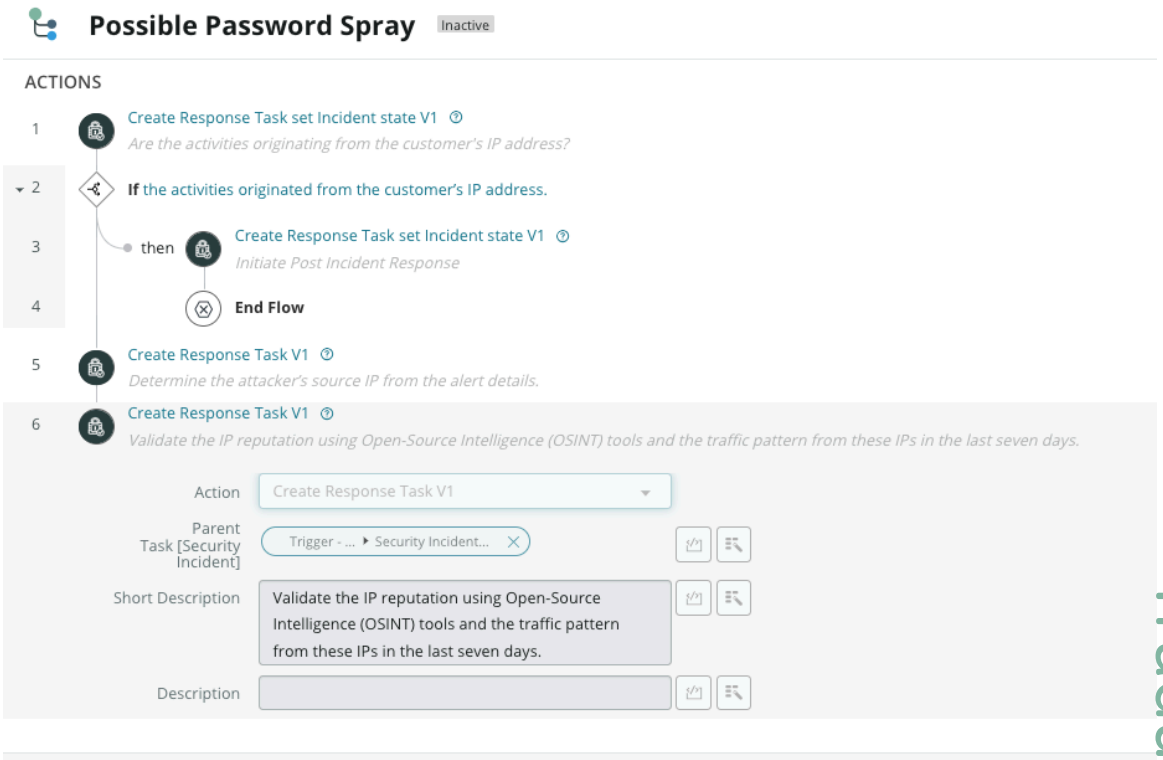
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se as atividades são originadas do endereço IP do cliente.
   Identifique os endereços IP que executam o ataque de pulverização de senha. Por exemplo, use os TXIDs (IDs de transação) do alerta e pesquise-os em relação aos logs F5.
2. Na Ação 2, se as atividades forem originadas do endereço IP do cliente, execute as seguintes ações:
   a. Na Ação 3, você precisa iniciar uma revisão pós-incidente do possível ataque de spray de senha.
   b. Na Ação 4, o fluxo termina.
3. Na Ação 5, se as atividades não forem originadas do endereço IP do cliente, determine o IP de origem do invasor a partir dos detalhes do alerta.
4. Na Ação 6, você precisa validar a reputação de IP usando ferramentas de Inteligência de código aberto (OSINT) e o padrão de tráfego desses IPs nos últimos sete dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Possível playbook de spray de senha



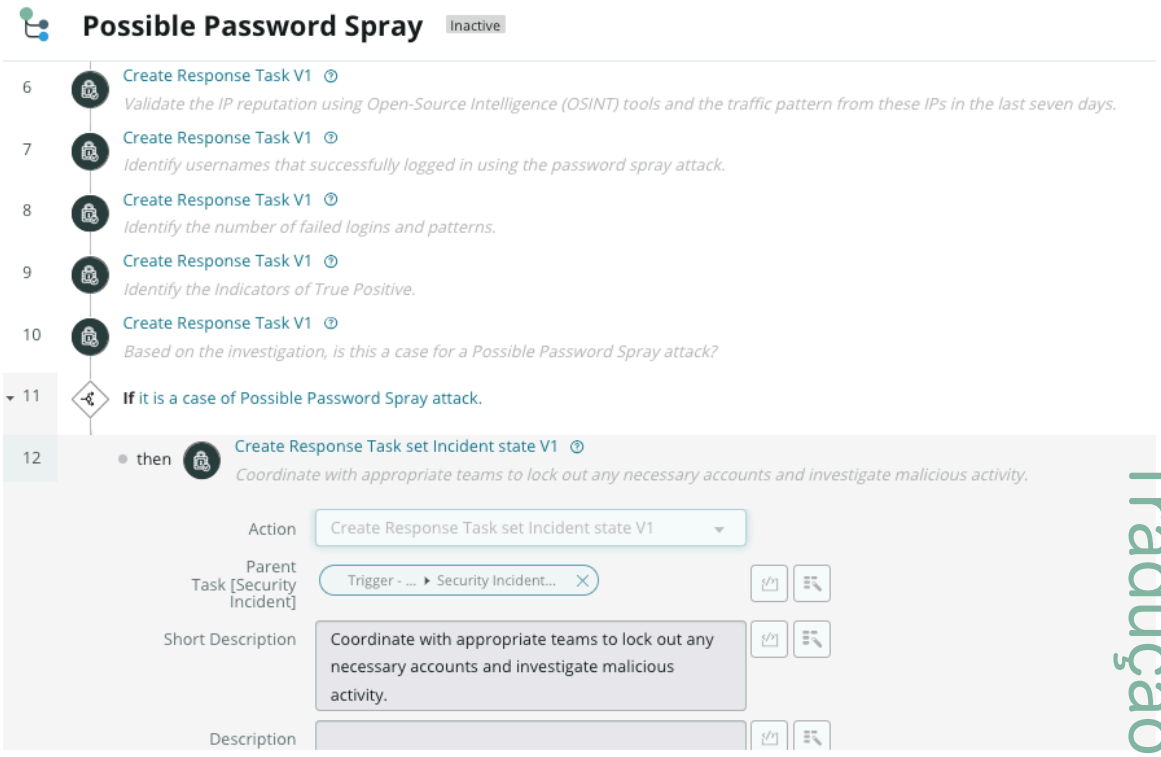
5. Na Ação 7, você precisa identificar os nomes de usuário que fizeram login com sucesso usando o ataque de spray de senha.
6. Na Ação 8, você precisa identificar o número de logins e padrões com falha.
7. Na Ação 9, você precisa identificar os indicadores de verdadeiro positivo.
   - Verifique o tráfego dos IPs de origem nos últimos 60 dias. Nenhum tráfego histórico pode ser uma indicação de um positivo verdadeiro.
   - Verifique os padrões de nome de usuário com falhas de autenticação e a contagem. Quanto maior a contagem, maior a probabilidade de que seja um verdadeiro positivo.
   - O nome de usuário se parece com uma base de dicionário (começando de A a Z) e pode ter nomes de administrador comuns, como admin, sysadmin, root e assim por diante
   - O mesmo nome de usuário pode ter padrões diferentes no ataque de pulverização, assim como o mesmo alerta pode ter falhas para john.doe, johnd, jdoe, john_doe, jdoe7 etc., indicando invasores adivinhando o padrão de nome de usuário com base em casos de uso comuns.
   - Observe o Agente do usuário e os URIs dos logs F5 na etapa acima e veja se os IOCs estão relacionados aos alertas do Red Condor. Se eles corresponderem, então é um evento realmente positivo.
8. Na Ação 10, com base na investigação feita até agora, você precisa verificar se este é um caso de possível ataque de Spray de senha ou não.
9. Na Ação 11, se este for o caso de um possível ataque de spray de senha, execute as seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 12, você precisa coordenar com as equipes apropriadas para bloquear todas as contas necessárias e investigar atividades mal-intencionadas.

Possível playbook de spray de senha



b. Na Ação 13, você precisa iniciar uma revisão pós-incidente do possível ataque de spray de senha.

c. Na Ação 14, o fluxo termina.

10. Na Ação 15, você precisa verificar se este não é um caso de possível ataque de spray de senha.

11. Na Ação 16, se este não for um caso de possível ataque de spray de senha, execute as seguintes ações:

a. Na Ação 17, você precisa documentar as descobertas até o momento.

b. Na Ação 18, você precisa iniciar uma revisão pós-incidente do possível ataque de spray de senha.

c. Na Ação 19, o fluxo termina.

12. Na Ação 20, você precisa consultar os colegas e o gerente do GIR para obter orientação.

13. Na Ação 21, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1003 - Detectar ferramentas de despejo de credenciais

Este playbook fornece etapas de correção sistemáticas para investigar um incidente que envolve atividades de despejo de credenciais.

Configure o playbook T1003 - Detectar ferramentas de despejo de credenciais

Use as etapas a seguir para configurar o playbook T1003 - Detectar ferramentas de despejo de credenciais.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

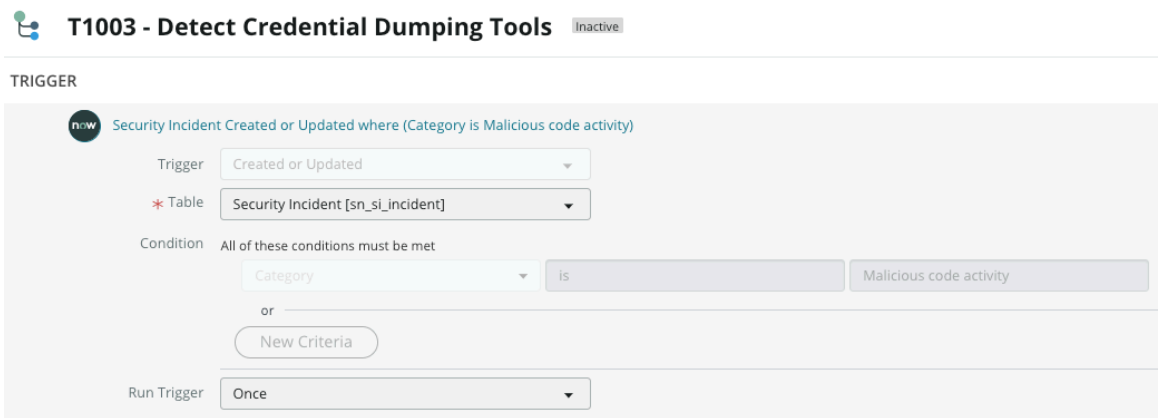
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **T1003 - Detectar ferramentas de despejo de credenciais** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook T1003 - Detectar ferramentas de despejo de credenciais e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique em  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Atividade de código mal-intencionado** .



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o playbook T1003 - Detectar ferramentas de despejo de credenciais

Use este playbook para investigar um incidente que envolve atividades de despejo de credenciais. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Detectar ferramentas de despejo de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

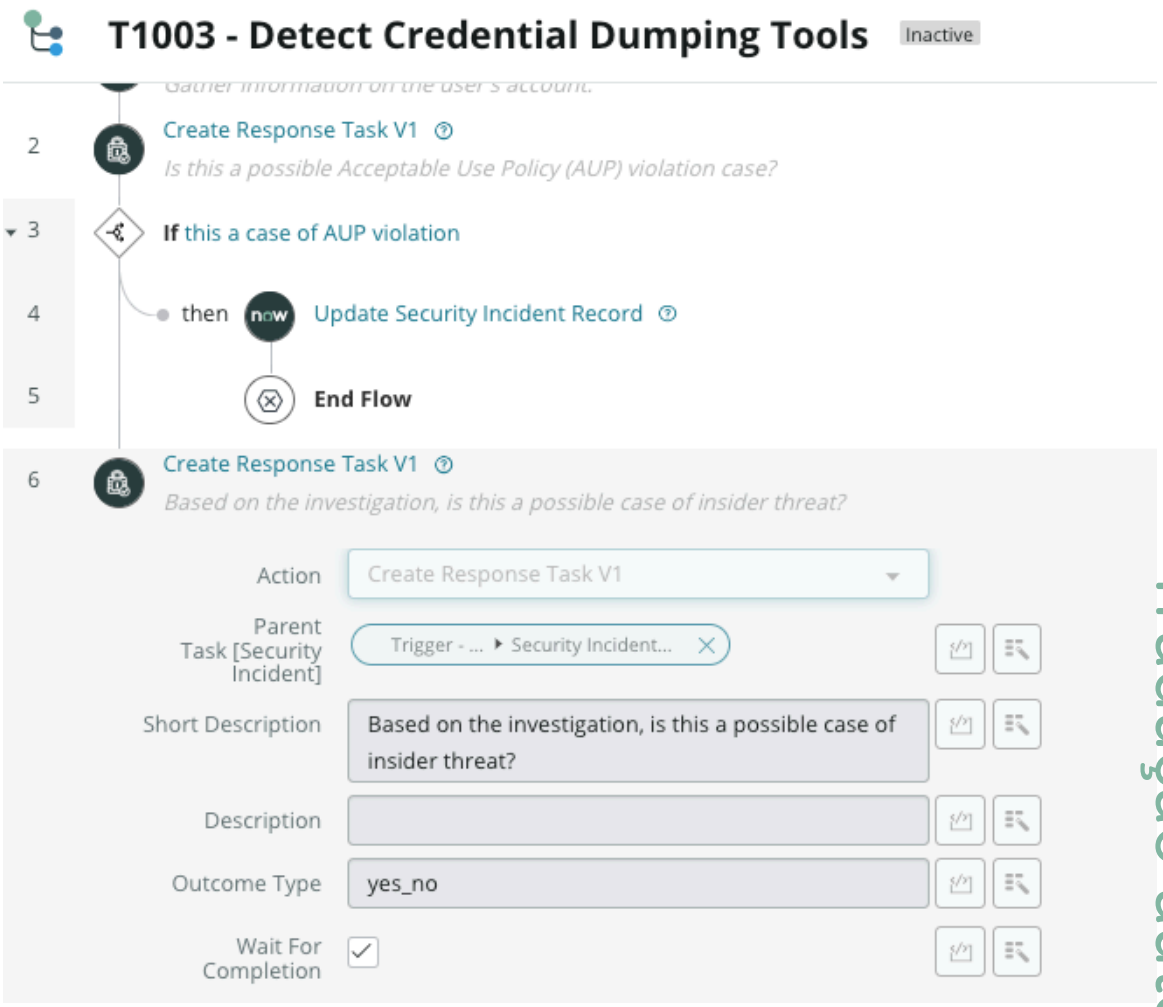
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa coletar informações sobre a conta do usuário.
   - Você precisa verificar a atividade do host para procurar atividades suspeitas.
   - Você precisa identificar o proprietário do Servidor/Endpoint/VM e capturar os dados correlacionados à ferramenta.
   - Você precisa coletar informações sobre as outras contas do usuário.
2. Na Ação 2, você precisa verificar se este é um possível caso de violação da Política de uso aceitável (AUP). Você pode fazer uma revisão por pares com as evidências coletadas e consultar o gerente de incidentes regional para entrar em contato com o usuário.
3. Na Ação 3, se este for um caso de violação da Política de uso aceitável (AUP), execute as seguintes ações:
   a. Na Ação 4, você precisa atualizar o incidente de segurança em que este é um caso de violação de AUP
   b. Na Ação 5, o fluxo termina.
4. Na Ação 6, com base na investigação feita até agora, você precisa verificar se este é um possível caso de ameaça interna ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

T1003 - Playbook Detectar ferramentas de despejo de credenciais



5. Na Ação 7, se este for um caso de ameaça interna, execute as seguintes ações:

a. Na Ação 8, você precisa entrar em contato com o suporte DE TI e solicitar um congelamento de conta.

b. Na Ação 9, você precisa bloquear IPs mal-intencionados.

c. Na Ação 10, você precisa entrar em contato com os funcionários internos por e-mail.
Você pode usar o modelo de e-mail fornecido para entrar em contato com seus funcionários internos.

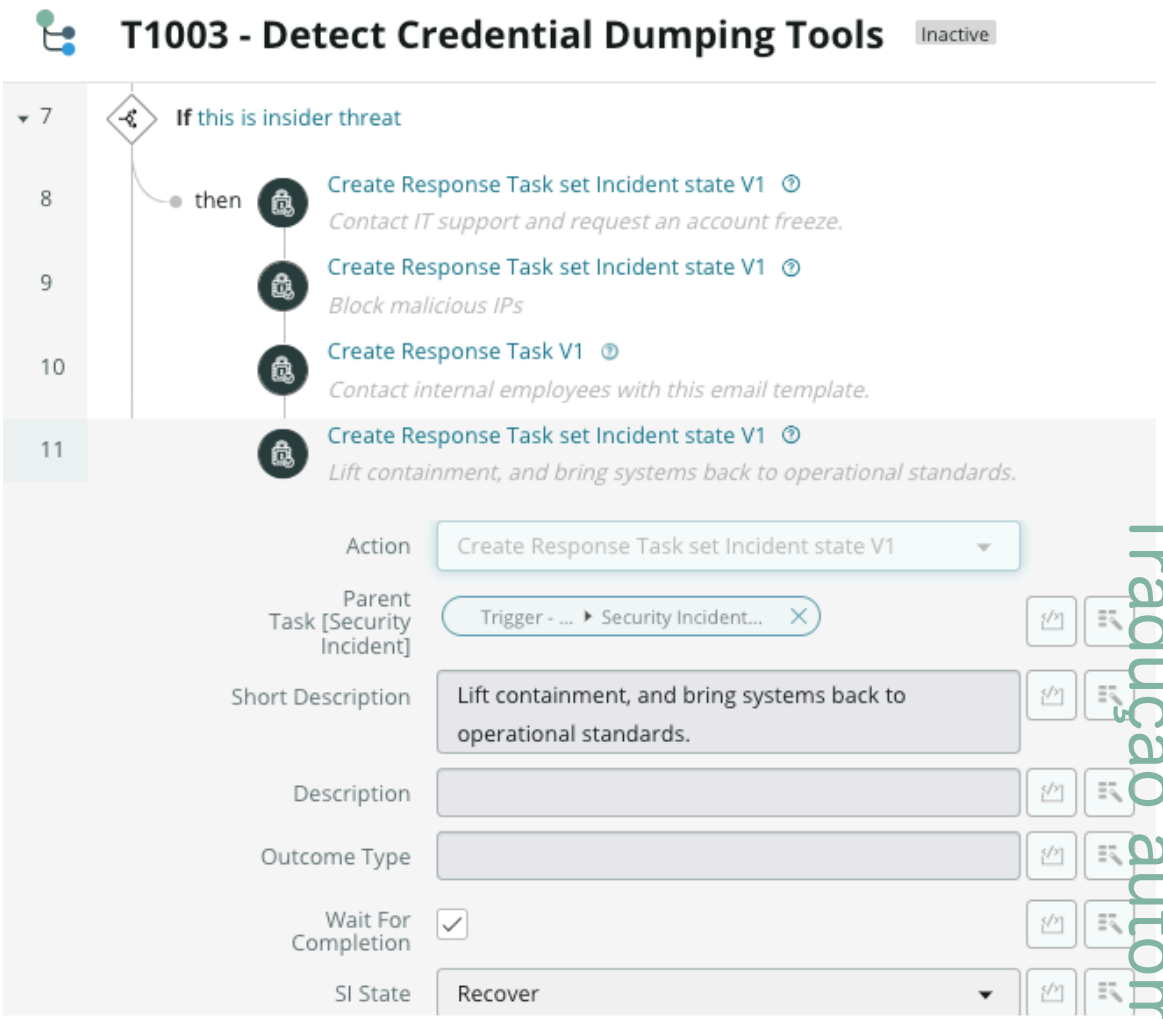
d. Na Ação 11, você precisa levantar a contenção e trazer os sistemas de volta aos padrões operacionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O fluxo termina.

Tarefas de resposta para levantar a contenção



6. Na Ação 12, se este não for um caso de ameaça interna, na Ação 13, você precisará executar uma revisão por pares para determinar se isso precisa ser adicionado à lista de exclusões.
   O fluxo termina.
7. Na Ação 14, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de falsificação de domínio de e-mail

Este playbook ajuda na triagem em fase inicial de envios de phishing relatados pelo usuário, alertando o analista sobre a possibilidade de um domínio semelhante no endereço de e-mail do phisher.

O playbook de detecção de spoofing do domínio de e-mail procura encontrar uma correspondência de semelhança entre o domínio de e-mail do remetente do phisher e um nome de domínio confiável existente no repositório observável. Quando uma correspondência de domínio de e-mail do remetente falsificado é identificada pelo playbook, os analistas são alertados com um marcador.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultados e o fluxo muda a direção com base no resultado de tais tarefas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o playbook de detecção de spoof por e-mail

Use as etapas a seguir para configurar o playbook de detecção de spoof por e-mail.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Playbook de detecção de falsificação de domínio de e-mail** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook de detecção de spoofing no domínio de e-mail e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique em ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

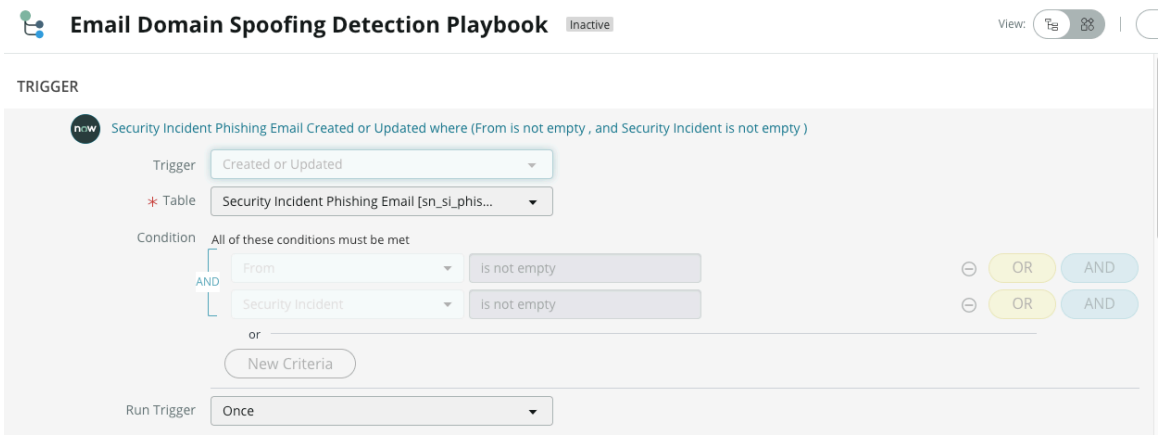
   

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **De** não é **vazio** .
- **Incidente de segurança** não é **vazio** .



Use o playbook de detecção de falsificação de domínio de e-mail

Use este playbook para encontrar uma correspondência de semelhança entre o domínio de e-mail do remetente do phisher com um nome de domínio confiável existente no repositório observável. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de spoofing do domínio de e-mail.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

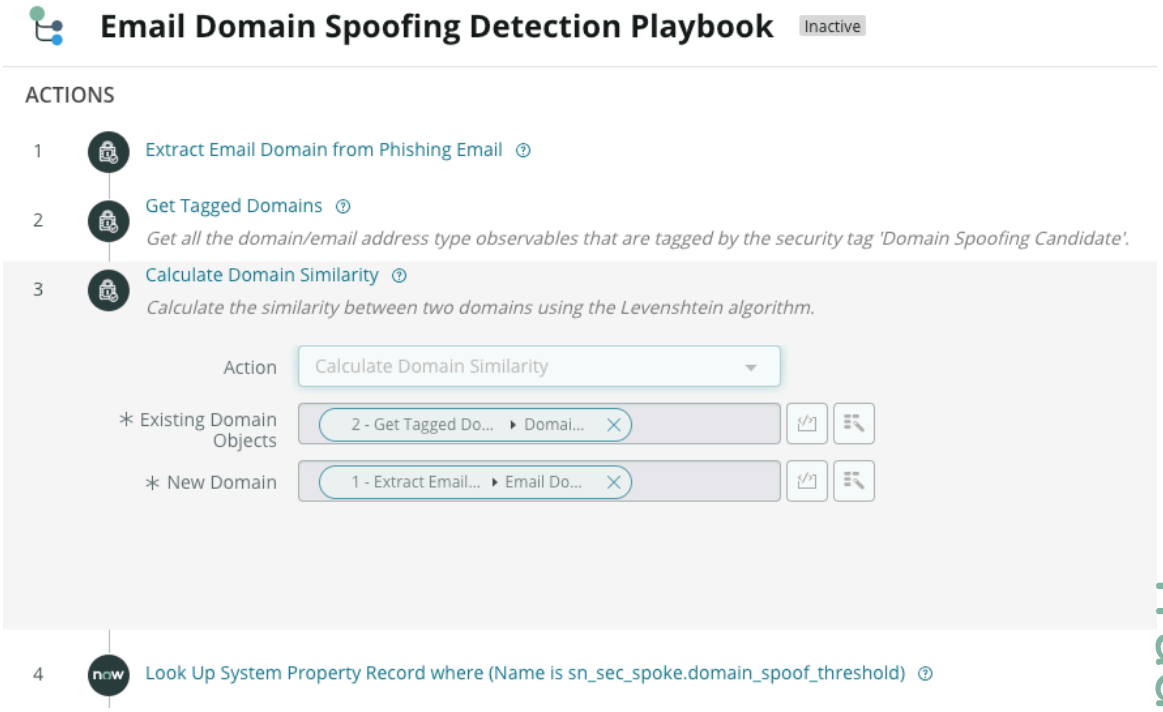
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, o playbook extrai o domínio de e-mail do e-mail de phishing.
2. Na Ação 2, o playbook recupera todos os observáveis de tipo de endereço de e-mail/domínio marcados pelo marcador de segurança "Candidato a spoofing de domínio".
3. Na Ação 3, o playbook calcula a semelhança entre o domínio Obter marcador e o domínio E-mail usando o algoritmo Levenshtein.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de detecção de falsificação de domínio de e-mail



4. Na Ação 4, o playbook pesquisa o registro de propriedade do sistema com base nas seguintes condições:
   - O nome é sn_sec_spoke.domain_spoof_threshold, (OU)
   - O nome é de a a z e, se vários registros forem encontrados, retornará somente o primeiro registro.
5. Na Ação 5, com base na investigação realizada até ao momento, o playbook verifica se a semelhança dos dois domínios excede ou não o limite.
   Se a semelhança dos dois domínios não exceder o limite, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado. Se a semelhança dos dois domínios exceder o limite, as ações 6 e 7 serão executadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A semelhança excede o limite



6. Na Ação 6, o playbook adiciona o marcador de segurança Spoofing de domínio de e-mail ao incidente de segurança.
7. Na Ação 7, o playbook adiciona um link de anotação de trabalho ao contexto usando a opção de script.
8. Na Ação 8, o fluxo termina.

Playbook para domínio ocupado Typo

Este playbook fornece procedimentos sistemáticos para investigar domínios com erros ortográficos e colaborar com o departamento jurídico da organização para remoções. Domínios com erros de digitação são nomes de domínio intencionalmente com erros ortográficos que se assemelham aos legítimos. Os invasores aproveitam os erros ortográficos para levá-los a um site mal intencionado para exploração financeira ou outras atividades mal-intencionadas.

Typo Squatted Domains são relatados à Equipe de operações de segurança de diferentes fontes, como soluções de proteção contra riscos digitais (Digital Shades) e plataformas de inteligência contra ameaças (Anomali Threatstream). Depois que um incidente de segurança é criado, esta solução ajuda a identificar se o domínio é realmente um domínio de ocupação Typo. Se for um Domínio ocupado por Typo, o analista poderá relatar isso à equipe jurídica para que outras ações possam ser tomadas.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultados e o fluxo muda de direção com base no resultado de tais tarefas.

Configure o playbook Domínio de ocupação do Typo

Use as etapas a seguir para configurar o playbook Domínio de ocupação do Typo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Domínio squatted de erros de digitação** playbook.
3. **Opcional:** Você pode criar uma cópia do fluxo do playbook Domínio de ocupação do Typo e fazer as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, clique em ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



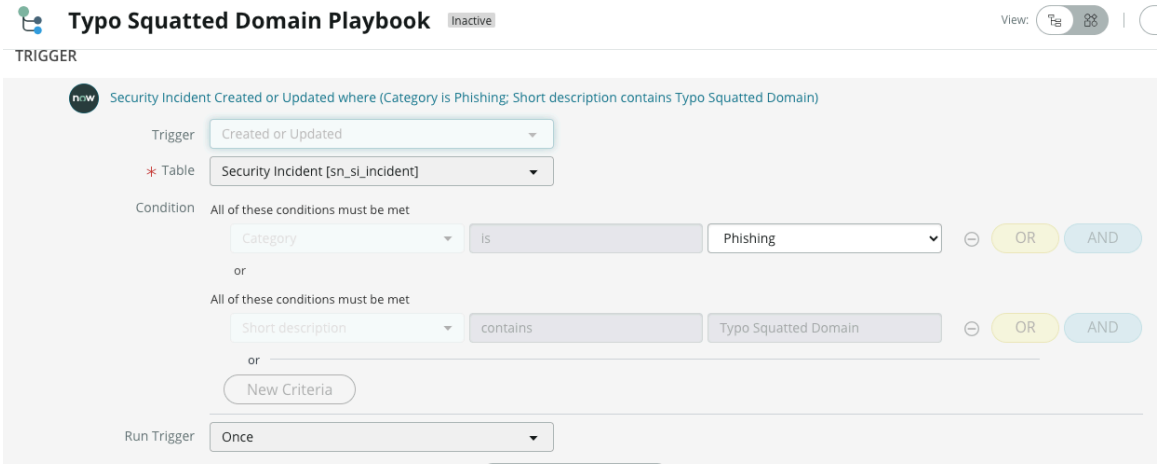
4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Categoria** . **Phishing** .
- **Descrição resumida** contém **Domínio squatted de erros de digitação** .



Use o playbook Domínio ocupado do Typo

Use este playbook para investigar domínios com erros ortográficos e colaborar com o departamento jurídico da organização para remoções. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Domínio de ocupação do Typo.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

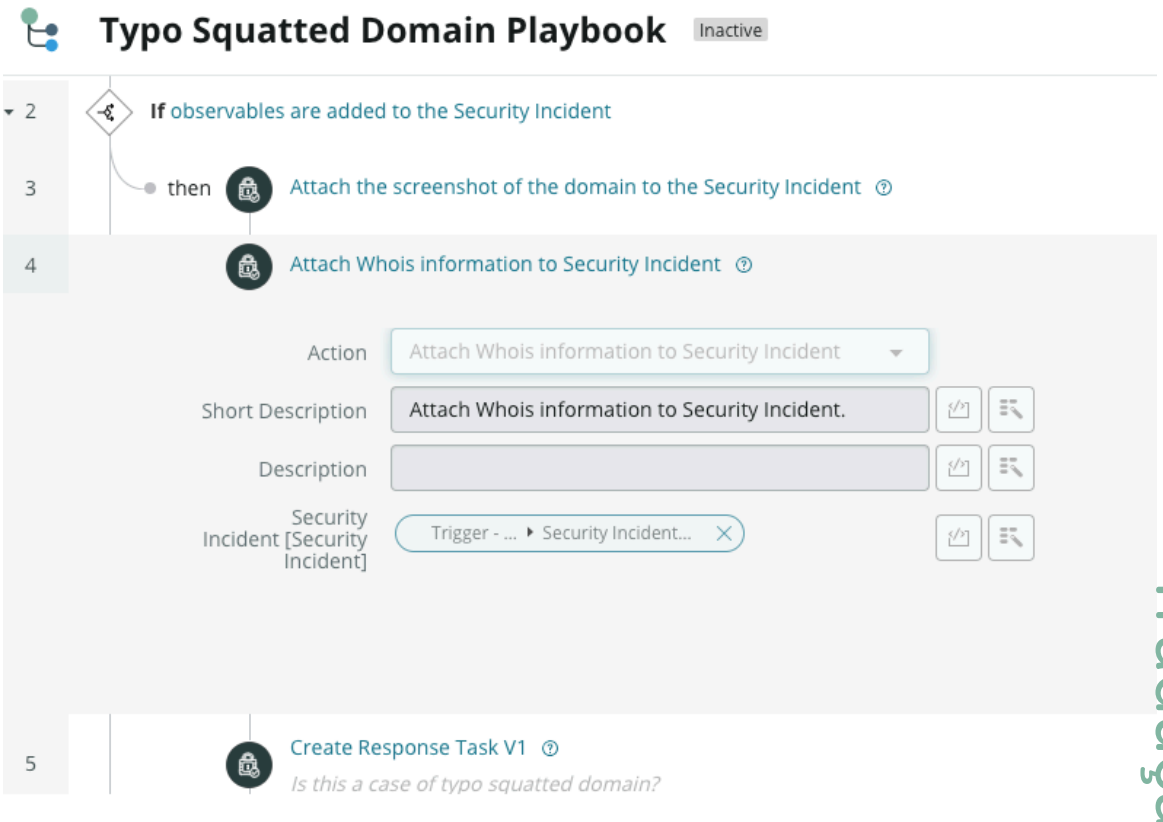
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se os observáveis foram adicionados à Resposta de incidente de segurança (SIR).
   Se os observáveis não forem adicionados ao SIR, adicione os observáveis antes de prosseguir. Se os observáveis não estiverem disponíveis, a Ação 10 será executada e o incidente de segurança será encerrado.
2. Na Ação 2, se os observáveis forem adicionados ao incidente de segurança, as ações a seguir serão executadas.
3. Na Ação 3, você precisa anexar a captura de tela do domínio Typo squatted ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de domínio de ocupação de erros de digitação

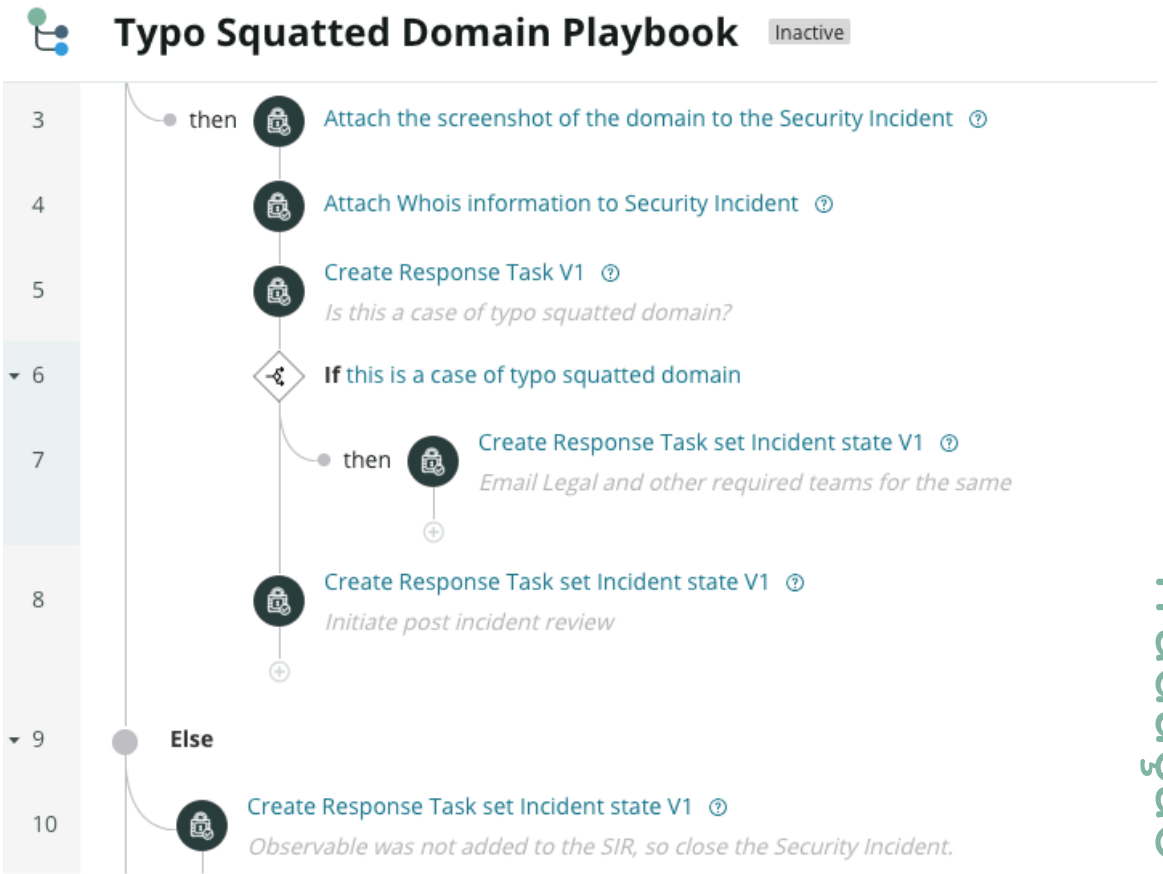


4. Na Ação 4, você precisa anexar as informações do Whois ao incidente de segurança.
5. Na Ação 5, com base na investigação realizada até ao momento, o playbook verifica se este é um caso de domínio de ocupação Typo ou não.
   Se este não for um caso de domínio Typo squatted, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
6. Na Ação 6, se este for um caso de domínio de ocupação Typo, a ação 7 será executada.
7. Na Ação 7, você precisa enviar um e-mail e informar o Jurídico e outras equipes necessárias que este é um caso de domínio Typo ocupado e tomar as ações necessárias para eliminá-lo.
   Se este não for um caso de domínio Typo squatted, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Domínio ocupado por Typo



8. Na Ação 9, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para Sniffing de credenciais

Este playbook fornece etapas de correção do sistema para investigar um incidente que envolve atividades de detecção de credenciais realizadas por meio do `sys_installation_exit`Tabela em uma instância da ServiceNow.

O playbook de sniffing de credenciais fornece um campo de script para processar os logins do banco de dados (DB), Single Sign-on (SSO) e LDAP (Lightweight Directory Access Protocol) usando os registros no `sys_installation_exit`tabela. Esses campos de script privilegiados permitem ouvir solicitações e parâmetros do usuário para as instâncias durante o login, incluindo credenciais do usuário, como nome de usuário e senha.

Um usuário mal-intencionado pode criar um script para ouvir as solicitações do usuário e registrar essas solicitações na instância. . `sys_installation_exit`a tabela em uma instância define as regras de processamento das atividades de login e logout de todos os usuários nessa instância.

Configure o playbook de sniffing de credencial

Use as etapas a seguir para configurar o playbook de sniffing de credencial.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

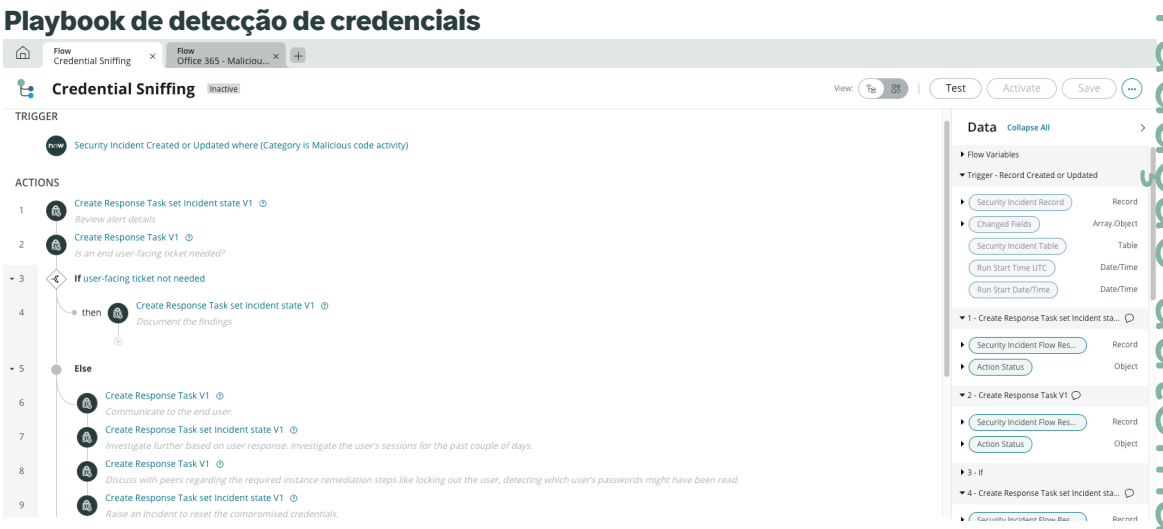
- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Detecção de credencial** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook de sniffing de credenciais e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



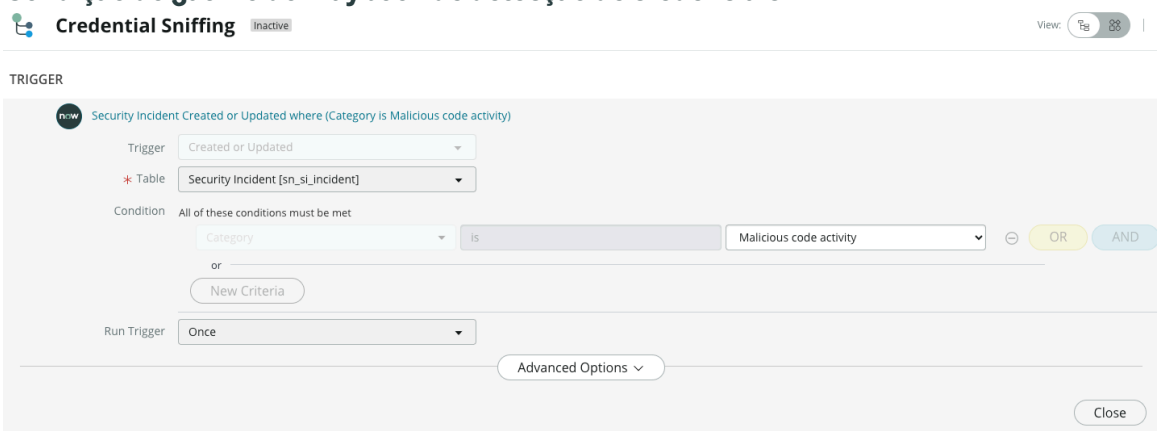
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Atividade de código mal-intencionado** .

Condição do gatilho do Playbook de detecção de credenciais



Use o playbook de sniffing de credencial

Use este playbook para investigar um incidente que envolve atividades de detecção de credenciais realizadas por meio do *sys_installation_exit*Tabela em uma instância da ServiceNow. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de sniffing de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, revise os detalhes do alerta a seguir.
   - Instância
   - ID da sessão
   - ID de Transação
   - _Raw: Fornece o script inteiro.

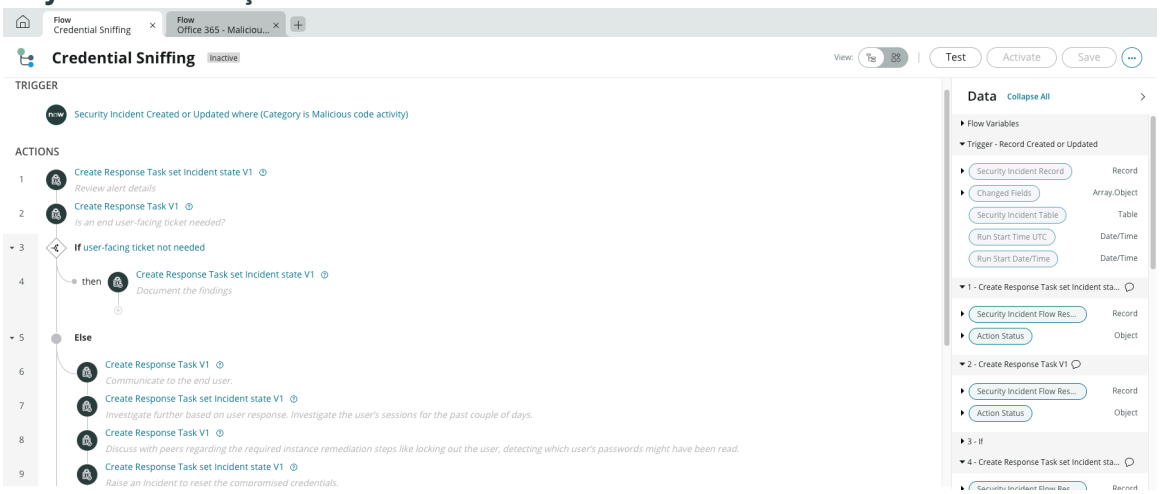
     Script de exemplo:

     ```
     Var pass= request.getParameter(“user_password”);
     Gs.log(pass);
     ```
2. Na Ação 2, com base nos dados coletados até o momento, verifique se um tíquete de usuário final é necessário ou não para este alerta.
3. Na Ação 3, se o alerta não exigir um tíquete de usuário final, na Ação 4, documente as descobertas até o momento.
   O fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de detecção de credenciais



4. Na Ação 5, se o alerta exigir um tíquete de usuário final, execute as seguintes etapas:

   a. Em Ação 6, informe ao usuário final que o alerta requer um tíquete de usuário final.

   b. Na Ação 7, investigue mais detalhadamente com base na resposta do usuário e nas sessões do usuário durante os últimos dois dias.

   c. Na Ação 8, converse com colegas sobre as etapas de correção da instância, como bloquear o usuário e detectar quais senhas do usuário podem ter sido lidas.

   d. Em Ação 9, gere um incidente ou tíquete para redefinir as credenciais do usuário comprometido.

   e. Na Ação 10, levante a contenção e traga os sistemas de volta aos padrões operacionais
   O fluxo termina.

5. Em Ação 11, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1070 - Logs de eventos do Windows limpos

Este playbook fornece etapas de correção para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. Sempre que o log de segurança é limpo, os eventos 517 e 1102 são registrados independentemente do status da política de evento do sistema de auditoria.

Este alerta pode rastrear os seguintes tipos de eventos:

- **Evento 517** : Os campos Nome de usuário primário e Nome de usuário do cliente identificam o usuário que limpou o log. O nome de usuário primário corresponde ao sistema e o nome de usuário do cliente indica o usuário que limpou o log.
- **Evento 1102** : Os campos Nome da conta e Nome do domínio identificam o usuário que limpou o log. O ID de logon permite que você correlacione o evento de logon e outros eventos registrados durante a mesma sessão de logon.

Configure o playbook T1070 - Logs de eventos do Windows limpos

Use as etapas a seguir para configurar o playbook T1070 - Logs de eventos do Windows limpos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **T1070 - Logs de eventos do Windows limpos** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook T1070 - Logs de eventos do Windows limpos e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



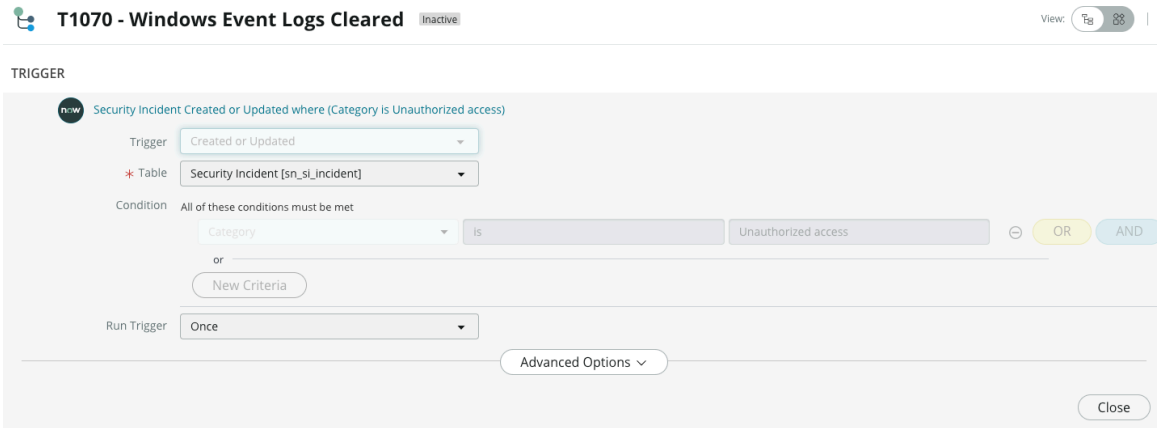
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Acesso não autorizado** .

T1070 - Logs de eventos do Windows limpos Condição do gatilho do playbook



Use o playbook T1070 - Logs de eventos do Windows limpos

Use este playbook para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1070 - Logs de eventos do Windows limpos.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, obtenha os detalhes do usuário do alerta.
2. Na Ação 2, verifique se o usuário foi identificado ou não.
3. Na Ação 3, se o usuário não tiver sido identificado, execute as seguintes etapas:

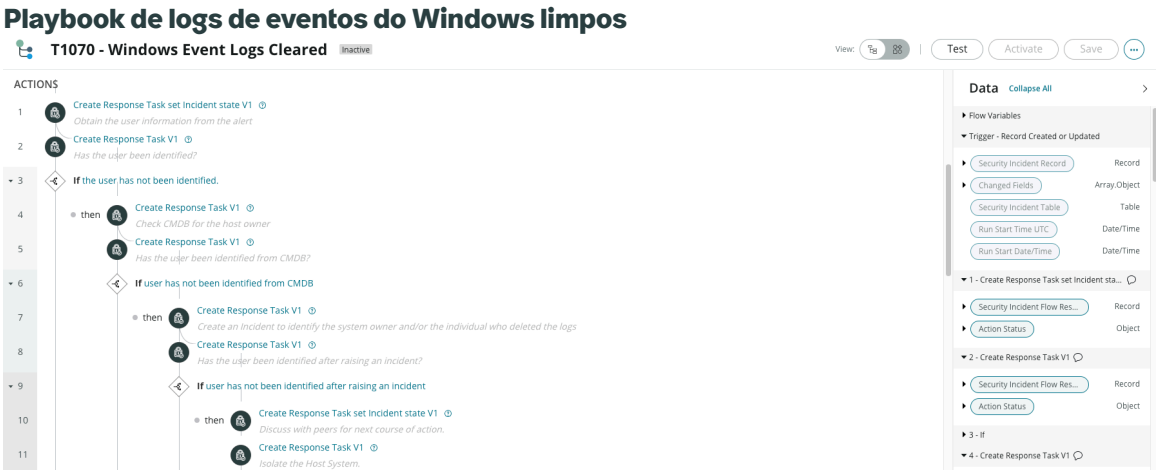
   a. Na Ação 4, verifique os detalhes do responsável pelo host no CMDB (Configuration Management Database).

   b. Na Ação 5, verifique se o usuário foi identificado no CMDB ou não.

      Se o usuário tiver sido identificado no CMDB, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na Ação 6, se o usuário não tiver sido identificado no CMDB, execute as seguintes etapas:

i. Em Ação 7, crie um incidente para identificar o responsável pelo sistema e o indivíduo que excluiu os logs.

ii. Na Ação 8, verifique se o usuário foi identificado após relatar um incidente ou não.

Se o usuário tiver sido identificado após gerar um incidente, uma tarefa de resposta manual será criada na Ação 8 e o fluxo será encerrado.

iii. Na Ação 9, se o usuário não tiver sido identificado após gerar um incidente, execute as seguintes etapas:

1. Na Ação 10, debata o próximo curso de ação com os colegas.

2. Em Ação 11, isole o sistema host.

3. Na Ação 12, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.

4. Na Ação 13, levante a contenção e traga os sistemas de volta aos padrões operacionais.

5. Em Ação 14, conclua a revisão pós-incidente antes de fechar a tarefa.

Na Ação 15, o fluxo termina.

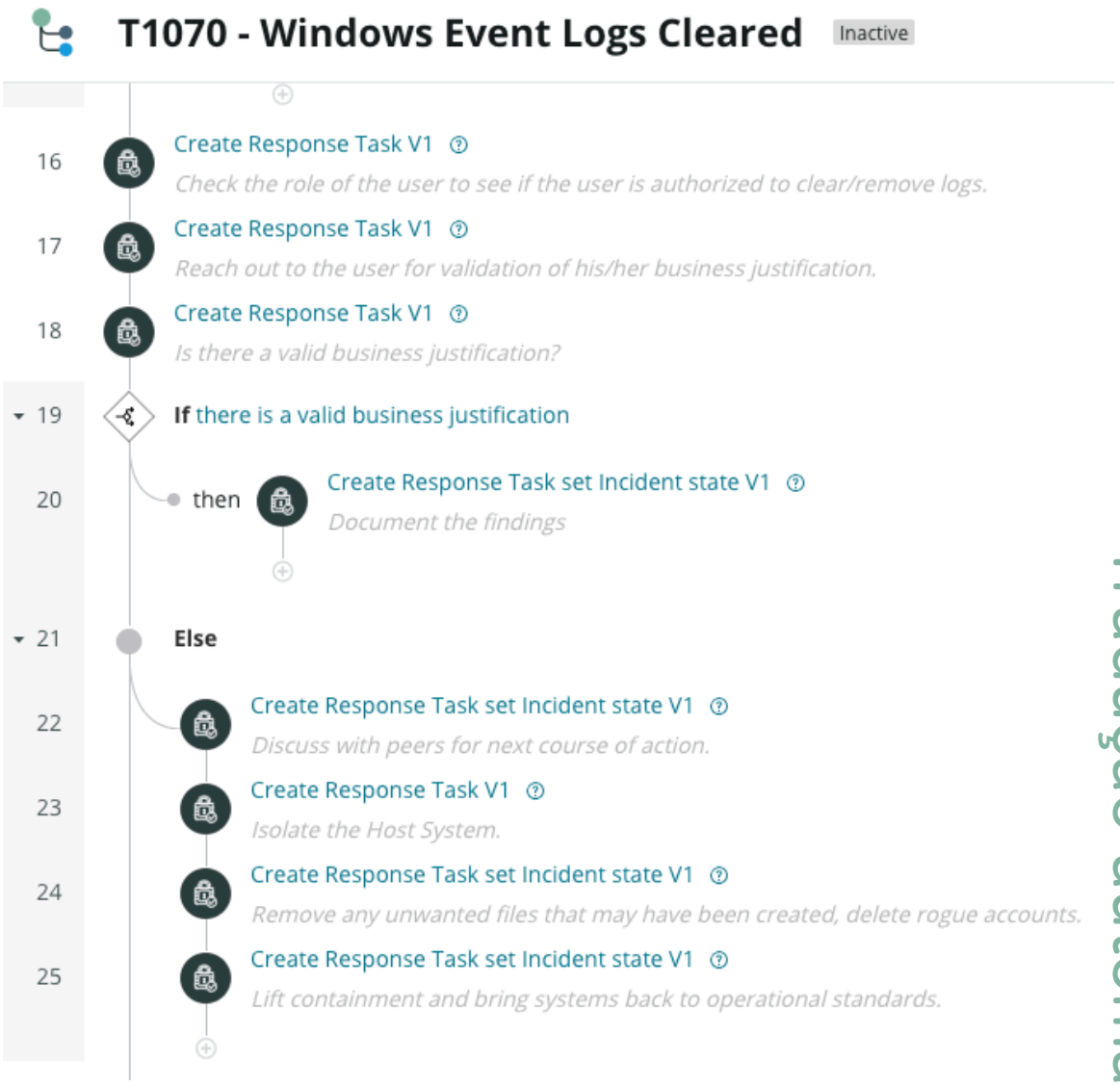
4. Na Ação 16, se o usuário tiver sido identificado, verifique a função do usuário para ver se ele está autorizado a limpar ou remover logs.

5. Na Ação 17, entre em contato com o usuário para validar sua justificativa de negócios.
Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook T1070 - Logs de eventos do Windows limpos



Tradução automática

6. Na Ação 18, verifique se uma justificativa comercial válida foi fornecida ou não.
7. Na Ação 19, se houver uma justificativa comercial válida fornecida, na Ação 20, documente as descobertas até agora.
   O fluxo termina.
8. Na Ação 21, se não houver justificativa comercial válida fornecida, execute as seguintes etapas:
   a. Na Ação 22, debata o próximo curso de ação com os colegas.
   b. Em Ação 23, isole o sistema host.
   c. Na Ação 24, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Na Ação 25, levante a contenção e traga os sistemas de volta aos padrões operacionais.
O fluxo termina.

9. Em Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para OSquery do endereço externo no arquivo /etc/hosts

Este playbook fornece etapas de correção sistemáticas para investigar incidentes que indicam que um nome de host ou domínio interno foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux.

Configure o OSquery do endereço externo no playbook do arquivo /etc/hosts

Use as etapas a seguir para configurar o OSquery do endereço externo no playbook de arquivo /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

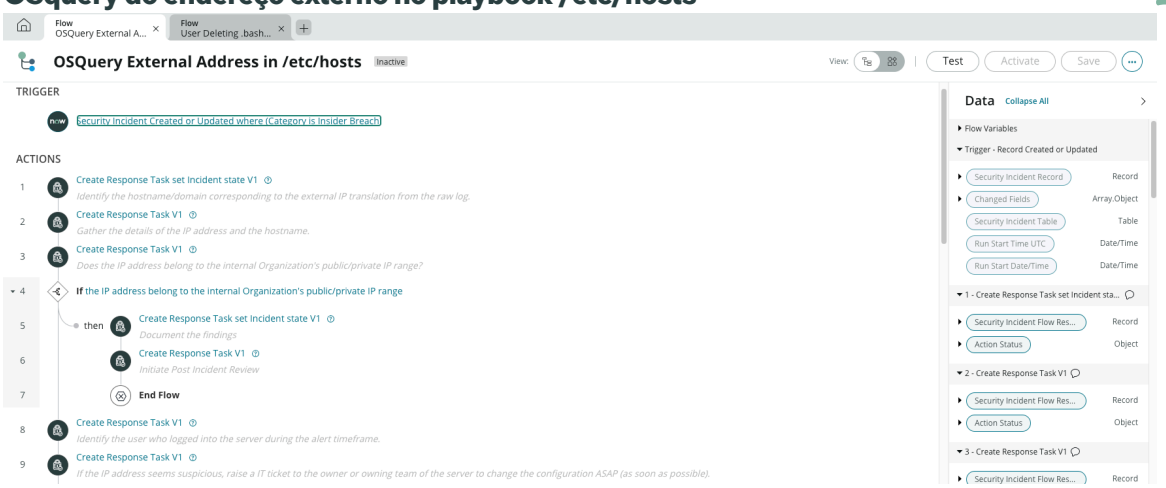
1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Tudo** > **Flow Designer** e selecione **Endereço externo OSquery em /etc/hosts** playbook.

3. **Opcional:** Crie uma cópia do endereço externo OSquery no fluxo do playbook /etc/hosts e faça as modificações necessárias.

(Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

OSquery do endereço externo no playbook /etc/hosts



4. Ative os playbooks.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

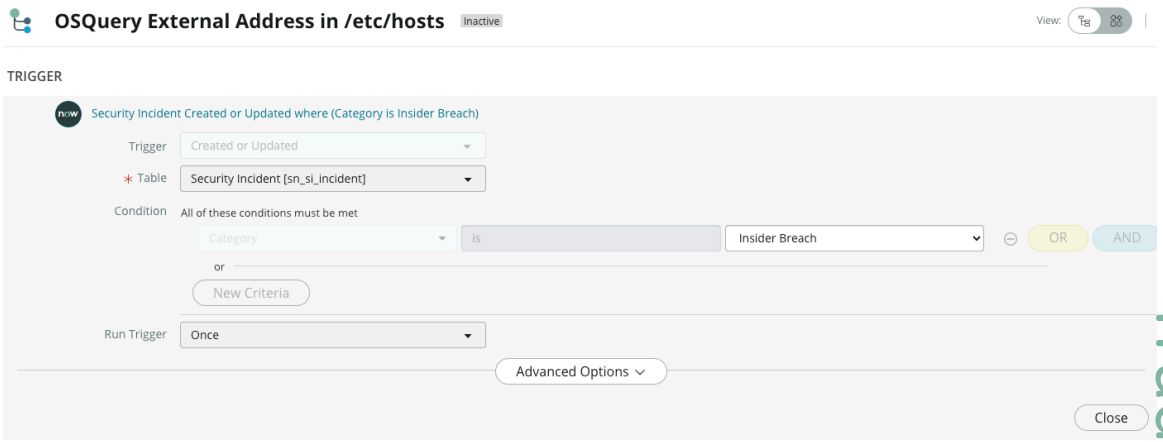
a. Ative o fluxo principal para usar o playbook disponível no sistema de base.

b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. Defina um **Condição do gatilho** para o playbook.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Violação interna** .

OSquery do endereço externo na condição do gatilho do playbook /etc/hosts



Use o OSquery do endereço externo no playbook do arquivo /etc/hosts

Use este playbook para investigar incidentes que indicam que um nome de host ou domínio interno foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no OSquery do endereço externo no playbook de arquivos /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, identifique o nome de host ou o nome de domínio correspondente à tradução de IP externo do log bruto.

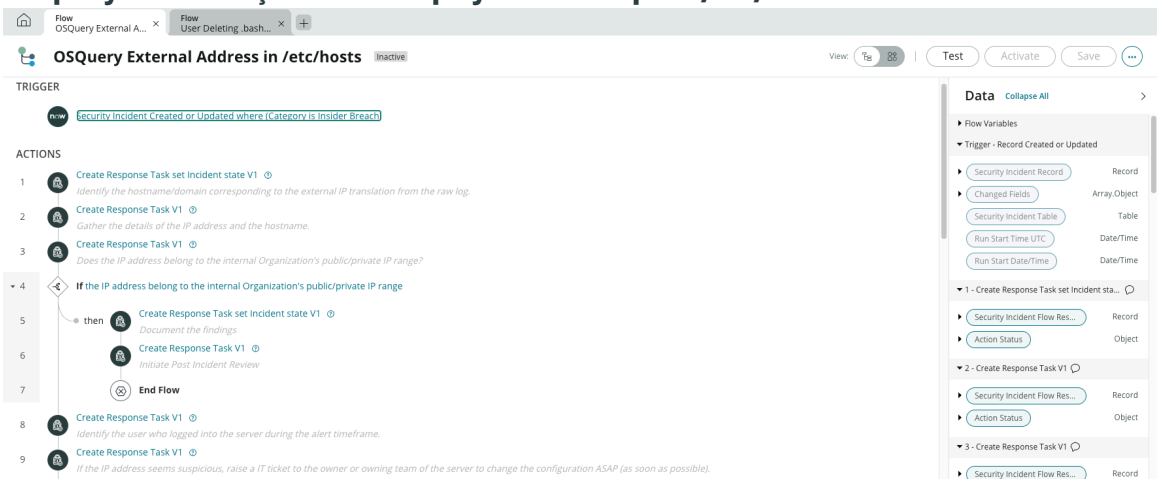
2. Em Ação 2, reúna os detalhes do endereço IP e do nome do host.

3. Na Ação 3, verifique se este endereço IP pertence ou não ao intervalo de IPs público/privado da organização interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

OSquery do endereço externo no playbook do arquivo /etc/hosts



4. Na Ação 4, se o endereço IP pertencer ao intervalo de IPs público/privado da organização interna, execute as seguintes etapas:

   a. Na Ação 5, documente as descobertas até agora.

   b. Em Ação 6, inicie uma revisão pós-incidente.
   Na Ação 7, após a revisão pós-incidente, o fluxo termina.

5. Se o endereço IP não pertencer ao intervalo de IPs público/privado da organização interna, na Ação 8, identifique o usuário que fez login no servidor durante o período de alerta.
6. Na Ação 9, se o endereço IP parecer suspeito, gere um tíquete DE TI para o proprietário ou a equipe do servidor para mudar a configuração o mais rápido possível.
7. Na Ação 10, verifique se houve alguma atividade mal-intencionada no servidor antes e depois de adicionar a entrada DNS.
8. Na Ação 11, verifique se há conexões com o endereço IP externo do servidor.
9. Na Ação 12, documente as descobertas até agora.
10. Na Ação 13, verifique se as informações do proprietário ou da equipe estão disponíveis ou não.
11. Na Ação 14, se as informações do proprietário ou da equipe estiverem disponíveis, execute as seguintes etapas:

    a. Na Ação 15, entre em contato com o proprietário ou com a equipe do servidor para ver se ele reconhece a atividade.
    Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário ou com a equipe do servidor.

    b. Na Ação 16, verifique se o proprietário ou a equipe forneceu uma justificativa comercial válida ou não.

    c. Na Ação 17, se o proprietário ou a equipe fornecida não forneceu uma justificativa comercial válida, o fluxo será encerrado.
    Mas, se o proprietário ou a equipe forneceu uma justificativa comercial válida, execute as seguintes etapas:

Tradução automática

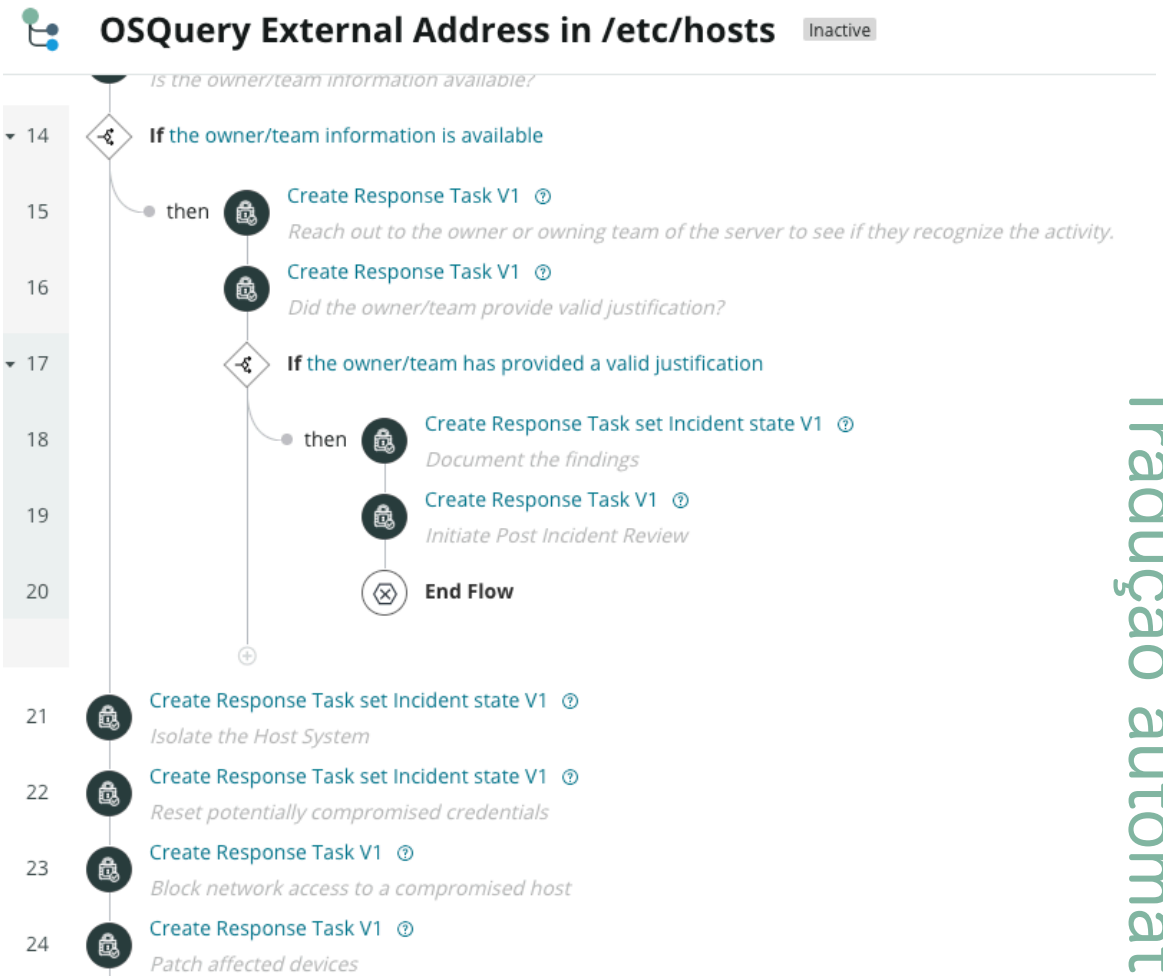
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Na Ação 18, documente as descobertas até agora.

ii. Em Ação 19, inicie uma revisão pós-incidente.

Na Ação 20, após a revisão pós-incidente, o fluxo termina.

Usando o OSquery do endereço externo no playbook de arquivos /etc/hosts



12. Na Ação 21, se as informações do proprietário ou da equipe não estiverem disponíveis, isole o sistema host.

13. Em Ação 22, redefina as credenciais potencialmente comprometidas.

14. Na Ação 23, bloqueie o acesso à rede ao host comprometido.

15. Em Ação 24, corrija os dispositivos afetados.

16. Na Ação 25, levante a contenção e traga os sistemas de volta aos padrões operacionais.

17. Em Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para usuário excluindo histórico de Bash - Nuvem

Este playbook fornece etapas de correção sistemáticas para investigar incidentes que indicam se alguém estava tentando remover o histórico de bash (`.bash_history`) De um servidor Linux.

Nota: Você precisa mitigar esse alerta com cuidado, pois esses alertas raramente são acionados e potencialmente indicam uma ameaça interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o playbook Usuário Excluindo histórico de Bash

Use as etapas a seguir para configurar o playbook Exclusão do histórico de Bash do usuário.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

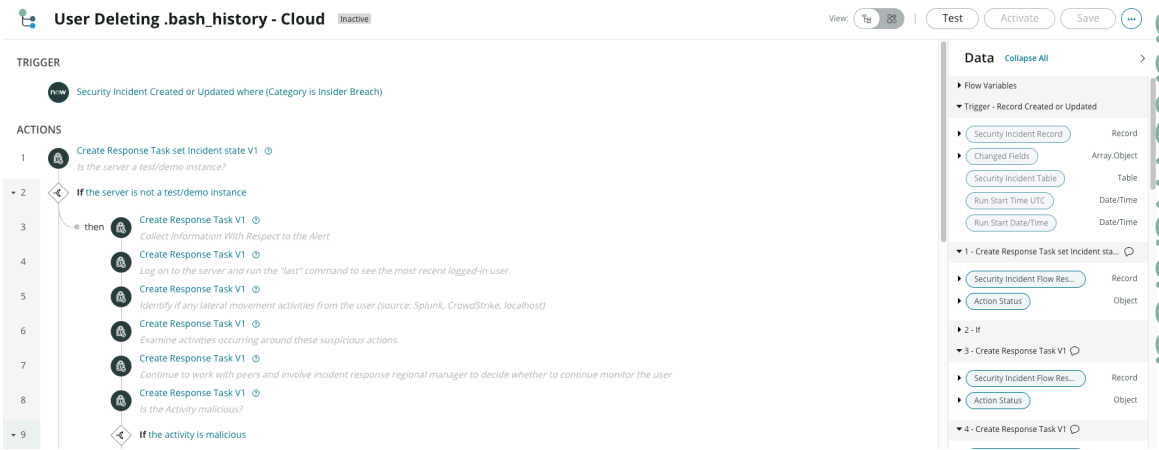
Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Usuário excluindo .bash_history - Nuvem** playbook.
3. **Opcional:** Crie uma cópia do fluxo Usuário Excluindo .bash_history - Playbook da nuvem e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   Usuário excluindo histórico de Bash - Playbook de nuvem

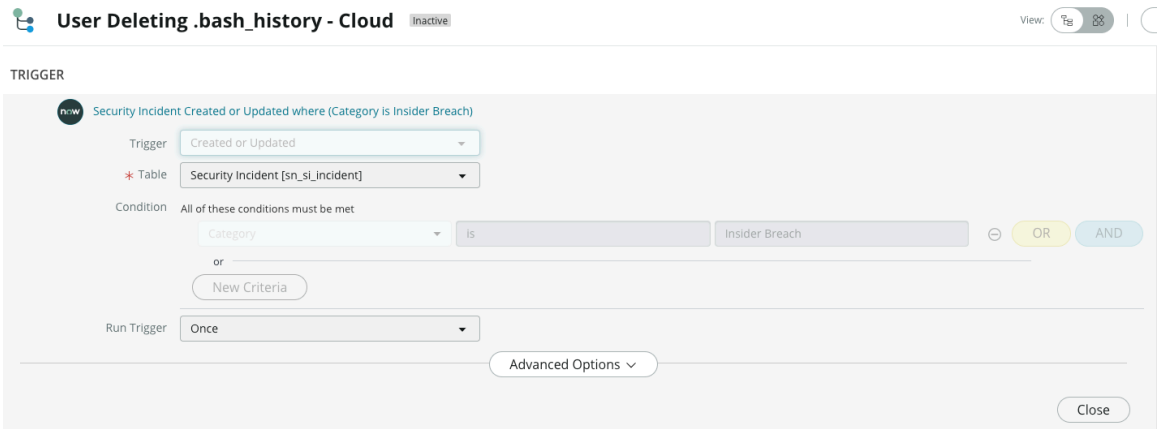
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Violação interna** .

Usuário excluindo histórico de Bash - condição do gatilho do Playbook na nuvem



Use o playbook Exclusão do histórico de Bash do usuário

Use este playbook para investigar incidentes que indicam se alguém estava tentando remover o arquivo de histórico de bash de um servidor Linux. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no usuário Excluindo o histórico de Bash (`.bash_history` playbook.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, verifique se o servidor é uma instância de teste ou demonstração.
2. Na Ação 2, se o servidor não for uma instância de teste ou demonstração, execute as seguintes etapas:

   a. Em Ação 3, colete as seguintes informações para o alerta:
      - Nome do usuário
      - Endereço IP
      - Comandos mal-intencionados que tentam excluir o histórico de bash
      - Todos os comandos executados pelo usuário, se disponíveis nos logs do CrowdStrike.

   b. Em Ação 4, faça login no servidor e execute o. `último` comando para exibir o usuário conectado mais recente.

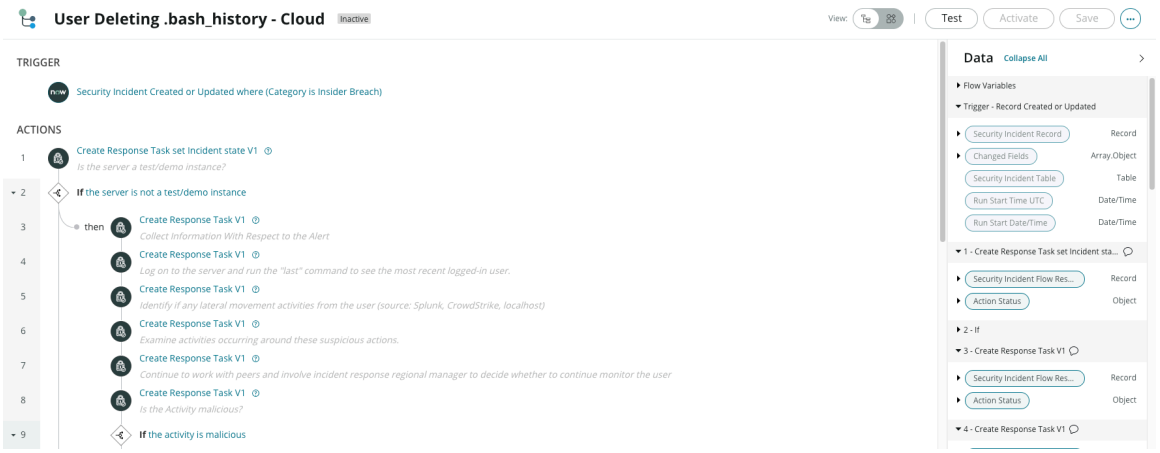
   c. Na Ação 5, identifique se houve atividades de movimento lateral do usuário (Origem: Splunk, CrowdStrike, localhost).

   d. Na Ação 6, examine as atividades que ocorrem em torno dessas ações suspeitas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook do Histórico de Bash excluído pelo usuário



e. Na Ação 7, continue trabalhando com colegas e envolva o gerente regional de resposta a incidentes na decisão de continuar monitorando o usuário.

f. Na Ação 8, determine se a atividade é mal-intencionada ou não.

g. Na Ação 9, se a atividade for mal-intencionada, execute as seguintes etapas:

i. Na Ação 10, durante a investigação, entre em contato com o Suporte DE TI e solicite um congelamento da conta.

ii. Na Ação 11, certifique-se de que a instância seja restaurada para um estado normal sem atividade mal-intencionada.

iii. Na Ação 12, levante a contenção e traga os sistemas de volta aos padrões operacionais.

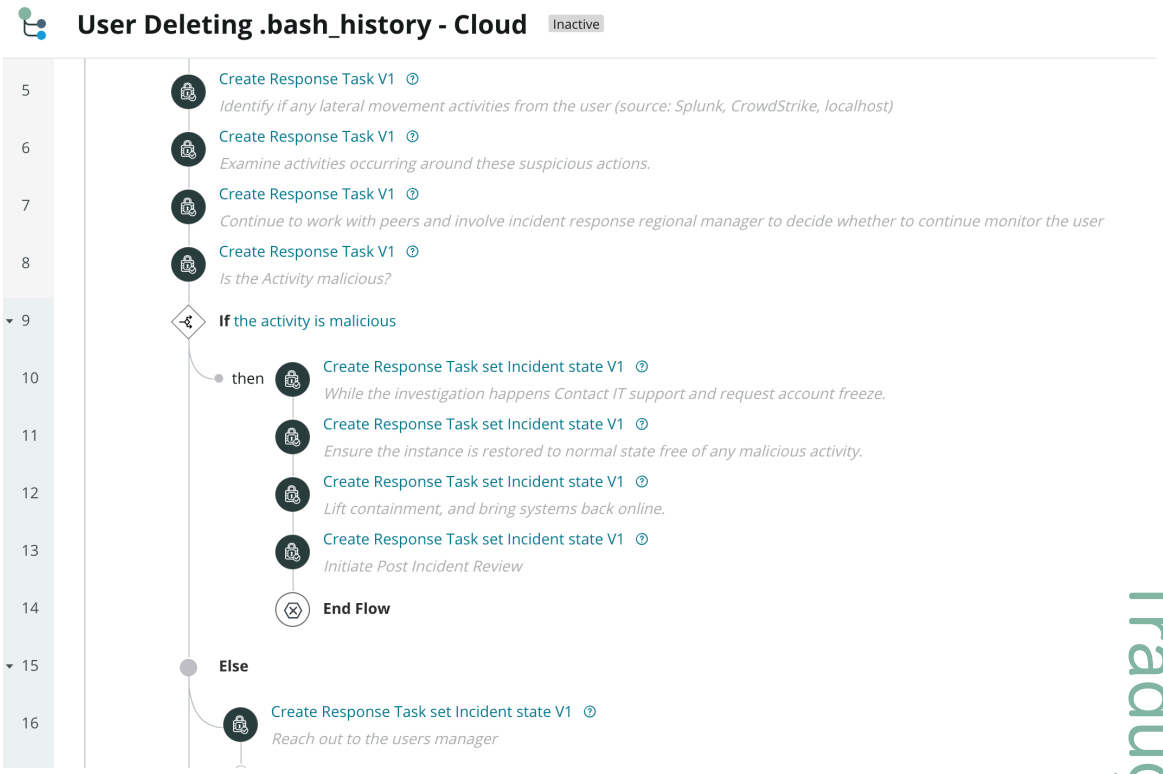
iv. Em Ação 13, inicie uma revisão pós-incidente.

Na Ação 14, após a revisão pós-incidente, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook Exclusão do histórico de Bash do usuário



h. Na Ação 15, se a atividade não for mal-intencionada, na Ação 16, entre em contato com o gerente do usuário.
Você pode usar o modelo de e-mail fornecido para entrar em contato com o gerente do usuário e informá-lo sobre a abordagem recomendada.

3. Na Ação 17, documente as descobertas até agora.

4. Em Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativas de VPN bem-sucedidas das contas de serviço - Corp/Cloud

Este playbook fornece etapas de correção sistemáticas para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As contas de serviço não devem ter eventos de login de uma VPN, e esses eventos podem ser indicadores de força bruta ou possível exposição das credenciais da conta.

Configure as tentativas de VPN bem-sucedidas no playbook de contas de serviço

Use as etapas a seguir para configurar as tentativas de VPN bem-sucedidas no playbook de Contas de serviço.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Tradução automática

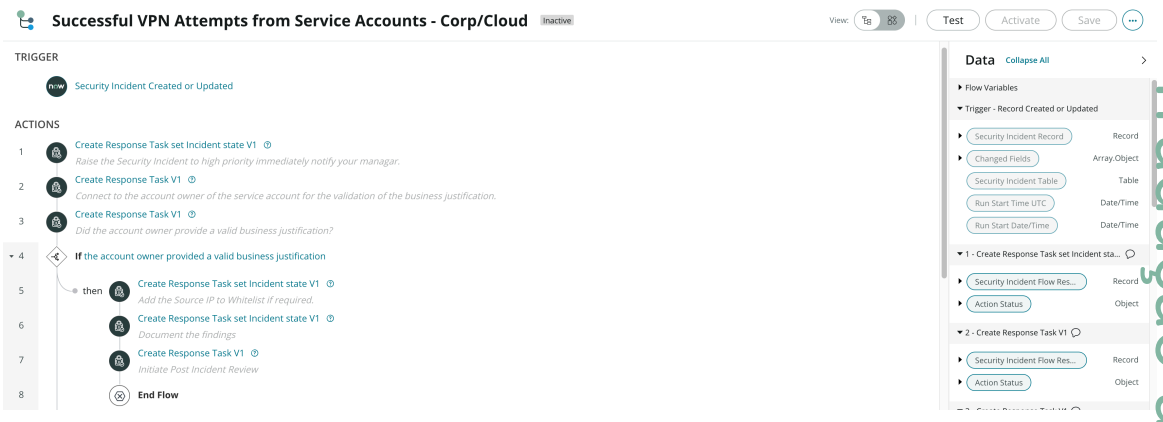
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Tentativas de VPN bem-sucedidas das Contas de serviço** playbook.
3. **Opcional:** Crie uma cópia das tentativas de VPN bem-sucedidas do fluxo do playbook de contas de serviço e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

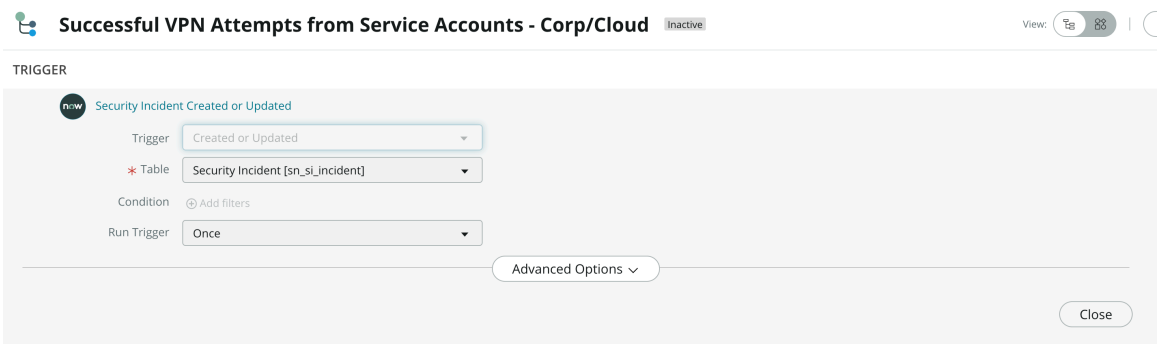
Tentativas de VPN bem-sucedidas do Playbook Contas de serviço - Corp/ Nuvem



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando o incidente de segurança é criado ou atualizado com base nas condições necessárias. Por exemplo, Quando **Categoria** . **Violação interna** .

Tentativas de VPN bem-sucedidas da condição de gatilho Contas de serviço - Playbook corporativo/nuvem



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use as tentativas de VPN bem-sucedidas do playbook de Contas de serviço

Use este playbook para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis nas tentativas de VPN bem-sucedidas do Playbook de contas de serviço.

Antes de Iniciar

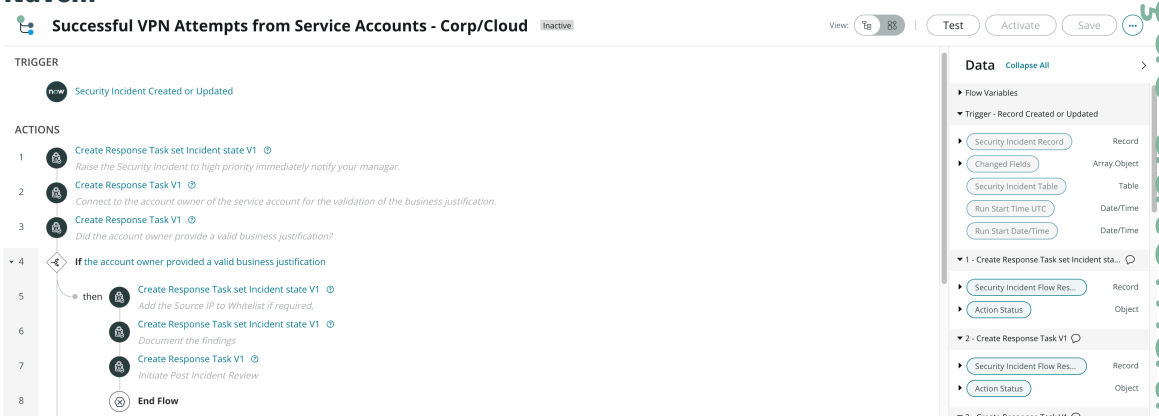
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, eleve o incidente de segurança para alta prioridade e notifique imediatamente seu gerente.
2. Na Ação 2, entre em contato com o responsável pela conta de serviço para validar a justificativa de negócios. Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário da conta de serviço para validar a justificativa de negócios.
3. Na Ação 3, verifique se o responsável pela conta de serviço forneceu uma justificativa comercial válida.

Tentativas de VPN bem-sucedidas do Playbook Contas de serviço - Corp/Nuvem



4. Na Ação 4, se o responsável pela conta de serviço forneceu uma justificativa comercial válida, execute as seguintes etapas:

   a. Em Ação 5, adicione o IP de origem à lista de permissões, se necessário.

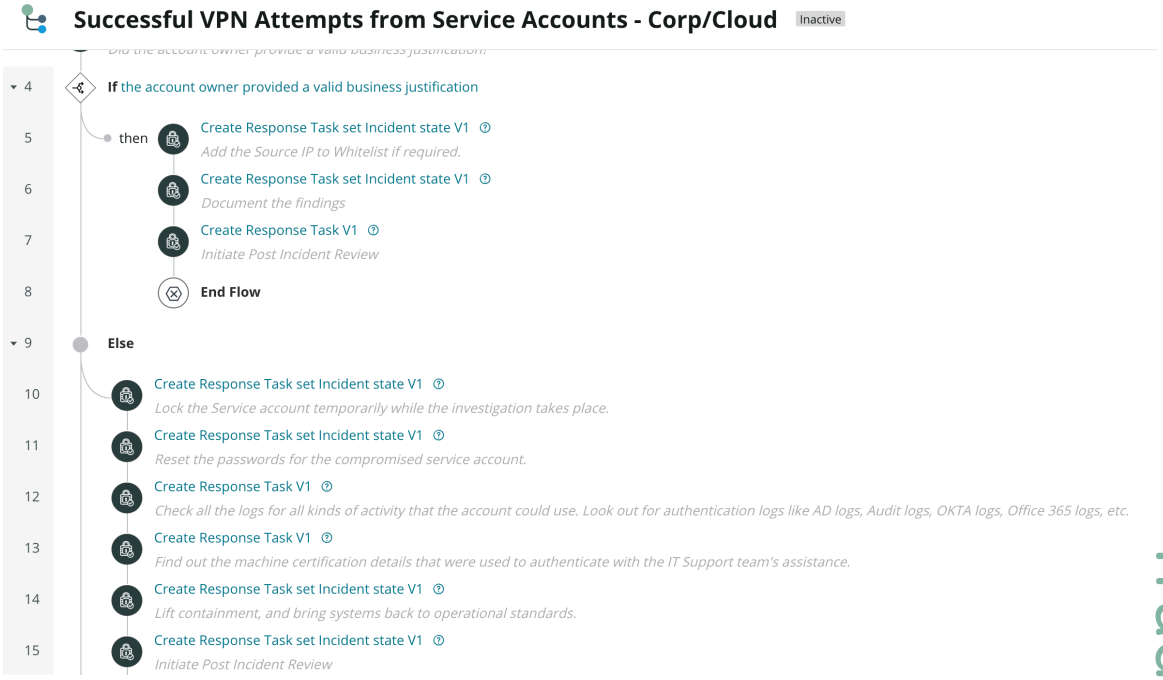
   b. Na Ação 6, documente as descobertas até agora.

   c. Em Ação 7, inicie uma revisão pós-incidente.
   Na Ação 8, após a revisão pós-incidente, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando as tentativas de VPN bem-sucedidas do playbook Contas de serviço - Corp/Nuvem



5. Na Ação 9, se o responsável pela conta de serviço não forneceu uma justificativa comercial válida, execute as seguintes etapas:

   a. Na Ação 10, bloqueie temporariamente a conta de serviço enquanto a investigação ocorrer.

   b. Em Ação 11, redefina as senhas da conta de serviço comprometida.

   c. Na Ação 12, verifique os logs para todos os tipos de atividade que a conta pode usar.
   Procure logs de autenticação, como logs do Active Directory, logs de auditoria, logs do Okta, logs do Office 365 e assim por diante.

   d. Em Ação 13, encontre os detalhes de certificação da máquina usados para autenticar com a assistência da equipe de suporte de TI.

   e. Na Ação 14, levante a contenção e traga os sistemas de volta aos padrões operacionais.

   f. Em Ação 15, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativa de acesso a contas desativadas

Este playbook é acionado quando um funcionário cuja conta está encerrada, desabilitada ou separada tenta fazer login com suas credenciais. O estado da identidade do usuário no Sail Point geralmente é atualizado para desabilitado na data de término.

30 dias é o tempo ideal a partir da data de término para que ele seja atualizado para um estado separado. Você pode usar a lógica de negócios no Sail point para excluir as contas RSA e remover as associações de grupo do Active Directory (AD) após 30 dias.

Configure o playbook da conta desativada de acesso de tentativa

Use as etapas a seguir para configurar o playbook da conta desativada de acesso tentado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Tentativa de acesso à conta desativada** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook da conta desativada de acesso tentado e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



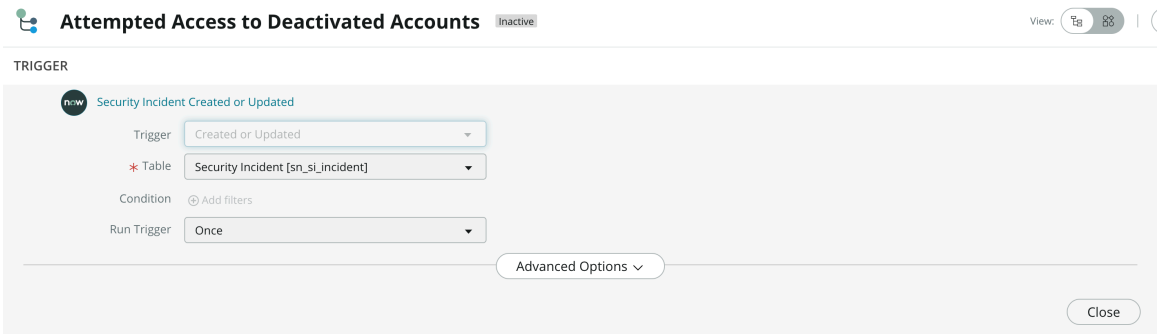
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado quando o incidente de segurança é criado ou atualizado com base nas condições necessárias. Por exemplo, Quando **Categoria** . **Violação interna**

Tentativa de acesso à condição do gatilho do playbook de contas desativadas



Use o playbook de tentativa de acesso a contas desativadas

Use este playbook quando um funcionário cuja conta está encerrada, desabilitada ou separada tentar fazer login com suas credenciais. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Acesso à tentativa de contas desativadas.

Antes de Iniciar

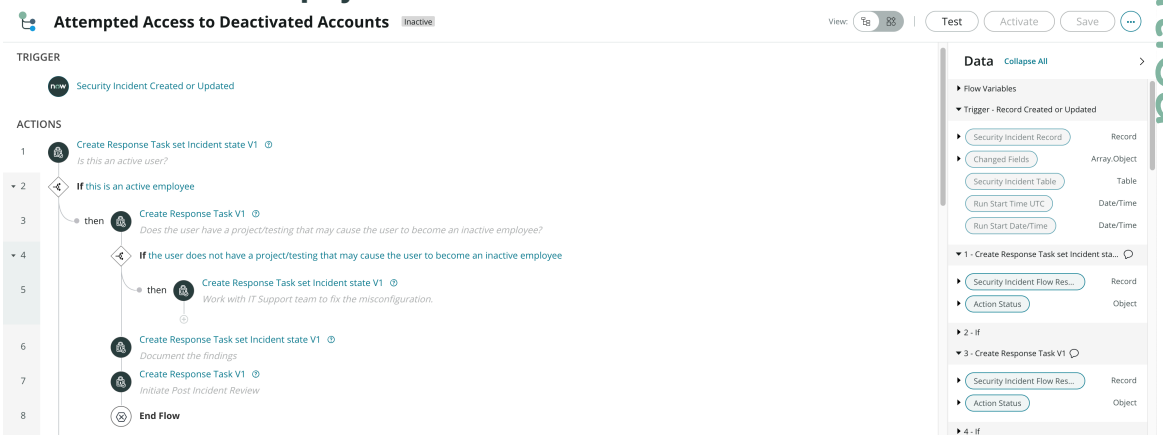
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, verifique se a tentativa de acesso às contas desativadas foi feita por um usuário ativo.
2. Na Ação 2, verifique se a tentativa de acesso às contas desativadas foi feita por um funcionário ativo.

Tentativa de acesso ao playbook de contas desativadas



3. Se a tentativa de acesso às contas desativadas tiver sido feita por um funcionário ativo, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 3, verifique se o usuário tinha um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo.

b. Na Ação 4, se o usuário não tiver um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo, trabalhe com a equipe de suporte DE TI para corrigir a configuração incorreta.
O fluxo termina.

c. Na Ação 5, se o usuário tinha um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo, execute as seguintes etapas:

i. Na Ação 6, documente as descobertas até agora.

ii. Em Ação 7, inicie uma revisão pós-incidente.

Na Ação 8, após a revisão pós-incidente, o fluxo termina.

4. Na Ação 9, se a tentativa de acesso à conta desativada não tiver sido feita por um funcionário ativo, execute as seguintes etapas:

a. Na Ação 10, verifique se o usuário teve logins bem-sucedidos.

b. Na Ação 11, verifique quando o funcionário foi desintegrado.

c. Na Ação 12, investigue os eventos no Splunk para examinar as atividades do usuário durante o período.

d. Na Ação 13, com base na investigação até o momento, determine se o usuário extrafiltrau dados.

e. Na Ação 14, se o usuário não tiver filtrado nenhum dado, execute as seguintes etapas:

i. Na Ação 15, trabalhe com a equipe de suporte de TI para encerrar todas as sessões ativas e desabilitar as contas.

ii. Na Ação 16, documente as descobertas até agora.

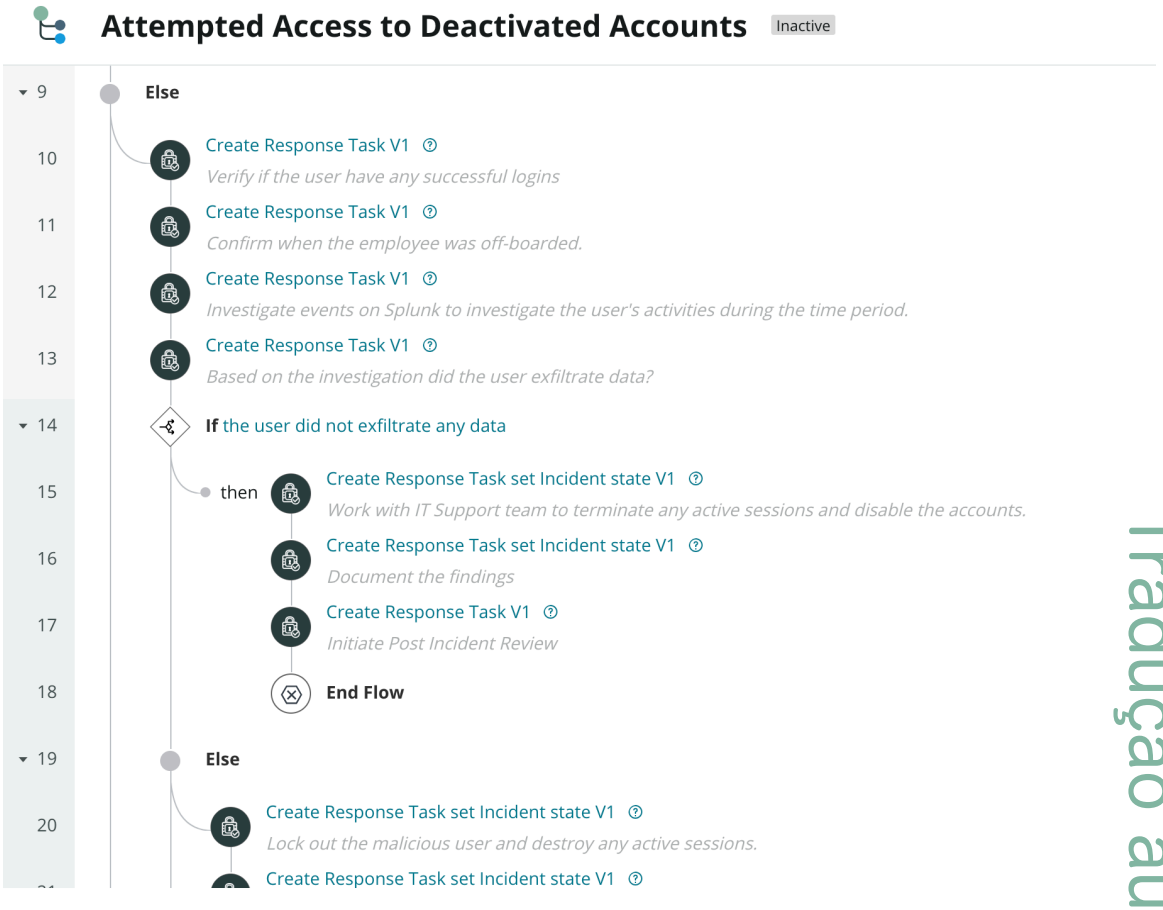
iii. Em Ação 17, inicie uma revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na Ação 18, após a revisão pós-incidente, o fluxo termina.

Usando o playbook de tentativa de acesso a contas desativadas



5. Na Ação 19, se o usuário tiver filtrado dados, execute as seguintes etapas:

a. Na Ação 20, bloqueie o usuário mal-intencionado e destrua todas as sessões ativas.

b. Na Ação 21, trabalhe com a equipe de suporte de TI para desabilitar todas as contas.

c. Na Ação 22, certifique-se de que os recursos sejam restaurados para o estado normal e livres de qualquer atividade mal-intencionada.
Se necessário, você pode recriar a imagem dos recursos.

d. Na Ação 23, levante a contenção e traga os sistemas de volta aos padrões operacionais.

e. Em Ação 24, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1003 - Evasão de defesa - Mimikatz DCShadow

Este playbook fornece etapas de correção sistemáticas para investigar incidentes suspeitos de serem causados pelo Mimikatz DCShadow. DCShadow é um recurso do Mimikatz que simula o comportamento de um controlador de domínio (um servidor que controla o Active Directory) para injetar seus próprios dados, ignorando a maioria dos controles de segurança padrão (incluindo SIEMs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Mimikatz DCShadow ajuda o invasor a estabelecer um controlador de domínio (DC) invasor que se torna parte do Active Directory (AD). Uma vez registrado, ele pode agir como um DC legítimo e causar danos.

Configure o playbook T1003 - Defesa Evasão - Mimikatz DCShadow

Use as etapas a seguir para configurar o playbook T1003 - Evasão de defesa - Mimikatz DCShadow.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

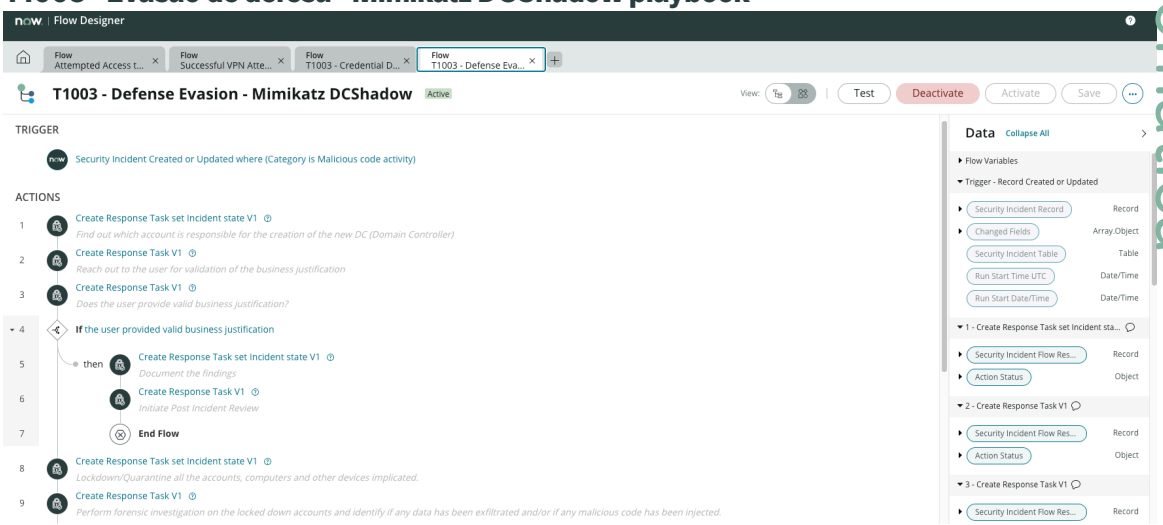
Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **T1003 - Defesa Evasão - Mimikatz DCShadow** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook T1003 - Evasão de defesa - Mimikatz DCShadow e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   T1003 - Evasão de defesa - Mimikatz DCShadow playbook

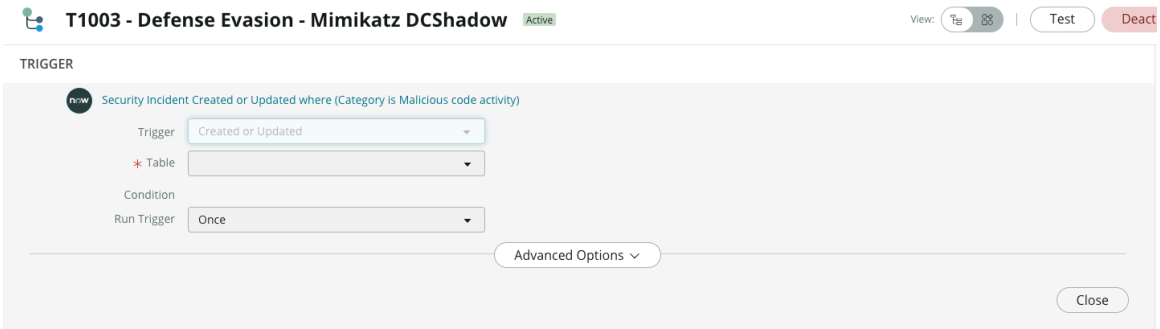
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Atividade de código mal-intencionado** .

T1003 - Evasão de defesa - Condição do gatilho do Playbook de Mimikatz DCShadow



T1003 - Defesa Evasão - Mimikatz DCShadow playbook

Use este playbook para investigar incidentes de segurança suspeitos de serem causados pelo Mimikatz DCShadow. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos disponíveis no playbook T1003 - Evasão de defesa - Mimikatz DCShadow.

Antes de Iniciar

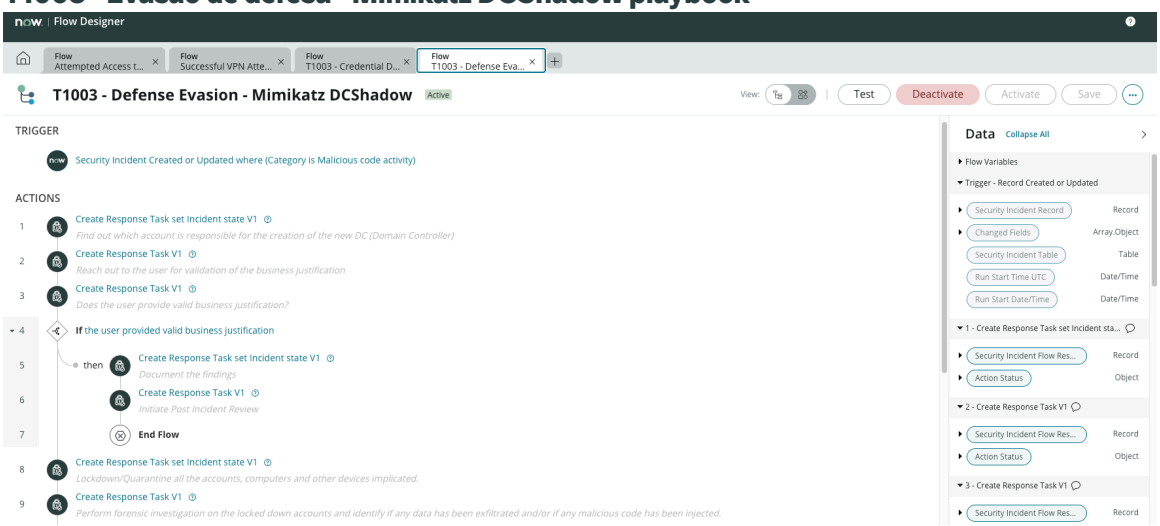
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, descubra qual conta é responsável pela criação do novo DC (Controlador de domínio).
2. Na Ação 2, entre em contato com o usuário para validar a justificativa de negócios.
   Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.
3. Na Ação 3, verifique se o usuário forneceu uma justificativa comercial válida.
4. Na Ação 4, se o usuário forneceu uma justificativa comercial válida, execute as seguintes etapas:

T1003 - Evasão de defesa - Mimikatz DCShadow playbook



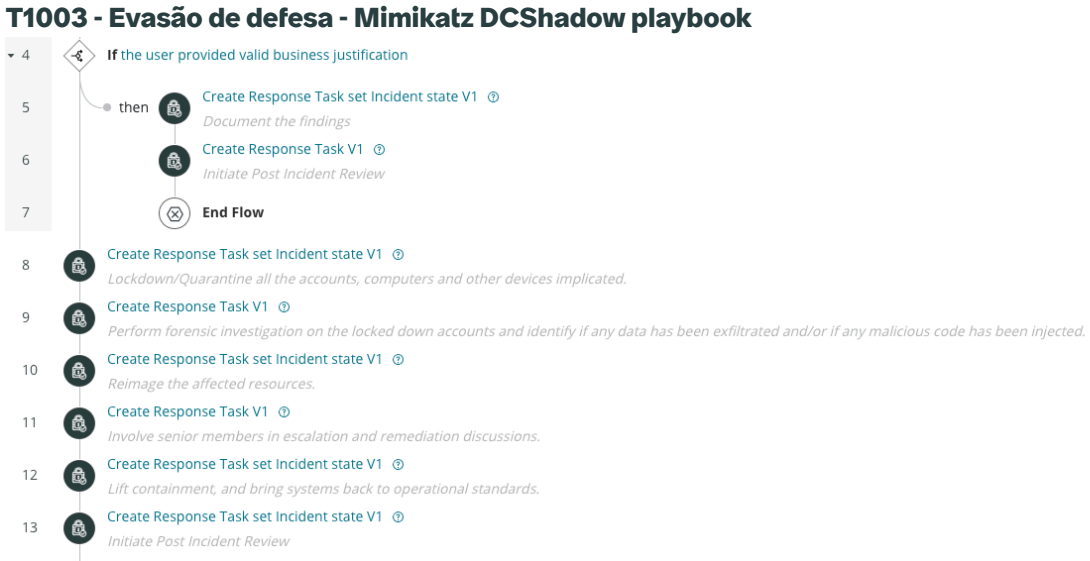
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 5, documente as descobertas até agora.

b. Em Ação 6, inicie uma revisão pós-incidente.
Na Ação 7, após a revisão pós-incidente, o fluxo termina.

5. Na Ação 8, se o usuário não forneceu uma justificativa comercial válida, execute as seguintes etapas:



a. Em Ação 9, bloqueie ou coloque em quarentena todas as contas, computadores e outros dispositivos envolvidos.

b. Na Ação 10, execute uma investigação forense nas contas bloqueadas e identifique se algum dado foi exfiltrado ou se algum código mal-intencionado foi injetado.

c. Na Ação 11, recrie a imagem dos recursos afetados.

d. Na Ação 12, levante a contenção e traga os sistemas de volta aos padrões operacionais.

e. Em Ação 13, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1003 - Dump de credenciais - Mimikatz DCSync

Este playbook fornece etapas de correção sistemáticas para investigar incidentes suspeitos de serem causados pelo Mimikatz DCSync. Este playbook é acionado quando uma das funções de Mimikatz (`lsadump::dcsync`) é usado. Normalmente, a função é usada em controladores de domínio (DC) atacados.

O Mimikatz é uma ferramenta de hacking popular que permite aos usuários emitir comandos que ajudam a recuperar dados confidenciais do sistema atacado. Os dados confidenciais incluem senhas, seus hashes e outros.

Nota: Este é um alerta de alta fidelidade, que é considerado raramente acionado. Quando for acionado, você deve notificar um membro sênior da equipe ou gerente imediatamente.

Configure o playbook T1003 - Dump de credenciais - Mimikatz DCsync

Use as etapas a seguir para configurar o playbook T1003 - Dump de credenciais - Mimikatz DCsync.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **T1003 - Dump de credenciais - Mimikatz DCsync** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook T1003 - Despejo de credenciais - Mimikatz DCsync e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione  e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



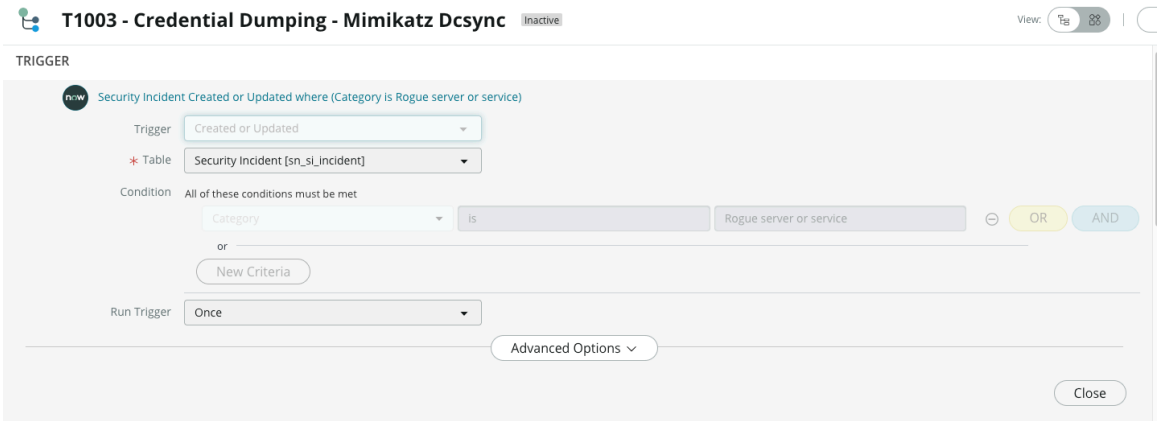
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Servidor ou serviço não autorizado** .

T1003 - Dump de credencial - Condição do gatilho do playbook do Mimikatz DCSync



Use o playbook T1003 - Dump de credenciais - Mimikatz DCsync

Use este playbook para investigar incidentes suspeitos de serem causados pelo Mimikatz DCSync. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no Playbook do T1003 - Despejo de credenciais - Mimikatz DCsync.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

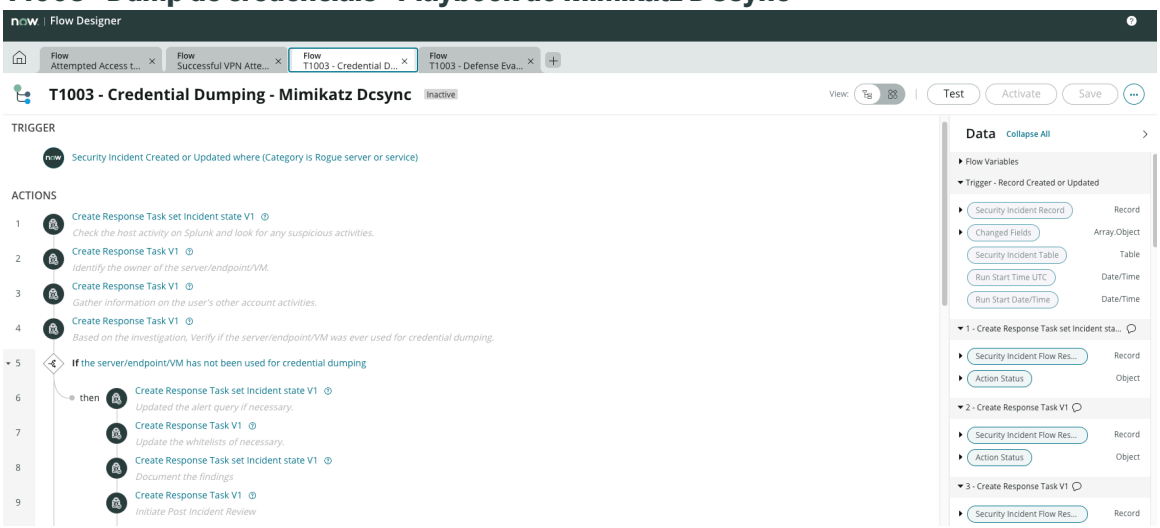
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, verifique a atividade do host no Splunk e procure atividades suspeitas.
2. Na Ação 2, identifique o proprietário do servidor/endpoint/VM.
   Se o usuário estiver online, execute o CrowdStrike EDR para coletar um escopo melhor das atividades do sistema.
3. Em Ação 3, colete informações sobre as outras atividades da conta do usuário.
4. Na Ação 4, com base na investigação, verifique se o servidor/endpoint/VM já foi usado para despejo de credenciais.
5. Na Ação 5, se o servidor/endpoint/VM não foi usado para despejo de credenciais, execute as seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

T1003 - Dump de credenciais - Playbook do Mimikatz DCsync



a. Na Ação 6, atualize a consulta de alerta, se necessário.

b. Na Ação 7, atualize a lista de permissões, se necessário.

c. Na Ação 8, documente as descobertas até agora.

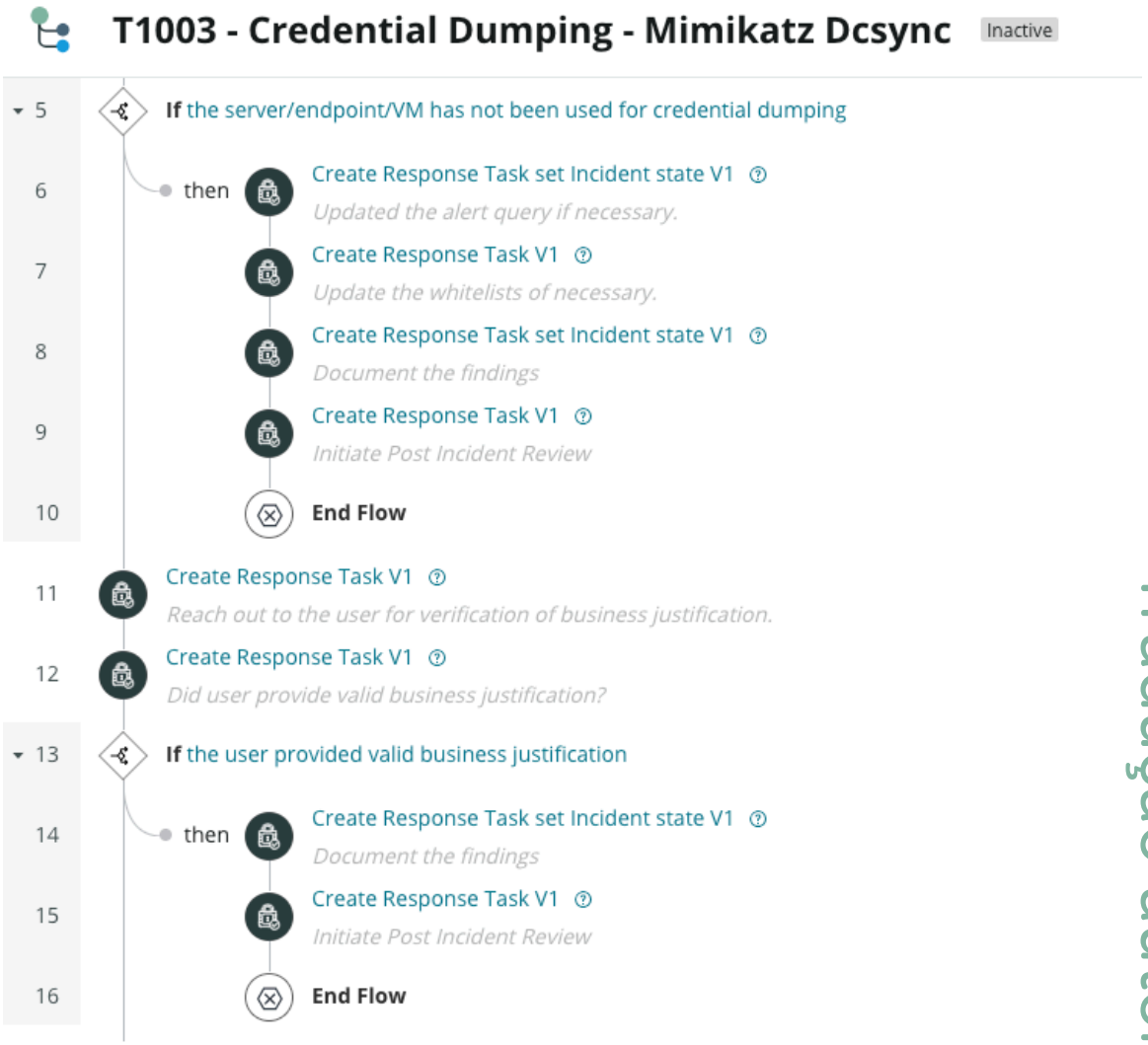
d. Em Ação 9, inicie uma revisão pós-incidente.
Na Ação 10, o fluxo termina.

6. Se o servidor/endpoint/VM foi usado para despejo de credenciais, na Ação 11, entre em contato com o usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook T1003 - Dump de credenciais - Mimikatz DCsync



7. Na Ação 12, entre em contato com o usuário para validar a justificativa de negócios.
8. Na Ação 13, se o usuário forneceu uma justificativa comercial válida, execute as seguintes ações:
   a. Na Ação 14, documente as descobertas até agora.
   b. Em Ação 15, inicie uma revisão pós-incidente.
      Na Ação 16, o fluxo termina.
9. Se o usuário não forneceu uma justificativa comercial válida, na Ação 17, coloque o sistema em quarentena.
10. Na Ação 18, remova todos os arquivos indesejados que possam ter sido criados ou excluídos pelas contas não autorizadas.
11. Na Ação 19, levante a contenção e traga os sistemas de volta aos padrões operacionais.
12. Em Ação 20, conclua a revisão pós-incidente antes de fechar a tarefa.

Falhas de login do usuário do Playbook para Okta de vários IPs

Este playbook fornece etapas de correção sistemáticas para investigar incidentes de falhas de login do usuário no Okta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O playbook Falhas de login do usuário do Okta de vários IPs fornece instruções sobre como analisar o alerta quando falhas de conta da ServiceNow são observadas no Okta de vários IPs não pertencentes à ServiceNow. O alerta relacionado a este playbook verifica os logs do Okta. Aciona um alerta quando ocorre falha de login para IDs de usuário da ServiceNow de mais de três intervalos de IP não pertencentes à ServiceNow em uma duração de 1 horas.

Configure as Falhas de login do usuário do Okta no playbook de vários IPs

Use as etapas a seguir para configurar as Falhas de login do usuário do Okta no playbook de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

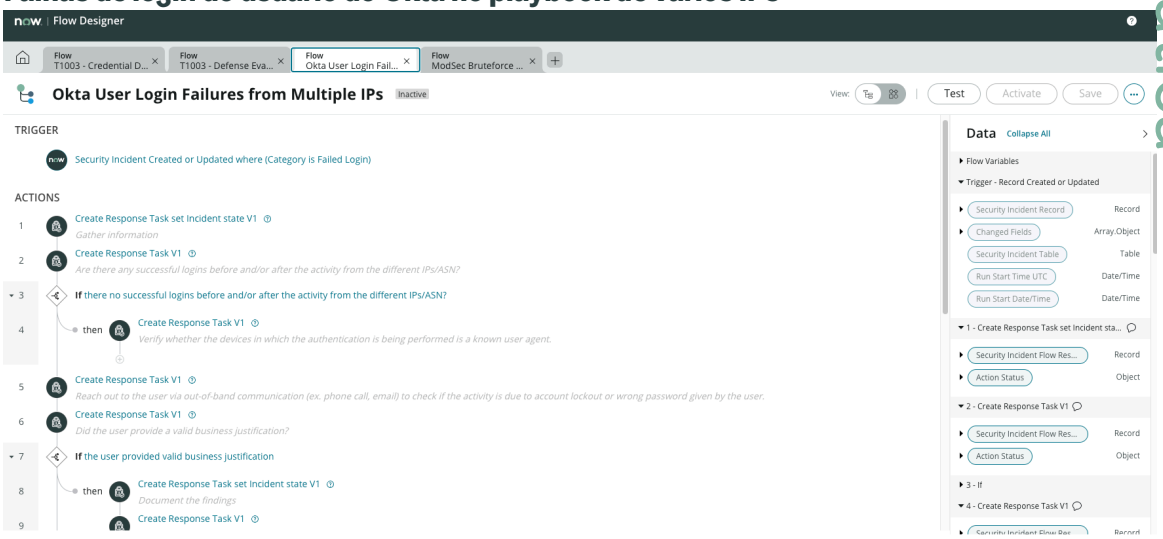
Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Falhas de login do usuário do Okta de vários IPs** playbook.
3. **Opcional:** Crie uma cópia das Falhas de login do usuário do Okta a partir do fluxo do playbook de vários IPs e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione ••• e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Falhas de login do usuário do Okta no playbook de vários IPs



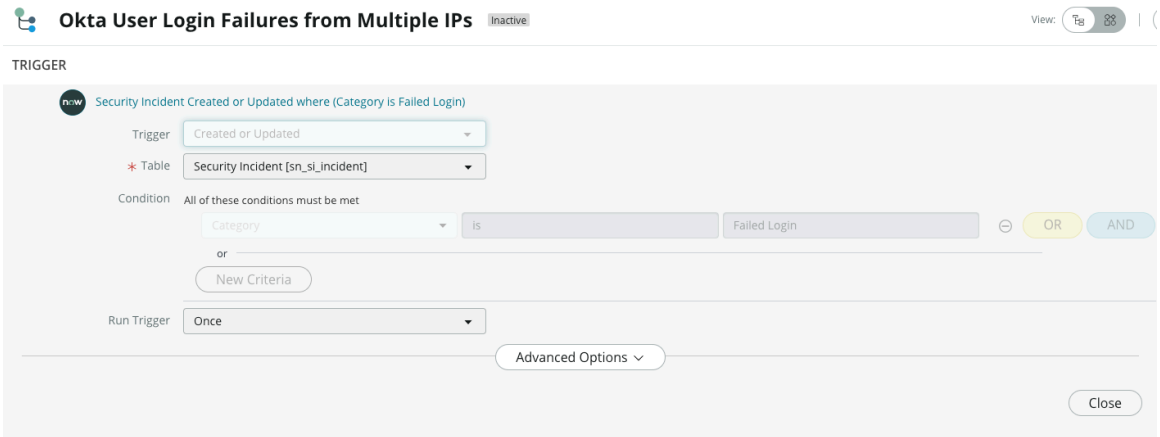
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando **Categoria** . **Login com falha** .

Condição de gatilho Falhas de login do usuário do Okta a partir de vários IPs playbook



Use o playbook Falhas de login do usuário do Okta de vários IPs

Use este playbook para investigar incidentes de segurança para falhas de login do usuário no Okta. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no Playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

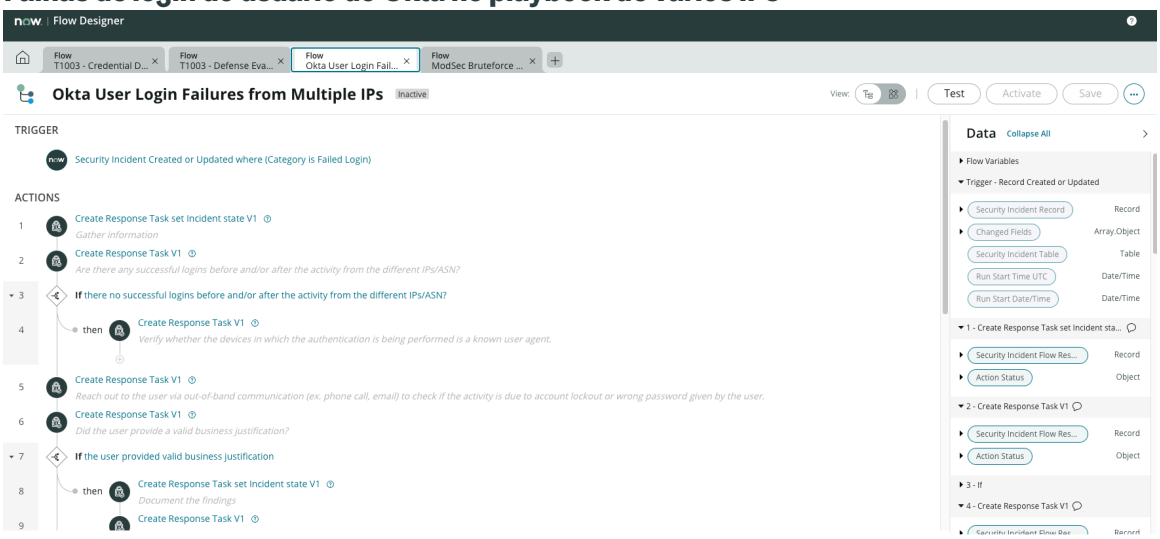
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, execute as seguintes tarefas:
   - Identifique a conta de usuário que está sendo direcionada.
   - Verifique a sub-rede IP e verifique se todas pertencem ao mesmo responsável pelo ASN (Autonomous System Number, número de sistema autônomo).
2. Na Ação 2, verifique se houve logins bem-sucedidos antes ou depois da atividade dos diferentes IPs/ASNs.
3. Na Ação 3, se não houve logins bem-sucedidos antes ou depois da atividade dos diferentes IPs/ASNs, na Ação 4, verifique se os dispositivos nos quais a autenticação está sendo realizada são agentes de usuário conhecidos.
   Se os dispositivos forem autenticados por agentes de usuário conhecidos, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falhas de login do usuário do Okta no playbook de vários IPs

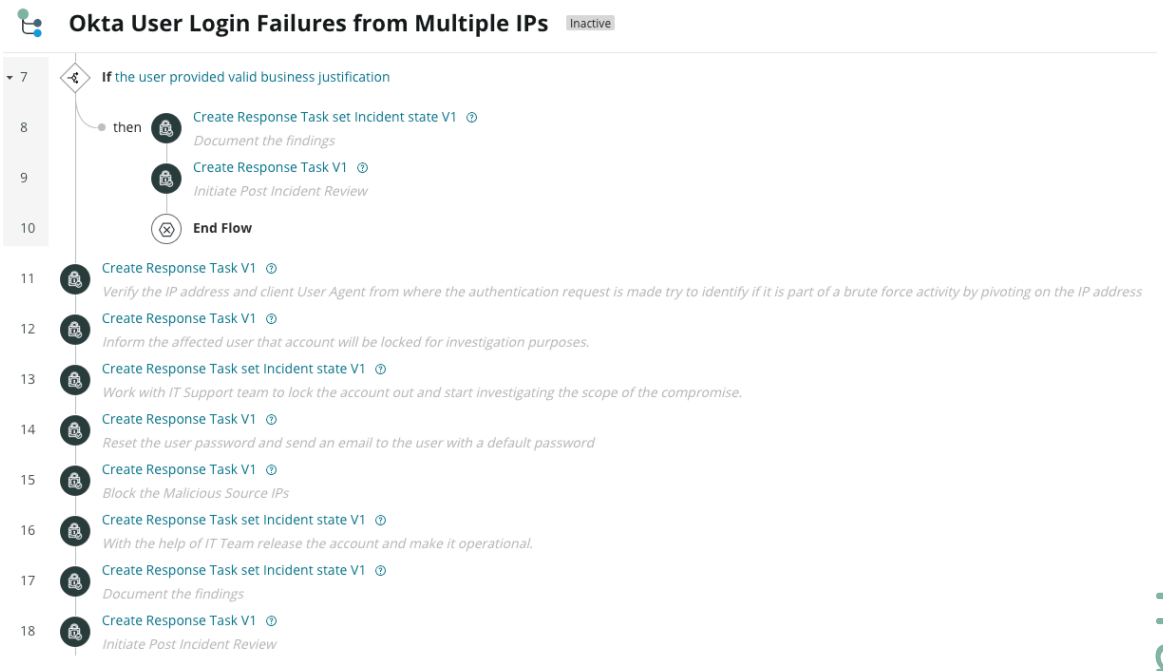


4. Na Ação 5, com base na investigação, entre em contato com o usuário por meio de comunicação fora de banda (por exemplo, chamada telefônica ou e-mail) para verificar se a atividade se deve ao bloqueio de conta ou a uma senha incorreta fornecida pelo usuário.
5. Na Ação 6, verifique se o usuário forneceu uma justificativa comercial válida.
6. Na Ação 7, se o usuário forneceu uma justificativa comercial válida, execute as tarefas a seguir.
   a. Em Ação 8, crie uma tarefa de resposta para documentar as descobertas até o momento.
   b. Em Ação 9, crie uma resposta para iniciar uma revisão pós-incidente.
   Na Ação 10, o fluxo termina.
7. Na Ação 11, verifique o endereço IP e o agente do usuário cliente de onde a solicitação de autenticação é feita e tente identificar se ele faz parte de uma atividade de força bruta girando o endereço IP.
8. Na Ação 12, informe ao usuário afetado que a conta será bloqueada para fins de investigação.
Você pode usar o modelo de e-mail fornecido para informar o usuário afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uso do playbook Falhas de login do usuário do Okta de vários IPs



9. Na Ação 13, trabalhe com a equipe de suporte de TI para bloquear a conta e começar a investigar o escopo do comprometimento.
10. Em Ação 14, redefina a senha do usuário e envie um e-mail para o usuário com a senha padrão.
11. Na Ação 15, bloqueie os IPs de origem mal-intencionada.
12. Na Ação 16, obtenha ajuda da Equipe de suporte DE TI para liberar a conta e trazê-la de volta aos padrões operacionais.
13. Na Ação 17, documente as descobertas até agora.
14. Em Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para ModSec força bruta por burst de IP

Este playbook fornece etapas de correção sistemáticas para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As condições do evento podem ser definidas na própria política do ModSec e gerarão um alerta no Splunk quando o evento for criado no ModSec.

Este playbook ajuda a detectar contagens anormais de tráfego na página de login. Duas explosões sucessivas de mais de 50 acessos/minuto devem ser de um IP para a página de login, o que indica uma tentativa de força bruta de fazer login.

Configure o playbook de força bruta do ModSec por IP Burst

Use as etapas a seguir para configurar o playbook de força bruta do ModSec por IP Burst.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o spoke do Security Operations (*sn_sec_spoke*).

Tradução automática

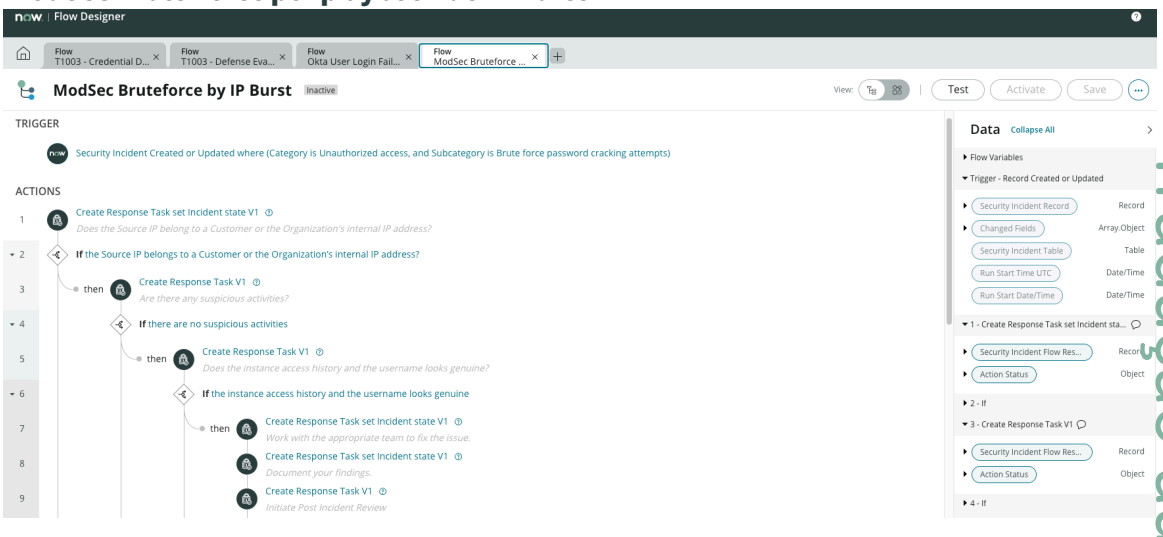
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione **Bruteforce do ModSec por burst de IP** playbook.
3. **Opcional:** Crie uma cópia do fluxo do playbook ModSec Bruteforce by IP Burst e faça as modificações necessárias.

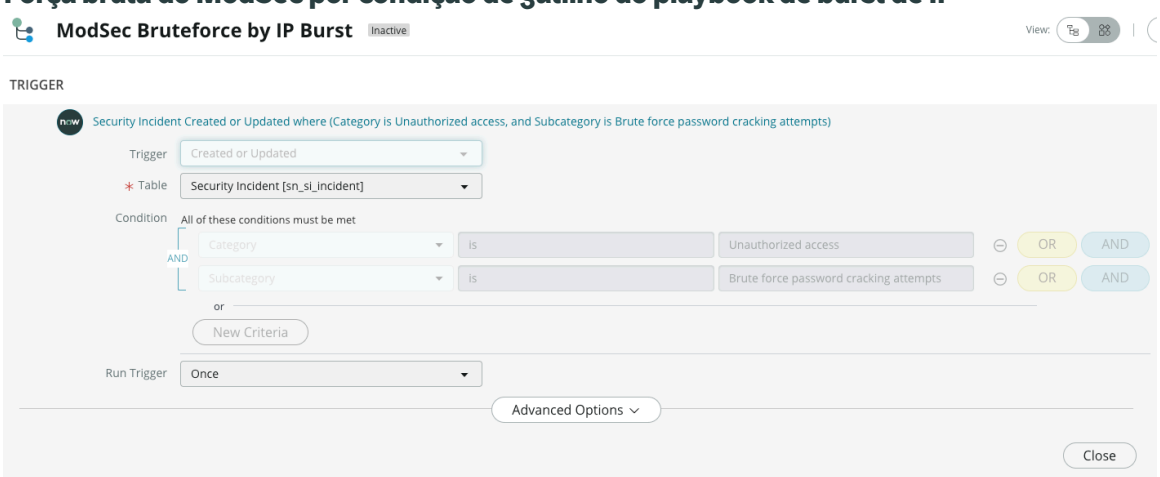
   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone do menu Mais ações ( ) e selecione **Copiar fluxo** . Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

ModSec Brute Force por playbook de IP Burst



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina um **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:
   - **Categoria** . **Acesso não autorizado** .
   - **Subcategoria** . **Tentativas de quebra de senha por força bruta** .

Força bruta do ModSec por condição de gatilho do playbook de burst de IP



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o playbook de força bruta do ModSec por IP Burst

Use este playbook para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de força bruta do ModSec por IP Burst.

Antes de Iniciar

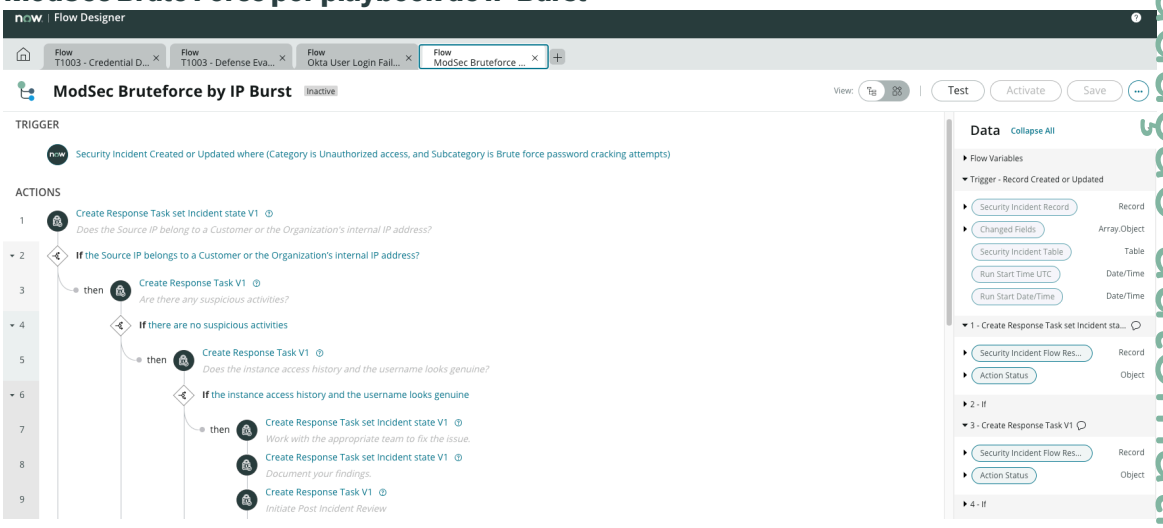
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, verifique se o IP de origem pertence a um cliente ou ao endereço IP interno da organização.
2. Na Ação 2, se o IP de origem pertencer a um cliente ou ao endereço IP interno da organização, execute as seguintes etapas:

ModSec Brute Force por playbook de IP Burst



   a. Na Ação 3, verifique se houve atividades suspeitas.

      - Verifique a atividade do IP de origem nos últimos dias. Se o IP teve tráfego insignificante, isso indica um ataque real.
      - Verifique os nomes de usuário de pulverização. Por exemplo, verifique se os nomes de usuário estão organizados em ordem alfabética.
      - Procure nomes de conta genéricos envolvidos. Por exemplo, admin, sysadmin, root, administrador, e outros nomes de conta da aplicação.

      Se não houver atividades suspeitas, o fluxo será encerrado.

   b. Na Ação 4, se houver atividades suspeitas, na Ação 5, verifique se o histórico de acesso à instância e o nome de usuário parecem genuínos.

      Verifique *Appnode*registra qualquer indicação de falha. Pode haver eventos de falha SAML, SSO ou LDAP, o que pode ser devido a um problema operacional.

      Se o histórico de acesso da instância e o nome de usuário não forem originais, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na Ação 6, se o histórico de acesso à instância e o nome de usuário forem originais, execute as seguintes etapas:

i. Na Ação 7, coordene com a equipe apropriada para corrigir o problema.

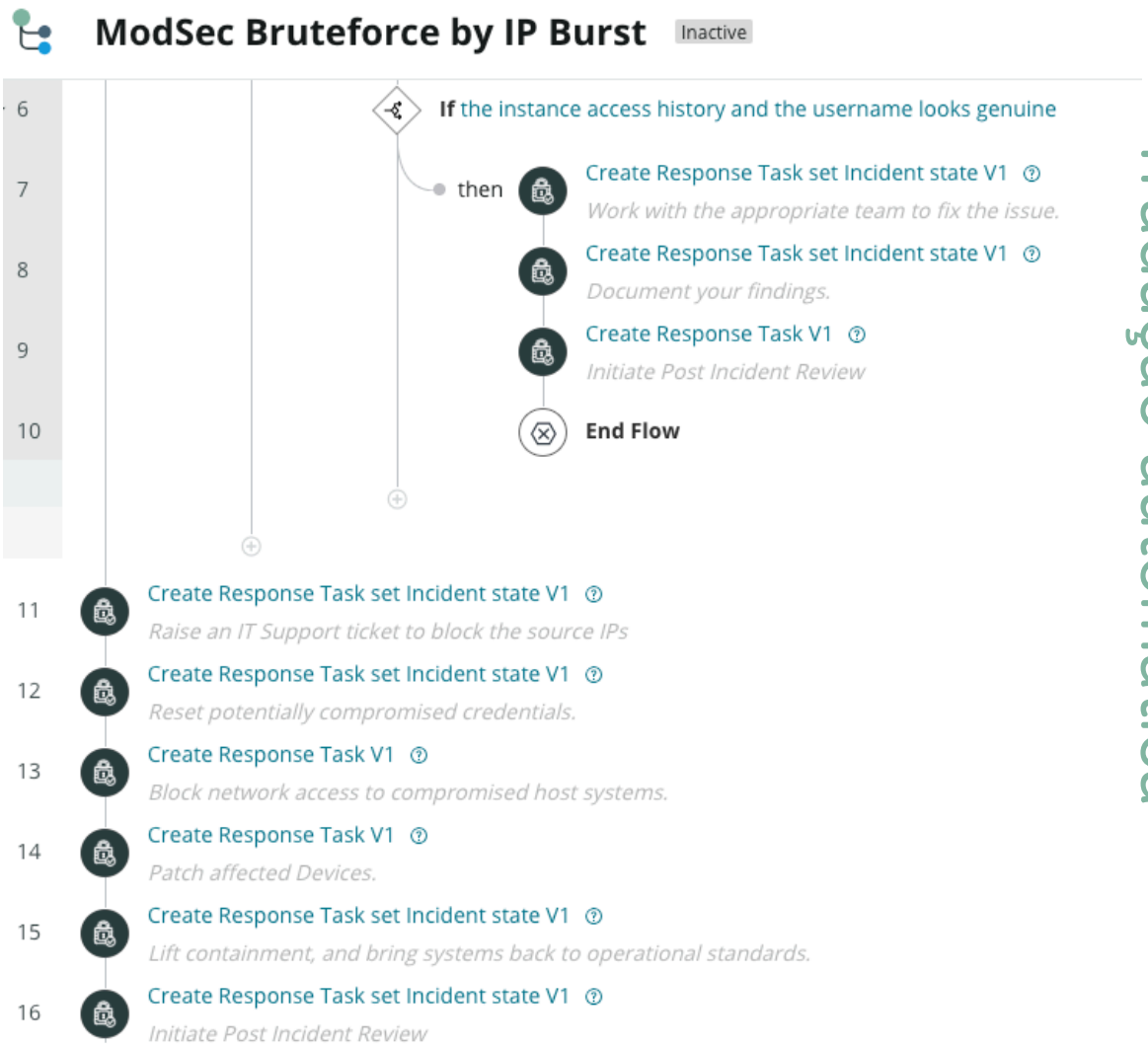
ii. Na Ação 8, documente as descobertas até agora.

iii. Em Ação 9, conclua a revisão pós-incidente antes de fechar a tarefa.

Na Ação 10, o fluxo termina.

3. Se o IP de origem não pertencer a um cliente ou ao endereço IP interno da organização, na Ação 11, gere um tíquete de suporte de TI para bloquear os IPs de origem.

Usando o playbook de força bruta do ModSec por IP Burst



4. Em Ação 12, redefina as credenciais potencialmente comprometidas.

5. Na Ação 13, bloqueie o acesso à rede aos sistemas host comprometidos.

6. Em Ação 14, corrija os dispositivos afetados.

7. Na Ação 15, levante a contenção e traga os sistemas de volta aos padrões operacionais.

8. Em Ação 16, conclua a revisão pós-incidente antes de fechar a tarefa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do playbook de resposta a incidentes de segurança

Esta seção descreve as ações fornecidas na biblioteca de ações do Flow Designer.

Nome da Ação	Descrição	Cenário de exemplo	
Adicione um marcador de segurança ao incidente de segurança	Use esta ação para adicionar um marcador de segurança automaticamente usando a lógica do Flow Designer.	. Se o fluxo detectar um IOC, o. **IOC detectado** o marcador pode ser adicionado automaticamente usando esta ação. **Fluxo** :	• Entrada: Incidente de segurança, marcador de segurança • Saída: Não aplicável
Adicione observáveis ao incidente de segurança	Use esta ação para adicionar observáveis a um incidente de segurança selecionado. • Por padrão, a lista de observáveis é separada pelo delimitador de vírgula (,), mas isso pode ser modificado. Você pode especificar outro caractere especial único como delimitador. Ao adicionar observáveis, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis são adicionados ao incidente de segurança, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis estão sendo adicionados, a opção Filtrar observáveis da lista permitida identifica observáveis da lista permitida e não os adiciona à lista relacionada de observáveis		• Entrada: ◦ incidente de segurança ◦ observáveis ◦ delimitador ◦ filtrar observáveis da lista permitida e publicar anotação de atividade • Saída: Não aplicável

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
	do incidente de segurança. Uma atividade automatizada do sistema (resposta) é adicionada para indicar que esses observáveis foram removidos.		
Obter usuários afetados (listas relacionadas) de vários incidentes de segurança V1	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para os incidentes de segurança especificados.	Você pode ter incidentes de segurança primários com vários incidentes de segurança secundários. Use esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para os incidentes de segurança primários correspondentes. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: Incidentes de segurança • Saída: ◦ usuário afetado ◦ contagem
Obter usuários afetados de vários incidentes de segurança	Recupera o usuário afetado primário do incidente de segurança especificado. Não inclui os usuários afetados da lista relacionada de usuários afetados.	• Ao investigar um incidente de segurança de phishing, envie um e-mail para os usuários primários afetados (que relataram o incidente de phishing) para confirmar se algum dos usuários clicou nos links maliciosos no e-mail de phishing. • Atualize a gravidade do incidente de segurança primário ou a pontuação de risco com base na contagem de usuários primários afetados.	• Entrada: Incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
Obter usuários afetados (lista relacionada) de um incidente de segurança	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para um incidente de segurança especificado.		• Entrada: Incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem
Adicione usuários afetados ao incidente de segurança	Adiciona todos os usuários afetados a um incidente de segurança.	Suponha que você tenha um incidente de segurança primário com vários incidentes de segurança secundários. Você pode usar esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para o incidente de segurança primário correspondente. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: ◦ incidente de segurança ◦ usuário • Saída: Não aplicável
Obtenha itens de configuração dos usuários afetados	Recupera os itens de configuração (ICs) de todos os usuários afetados.	Em cenários de phishing ou malware, você pode usar esta ação para atualizar a lista relacionada de Itens de configuração (IC) afetados e investigar os ICs. Você pode atualizar a gravidade ou a pontuação de risco do incidente de segurança com base no número de ICs identificados.	• Entrada: Usuários • Saída: ◦ itens de configuração ◦ contagem
Obtenha todos os incidentes de segurança secundários de um incidente de segurança	Recupera todos os incidentes de segurança secundários relacionados a um incidente de segurança primário específico.	Cenário de exemplo: Use esta ação para: • Atualize o status dos incidentes de segurança secundários quando o status de incidentes de segurança primário correspondente for atualizado. • Atualize a gravidade ou a pontuação de	• Entrada: ◦ incidente de segurança ◦ estado do incidente • Saída: ◦ incidente de segurança secundário ◦ contagem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		risco do incidente de segurança automaticamente com base no número de incidentes de segurança secundários.	
Obter itens de configuração para os observáveis (tipo endereço IP)	Recupera todos os itens de configuração (ICs) para observáveis do tipo endereço IP.	Um observável de endereço IP pode ser associado a um item de configuração. Por exemplo, o endereço IP de um servidor. Se você usar esta ação, poderá recuperar informações do servidor.	• Entrada: Endereço ip observável • Saída: ◦ itens de configuração ◦ contagem
Observável mal-intencionado	Confirma a presença de um ou mais observáveis mal-intencionados em um conjunto de observáveis.	Depois que a pesquisa de ameaças for concluída e você identificar a presença de observáveis mal-intencionados, poderá aumentar a gravidade ou a pontuação de risco de um incidente de segurança.	• Entrada: Incidente de segurança • Saída: Mal-intencionado (verdadeiro/falso)
Enviar e-mail para confirmar a interação do usuário	Envia e-mail em resposta a uma resposta do usuário.	Se um usuário tentar fazer login várias vezes em uma aplicação e falhar, isso resultará em um cenário de login com falha. Nesse caso, um e-mail é enviado ao usuário para confirmar se o usuário tentou fazer login ou não. Dependendo da resposta do usuário (Sim ou Não), diferentes ações podem ser realizadas. **Fluxo** Playbook manual de login com falha	
Filtrar observáveis da lista permitida	Use esta ação para permitir a lista de observáveis de um determinado conjunto de observáveis.	Você pode identificar determinados observáveis que podem ser ignorados de um conjunto de observáveis. Esses observáveis não serão levados em conta ao	• Entrada: Incidente de segurança • Saída: ◦ observáveis de lista permitidos ◦ contagem

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		resolver o incidente de segurança.	
Redefina a senha dos usuários afetados	Use esta ação para redefinir a senha dos usuários afetados.	Se uma conta de usuário tiver sido invadida ou um usuário solicitar que uma senha seja redefinida, um e-mail será enviado ao usuário para redefinir a senha. **Fluxo** Playbook manual de login com falha.	
Obter grupo de usuários do usuário afetado	Recupera os detalhes do grupo de usuários afetados.	Em uma organização, se dois ou mais usuários denunciarem e-mails de phishing, você poderá descobrir o grupo ao qual pertencem e identificar se mais usuários foram afetados	• Entrada: Usuário • Saída: ◦ grupos de usuários ◦ contagem

Representação visual da emissão de relatórios de resposta a incidentes de segurança

Os gerentes de segurança podem usar as interfaces gráficas de alto nível, como mapas e mapas de árvore, para identificar áreas de preocupação.

Para exibir Resposta a incidentes de segurança Painel do Explorer em Espaço de resposta a incidentes de segurança em detalhes, consulte Exibição de painéis do Espaço SIR.

Painel Visão geral do Resposta a incidentes de segurança

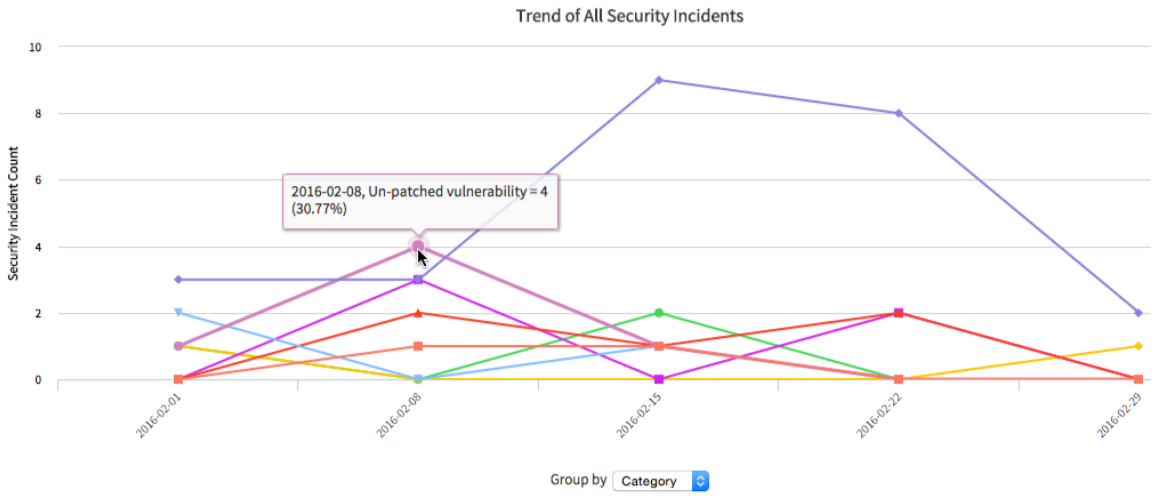
. Resposta a incidentes de segurança O painel de visão geral fornece uma exibição executiva da atividade de incidente de segurança, fornecendo tendências e relatórios e detalhamentos em dados específicos.

O módulo Visão geral exibe informações do incidente de segurança que são personalizadas para a função do usuário. Você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados, mapa térmico e assim por diante) para exibir dados gerais específicos dessa parte. Veja a imagem a seguir. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tendência de todos os incidentes de segurança



Visão geral do gerenciador de Incidentes de segurança

Usuários com as funções Administrador de incidentes de segurança e Gerenciador de incidentes de segurança exibem a Visão geral do Gerenciador de incidentes de segurança. Ele contém os seguintes relatórios no sistema de base.

Relatórios Visão geral do Gerenciador de incidentes de segurança

Nome	Visual	Descrição
Incidentes de segurança críticas da equipe	Pontuação única	O número de incidentes de segurança críticos atribuídos à equipe.
Incidentes de alta segurança da equipe	Pontuação única	O número de incidentes de alta segurança atribuídos à equipe.
ANS que expiram em 24 horas	Pontuação única	O número de ANS que expiram nas próximas 24 horas.
Risco versus gravidade	Mapa térmico	A distribuição de incidentes de segurança atribuídos à equipe por risco e gravidade.
Incidentes de segurança por classe de IC, últimos 3 meses	Gráfico de barras	A contagem de incidentes de segurança atribuídos à equipe por classe de item de configuração.
Tendência de todos os incidentes de segurança	Tendência	Plota a contagem do número de incidentes de segurança recebidos por categoria ou prioridade.
Incidentes de segurança de acesso não autorizado	Gráfico de barras	Exibe os tipos de categorias de incidentes de segurança recebidas ao longo do tempo.
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio para identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Visão Geral de Análise de Segurança

Usuários com a função Analista de incidentes de segurança exibem a Visão geral do analista de segurança. Ele contém os seguintes relatórios no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios Visão geral do analista de segurança

Nome	Visual	Descrição
Meu trabalho de prioridade crítica	Pontuação única	O número de incidentes de segurança críticos atribuídos a mim.
Meu trabalho de alta prioridade	Pontuação única	O número de incidentes de alta segurança atribuídos a mim.
Meus ANS que expiram em 24 horas	Pontuação única	O número de SLAs atribuídos a mim que expiram nas próximas 24 horas.
Incidentes de segurança atribuídos a mim	Gráfico de barras	Incidentes de segurança atribuídos a mim por estado ou categoria de incidente.
Trabalho atribuído a mim por tipo	Gráfico de barras	Tarefas de segurança (incidentes, tarefas ou solicitações) atribuídas a mim por tipo ou prioridade.
Incidentes de segurança, solicitações e tarefas atribuídos a mim	Lista	Uma lista de todos os incidentes de segurança, solicitações de segurança e tarefas atribuídas a mim.
Local do incidente de segurança	Mapa	Local regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espectro de cores.
Porcentagem de contagem	Mapa	Percentual da contagem total de incidentes por região.

Visão geral do CISO do incidente de segurança com Análise de incidentes de segurança ativada

. Análise de incidente de segurança O plug-in está ativado, os usuários com as funções de CISO de incidente de segurança e Administrador do sistema exibem a Visão geral do CISO de incidente de segurança. Os relatórios de CISO a seguir são fornecidos no sistema de base.

Relatórios de visão geral do CISO do incidente de segurança (com Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança recebidos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução por 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução por 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.
Novos incidentes de segurança diários versus incidentes de segurança encerrados	Tendência	Contagens de incidentes de segurança novos e encerrados ao longo do tempo por dia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do CISO do incidente de segurança (com Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos incidentes de segurança semanais versus incidentes de segurança encerrados	Tendência	Incidentes de segurança novos e encerrados ao longo do tempo por semana.
Código de fechamento de incidentes de segurança	Tendência	Contagem completa de códigos de fechamento ao longo do tempo.
Impacto de Incidente de segurança nos negócios	Mapa de Árvore	Serviços de negócio com incidentes de segurança com agrupamentos disponíveis por criticidade de negócios.
Tempo Médio para Conter (Por Semana)	Tendência	O tempo médio de 7 dias que leva para conter um incidente de segurança ao longo do tempo.
Tempo Médio para Eliminar (Por Semana)	Tendência	Tempo médio de 7 dias necessário para erradicar um incidente de segurança ao longo do tempo.
Tempo médio para identidade (semanal)	Tendência	Tempo médio de 7 dias necessário para identificar um incidente de segurança ao longo do tempo.
Local do incidente de segurança	Mapa	Local regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espectro de cores.
Porcentagem de contagem	Mapa	Percentual da contagem total de incidentes por região.

Visão geral do CISO do incidente de segurança sem a Análise de incidentes de segurança ativada

. Análise de incidente de segurança O plug-in não está ativado, os usuários com as funções de CISO de incidente de segurança e Administrador do sistema exibem a Visão geral do relatório de CISO de incidente de segurança. Os relatórios de CISO a seguir são fornecidos no sistema de base.

Relatórios de Visão geral do CISO do incidente de segurança (sem Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança abertos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução por 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução por 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.
Novos incidentes de segurança semanalmente	Tendência	Os novos incidentes de segurança eram abertos semanalmente.
Incidentes de segurança encerrados semanalmente	Tendência	Os incidentes de segurança eram encerrados semanalmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de Visão geral do CISO do incidente de segurança (sem Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Códigos de fechamento de incidentes de segurança	Tendência	Códigos de fechamento de incidentes de segurança ao longo do tempo.
Serviços de negócio com incidentes de segurança - Impacto nos negócios	Mapa de Árvore	Serviços de negócio com incidentes de segurança com agrupamentos disponíveis por criticidade de negócios.
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio para identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Nota: . Resposta a incidentes de segurança O sistema de base inclui Soluções de Performance Analytics para exibir painéis de práticas recomendadas pré-configurados. Os painéis apresentam métricas importantes para analisar seu processo de Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto. Para obter mais informações e instruções de instalação, consulte Resposta a incidentes de segurança Soluções para Análise da plataforma e relatórios.

Acesse o Security Incident Response Explorer

Você pode acessar Resposta a incidentes de segurança Painel do Explorer para exibir a atividade de incidente de segurança para identificar instantaneamente áreas de preocupação e resolver problemas rapidamente.

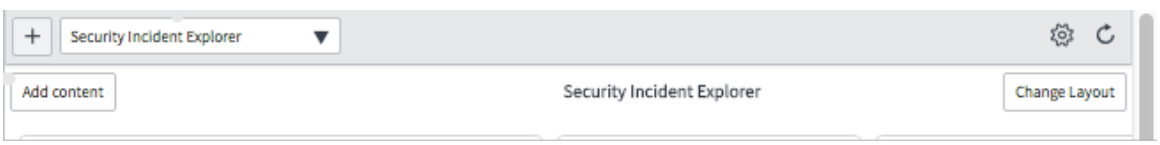
Antes de Iniciar

Funções necessárias:

- sn_si.admin (para gravar)
- sn_si_basic (para ler)

Procedimento

1. Navegar até **Tudo** > **Autoatendimento** > **Página inicial** ou navegue até **Autoatendimento** > **Painéis**.
2. Escolha Explorador de incidentes de segurança na lista de relatórios.



Resultado

. Resposta a incidentes de segurança O painel do Explorer é exibido.

O que Fazer Depois

Para exibir Resposta a incidentes de segurança Painel do Explorer em Espaço de resposta a incidentes de segurança em detalhes, consulte Exibição de painéis do Espaço SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapa de incidentes de segurança

O mapa de incidentes de segurança fornece dados por localização geográfica. O mapa-múndi é realçado em todas as áreas em que ocorre um incidente. . Análise de incidente de segurança o plug-in está ativado, você pode adicionar o mapa de incidentes de segurança ao Resposta a incidentes de segurança visão geral. Depois de adicionado, você pode configurar o mapa modificando os filtros de mapa.

Adicionar mapa a. Resposta a incidentes de segurança visão geral

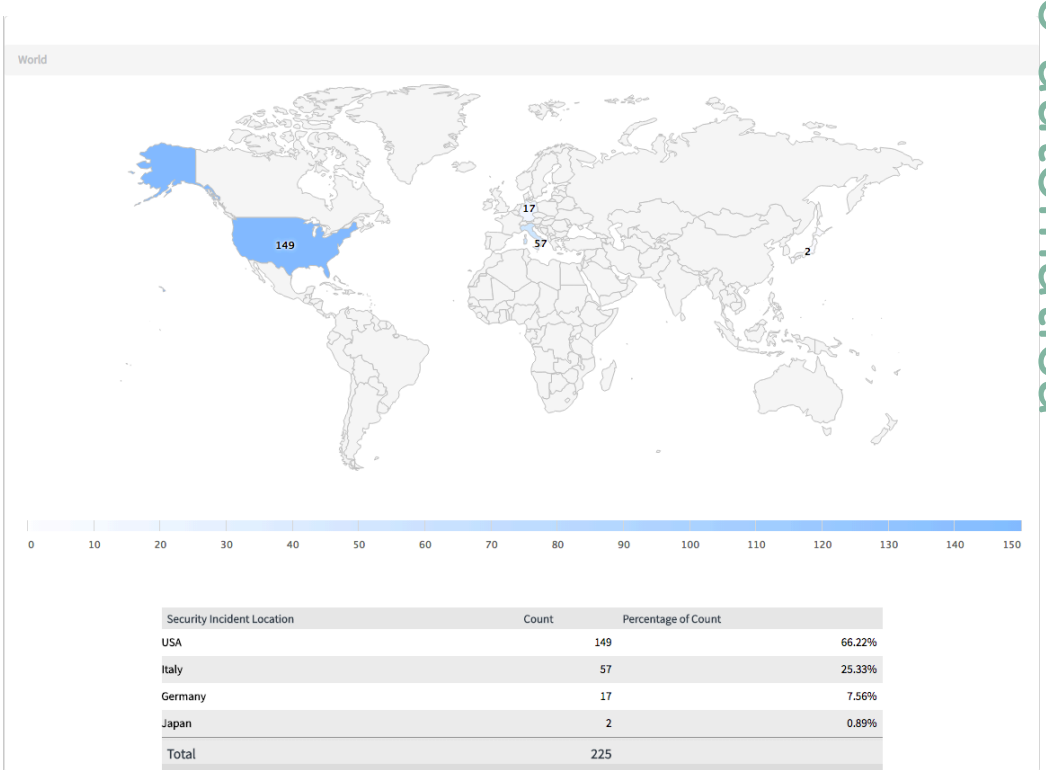
Você pode adicionar o mapa ao Resposta a incidentes de segurança visão geral para exibir dados de incidentes de segurança por localização geográfica. Um mapa permite detalhar as informações do incidente de segurança por local.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em **Relatórios** .
4. Na segunda caixa de seleção, clique em **Incidente de segurança** .
5. Na terceira caixa de seleção, clique em **Mapa de incidentes de segurança** .



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. Na parte inferior da tela, clique no local na tela que você deseja adicionar ao relatório.
7. Feche o. **Adicionar conteúdo** caixa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modificar mapa de incidentes de segurança

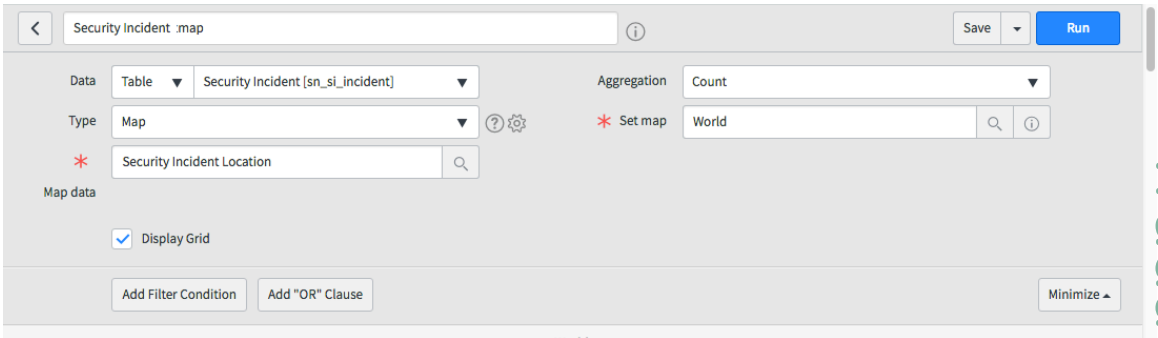
Os administradores no domínio global podem modificar como o mapa de incidentes de segurança lida com incidentes de segurança usando filtros.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Relatórios** > **Administração** > **Tudo**.
2. Pesquisar **Mapa de incidentes de segurança** .
3. Clique em **Editar Relatório** .



4. Clique em **Adicionar condição de filtro** para adicionar ou editar filtros.
5. Clique em **Executar** para ver as mudanças aplicadas.
6. Clique em **Salvar**.

Mapas em árvore de incidentes de segurança

. Análise de incidente de segurança se o plug-in estiver ativado, você pode adicionar os mapas de árvore de incidente de segurança - impacto no serviço e incidente de segurança - em tempo real ao Resposta a incidentes de segurança visão geral. Depois que eles forem adicionados, você pode configurar os mapas de árvore modificando as categorias e os indicadores do mapa de árvore.

Adicione mapas de árvore à visão geral da Resposta do incidente de segurança

Os mapas de árvore exibem dados hierárquicos (estruturados em árvore) como um conjunto de retângulos aninhados. Cada ramificação da árvore recebe um retângulo, que é então lado a lado com retângulos menores que representam subramificações. Os mapas de árvore permitem exibir informações de incidentes de segurança de maneira dinâmica e envolvente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em **Mapa de árvore** .

Tradução automática

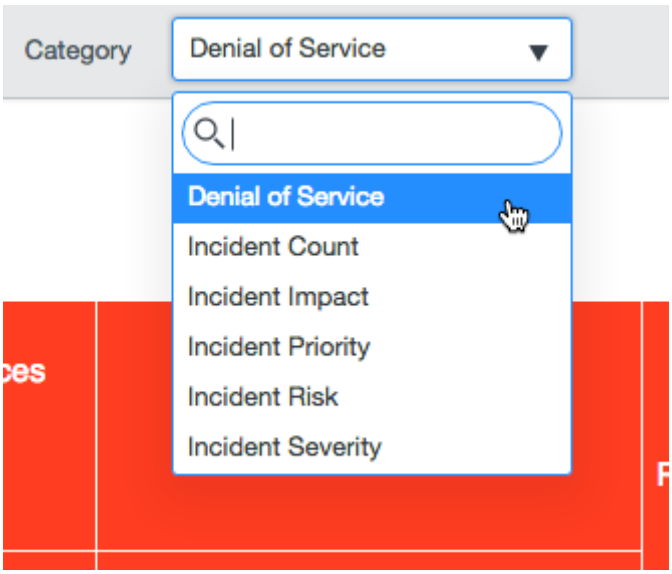
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na segunda caixa de seleção, selecione o mapa de árvore que você deseja inserir na lista a seguir:
   - Incidente de segurança - Impacto no serviço
   - Incidente de segurança - Tempo real
   - Incidente de segurança - Impacto nos negócios
   - Importância da vulnerabilidade

   Nota: O mapa de árvore Impacto nos negócios aparece no Resposta a incidentes de segurança página inicial por padrão. Os mapas em árvore Impacto no serviço e Tempo real exigem que o plug-in Análise de incidentes de segurança esteja ativado.

5. Na terceira caixa de seleção, selecione o nível de granularidade das informações que você deseja recuperar para o mapa de árvore selecionado.

   Nota: Para o mapa de árvore Incidente de segurança - Impacto no serviço, selecione **Incidente de segurança** na terceira caixa de seleção. Esta seleção fornece uma lista suspensa com várias categorias de dados.



6. Na parte inferior da tela, clique no local na tela em que você deseja adicionar o medidor.
7. Feche o. **Adicionar conteúdo** caixa.

Criar ou atualizar uma categoria de mapa de árvore

Você pode modificar as categorias predefinidas para os mapas em árvore de incidentes de segurança ou criar categorias conforme necessário.

Antes de Iniciar
Função necessária: sn_si.admin

Os mapas de árvore usam a análise de desempenho como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Por Que e Quando Desempenhar Esta Tarefa
No sistema de base, as categorias de mapa de árvore, como Risco de incidente, Negação de serviço e Severidade do incidente, estão incluídas. Você pode modificar essas categorias ou definir mais categorias conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração**e abra a definição de mapa de árvore para a qual você deseja configurar as categorias:
   - **Definição da emissão de relatórios de criticidade do serviço**
   - **Definição em tempo real**
2. **Opcional:** Mude o nome da definição do mapa de árvore.
   No sistema de base, o nome padrão para a definição do mapa de árvore do impacto do serviço é **Incidente de segurança** . O nome padrão para a definição do mapa de árvore em tempo real é **Incidente de segurança - Tempo real** .
3. A menos que você esteja usando um mapa de árvore personalizado, não mude **Grupo de indicadores de PA** valor.
4. Para desativar a definição do mapa de árvore, limpe **Ativo** caixa de seleção.
   Se, por exemplo, você desativar a categoria Negação de serviço no painel Impacto do sistema, essa categoria de mapa de árvore não estará disponível.
5. Em **Categorias de mapa de árvore** lista relacionada, selecione uma categoria para modificar ou clique em **Novo** para criar uma nova categoria.
6. Preencha os campos.

Formulário Categoria de mapa de árvore

Campo	Descrição
Nome	O nome exibido para a categoria em **Categorias** lista acima do mapa de árvore.
Ordem	A ordem em que a categoria aparece **Categorias** lista acima do mapa de árvore.
Mapa de Árvore	O nome do mapa de árvore que usa esta categoria.
Cor	A cor exibida para esta categoria no mapa de árvore.
Ativo	Selecione para ativar esta categoria.
Descrição	Uma descrição da categoria.
Visível para todas as funções	Selecione para tornar esta categoria visível para todos os usuários, independentemente de sua função.
Funções	Se você não selecionou **Visível por todas as funções** marque as funções capazes de exibir esta categoria.

7. Clique em **Enviar** ou **Atualizar**.

Crie ou atualize um indicador de mapa de árvore

Você pode modificar os indicadores predefinidos para uma categoria de mapa de árvore ou criar novos indicadores. Para cada indicador, você pode configurar sua fonte de dados e especificar como as listas de incidentes de segurança são abertas a partir de mapas de árvore que são exibidos com o indicador.

Antes de Iniciar

Função necessária: sn_si.admin

Os mapas de árvore usam a análise de desempenho como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra a definição de mapa de árvore para a qual você deseja configurar indicadores.

Definição de mapa de árvore	Ação
Mapa de árvore do impacto do serviço	Navegar até **Incidente de segurança** > **Administração** > **Definição de Impacto de Serviço**.
Mapa de árvore em tempo real	Navegar até **Incidente de segurança** > **Administração** > **Definição em tempo real**.

2. Em **Categorias de mapa de árvore** lista relacionada, selecione a categoria para a qual você deseja configurar indicadores.
3. Em **Indicadores de mapa de árvore** lista relacionada, selecione um indicador para modificar ou clique em **Novo** para criar um novo indicador.
4. Preencha os campos.

Formulário Indicador de mapa de árvore

Campo	Descrição
Nome	O nome exibido para o indicador no **Indicadores** lista no painel de impacto do serviço.
Descrição resumida	Uma descrição que é exibida para o indicador no **Indicadores** lista acima do mapa de árvore.
Limite do resultado	O número máximo de resultados permitidos. O limite superior é 100.
Precisão do resultado	O número de dígitos a serem exibidos após a vírgula decimal. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Ativo	Marque a caixa para ativar este indicador.
Categoria	O nome da categoria inserido na tela anterior.
Direção	Indica se o bloco no mapa de árvore está minimizado ou maximizado. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Unidade	A unidade de medida a ser usada para a métrica. Este campo é exibido somente para a definição em tempo real.
Intervalo de atualização automática	Com que frequência atualizar o mapa de árvore.
Ordem	A ordem em que o indicador aparece **Indicadores** lista acima do mapa de árvore.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Configuração da fonte de dados** e configure uma das seguintes opções de fonte de dados para o indicador.

Opção	Ação
Análise de desempenho	Selecione **Performance Analytics** em **Fonte de dados** e faça as seguintes entradas: ○ **Indicador:** O indicador usado para agru–par os dados de PA. ○ **Detalhamento padrão:** O detalhamento padrão usado para dividir o indicador de PA selecionado em várias partes.
Script personalizado	Selecione **Script personalizado** em **Fonte de dados** campo. Em seguida, use o editor de HTML para personalizar o script conforme necessário. O re-sultado da execução do script deve ser uma matriz para que as informações sejam exibidas no mapa de árvore.
Condições da consulta	Selecione **Condição de consulta** em **Fonte de dados** e, em seguida, faça as seguintes entradas: ○ **Tabela de consulta:** A tabela base a ser consultada. ○ **Tipo de agregado:** O tipo de agregado (SOMA, COUNT, AVG, MIN, MAX) a ser usado. ○ **Campo agregado:** O campo a ser usado pela consulta. ○ **Agrupar por:** O campo para classificar os dados consultados. **Nota:** Para aprimorar a consulta, clique em **Adicionar condição de filtro** e. **Adicione cláusula "OR"** .

6. Clique em **Clique em** e especifique como as listas de incidentes de segurança são abertas no mapa de árvore.
   a. Em **Por meio do tipo de navegação de URL** selecione se você deseja que a lista de incidentes de segurança seja aberta em uma nova janela, na mesma janela ou em uma caixa de diálogo.
   b. **Opcional:** Em **Clique no script de URL** modifique o script de amostra, se necessário.
7. Clique em **Enviar** ou **Atualizar**.

Adicione gráficos de significância de vulnerabilidade a uma visão geral

. Resposta a vulnerabilidades O plug-in está ativado, você pode adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

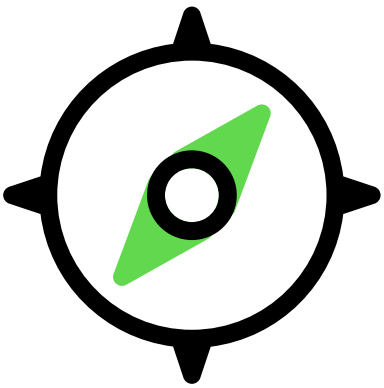
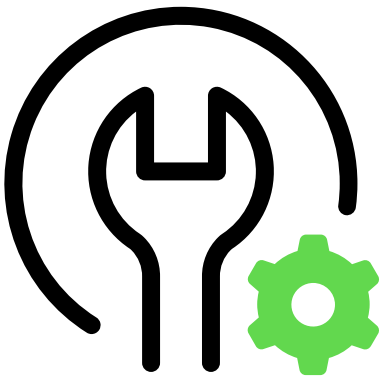
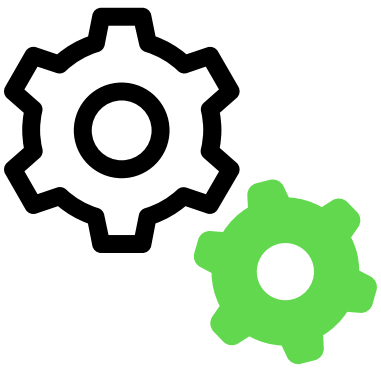
Procedimento

1. Navegue até a página Visão geral à qual você deseja adicionar o medidor de significância da vulnerabilidade.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Nas três caixas de seleção, faça as seleções dependendo do medidor (mapa de árvore ou relatório de pontuação) que você deseja adicionar:
   - Para adicionar o mapa de árvore Significância da vulnerabilidade, faça estas seleções:
     - Mapa de Árvore
     - Importância da vulnerabilidade
     - Importância da vulnerabilidade
   - Para adicionar o relatório de pontuação de significância da vulnerabilidade, faça estas seleções:
     - Performance Analytics
     - Pontuação
     - Serviços com significância de vulnerabilidade
4. Clique no local na tela em que você deseja adicionar o medidor.
5. Feche o. **Adicionar conteúdo** caixa.

Gestão de incidentes graves de segurança

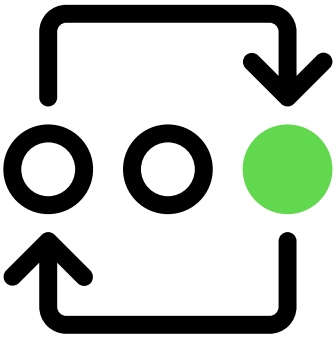
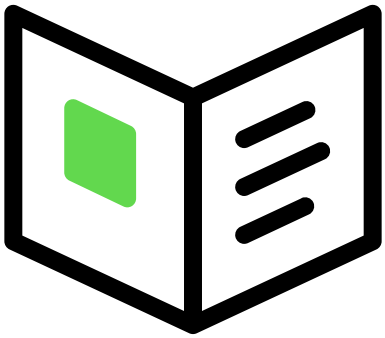
. ServiceNow® Gestão de incidentes graves de segurança a aplicação rastreia o andamento de Incidente grave de segurança(MSI) Da descoberta à análise, propor, promover e vincular incidentes de segurança e fechamento.

Gestão de incidentes graves de segurança

Explorar	Configurar	Integrar
		
Saiba mais sobre como analistas, administradores e gerentes usam a Gestão de incidentes de segurança graves (MSIM)	Planeje e configure sua implementação	Estenda os recursos do MSIM integrando com outros Microsoft aplicações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administrar	Uso	Relatórios de Status
		
Tarefas de administração sobre como marcar registros de incidentes e configurar rótulos	Propor, promover, vincular e rejeitar registros de incidentes de segurança graves por meio da gestão do espaço	Monitore tarefas relacionadas a incidentes e melhore os processos por meio de métricas, gráficos de tendências e relatórios

Capacidades adicionais

Configure informações para acumular registros

Tradução automática

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Solicitar um aplicativo Operações de segurança na Store

Se você é um novo Operações de segurança cliente em Rome ou, mais tarde, visite ServiceNow Store site para exibir os apps disponíveis e informações sobre como enviar solicitações para a loja.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solucionar problemas e obter ajuda

- Gestão de incidentes graves de segurança fórum em Comunidade ServiceNow.
- Biblioteca de recursos de operações de segurança
- Comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorar a Gestão de incidentes de segurança graves

Explorar Gestão de incidentes graves de segurança entender como a aplicação funciona em termos de rastrear incidentes de segurança críticos de alta prioridade, que são identificados como uma ameaça para a organização.

Use esta seção para conhecer os principais recursos e as várias funções envolvidas no trabalho com registros de incidentes de segurança graves. Esta seção também ajuda você a entender como começar a usar a aplicação, os pré-requisitos e os plug-ins necessários para trabalhar com a aplicação.

Gestão de incidentes graves de segurança

Rastreie e gerencie várias atividades que normalmente fazem parte da resolução de um incidente de segurança grave por meio do Gestão de incidentes graves de segurança. Por meio de um espaço intuitivo, os gerentes de incidentes e aqueles que trabalham em um incidente podem propor e promover incidentes a incidentes graves, rastrear atividades de incidentes de segurança graves e colaborar facilmente com os colegas.

Visão geral

Os recursos de gestão de incidentes de segurança graves funcionam em conjunto com os recursos de produto de resposta a incidentes de segurança existentes. Isso inclui a capacidade de um analista de segurança escalar um incidente de segurança padrão para um incidente de segurança grave, para que os novos recursos do produto estejam disponíveis para oferecer suporte ao processo de correção.

Depois de instalar em seu ServiceNow um analista de incidentes de segurança pode:

- Propor um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão sobre a necessidade de criar um incidente de segurança grave.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem a necessidade de um processo de revisão adicional.
- Rejeitar um incidente de segurança proposto como incidente de segurança grave (MSI).
- Vincule um incidente de segurança como incidente secundário ao incidente de segurança grave (MSI) para que todos os incidentes de segurança possam ser resolvidos.

Principais recursos

A Gestão de incidentes de segurança graves (MSIM) melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves projetado para a função de usuário de gerente de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança "secundários".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Automatizar a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.
- Componente explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de um Microsoft SharePoint integração.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, DE TI e DE segurança por meio de um Microsoft Teams integração.

Componentes do espaço

. Gestão de incidentes graves de segurança o produto contém vários novos componentes do espaço e páginas de interface do usuário que fornecem a funcionalidade de recursos principais:

- Espaço dedicado para gerenciar incidentes de segurança graves, projetado especificamente para a função de usuário do Gerenciador de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança secundários.
- Automatizar a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.
- Componente explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de um Microsoft SharePoint integração.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, DE TI e DE segurança por meio de um Microsoft Teams integração.

Versões compatíveis com a Gestão de incidentes de segurança graves

Gestão de incidentes graves de segurança(MSIM) requer ServiceNow AI Platform® Versão Rome.

Este recurso oferece suporte a Microsoft Teams, que é um espaço centrado no bate-papo no Microsoft Office 365 pacote. Anterior Microsoft Teams foi uma instalação separada de Microsoft Office 365 aplicações.

Versões da ServiceNow AI Platform compatíveis

Este recurso é compatível com Rome e versões posteriores.

A seguir Operações de segurança as aplicações são o padrão Resposta a incidentes de segurança plug-ins que provavelmente serão instalados para a maioria dos usuários se eles já estiverem usando Resposta a incidentes de segurança(SIR). Se não estiver instalado, você deverá instalar e ativar a partir de ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem mencionada para garantir uma instalação tranquila:

1. Resposta a incidentes de segurança: com.snc.si_dep é o plug-in dependente. Instalar este plug-in ativa as outras aplicações de Operações de segurança.
2. Framework de integração de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Security Support Common
4. Orquestração do Security Support Common

Para começar com MSIM

Revise as informações a seguir antes de começar a trabalhar com Gestão de incidentes graves de segurança.

Função necessária: sn_msi.workspace_admin.

Para uma instalação e configuração fáceis do Gestão de incidentes graves de segurança, talvez você precise verificar se os plug-ins a seguir estão ativados.

Importante: Um conjunto de atualizações (KB1289784) Está disponível no Guia de início rápido da Gestão de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações depois de concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de início rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Pré-requisito

Tarefa	Descrição
Antes de começar com a aplicação, certifique-se de ter os plug-ins dependentes necessários.	Como primeira etapa, instale: • ServiceNow IntegrationHub Installer (com.glide.hub.integrations) • ServiceNow® IntegrationHub Tempo de execução (com.glide.hub.integration.runtime). • ServiceNow® IntegrationHub Etapa de ação - REST (com.glide.hub.action_step.rest) • ServiceNow® IntegrationHub Modelo de ação - Fluxo de dados (com.glide.hub.action_type.datastream) • ServiceNow® IntegrationHub Flow Designer - Entradas dinâmicas (com.glide.hub.dynamic_inputs) **Nota:** Se você não tiver os privilégios necessários para nenhum dos listados ServiceNow® IntegrationHub e, em seguida, crie um tíquete de suporte para instalar esses aplicativos de pré-requisito.
Verifique se você tem o acesso necessário para instalar Microsoft SharePoint Spoke e. Microsoft Teams Graph Spoke. **Nota:** As principais aplicações dependentes listadas acima são as principais aplicações dependentes com as quais começar Gestão de incidentes graves de segurança.	Antes de instalar Microsoft SharePoint Spoke e. Microsoft Teams Graph Spoke, certifique-se de ter o acesso necessário ao ServiceNow IntegrationHub aplicações. **Nota:** Microsoft SharePoint Spoke e. Microsoft Teams Graph os spoke são aplicações dependentes do ServiceNow® IntegrationHub aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para MSIM configuração

Antes de usar o. ServiceNow® Gestão de incidentes graves de segurança(MSIM), baixe o aplicativo do ServiceNow® Store.

Acompanhe seu andamento com a instalação, a instalação e a configuração da tabela a seguir.

Nota: As funções atribuídas para Gestão de incidentes graves de segurança as aplicações estão listadas nas seções a seguir. para obter mais informações, consulte Gestão de incidentes graves de segurança funções.

Use a check-list a seguir para orientá-lo pelas etapas completas para instalar e configurar Gestão de incidentes graves de segurança aplicação.

Check-list

Configuração de tarefa	Descrição
Verifique se o Gestão de incidentes graves de segurança a aplicação é instalada e ativada no ServiceNow® Store.	Gestão de incidentes graves de segurança v1.1.1 está disponível em ServiceNow® Store. Siga estas instruções: baixando uma aplicação do ServiceNow Store.
Verifique se os seguintes aplicativos estão instalados na ordem fornecida.	Os seguintes aplicativos serão instalados por padrão após a instalação Gestão de incidentes graves de segurança aplicação na versão de lançamento atual da aplicação: • File Explorer Core for Operações de segurança v1.1.1 • Microsoft SharePoint File Explorer Conector para Operações de segurança v1.1.1 • File Explorer Componente para Operações de segurança v1.0.0 • Microsoft Teams Conector de bate-papo para Operações de segurança v1.0.0 • Núcleo de bate-papo para Operações de segurança v1.0.0 • Incidente grave de segurança Resposta v1.1.1 • Cartão EVAM de bate-papo colaborativo para MSIM Espaço v1.0.0 (Esta aplicação é configurada somente para as visualizações de IU no plano de fundo da aplicação para Gestão de incidentes graves de segurança) • Componente de IU do Organizador de tarefas para Gestão de incidentes graves de segurança espaço 1.0.0 • Resposta a incidentes de segurança v12.8.1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se as funções de usuário estão atribuídas a. Incidente grave de segurança conforme apropriado.	A seguir estão as funções envolvidas durante todo o ciclo de vida do incidente de Incidente grave de segurança processo de correção: • Administrador MSI [sn_msi.workspace_admin] • MSI Manager [sn_msi.workspace_manager] • Respondente MSI [sn_msi.workspace_responder Para obter informações mais detalhadas sobre cada função, consulte Gestão de incidentes graves de segurança funções.
Verifique se você configurou com sucesso Microsoft SharePoint v1.0.0 configuração.	Microsoft SharePoint gerencia sites, pastas, arquivos, grupos e usuários no Microsoft SharePoint. Adicionar Microsoft SharePoint dados para seu ServiceNow® instância. Para fazer isso, você deve configurar as conexões do Graph e REST. Para obter informações, consulte Microsoft SharePoint Spoke v1.1.2 Documentação sobre como configurar a Configuração de conexões REST e Graph. Estabeleça uma conexão do Graph e REST para se conectar ao seu ServiceNow® instância de Microsoft SharePoint.
Verifique se você criou um Microsoft SharePoint site para criar uma biblioteca de documentos.	Crie um Microsoft SharePoint se necessário, ou você pode usar um site existente para criar nossa biblioteca de documentos.
Verifique se você criou uma biblioteca de documentos em Microsoft SharePoint site.	Crie uma biblioteca de documentos dedicada em um novo ou existente Microsoft SharePoint site.
Verifique se as permissões necessárias foram fornecidas aos usuários e atribuídas aos grupos de usuários necessários no Microsoft SharePoint.	Gerenciar acesso de Microsoft SharePoint site para diferentes usuários e grupos de usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se você criou e configurou Microsoft SharePoint E definições de configuração necessárias.	Para verificar as configurações da unidade, configure Microsoft SharePoint Conector do Explorador de arquivos, Ações de pasta e arquivo e Modelos de pasta: • Configurar o Explorador de arquivos Repositório Unidade: Criar conexão de Microsoft SharePoint. ServiceNow® instância. • Defina as Configurações de ação de pasta e arquivo: Configure e controle as ações individuais de pasta e arquivo exibidas no componente Explorador de arquivos. • Criar modelos de pasta: Configure para criar pastas exclusivas para diferentes tipos de Incidentes de segurança graves.
Verifique se você estabeleceu uma conexão com a aplicação Conector de bate-papo do Microsoft Teams.	Para estabelecer a conexão da aplicação Conector de bate-papo do Microsoft Teams com ServiceNow®, siga o procedimento explicado aqui: Estabelecer conexão do MS Teams Graph em ServiceNow AI Platform.
Verifique se você configurou o Microsoft Teams com ServiceNow AI Platform®configurações de instância e conexões e credenciais criadas.	Para verificar Microsoft Teams configuração com ServiceNow®, siga o procedimento conforme explicado aqui: • Estabelecer conexão do MS Teams Graph em ServiceNow AI Platform • Crie um modelo de canal de bate-papo
Verifique se as definições Administração de incidentes de segurança graves - Configuração foram bem-sucedidas.	Como administrador MSI, você deve ser capaz de: • determine se os analistas de segurança podem propor e promover o incidente e vincular outros incidentes de segurança. • habilite ou desabilite as notificações quando um incidente for proposto ou promovido. Capacidade de editar mensagens de modelo padrão. • configure marcadores de segurança que aparecem na interface do analista de segurança para diferenciar os incidentes que foram propostos como candidatos a incidentes de segurança graves ou promovidos a incidentes de segurança graves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se as configurações Administração de incidentes de segurança graves - Notificações foram bem-sucedidas.	Como administrador MSI, acione notificações por e-mail quando um incidente de segurança for proposto e for enviado para todos os usuários e grupos configurados para a lista de notificações. Para obter mais informações, consulte Definir preferências de notificação para MSIM.

Gestão de incidentes graves de segurança funções

Atribua funções para garantir que os usuários possam executar todas as ações necessárias na aplicação MSIM.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
Administrador MSI	sn_msi.workspace_admin	Posso instalar e configurar Gestão de incidentes graves e configurar as aplicações dependentes, como File Explorer(FE), Microsoft Teams e configuração de canal de bate-papo, configuração do espaço e Administração MSI: Configurações e configuração de notificações. Como configurar: • Componente do Explorador de arquivos (FE): ◦ Configurar repositório de arquivos. ◦ Configure ações de arquivo e pasta, que são fornecidas no componente Explorador de arquivos da guia Colaboração no espaço Gestão de incidentes de segurança graves. ◦ Crie as pastas raiz e as subpastas e forneça acesso às subpastas. • Gestão de canais de bate-papo ◦ Ativar e configurar Microsoft Teams validando Microsoft Teams conexão. ◦ Crie equipes de bate-papo e canais de bate-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		papo, adicione usuários e atribua usuários aos vários grupos de usuários. • Administração MSI: ○ Configurações: Configure as ações dos analistas de segurança, as notificações enviadas quando os incidentes são propostos e promovidos e exiba marcadores para os incidentes de segurança. ○ Notificações: Automatize o processo de notificação por e-mail e as notificações do usuário quando um incidente de segurança é proposto ou promovido como um incidente de segurança grave.
MSI Manager	sn_msi.workspace_manager	• Exiba o acesso à página de definições de configuração da Gestão de incidentes de segurança graves. Restrição de modificar qualquer uma das definições de configuração. • Exibir e editar dados de registro de incidente no **Detalhes** , **Colaboração** e **Organizador de tarefas** guias do Gestão de incidentes graves espaço. • Promova o incidente de segurança a um incidente de segurança grave. • Configure ações de arquivo e pastas disponíveis no componente Explorador de arquivos no **Colaboração** . Gestão de incidentes graves espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		• Vincular e desvincular registros adicionais a incidentes de segurança graves do espaço.
Respondente MSI	sn_msi.workspace_responder	• Função opcional para exibir, editar e responder a incidentes de segurança graves no **Detalhes** e **Tarefas** guias do Gestão de incidentes graves espaço. • Vincular e desvincular registros adicionais a incidentes de segurança graves do espaço.

Integrar Gestão de incidentes graves de segurança

Estenda os recursos de Gestão de incidentes graves de segurança e conecte-se com ServiceNow AI Platform integração com Microsoft aplicações.

Importante: Um conjunto de atualizações (KB1289784) Está disponível no Guia de início rápido da Gestão de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações depois de concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de início rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Integrar Gestão de incidentes graves de segurança com Microsoft SharePoint

Integre seu Microsoft SharePoint com Gestão de incidentes graves de segurança.

Registre uma nova aplicação no portal do Azure para conexões do SharePoint

Registre uma nova aplicação no portal do Azure para Microsoft SharePoint integração.

Antes de Iniciar

Função necessária: administrador, administrador do Azure

Procedimento

1. Entre em Microsoft Azure Usando sua conta da Microsoft como administrador do Azure.
2. Navegar até **Serviços do Azure** > **Registro da aplicação** > **Novo registro**.

   Nota: Se você não encontrar, navegue até **Serviços do Azure** e pesquise **Registro da aplicação** .

3. Insira o nome da aplicação.
   Por exemplo, Microsoft SharePoint gráfico.
4. Selecione **Tipos de conta compatíveis: Contas somente neste diretório organizacional (Somente Service Now - locatário único**).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Web** Digite na lista suspensa no campo URI de redirecionamento (opcional).
6. Insira ServiceNow AI Platform® URL de redirecionamento da instância no campo URL de redirecionamento permitido.
   Por exemplo, `https://<InstanceName>.service-now.com/oauth_redirect.do` .
7. Clique em **Registre-se** e certifique-se de que a página seja exibida com **Visão geral** seção.
8. Anote ID do cliente e. ID do locatário de **Essencial** Da página Visão geral.
9. Em **Permissões de API** , Adicione a permissão do Microsoft Graph:
   a. Clique em **Adicione uma permissão** .
   b. Selecione **Microsoft Graph** .
   c. Selecione **Permissões da aplicação** .
   d. Em **Sites** , selecione **Sites.Selecionado** permissão.
   e. Clique em **Adicionar permissões** .
10. Em **Permissões de API** , Adicione a permissão do SharePoint:
    a. Clique em **Adicione uma permissão** .
    b. Selecione **SharePoint** .
    c. Selecione **Permissões da aplicação** .
    d. Em **Sites** , selecione **Sites.Selecionado** permissão.
    e. Clique em **Adicionar permissões** .
11. Depois de adicionar as permissões, clique em **Conceda consentimento do administrador** .
    Agora, todas as permissões são consentidas pelo administrador.

Use certificados para autenticação

Solicite um token de acesso com uma credencial de certificado.

Antes de Iniciar

1. Você pode usar um certificado autoassinado ou um certificado emitido por CA. Você pode criar um certificado autoassinado executando o script PowerShell conforme descrito em Configuração de um aplicativo do Azure AD para acesso somente por aplicativo . O script gera dois arquivos: Arquivo .pfx e .cer.

   Nota: Certifique-se de estar ciente da senha usada para criptografar a chave privada para gerar os arquivos .pfx e .cer.

2. Use o arquivo .pfx para criar um arquivo Java Key Store (JKS).

   Nota: Certifique-se de estar ciente da senha usada para gerar o arquivo JKS a partir do arquivo .pfx.

Função necessária: administrador

Procedimento

1. Navegue até **Registros de aplicações** No portal do Azure AD.
2. Clique em **Certificados e segredos** em **Gerenciar** seção.
3. Em **Certificados** clique em **Carregar certificado** .
4. No formulário, preencha estes valores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Carregue um certificado (chave pública) com um dos seguintes tipos de arquivo: .Cer, .pem, .crt	Arquivo .cer gerado usando o script PowerShell.
Descrição	Descrição do certificado.

5. Clique em **Adicionar**.
   O certificado é carregado e seus detalhes são exibidos em **Certificados** guia.
6. Copie o. **Impressão digital** valor do certificado carregado.

   Nota: . **Impressão digital** o valor é um valor hexadecimal.

7. Codifique o. **Impressão digital** Valor para um valor Base64 e registre o valor para uso posterior.

   Nota: Você pode usar uma ferramenta de conversão hexadecimal para Base64 (Hex para Base64) para codificar o. **Impressão digital** Valor para um valor Base64.

Configurar Microsoft SharePoint com Gestão de incidentes graves de segurança

Configurar Gestão de incidentes graves de segurança com Microsoft SharePoint conexão.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Administração**.
2. Selecione **Colaboração de documentos** e, em seguida **Configuração do Microsoft SharePoint** .
3. Selecione **Conceda acesso ao aplicativo do Azure ao site do SharePoint** no menu de contexto.
4. Conceda acesso à sua aplicação registrada usando um dos seguintes métodos: Comandos curl, CLI do Azure ou PowerShell.

   Nota:

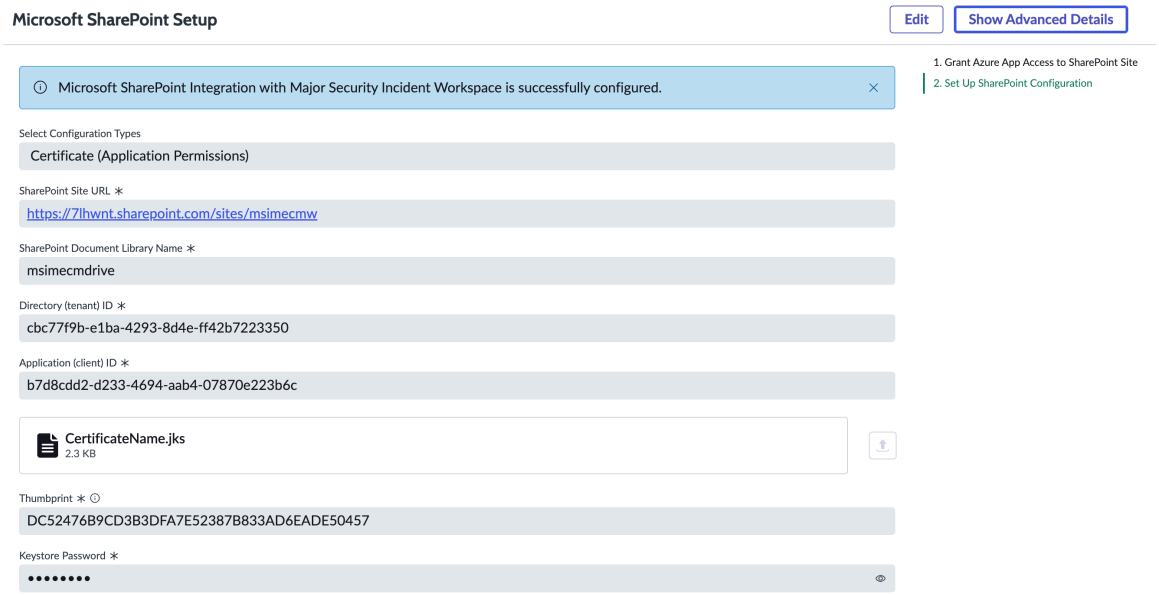
   - O administrador do Azure deve fornecer a configuração de acesso.
   - Conceda a permissão Sites.FullControl.all para a aplicação registrada.
   - Remova a permissão Sites.FullControl.all quando o acesso for concedido com sucesso.

5. Selecione **Configurar a configuração do SharePoint** no menu de contexto.
6. Selecione um tipo de configuração em **Selecione Configurações Tipos** e configure o seguinte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Certificado (permissões de aplicações)



Configurações do SharePoint para certificado

Campo	Descrição
URL do site do SharePoint	. Microsoft SharePoint URL do site.
Nome da biblioteca de documentos do SharePoint	Nome do Microsoft SharePoint biblioteca de documentos.
ID do diretório (locatário)	O identificador exclusivo da sua instância do Azure Active Directory.
ID da aplicação (cliente)	O identificador exclusivo da sua aplicação registrada no Azure.
Carregar certificado	O arquivo de certificado para a autenticação.
Impressão digital	A impressão digital do certificado.
Senha de armazenamento de chaves	A senha do armazenamento de chaves para acessar a impressão digital do certificado.

- Segredo do cliente (permissões de aplicações)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurações do SharePoint para Segredo do cliente

Campo	Descrição
URL do site do SharePoint	. Microsoft SharePoint URL do site.
Nome da biblioteca de documentos do SharePoint	Nome do Microsoft SharePoint biblioteca de documentos.
ID do diretório (locatário)	O identificador exclusivo da sua instância do Azure Active Directory.
ID da aplicação (cliente)	O identificador exclusivo da sua aplicação registrada no Azure.
Segredo do cliente	A cadeia de caracteres secreta da aplicação usada para solicitar um token.

7. Selecione **Configurar e obter token OAuth** .
   Um prompt de login é exibido para fornecer os detalhes da sua conta da Microsoft.
8. Forneça os detalhes e o login da sua conta da Microsoft.
   Uma mensagem bem-sucedida é exibida e a conexão é estabelecida.

Integrar Gestão de incidentes graves de segurança com Microsoft Teams

Integre seu Microsoft Teams com Gestão de incidentes graves de segurança.

- Registre uma nova aplicação no portal do Azure para Microsoft Teams conexões
- Configurar Microsoft Teams conexão com Gestão de incidentes graves de segurança

Registre uma nova aplicação no portal do Azure para Microsoft Teams conexões

Registre uma nova aplicação no portal do Azure para Microsoft Teams E conceda acesso ao aplicativo Azure.

Antes de Iniciar

Nota: Se quiser, você pode usar a mesma aplicação que criou para o SharePoint para estabelecer a conexão do Microsoft Teams Graph.

Função necessária: administrador, administrador do Azure

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Entre no portal do Azure usando sua conta da Microsoft.
2. Navegar até **Serviços do Azure** > **Registro da aplicação** > **Novo registro**.
3. Insira o nome da aplicação.
   Por exemplo, Microsoft Teams Graph.
4. Selecione **Tipo de conta compatível: Contas somente neste diretório organizacional (somente Service Now - locatário único)** .
5. Selecione **Web** Digite na lista suspensa na URL de redirecionamento.
6. Insira ServiceNow AI Platform® URL de redirecionamento da instância no campo URL de redirecionamento permitido.
   Por exemplo, https:// <InstanceName>>.service-now.com/oauth_redirect.do
7. Clique em **Registre-se** e certifique-se de que a página seja exibida com **Visão geral** seção.
8. Anote ID do cliente e. ID do locatário em **Essencial** . **Visão geral** página.
9. Você pode seguir a Etapa 6,1 ou a Etapa 6,2 para concluir o procedimento de estabelecer uma conexão no seu ServiceNow instância.

Configurar Microsoft Teams conexão com Gestão de incidentes graves de segurança

Configurar Gestão de incidentes graves de segurança com Microsoft Teams conexão.

Antes de Iniciar

Pré-requisito: Certifique-se de ter registrado uma aplicação no Azure Active Directory com as permissões de delegação necessárias.

Função necessária: administrador

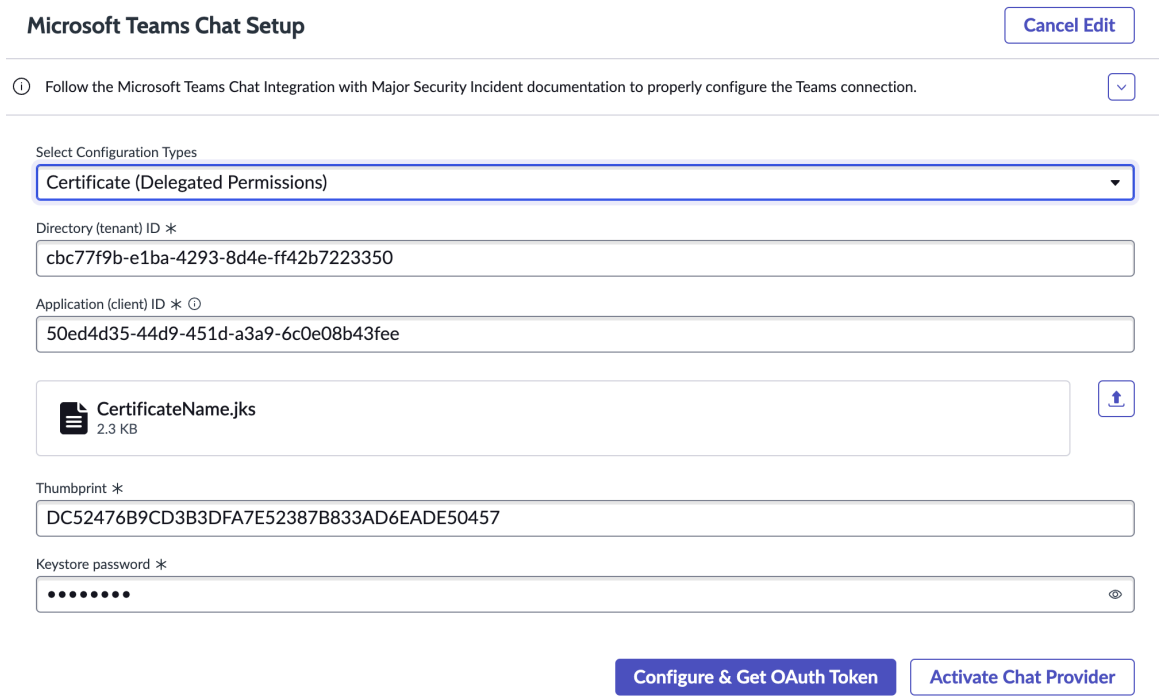
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Administração**.
2. Selecione **Colaboração de bate-papo** e, em seguida **Configuração do Microsoft Teams** .
3. Selecione um tipo de configuração no **Selecione Configurações Tipos** e configure o seguinte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Certificado (permissões delegadas)



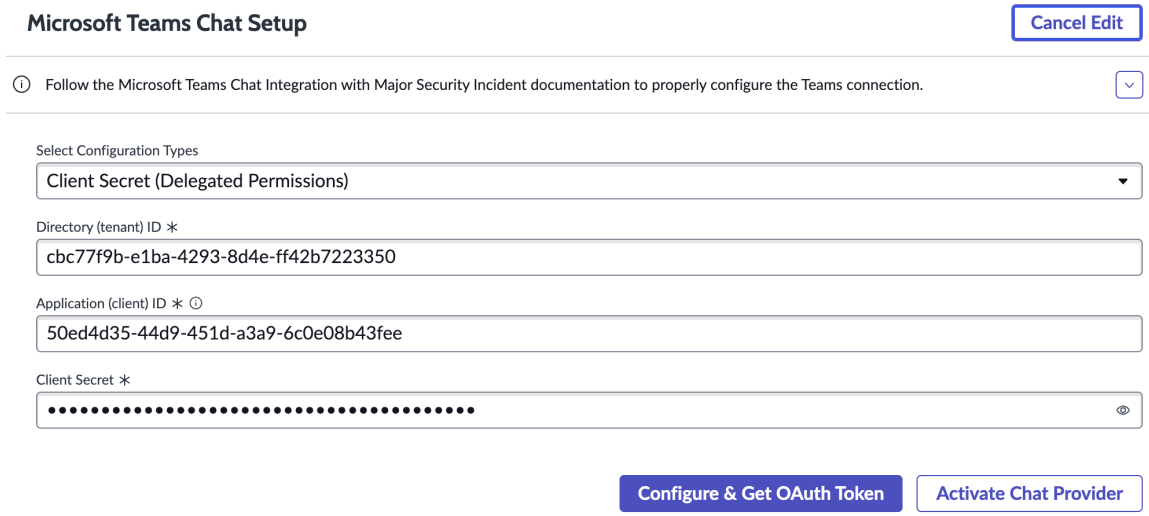
Configurações do Microsoft Teams para Certificado

Campo	Descrição
ID do diretório (locatário)	O identificador exclusivo da sua instância do Azure Active Directory.
ID da aplicação (cliente)	O identificador exclusivo da sua aplicação registrada no Azure.
Carregar certificado	O arquivo de certificado para a autenticação.
Impressão digital	A impressão digital do certificado.
Senha de armazenamento de chaves	A senha do armazenamento de chaves para acessar a impressão digital do certificado.

- Segredo do cliente (permissões delegadas)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurações do Microsoft Teams para Segredo do cliente

Campo	Descrição
ID do diretório (locatário)	O identificador exclusivo da sua instância do Azure Active Directory.
ID da aplicação (cliente)	O identificador exclusivo da sua aplicação registrada no Azure.
Segredo do cliente	A cadeia de caracteres secreta da aplicação usada para solicitar um token.

4. Selecione **Configurar e obter token OAuth** .
   Um prompt de login é exibido para fornecer os detalhes da sua conta da Microsoft.
5. Forneça os detalhes e o login da sua conta da Microsoft.
   Uma mensagem bem-sucedida é exibida e a conexão é estabelecida.
6. Selecione **Ativar provedor de bate-papo** para habilitar Microsoft Teams conexão.
7. **Opcional:** Selecione **Mostrar detalhes avançados** para exibir os detalhes da configuração.

Estabelecer conexão do MS Teams Graph em ServiceNow AI Platform

Integrar ServiceNow AI Platform instância e. Microsoft Teams estabelecendo um Microsoft Teams Graph conexão.

Antes de Iniciar

Se quiser, você pode usar a mesma aplicação que criou para o SharePoint para estabelecer a conexão do Microsoft Teams Graph.

Função necessária: administrador, administrador do Azure

Registre uma nova aplicação no Azure para Conexão do Microsoft Teams Graph

Procedimento

1. Entre em Azure usando seu Microsoft conta.
2. Navegar até **Serviços do Azure** > **Registro da aplicação** > **Novo registro**.
3. Insira o nome da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, Microsoft Teams Graph.

4. Selecione o respectivo **Tipos de conta compatíveis** a opção que for aplicável à sua organização.
   Por exemplo, selecione **Somente contas neste diretório organizacional (Somente Service Now - locatário único)** opção.

   Nota: Para obter informações sobre os tipos de conta compatíveis, consulte Registre uma aplicação na plataforma de identidade da Microsoft .

5. Selecione **Web** Digite na lista suspensa na URL de redirecionamento.
6. Insira ServiceNow AI Platform URL de redirecionamento da instância no campo URL de redirecionamento permitido.
   Por exemplo, https:// <InstanceName>>.service-now.com/oauth_redirect.do
7. Clique em **Registre-se** para registrar sua nova aplicação e garantir que a página seja exibida com **Visão geral** seção.

Usando certificados para autenticação

Solicite um token de acesso com uma credencial de certificado.

Antes de Iniciar

1. Você pode usar um certificado autoassinado ou um certificado emitido por CA. Você pode criar um certificado autoassinado executando o script PowerShell conforme descrito em Configuração de um aplicativo do Azure AD para acesso somente por aplicativo . O script gera dois arquivos: Arquivo .pfx e .cer.

   Nota: Certifique-se de estar ciente da senha usada para criptografar a chave privada para gerar os arquivos .pfx e .cer.

2. Use o arquivo .pfx para criar um arquivo Java Key Store (JKS).

   Nota: Certifique-se de estar ciente da senha usada para gerar o arquivo JKS a partir do arquivo .pfx.

Função necessária: administrador

Procedimento

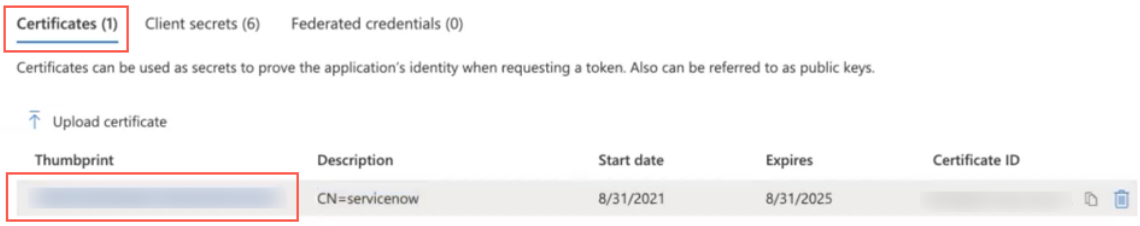
1. Navegue até **Registros de aplicações** No portal do Azure AD.
2. Clique em **Certificados e segredos** em **Gerenciar** seção.
3. Em **Certificados** clique em **Carregar certificado** .
4. No formulário, preencha estes valores.

Campo	Descrição
Carregue um certificado (chave pública) com um dos seguintes tipos de arquivo: .Cer, .pem, .crt	Arquivo .cer gerado usando o script PowerShell.
Descrição	Descrição do certificado.

5. Clique em **Adicionar**.
   O certificado é carregado e seus detalhes são exibidos em **Certificados** guia.
6. Copie o. **Impressão digital** valor do certificado carregado.
   . **Impressão digital** o valor é um valor hexadecimal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Codifique o. **Impressão digital** Valor para um valor Base64 e registre o valor para uso posterior.

> **Nota:** Você pode usar uma ferramenta de conversão hexadecimal para Base64 (Hex para Base64) para codificar o. **Impressão digital** Valor para um valor Base64.

Anexe um certificado Java Key Store para MS Teams

Habilite a autenticação de token de concessão do portador JWT anexando um certificado Java Key Store (JKS) válido.

Antes de Iniciar

Faça login na sua instância da ServiceNow para executar o procedimento a seguir.

- Certificado Java Key Store válido
- Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Certificados**.
2. Abra o registro **Certificado do Conector do Microsoft Teams** .
   Certifique-se de usar o registro padrão **Certificado do Conector do Microsoft Teams** apenas.
3. Insira a senha associada ao arquivo JKS em **Senha do armazenamento de chaves** .
4. Clique no ícone Anexos (E anexe o certificado JKS que você gerou.
   Para obter mais informações, consulte .
5. Clique em **Validar armazenamentos/certificados** .
6. Clique em **Atualizar**.

Configure a chave de assinatura JWT para MS Teams

Crie uma chave de assinatura JSON Web Token (JWT) para atribuir ao seu certificado Java Key Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Chaves de JWT**.
2. Abra o registro **JWT do conector do Microsoft Teams** .
3. Insira a senha usada para criptografar a chave privada para gerar o arquivo .pfx e o arquivo .cer em **Senha da chave de assinatura** .
4. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o provedor JWT para MS Teams

Adicione um provedor JSON Web Token (JWT) à sua instância da ServiceNow.

Antes de Iniciar

- Copie e registre o valor de **ID da aplicação (cliente)** e. **ID do diretório (locatário)** Da aplicação que você registrou no portal do Azure.



- Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Provedores JWT**.
2. Abra o registro **Provedor JWT do conector do MS Teams** .
3. Insira valores para **iss** , **sub** e **aud** Na lista relacionada Declarações padrão.

Campo	Valor
aud	URL do Microsoft Online neste formato: `https://login.microsoftonline.com/<tenant-id>/oauth2/token` . Substituir `<tenant-id>` com **ID do diretório (locatário)** O valor da sua aplicação foi registrado no portal do Azure.
iss	**ID da aplicação (cliente)** Da aplicação que você registrou no portal do Azure.
sub	**ID da aplicação (cliente)** Da aplicação que você registrou no portal do Azure.

4. Clique em **Atualizar**.

Estabeleça uma conexão usando certificados

Estabeleça uma conexão entre a aplicação de gráfico do Microsoft Teams recém-criada usando certificados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Aberto **Spoke do Microsoft Teams** .
3. Modifique o valor do campo **Modelo de configuração: Modelo de código MSIM do Microsoft Teams ConnectorAuthorization** e salve o formulário.

Nota: Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na seção Links relacionados, clique em Criar **Nova conexão e credencial** .

Nome	Qualquer nome exclusivo.
URL de conexão	URL de conexão. Por exemplo, https://graph.microsoft.com
Versão da API	Versão da API. Por exemplo, v1.0
URL de Autorização	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/Authorize
URL do token	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/token
URL de revogação do token	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/revogar
ID do cliente do OAuth	ID do cliente.
Segredo do cliente do OAuth	Você pode inserir qualquer valor. **Nota:** Isso não é importante, pois você usará a autenticação baseada em certificado.

5. Clique em **Criar e obter token OAuth** .
   Uma mensagem de erro é exibida solicitando 401- Não autorizado.
6. Recarregue o formulário e abra o registro na lista relacionada Conexões.
7. Insira o Base64 codificado **Impressão digital** valor em **Impressão digital do certificado codificado** atributo no **Atributos** seção.

   Nota: O valor de impressão digital é um valor hexadecimal. Você pode usar uma ferramenta de conversão hexadecimal para Base64 (Hex para Base64) para codificar o valor de impressão digital para um valor Base64.

8. Navegar até **OAuth de Sistema** > **Registro de aplicações**
9. Aberto **Código de autorização do Conector do Microsoft Teams MSIM** registro.
10. Modificar o script da API OAuth: **OAuthUtilJWTMSTeamsConnector** .
11. Navegar até **Conexões e Credenciais** > **Credenciais**.
12. Abra o registro **Credencial do Conector do Microsoft Teams do MSIM** .
13. Em Links relacionados, clique em **Obter token OAuth** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Usando o valor do segredo do cliente

Use o valor do segredo do cliente para configurar o registro do registro da aplicação Graph.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Registros de aplicações** No portal do Azure AD.
2. Clique em **Certificados e segredos** em **Gerenciar** seção.
3. Clique em **Novo segredo do cliente** .
4. Copie e anote o segredo do cliente criado no **Valor** campo.

Estabeleça uma conexão usando o segredo do cliente

Estabeleça uma conexão entre a aplicação de gráfico do Microsoft Teams recém-criada com ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Aberto **Spoke do Microsoft Teams** .
3. Modifique o valor do campo **Modelo de configuração: Modelo de código MSIM do Microsoft Teams ConnectorAuthorization** e salve o formulário.

   Nota: Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

4. Na seção Links relacionados, clique em Criar **Nova conexão e credencial** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Qualquer nome exclusivo.
URL de conexão	URL de conexão. Por exemplo, https://graph.microsoft.com
Versão da API	Versão da API. Por exemplo, v1.0
URL de Autorização	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/Authorize
URL do token	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/token
URL de revogação do token	https://login.microsoftonline.com/<<tenant ID>/oAuth2/v2.0/revogar
ID do cliente do OAuth	ID do cliente.
Segredo do cliente do OAuth	Segredo do cliente.

5. Clique em **Criar e obter token OAuth** .
   Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Tradução automática

Ative o conector de bate-papo do MS Teams para o usuário do spoke do MS Teams Graph

Se você for um usuário existente, siga o procedimento nesta seção para ativar o conector de bate-papo do Microsoft Teams para o usuário do spoke do MS Teams Graph.

Antes de Iniciar

Função necessária: administrador

Procedimento

Se você já for um usuário do Microsoft Teams Graph Spoke, siga as etapas abaixo:

- Navegue até sua aplicação registrada no portal do Azure que é usada pelo Microsoft Teams Graph Spoke.
- Navegue até **Permissões de API** Seção para configurar as permissões de API necessárias.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Clique em **Adicione uma permissão** .
- Selecione **Microsoft Graph** .
- Para usar a aplicação Conector do Microsoft Teams, você precisa adicionar mais duas permissões delegadas à sua aplicação no portal do Azure: "ChannelMember.ReadWrite.all" e "TeamMember.ReadWrite.all".
- Depois de adicionar as permissões necessárias acima, clique em **Conceda consentimento do administrador** .

Configure o MS Teams no *ServiceNow AI Platform***Instância de um usuário existente:**

- Navegue até **Aliases de conexão e credencial** .
- Selecione **Spoke do Microsoft Teams** registro.
- Selecione o registro de credencial associado ao spoke do Microsoft Teams.
- Clique em **Obter token OAuth** . Uma mensagem de confirmação exibe que o token de atualização OAuth está disponível.

Como um usuário existente, você concluiu a integração da aplicação Conector de bate-papo do Microsoft Teams com a API do Microsoft Teams Graph.

Gestão de incidentes graves de segurança Integração de chamada em conferência

Com Gestão de incidentes graves de segurança integração de chamadas em conferência, você pode colaborar com seus clientes e agentes pares para resolver problemas do cliente usando as opções de compartilhamento de vídeo e tela em Microsoft Teams, Cisco Webex ou Zoom Da aplicação MSIM.

. Gestão de incidentes graves de segurança A integração de Chamada em conferência permite integrar o canal de comunicação em conferência com o. Notify canal de comunicação gerenciando e iniciando um Microsoft Teams, Cisco Webex ou Zoom reunião diretamente do Gestão de incidentes graves de segurança aplicação.

Como gerente MSI, você pode usar a integração de Chamada em conferência do MSIM para iniciar Microsoft Teams, Cisco Webex ou Zoom reuniões. Integrar o. Gestão de incidentes graves de segurança Chamada em conferência com os provedores de serviços terceirizados como um canal de comunicação para se reunir com as partes interessadas para resolver os incidentes de segurança graves.

Principais recursos

. Incidente grave de segurança A integração de Chamada em conferência de gestão fornece os seguintes recursos principais:

- Gerentes MSI podem iniciar um Microsoft Teams, Cisco Webex ou Zoom chamada em conferência diretamente do incidente de segurança grave.
- Convide participantes adicionais para a chamada.
- Exibir gravações de chamadas e detalhes de bate-papo.
- Envia convites aos participantes por e-mail e Microsoft Teams bate-papo.

Como iniciar uma chamada em conferência

Inicie uma chamada em conferência a partir de uma tarefa ou de uma segurança importante convidando um ou mais usuários para ingressar em uma chamada em conferência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A chamada em conferência só será iniciada quando pelo menos dois participantes ingressarem.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Certifique-se de ter feito o seguinte no ServiceNow® instância:

- Instalado e ativado o. Notify plug-in (com.snc.notify).
- Instalado Notify Componentes de IU do app Espaços configuráveis.
- Instalado e ativado o plug-in Visual Task Board (com.devsnc.snb_vtb).

Para obter mais informações, consulte Solicitação de IntegrationHub .

Por Que e Quando Desempenhar Esta Tarefa

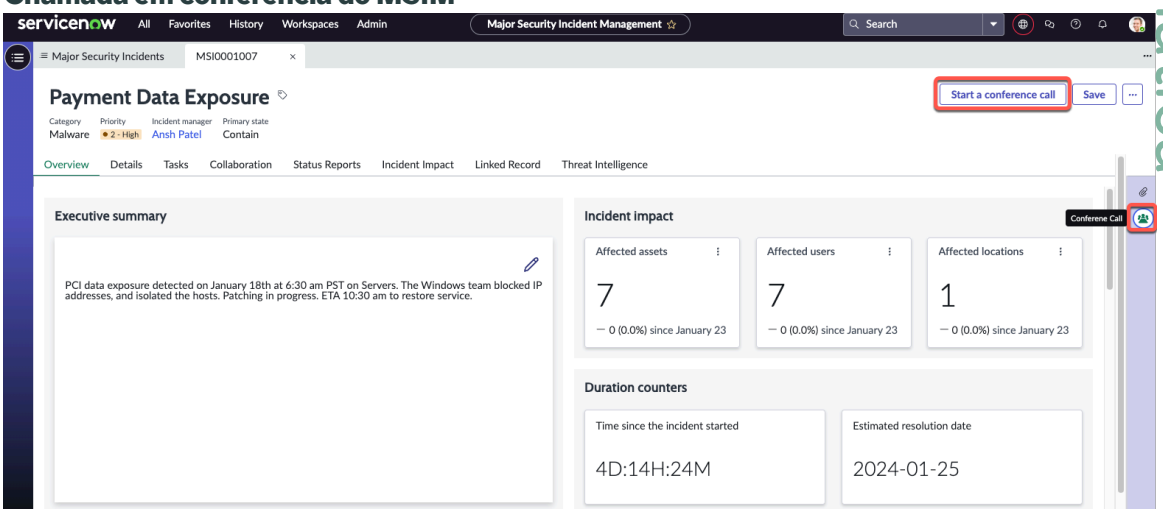
Os participantes da chamada podem incluir o seguinte:

- Usuários aos quais foram atribuídas responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione **Iniciar uma chamada em conferência** ação.
4. Você também pode iniciar uma chamada em conferência selecionando no menu de contexto direito e selecionando o ícone de adição.
   O pop-up Iniciar chamada em conferência é exibido.

Chamada em conferência do MSIM



5. No campo Ponte de conferência, escolha um **Ponte de conferência** do qual você deseja se conectar. Por exemplo, Microsoft Team, Zoom ou Cisco Webex.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência.
7. No campo Adicionar participantes, selecione os participantes da chamada em conferência.

Tradução automática

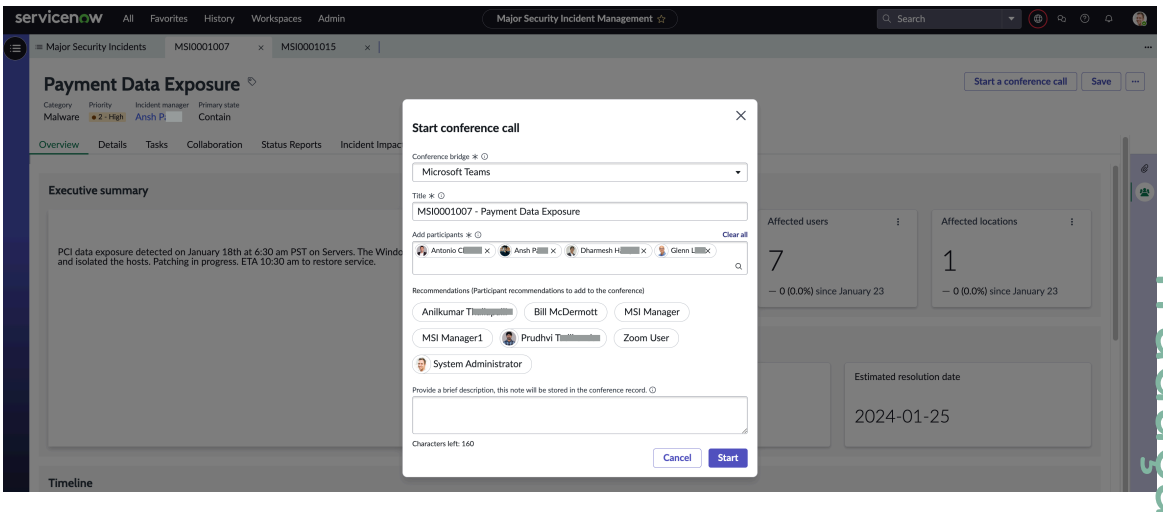
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes no **Recomendações** , que fornece recomendações de participantes para adicionar à chamada em conferência.

O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão em **Recomendações** lista.

Nota: Certifique-se de que os participantes selecionados tenham um endereço de e-mail válido.

Como iniciar uma chamada em conferência



8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar** .
   A chamada em conferência começa na ponte de conferência selecionada. Todos os participantes são notificados por e-mail e também são notificados por meio da respectiva ponte de conferência selecionada.
10. Selecione **Clique aqui** opção além do incidente de segurança grave para ingressar na chamada em conferência.
    Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.
11. Abra o incidente de segurança grave associado para exibir os detalhes da chamada em conferência.
    Quando o participante final sai da conferência, a chamada em conferência termina ou seleciona **Encerrar chamada** para encerrar a chamada em conferência.

Como adicionar participantes a uma chamada em conferência

Adicione participantes a uma chamada em conferência usando a opção de pesquisa no **Iniciar chamada em conferência** pop-up para localizar e adicionar os participantes necessários. Você também pode adicionar participantes selecionando os participantes na lista Recomendações, que fornece recomendações de participantes para adicionar à chamada em conferência.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa
O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista Recomendações.

Tradução automática

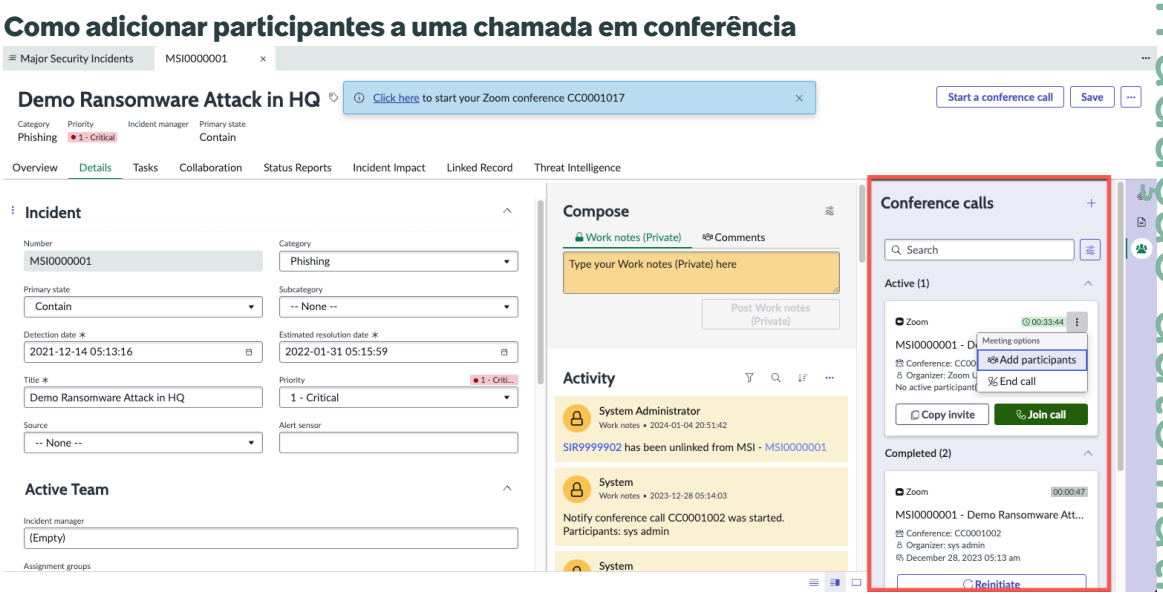
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os participantes da chamada podem incluir o seguinte:

- Usuários aos quais foram atribuídas responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência. Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.
4. Selecione ao lado da chamada em conferência ativa e selecione **Adicionar participantes** opção.



5. Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes no **Recomendações** , que fornece recomendações de participantes para adicionar à chamada em conferência.
6. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   Todos os participantes são notificados por e-mail e também são notificados por meio da respectiva ponte de conferência selecionada. Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.
7. Como alternativa, você pode adicionar participantes selecionando **Copiar convite** Na seção Chamadas em conferência no menu de contexto direito e você pode compartilhar com os participantes necessários.

Silenciar participantes em uma chamada em conferência

Como gerente MSI ou host de chamada em conferência, você tem a opção de silenciar um participante específico ou todos os participantes na chamada em conferência.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de iniciar este procedimento, verifique se há uma chamada em conferência ativa com um ou mais participantes.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência.
4. Selecione **Ingressar na chamada** na ponte de conferência ativa.
5. Depois de ingressar na chamada em conferência, selecione um participante que você deseja desativar o mudo e selecione **Mudo** na ponte de conferência.
6. Para silenciar todos os participantes na chamada em conferência, selecione **Participantes** nos controles de reunião e selecione **Mudo tudo** .

Exibir detalhes da chamada em conferência

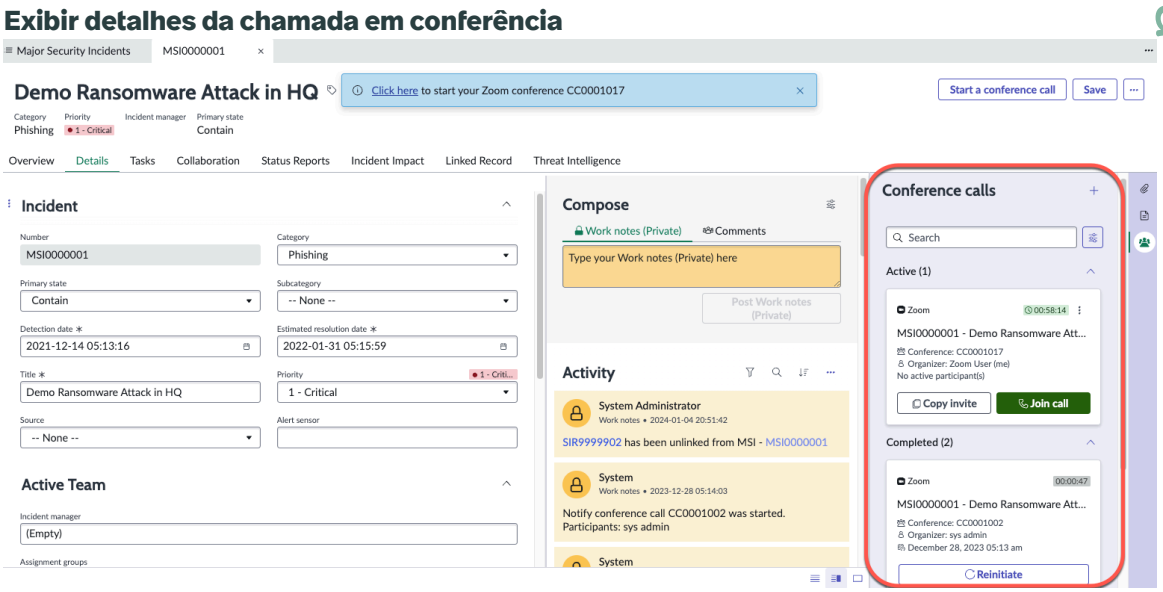
As chamadas em conferência são listadas como atividades do sistema na seção Atividade do incidente de segurança grave e também listadas na lista relacionada Chamadas em conferência. Você pode exibir detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência. Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Você pode usar a opção de pesquisa para procurar uma chamada em conferência específica. Pode haver várias chamadas para o mesmo incidente de segurança grave.
5. Para adicionar participantes a uma chamada em conferência, selecione ⋮ ao lado da chamada em conferência ativa e selecione **Adicionar participantes** opção.
6. Você também pode adicionar participantes usando **Copiar convite** e compartilhamento do link com os participantes necessários.
7. Para ingressar em uma chamada em conferência, navegue até a seção Ativo e selecione **Ingressar na chamada** opção da chamada em conferência necessária.
8. Para encerrar uma chamada em conferência, selecione ⋮ ao lado da chamada em conferência ativa e selecione **Encerrar chamada** opção.
9. Para reiniciar uma chamada em conferência, navegue até a seção Concluído e selecione **Reiniciar** opção da chamada em conferência necessária.

Integrar Chamadas em conferência do MSIM com Microsoft Teams

A chamada em conferência Microsoft Teams a integração permite gerenciar e iniciar um Microsoft Teams chamada em conferência diretamente de um incidente de segurança grave.

Principais recursos

- Início e término Microsoft Teams chamadas em conferência diretamente de incidentes de segurança graves ou de uma tarefa do workbench de segurança principal.
- Gerenciar um Microsoft Teams chamada em conferência adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou o seguinte IntegrationHub plug-ins no seu ServiceNow instância.

- Notify plug-in (com.snc.notify)
- Microsoft Teams Plug-in Communications Spoke (sn_msteams_com_spk).
- Plug-in Mapeamento de usuário do Azure Active Directory (sn_now_azure).
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

- Para configurar a Chamada em conferência do MSIM Microsoft Teams integração usando o app pré-configurado, consulte Integre o aplicativo pré-publicado do Conector Notify ao Microsoft Teams .
- Para configurar a Chamada em conferência do MSIM Microsoft Teams integração usando o app autoconfigurado, consulte Integrat ing Aplicativo autoconfigurado do Conector do Notify com Microsoft Teams .

Use a Chamada em conferência do MSIM Microsoft Teams integração

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar um Microsoft Teams chamada em conferência diretamente de um incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

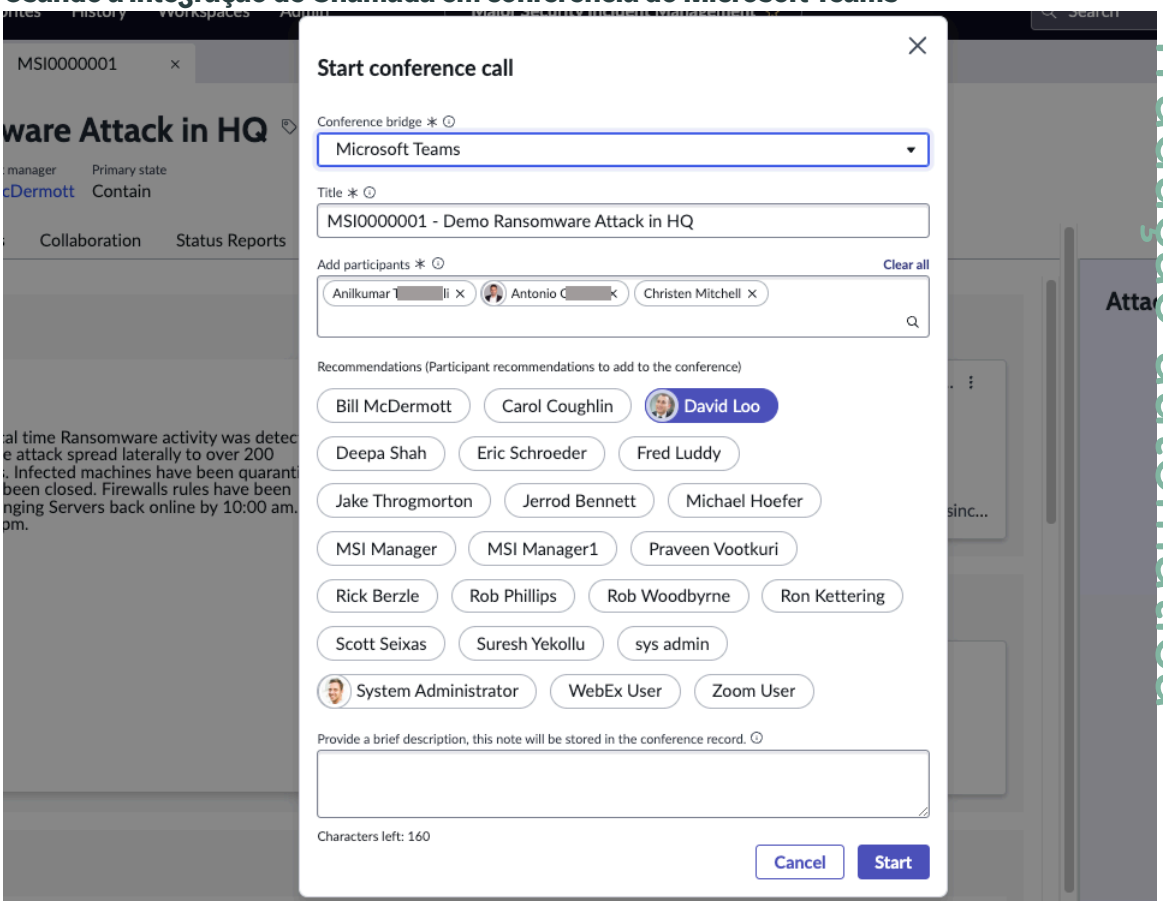
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione **Iniciar uma chamada em conferência** ação.
4. Você também pode iniciar uma chamada em conferência selecionando no menu de contexto direito e selecionando o ícone de adição.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **Microsoft Teams** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Microsoft Teams.

Usando a integração de Chamada em conferência do Microsoft Teams



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Microsoft Teams.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes no **Recomendações** , que fornece recomendações de participantes para adicionar à chamada em conferência do Microsoft Teams.

   O usuário (host) que inicia a chamada em conferência do Microsoft Teams é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão em **Recomendações** lista.

Nota: Certifique-se de que os participantes selecionados tenham um endereço de e-mail válido.

Tradução automática

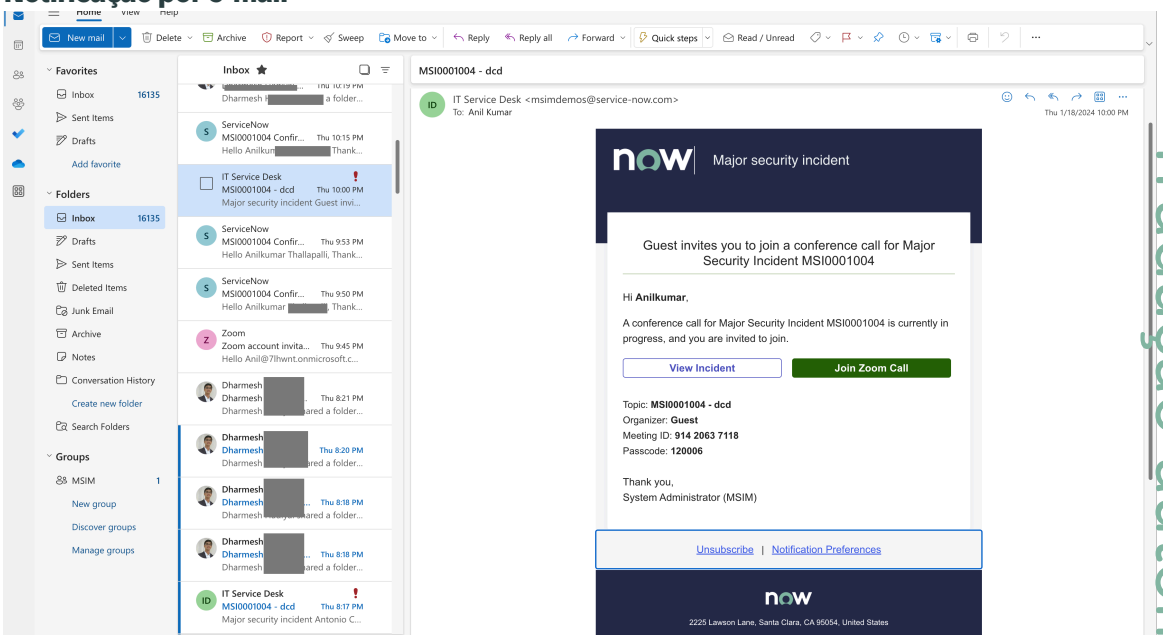
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.

9. Depois que a lista de participantes for finalizada, selecione **Iniciar** .
   A chamada em conferência começa no aplicativo Microsoft Teams. Todos os participantes são notificados por meio de um e-mail do aplicativo MSIM e a outra notificação é enviada por meio de um bot no aplicativo Microsoft Teams.

10. Selecione **Clique aqui** Opção além do incidente de segurança grave para ingressar na chamada em conferência no aplicativo Microsoft Teams.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Microsoft Teams para ingressar na chamada.

Notificação por e-mail



11. Abra o incidente grave de segurança associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou seleciona **Encerrar chamada** Na seção Chamada em conferência para encerrar a chamada em conferência.

Integrar Chamadas em conferência do MSIM com Zoom

A chamada em conferência Zoom a integração permite gerenciar e iniciar um Zoom chamada em conferência diretamente de um incidente de segurança grave.

Principais recursos

- Início e término Zoom reuniões diretamente de qualquer registro de tarefa, como um incidente de segurança grave, uma mudança ou até mesmo do workbench de incidente grave.
- Gerenciar Zoom adicionando ou removendo participantes.
- Rastreie e relate os detalhes da reunião, como a duração da reunião e os participantes, para análise posterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Verifique se você instalou o seguinte IntegrationHub plug-ins no seu ServiceNow instância.

- Notify plug-in (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

Para configurar a Chamada em conferência do MSIM Zoom integração usando Notify canal de comunicação, consulte Configuração do conector Notify para Zoom no Notify .

Use a Chamada em conferência do MSIM Zoom integração

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar um Zoom chamada em conferência diretamente de um incidente de segurança grave.

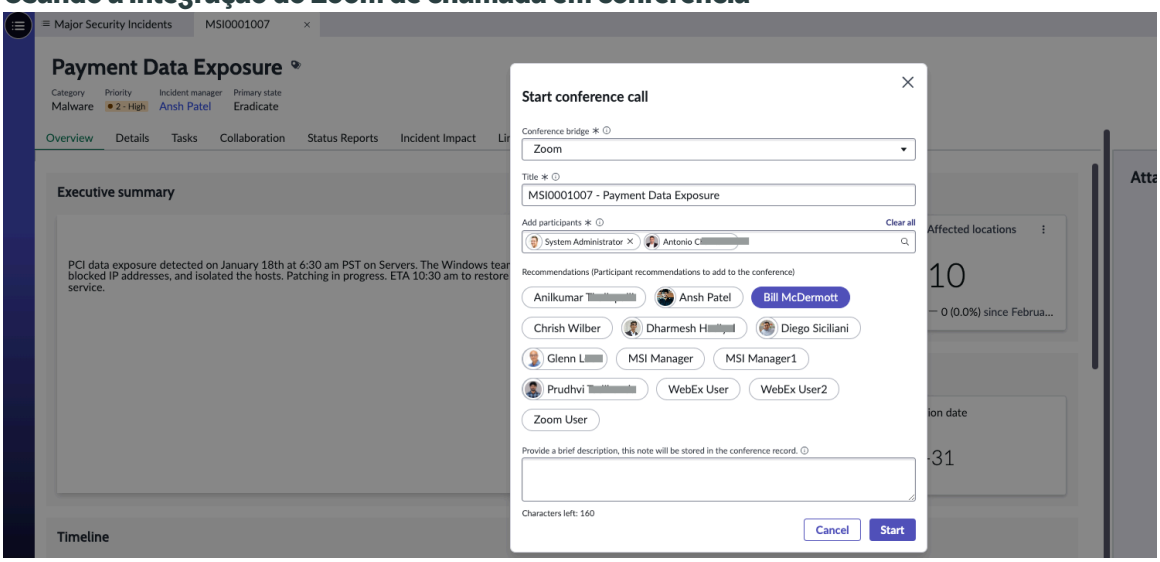
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Clique em **Iniciar uma chamada em conferência** ação.
4. Você também pode iniciar uma chamada em conferência clicando em  no menu de contexto direito e selecionando o ícone de adição.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **Zoom** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Zoom.

Usando a integração do Zoom de chamada em conferência



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Zoom.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes no **Recomendações** , que fornece recomendações de participantes para adicionar à chamada em conferência do Zoom.

   O usuário (host) que inicia a chamada em conferência do Zoom é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão em **Recomendações** lista.

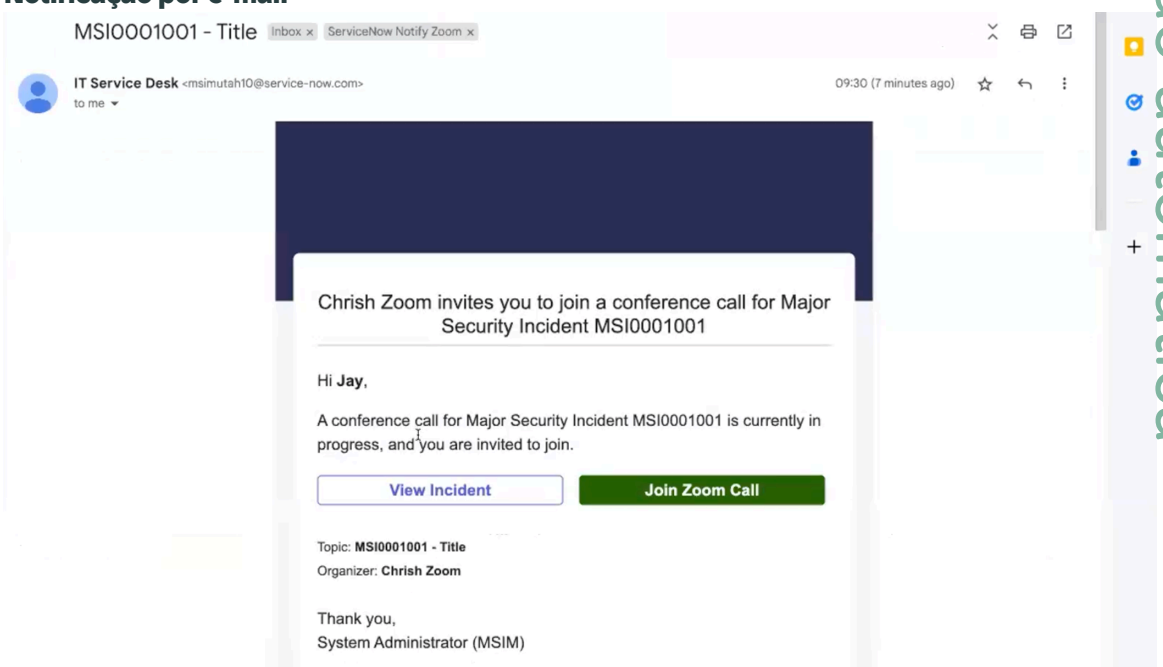
   Nota: Certifique-se de que os participantes selecionados tenham um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.

9. Depois que a lista de participantes for finalizada, clique em **Iniciar** .
   A chamada em conferência começa no aplicativo Zoom. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado para os participantes do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência do Zoom.

10. Selecione **Clique aqui** Opção além do incidente de segurança grave para ingressar na chamada em conferência no aplicativo Zoom.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Zoom para ingressar na chamada.

Notificação por e-mail



11. Abra o incidente grave de segurança associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou seleciona **Encerrar chamada** Na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrar Chamadas em conferência do MSIM com Cisco Webex

A chamada em conferência do MSIM Cisco Webex a integração permite gerenciar e iniciar um Cisco Webex chamada em conferência diretamente de um incidente de segurança grave.

Principais recursos

- Início e término Cisco Webex reuniões diretamente de incidentes de segurança graves.
- Gerenciar um Cisco Webex reunião adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou o seguinte IntegrationHub plug-ins no seu ServiceNow instância.

- Notify plug-in (com.snc.notify)
- Notify Cisco Webex Conector (sn_notify_webex)
- Cisco Webex Spoke do Teams (sn_cisco_teams_spk)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

Para configurar a Chamada em conferência do MSIM Cisco Webex integração usando Notify canal de comunicação, consulte Configuração do Notify Cisco Webex Connector .

Use as Chamadas em conferência Cisco Webex integração

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar um Cisco Webex chamada em conferência diretamente de um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

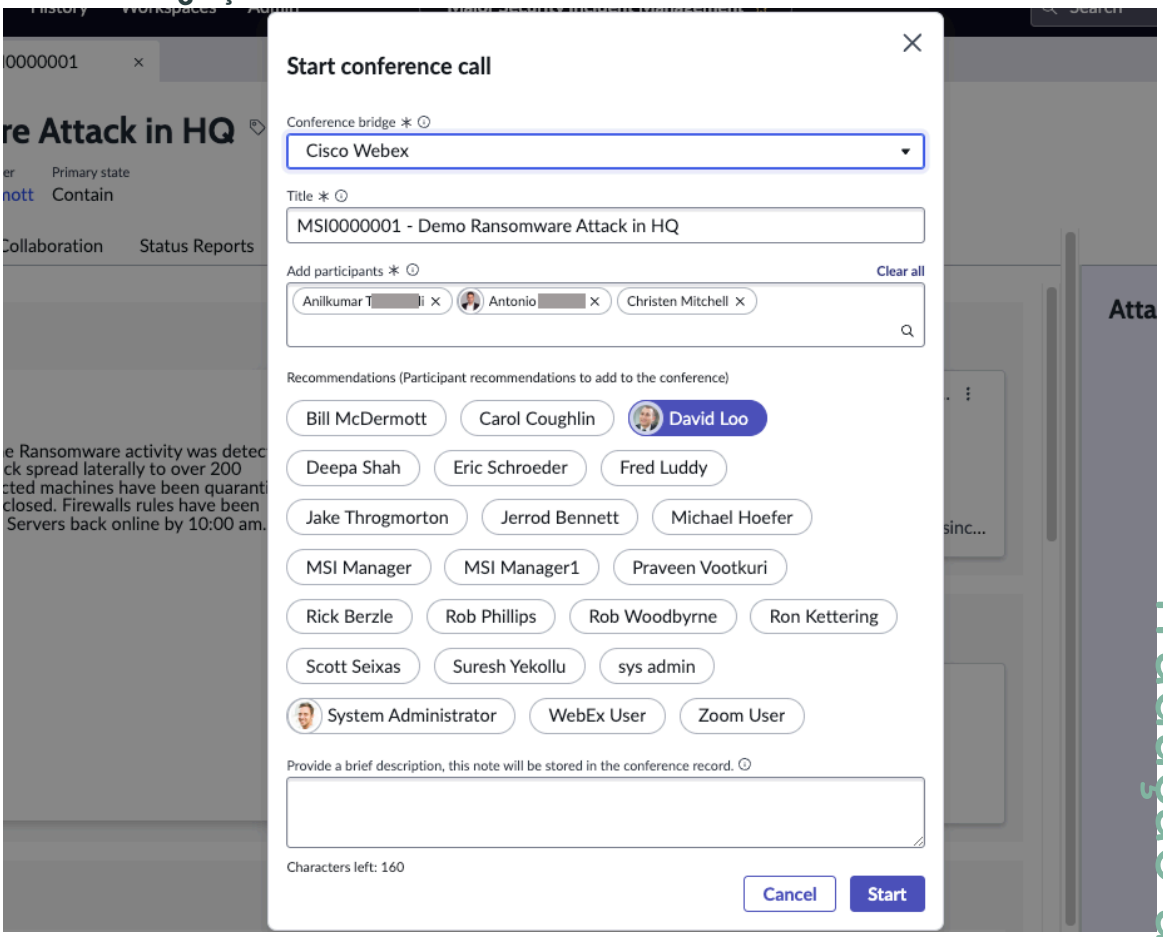
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione **Iniciar uma chamada em conferência** ação.
4. Você também pode iniciar uma chamada em conferência selecionando  no menu de contexto direito e selecionando o ícone de adição.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **Cisco Webex** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência Cisco Webex.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando a integração do Cisco Webex de chamada em conferência



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência Cisco Webex. Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes no **Recomendações** , que fornece recomendações de participantes para adicionar à chamada em conferência Cisco Webex.

   O usuário (host) que inicia a chamada em conferência Cisco Webex é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão em **Recomendações** lista.

   Nota: Certifique-se de que os participantes selecionados tenham um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.

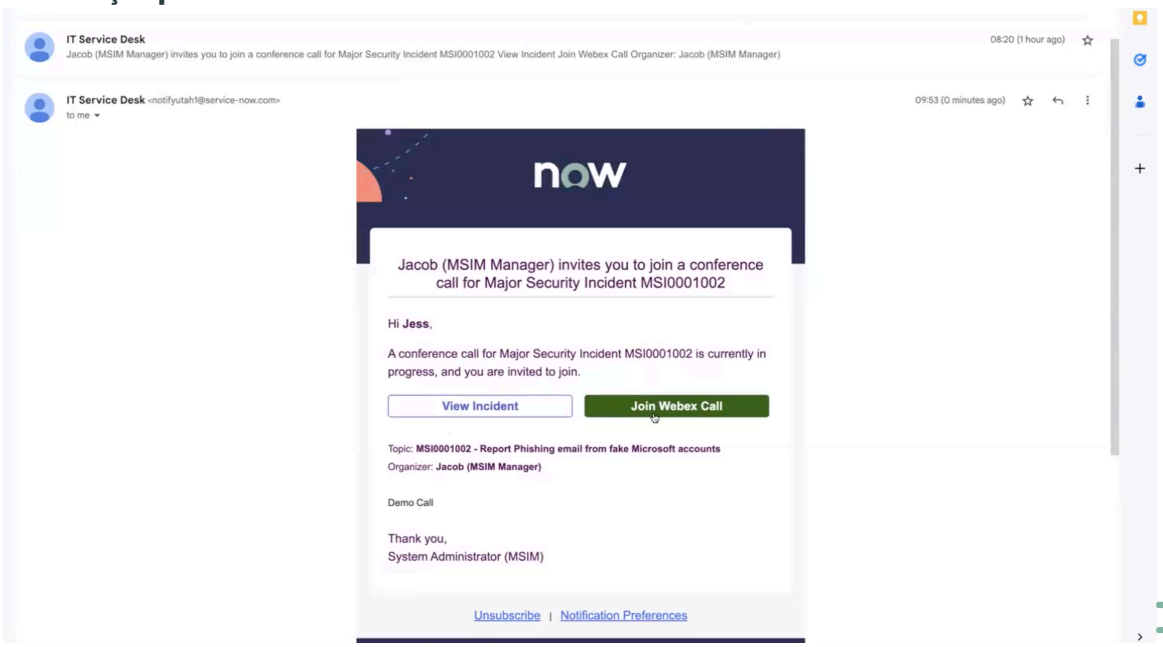
9. Depois que a lista de participantes for finalizada, selecione **Iniciar** .
   A chamada em conferência começa no aplicativo Cisco Webex. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado para os participantes a partir do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência Cisco Webex.

10. Selecione **Clique aqui** Opção além do incidente de segurança grave para ingressar na chamada em conferência no aplicativo Cisco Webex.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Cisco Webex para ingressar na chamada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificação por e-mail



11. Abra o incidente grave de segurança associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou seleciona **Encerrar chamada** Na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Configuração da Gestão de incidentes graves de segurança

Instalar e configurar Gestão de incidentes graves de segurança aplicação.

Importante:

- Para começar rapidamente com Gestão de incidentes graves de segurança configuração, você pode consultar Guia de início rápido da Gestão de incidentes de segurança graves (MSIM) Na ServiceNow Store.
- Depois de instalar o. Gestão de incidentes graves de segurança, certifique-se de importar o conjunto de atualizações em KB1289784 para carregar os arquivos parcialmente pré-configurados.

Use esta seção para saber como definir as configurações necessárias para trabalhar com Incidente grave de segurança integrando com outro externo Microsoft aplicações com as quais estabelecer conexões ServiceNow instância.

Configure o componente do Explorador de arquivos

O componente do espaço do Explorador de arquivos organiza e rastreia a coleção de artefatos (arquivos) relacionados a um incidente de segurança grave. Ele foi projetado para oferecer suporte à integração com qualquer provedor de hospedagem de arquivos de terceiros, como Microsoft SharePoint em Gestão de incidentes graves de segurança espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- File Explorer Componente: Fornece uma interface gráfica do usuário para exibir o sistema de arquivos e permite que os usuários executem operações de arquivo.
- File Explorer Core: Fornece uma camada de abstração que permite que o componente Explorador de arquivos exiba o sistema de arquivos e execute várias operações de arquivo sem saber nada sobre o conector subjacente usado para se comunicar com repositórios externos.
- File Explorer Microsoft SharePoint Aplicação do conector: Fornece os módulos de implementação necessários para rastrear e buscar metadados de arquivos/pastas de um Microsoft SharePoint biblioteca de documentos e executar operações de arquivo.

. File Explorer O componente principal fornece uma infraestrutura de base necessária para que as diferentes aplicações do conector de compartilhamento de arquivos definam suas propriedades de conexão.

Você deve instalar e configurar a unidade do repositório de arquivos e o provedor do repositório de arquivos adicionando as propriedades de conexão para extrair os metadados dos arquivos de um local do provedor de hospedagem de arquivos.

Para esta versão atual do File Explorer, essas instruções incluem configurar e assinar um arquivo de recuperação metadados como Microsoft SharePoint atualizações de arquivo e pasta, operações de arquivo e atividade de registro em log. Designado Microsoft SharePoint a biblioteca de documentos e a configuração da unidade relacionada serão necessárias para criar pastas individuais específicas de um incidente de segurança grave.

File Explorer também permite aplicações de conector, como Microsoft SharePoint. Você pode usar este exemplo para configurar suas implementações de operação de arquivo, como **Download** ou **Renomear** As ações de pasta e arquivo serão habilitadas no componente do espaço do Explorador de arquivos. Essas ações são habilitadas e executadas usando os subfluxos do Flow Designer integrado. Para obter mais informações, consulte Configurações de ação de pasta e arquivo .

File Explorer configuração inclui a seguinte configuração:

- Configurar o Explorador de arquivos Repositório Unidade
- Defina as Configurações de ação de pasta e arquivo
- Criar modelos de pasta

Comece a usar o Explorador de arquivos

Revise as informações a seguir antes de começar a trabalhar com File Explorer Componente.

Revise as informações a seguir antes de começar a estabelecer a conexão com Microsoft SharePoint criando ações de pasta e arquivo e criando modelos de pasta para o componente do gerenciador de arquivos.

Pré-requisitos

Nome	Descrição
Microsoft SharePoint spoke, versão 2.0.2 para ServiceNow® IntegrationHub.	Usar **sn_sp_spoke** ID do plug-in para pesquisar e instalar Microsoft SharePoint spoke.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Nome	Descrição
	A instalação deste plug-in fornece fluxos e ações para automatizar a colaboração, a gestão de documentos e os direitos de acesso do usuário no Microsoft SharePoint.
Componente do Explorador de arquivos v1.1.0	Usar **sn_file_explorer** ID do plug-in para pesquisar e instalar o componente do Explorador de arquivos v1.1.0 A instalação deste plug-in fornece uma interface gráfica do usuário para navegar pelo sistema de arquivos, que está disponível no núcleo do gerenciador de arquivos.
Explorador de arquivos Core para operações de segurança v1.1.1	Usar **sn_fe** ID do plug-in para pesquisar e instalar o File Explorer Core. A instalação deste plug-in fornece infraestrutura de base para integração com qualquer provedor de hospedagem de arquivos de terceiros.
Microsoft SharePoint Conetor do Explorador de arquivos para operações de segurança v1.1.1	Usar **sn_fe_sharepoint** ID do plug-in para pesquisar e instalar Microsoft SharePoint Conector do Explorador de arquivos. Instalar este plug-in gerenciará o. Microsoft SharePoint Arquivos/pastas usando o Gerenciador de arquivos.

Configurar o Explorador de arquivos Repositório Unidade

. Microsoft SharePoint o conector fornece vários recursos a serem implementados em Microsoft SharePoint Recursos do Explorador de arquivos gerenciando e rastreando os metadados do arquivo.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança grave** > **Gerenciador de Arquivos** > **Configuração do repositório de arquivos**.
2. Preencha os seguintes campos conforme descrito na tabela a seguir:

Nome do Campo	Descrição de Campo
Nome	Nome do registro do repositório de arquivos que identifica o uso. Por exemplo, MSIM.
Provedor	Nome do provedor que é o provedor de repositório de hospedagem de arquivos de terceiros. Por exemplo, Microsoft SharePoint.

Tradução automática

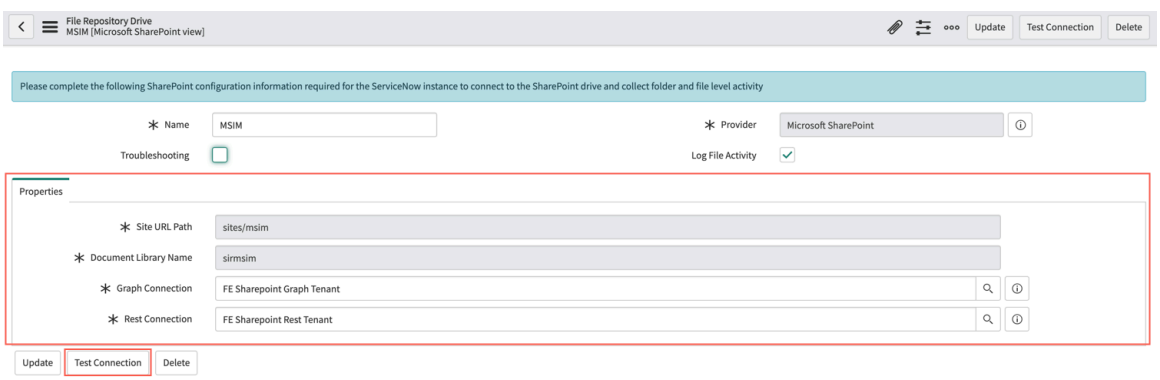
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição de Campo
Propriedades	
Caminho de URL de site	Insira um Microsoft SharePoint URL com um caminho de site específico. Forneça somente o caminho relativo para o site e uma URL completa do site pode não ser necessária. Por exemplo, Sites/MSIM.
Nome da biblioteca de documentos	Crie uma biblioteca de documentos em Microsoft SharePoint e forneça o mesmo nome de biblioteca de documentos aqui. Esta seria a mesma biblioteca de documentos que você criou no Microsoft SharePoint Configuração da unidade do conector.
Conexão do Graph	Selecione o registro de locatário do Gráfico do Explorador de arquivos. Para obter mais informações sobre a configuração da conexão do locatário, consulte Spoke do Microsoft SharePoint .
Conexão REST	Selecione o registro de locatário REST do Explorador de arquivos. Para obter mais informações sobre a configuração da conexão do locatário, consulte Spoke do Microsoft SharePoint .

3. Selecione **Save** (Salvar).
4. Clique **Testar conexão** para testar a conexão e validar as propriedades de configuração da unidade do repositório de arquivos.

   Nota: Antes **Ativando** repositório de arquivos, certifique-se de que a biblioteca de documentos correspondente esteja em Microsoft SharePoint não tem dados de pasta ou arquivo.

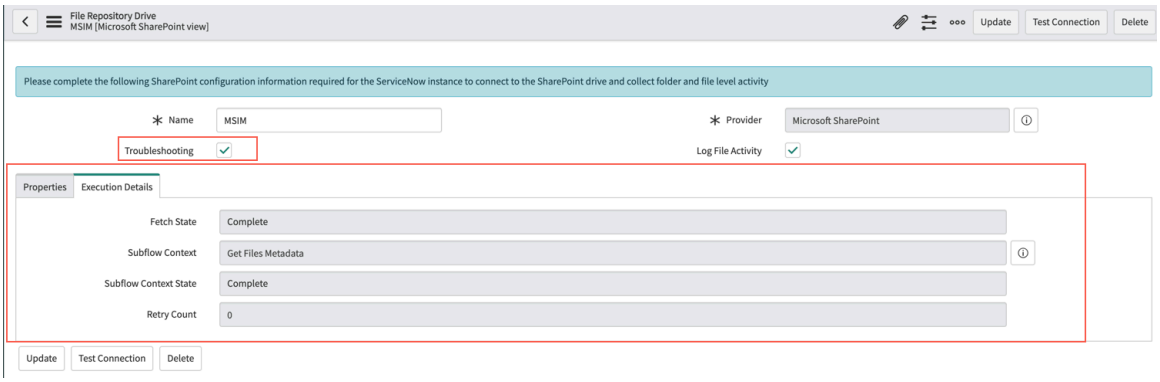
5. Clique em **Ativar** para ativar o repositório de arquivos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Solução de problemas** marque a caixa para verificar o repositório de arquivos **Detalhes da execução** e verifique **Buscar estado** está concluído e certifique-se de que Microsoft SharePoint As assinaturas da unidade são criadas e o estado é Concluído.



Nota: Usando o. **Testar conexão** Administrador MSI ou Gerenciador MSI só podem validar a configuração do repositório de arquivos.

Defina as Configurações de ação de pasta e arquivo

C onfigure . Ações de pasta e arquivo que você deseja habilitar no componente Explorador de arquivos no espaço Gestão de incidentes de segurança graves , Usando a página de configuração Configurações de ação de pasta e arquivo . Como administrador MSI, você pode controlar as ações individuais de pasta e arquivo exibidas no componente Explorador de arquivos.

Antes de Iniciar

A seguir estão os recursos de operações de arquivo implementados no componente do gerenciador de arquivos usando ServiceNow® flow designer:

Recursos de Operações de arquivo

Operação de arquivo	Descrição
Aberto em Microsoft SharePoint	Abre uma nova guia do navegador para exibir Microsoft SharePoint exibição de arquivos da biblioteca de documentos
Criar pasta	Capacidade de criar pastas ad hoc adicionais após a criação do incidente de segurança grave.
Renomear pasta	Capacidade de renomear as pastas criadas.
Mover arquivo	Permite mover arquivos entre pastas no componente Explorador de arquivos do espaço, resultando na movimentação de arquivos no Microsoft SharePoint
Localizar arquivo	Mostra o local da pasta ao usar **Recentes** Exibição do Explorador de arquivos.
Exclusão de arquivo	Exclua o arquivo.
Excluir pasta	Exclua a pasta.
Baixar arquivo	Baixa o arquivo na guia do navegador do Espaço MSIM existente para exibição rápida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos de Operações de arquivo

Operação de arquivo	Descrição
Renomear arquivo	Renomeia o arquivo.

Nota:

1. No momento, todas as ações listadas estão habilitadas por padrão. Você precisará editar o. **Configurações de ação de arquivo** se você não quiser que determinadas ações sejam exibidas. No momento, todas as configurações são globais para todos os usuários, o que significa que não há capacidade de habilitar ações para um subconjunto de usuários que têm uma função específica.
2. **Revogar acesso do usuário** e **Adicionar permissão** ações são ações relacionadas ao sistema. Não é recomendável modificar essas ações de arquivo.

A amostra a seguir procedimento descreve um dos recursos de operações de arquivo ies Para desabilitar qualquer ação específica de pasta e arquivo durante a configuração do Repositório do Explorador de arquivos. Este procedimento é aplicável a todas as outras ações que podem precisar ser editadas :

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Gerenciador de Arquivos** > **Configurações de ação de pasta e arquivo**.
2. Selecione o registro desejado para habilitar ou desabilitar a ação de pasta ou arquivo, respectivamente.
3. Desmarcar . **Ativo** caixa de seleção para desabilitar a ação de pasta e arquivo.

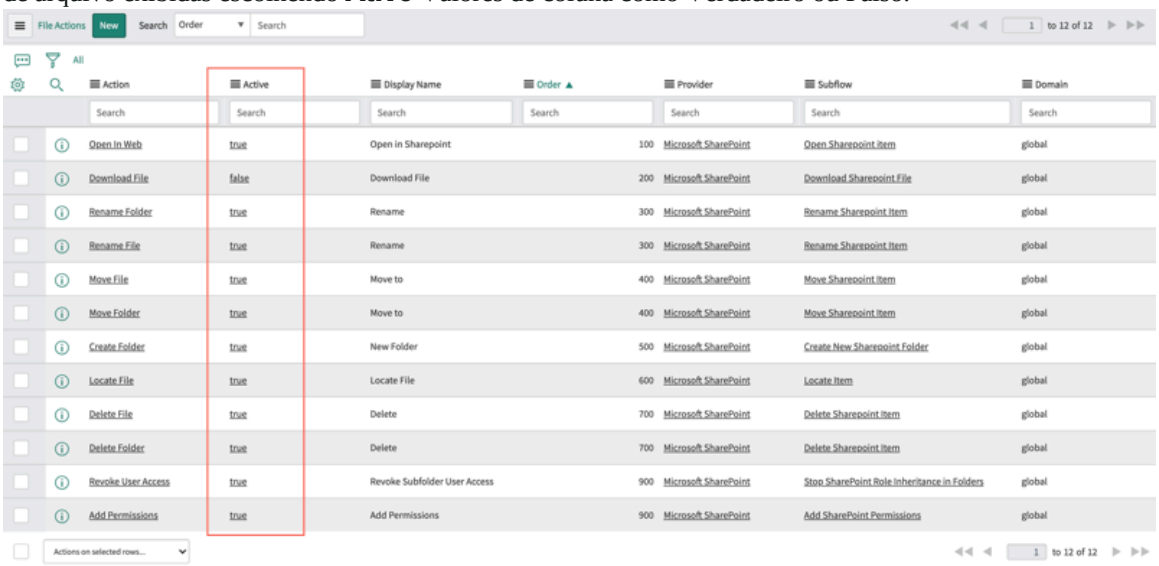


Tradução automática

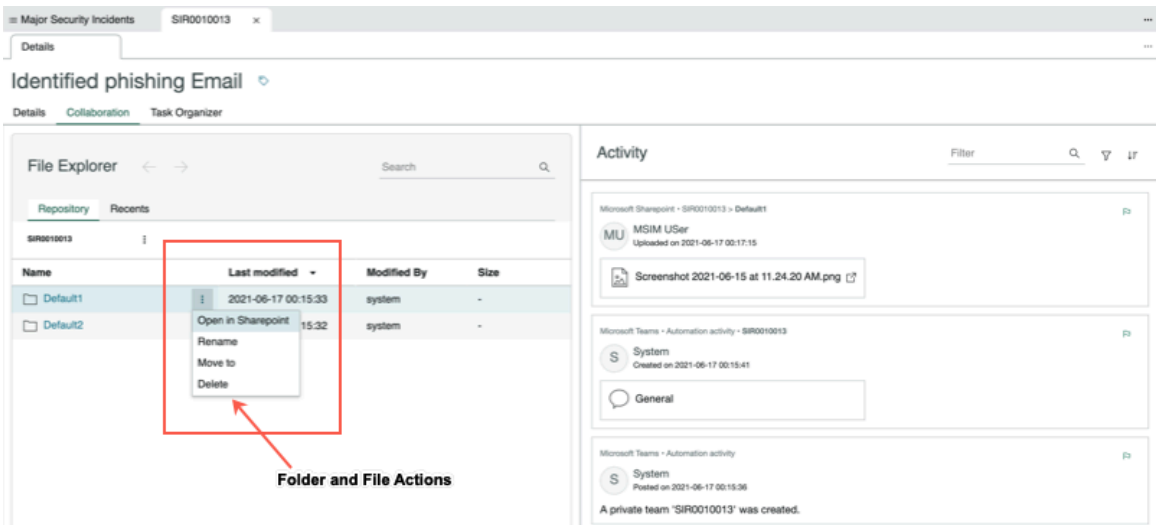
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Atualização** o registro da unidade.

Nota: Você também pode executar a ação de arquivo diretamente na lista de operações de arquivo exibidas escolhendo **Ativo** Valores de coluna como Verdadeiro ou Falso.



Se a ação de arquivo realizada estiver desabilitada, a ação não será exibida no **Colaborações** . **Gestão de incidentes graves de segurança** espaço.



Criar modelos de pasta

Use Modelos de pasta para criar automaticamente pastas exclusivas para diferentes tipos de incidentes de segurança graves. Os modelos de pasta no componente Explorador de arquivos são usados para criar uma estrutura de pasta de base para o incidente de segurança no Microsoft SharePoint.

Antes de Iniciar

Como administrador MSI, você define a estrutura de pasta inicial necessária para permitir a colaboração entre diferentes grupos de respondentes a incidentes e atribui privilégios de acesso apropriados em um nível de subpasta. Várias configurações podem ser criadas para diferentes Incidente grave de segurança tipos que usam um construtor de condições para específico Incidente grave de segurançavalores de campo, que incluem a permissão de acesso a diferentes usuários e grupos de usuários em cada nível de subpasta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esses modelos de pasta são usados por todos os incidentes de segurança graves que atendem às condições especificadas no Construtor de condições. É recomendável que você considere o uso de variáveis de campo de incidente, como o número ou a categoria do incidente, para criar nomes de pasta raiz exclusivos que diferenciem um conjunto de subpastas com nomes de pasta comuns para um incidente de segurança grave de pastas semelhantes com esses nomes que fazem parte de um incidente de segurança grave diferente.

A configuração de Modelos de pasta definidos é aplicada ao incidente de segurança grave somente quando a condição é correspondida.

Nota: Uma configuração do sistema de base (sem subpastas) é aplicada a todos os incidentes de segurança. Você pode editar esta configuração padrão para incluir subpastas específicas ou criar uma nova configuração com base em um conjunto especificado de valores de campo de incidente de segurança grave. Atividade de código mal-intencionado.

Função necessária: sn_msi.workspace_admin

Procedimento

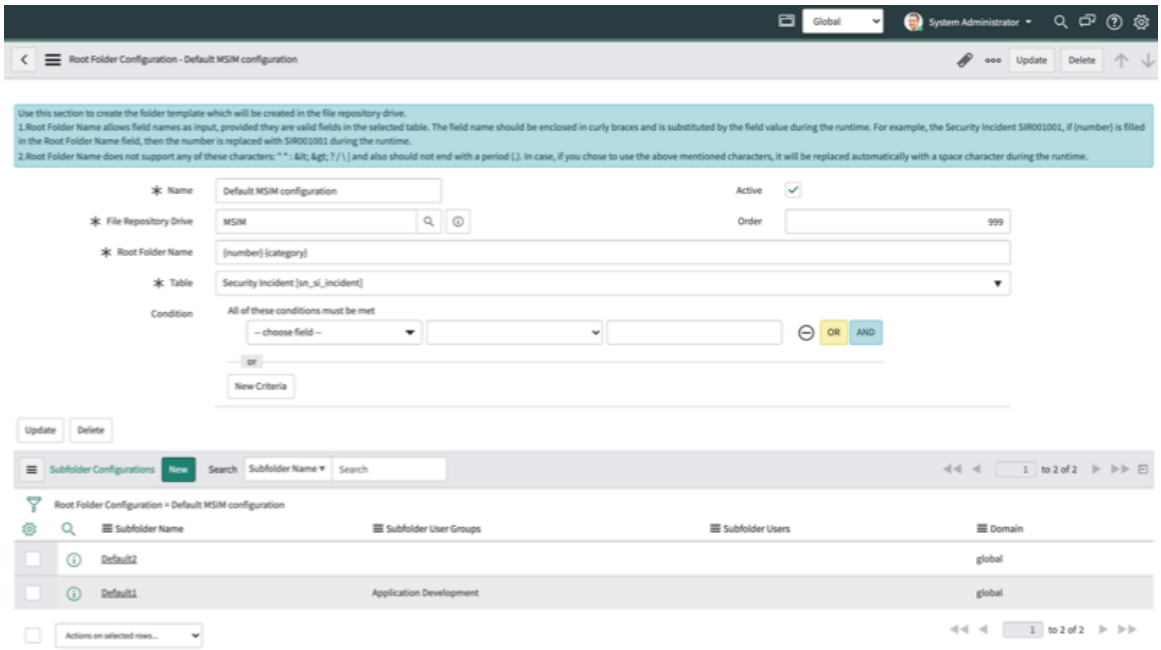
1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Gerenciador de Arquivos** > **Modelos de pasta**.
2. Clique **Novo(a)** Para Configuração da pasta raiz.
3. No formulário, preencha os campos.

Nome do Campo	Descrição
Nome	Nome do modelo de pasta.
Unidade de repositório de arquivos	
Nome da pasta raiz	Nome da pasta raiz que aparecerá em Microsoft SharePoint E o Explorador de arquivos e provavelmente devem incluir variáveis de campo de incidente, como o número e a categoria do incidente de segurança grave, para que um incidente de segurança grave possa ser diferenciado de outro.
Tabela	

4. Defina o incidente de segurança **Condição** valores.

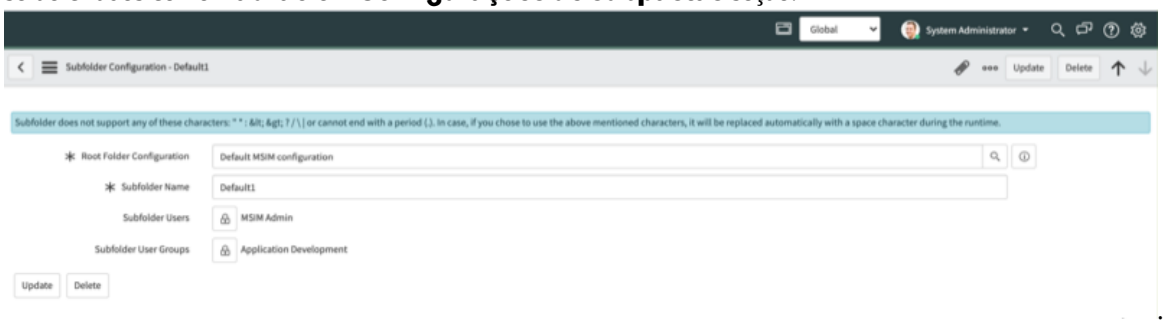
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. **Atualizar** o registro.
   As subpastas são criadas com os valores definidos.

6. Clique no desejado **Subpasta** .
   Se você não criar uma subpasta com um nome apropriado, os nomes das subpastas serão criados como **Padrão** em **Configurações de subpastas** seção.



A mesma estrutura de pastas será criada automaticamente em Microsoft SharePoint usando os mesmos privilégios de acesso que estão configurados no **Modelos de pasta** página.

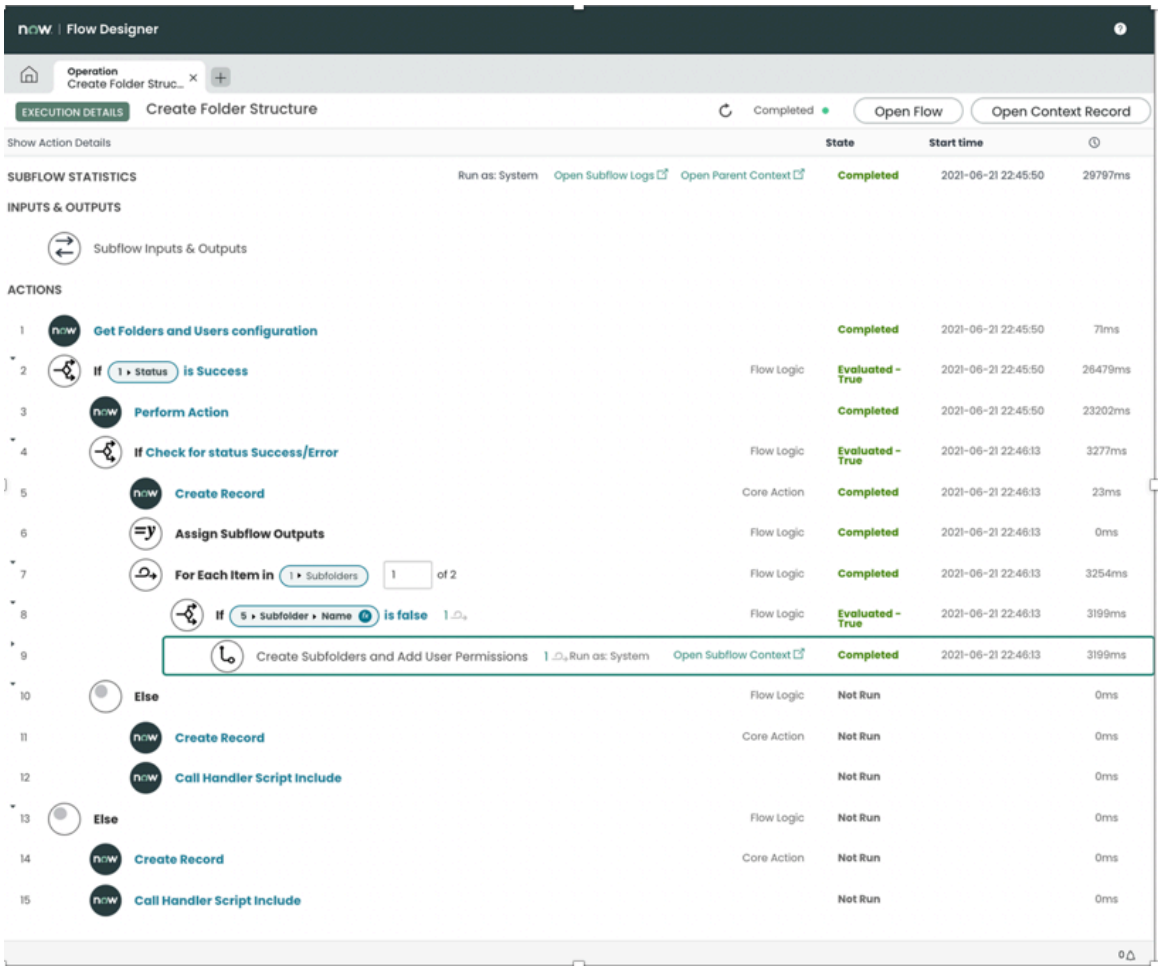
Nota:

- **Nome da pasta raiz** permite nomes de variáveis de campo como entrada, desde que sejam campos válidos na tabela selecionada. O nome do campo deve estar entre chaves e é substituído pelo valor do campo durante o tempo de execução do fluxo. Por exemplo, o Incidente de segurança SIR001001, se a variável Número estiver configurada no **Nome da pasta raiz** , o número é substituído por SIR001001 durante o tempo de execução.
- **Nome da pasta raiz** não é compatível com nenhum destes caracteres: " * : " e também, não devem terminar com um ponto (.). Se você usar os caracteres mencionados acima, eles serão substituídos automaticamente por um caractere de espaço durante o tempo de execução.
- . **Pasta raiz** e. **Subpasta** o nome excede o limite definido (256 caracteres) e o nome da pasta é truncado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está a execução do tempo de execução do subfluxo Criar estrutura de pasta:



File Explorer Fluxo de atividades no espaço

Use a seção Explorador de arquivos do Gestão de incidentes graves de segurança espaço para exibir as pastas e os arquivos, a sequência em que foram criados Microsoft SharePoint biblioteca de documentos.

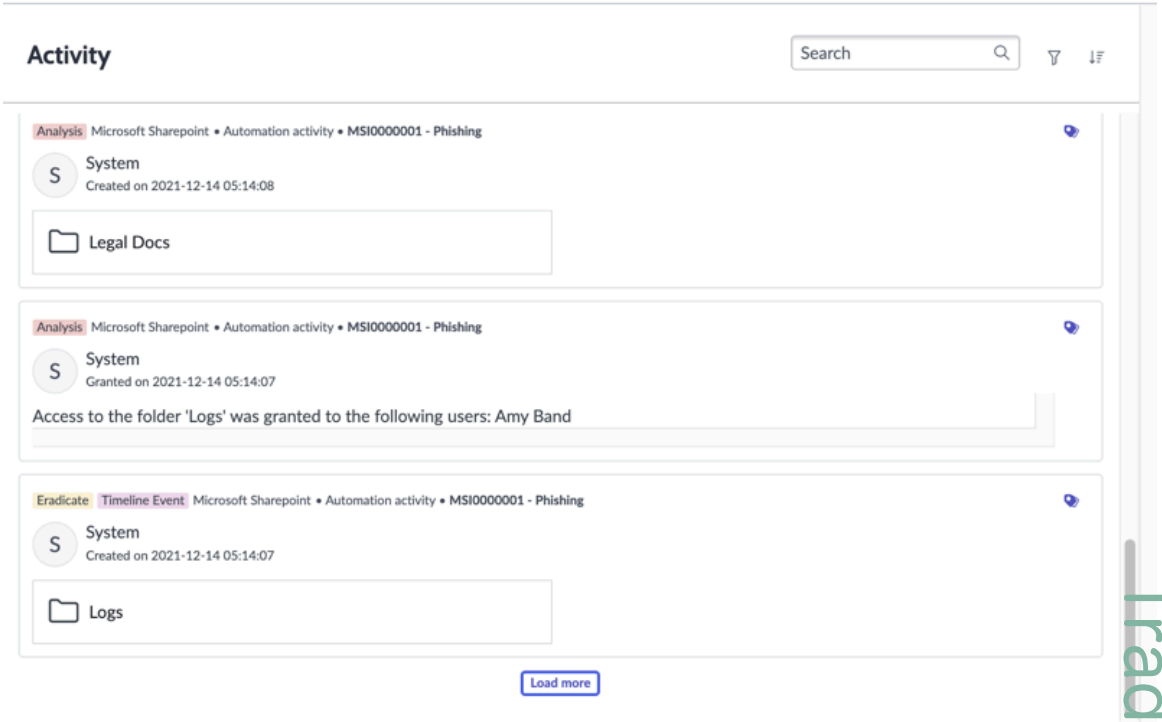
O fluxo de atividades lista todas as publicações de atividades de automação sempre que qualquer atividade de pasta e arquivo ou logs que ocorrem durante Incidente grave de segurança resolução. A estrutura do fluxo de atividades está alinhada no mesmo formato do Microsoft SharePoint biblioteca que mostra as pastas que foram criadas e quais usuários ou grupos de usuários foram atribuídos a essas pastas.

O fluxo de atividades permite que os gerentes do espaço e outros usuários ou grupos de usuários se comuniquem e colaborem com eficácia, listem as atividades que foram realizadas em Microsoft SharePoint monitorar o status do incidente, publicar as anotações ou adicionar comentários adicionais que eles têm no registro do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os gerentes de espaço podem escolher e trabalhar com base na última atividade



atualizada.

Solução de problemas File Explorer

A seção de solução de problemas pode ajudá-lo a resolver alguns dos problemas técnicos que você pode encontrar ao configurar File Explorer componente.

Consulte a seção a seguir sobre os trabalhos agendados, as propriedades do sistema e File Explorer subfluxos do flow designer em detalhes.

Trabalhos agendados para File Explorer

Trabalhos agendados são trabalhos automatizados executados para processar as notificações do Microsoft SharePoint, ingira os metadados dos arquivos no ServiceNow e renovar as assinaturas do repositório de arquivos em uma programação recorrente.

Trabalhos agendados são trabalhos automatizados que são executados em segundo plano para:

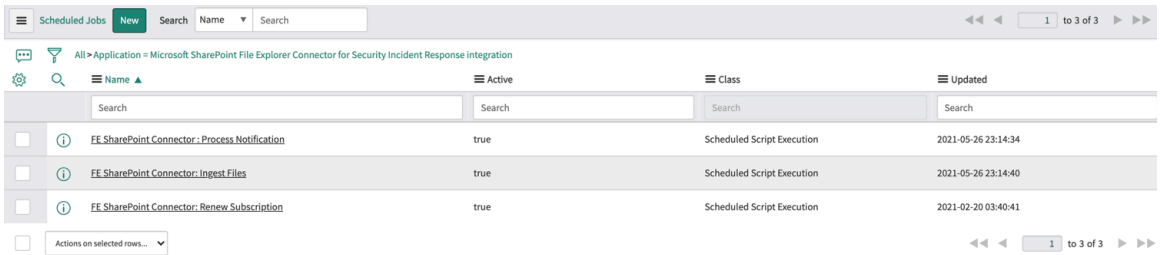
- Processe as notificações da Microsoft Microsoft SharePoint.
- ingira os metadados dos arquivos no ServiceNow AI Platform instância.
- renove a assinatura com Microsoft SharePoint biblioteca de documentos para receber notificações.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: Notificação de processo	É executado a cada 30 segundos e é responsável por ler as notificações, o que indica que ocorreu qualquer mudança na biblioteca de documentos assinados e marca o estado das unidades (sn_fe_file_repo_drive) como pendente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: Ingerir arquivos	É executado a cada 30 segundos e é o principal responsável pelo processamento das unidades (sn_fe_file_repo_drive) que estão no estado pendente e extrai as mudanças do arquivo delta do configurado Microsoft SharePoint biblioteca de documentos desde a última extração.
Microsoft SharePoint File Explorer Renovar assinatura	Executado a cada 10 minutos e responsável pela renovação do Microsoft SharePoint assinatura da biblioteca de documentos um dia antes da data de vencimento. Essas assinaturas expiram em 30 dias.



Propriedades do sistema do Explorador de arquivos disponíveis

A seguir estão disponíveis Microsoft SharePoint Propriedades do sistema do Conector do Explorador de arquivos.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_fe_sharepoint.max_retry_count	Controla a frequência de tentativas que Microsoft SharePoint a aplicação do conector tentou extrair a unidade com falha ou renovar a assinatura com falha. O valor de frequência padrão é definido como 50.
sn_fe_sharepoint.retry_after_seconds	Intervalo de tempo entre cada tentativa de extrair a unidade com falha ou renovar a assinatura. O valor padrão é definido como 900 segundos ou 15 minutos.
sn_fe_sharepoint.max_subscription_expiration_time	Período máximo de expiração da assinatura em número de dias para Microsoft SharePoint. O período de expiração padrão é definido como 30 dias.

File Explorer Subfluxos do Flow Designer

A seguir estão os subfluxos do Flow Designer instalados com Microsoft SharePoint File Explorer conector.

Subfluxos

Nome	Descrição
Adicionar Microsoft SharePoint Permissões	Concede permissão de edição para uma pasta específica a usuários específicos.
Criar assinatura do Drive	Assina com um configurado Microsoft SharePoint biblioteca de documentos para receber notificações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Subfluxos

Nome	Descrição
	sobre quaisquer atualizações que ocorram na biblioteca de documentos.
Criar Novo Microsoft SharePoint Pasta	Cria um novo Microsoft SharePoint pasta em uma determinada pasta primária.
Excluir Microsoft SharePoint Item	Exclusões Microsoft SharePoint arquivos e pastas.
Download Microsoft SharePoint Arquivo	Retorna o URL de download de Microsoft SharePoint arquivos
Obter metadados de arquivos	Assina e extrai as mudanças de Microsoft SharePoint biblioteca de documentos.
Mover Microsoft SharePoint Item	Move o. Microsoft SharePoint arquivos/pastas para a pasta de destino
Aberto Microsoft SharePoint Item	Retorna o URL da web de Microsoft SharePoint arquivo/pasta a ser aberto em um navegador.
Renovar assinatura do Drive	Renova a assinatura com Microsoft SharePoint biblioteca de documentos.
Criar estrutura de pastas	Segue as configurações do modelo de pasta e cria a estrutura de pastas em Microsoft SharePoint biblioteca de documentos.

Como configurar o Microsoft Teams

Configurar Gestão de incidentes graves de segurança com Microsoft Teams que ajuda a comunicação pelo bate-papo a resolver Incidente grave de segurança.

Configurar e assinar um Microsoft Teams O ambiente de bate-papo, a recuperação de conversas de bate-papo de dentro dos canais especificados e o arquivamento da equipe e dos canais associados estão incluídos como parte do processo de fechamento do incidente. Designado Microsoft Teams ambiente e relacionado Microsoft Teams Graph A configuração da API é necessária para criar canais individuais específicos de um Incidente grave de segurança.

Para configurar o Microsoft Teams, ative o Teams como o provedor de bate-papo. Em seguida, você pode criar canais de bate-papo para as várias partes interessadas e grupos que se comunicam sobre atividades e rastrear conversas de bate-papo para resolver o. Incidente grave de segurança. A configuração da API do Microsoft Teams e do Microsoft Graph inclui:

- Estabelecer conexão do MS Teams Graph em ServiceNow AI Platform
- Ative o MS Teams como um provedor de bate-papo
- Crie um modelo de canal de bate-papo
- Exibir atividade de mensagem de bate-papo

Para começar com Microsoft Teams

Revise as informações a seguir antes de começar a trabalhar com Microsoft Teams como uma aplicação de conector.

Certifique-se de que os plug-ins a seguir estejam instalados antes de começar a estabelecer, ativar e validar Microsoft Teams configurar conexões.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-ins necessários

Nome	Descrição
Integração de bate-papo com a Gestão de incidentes de segurança	Usar **sn_chat_collab_core** ID do plug-in para pesquisar e instalar Microsoft Teams Bate-papo. Instalar este plug-in permite rastrear a atividade de bate-papo para aplicativos de terceiros, como o Microsoft Teams (ou Slack e outros aplicativos de bate-papo de terceiros).
Conector de bate-papo do Microsoft Teams para Gestão de incidentes de segurança	Usar **sn_ms_teams_connector** ID do plug-in para pesquisar e instalar o Conector de bate-papo do Microsoft Teams para Gestão de incidentes de segurança graves. Instalar este plug-in permite rastrear as atividades de bate-papo usando o componente de colaboração específico para Microsoft Teams.
Microsoft Teams Spoke do gráfico	A instalação deste plug-in estabelece uma conexão do Graph Spoke com Microsoft Teams. Para obter mais informações, consulte Spoke do Microsoft Teams Graph

Ative o MS Teams como um provedor de bate-papo

Ativar Microsoft Teams validando o. Microsoft Teams Conexão.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Quando a conexão é ativada e validada, uma mensagem informativa é exibida informando que a conexão do provedor foi validada com sucesso. Você pode modificar a configuração do canal adicionando e removendo usuários e, possivelmente, adicionando mais canais ou renomeando os canais existentes.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Configuração do provedor de bate-papo**.
2. Selecione **Registro do Microsoft Teams** .
3. Clique em **Validar conexão** .
   Uma mensagem de confirmação é exibida informando que a conexão do provedor foi validada com sucesso.
4. Selecione **Ativo** caixa de seleção para ativar o registro do provedor.
   Uma mensagem de confirmação é exibida informando que a conexão do provedor foi validada com sucesso.
5. **Salvar** depois de ativar a configuração do provedor de bate-papo.
   Com essa conexão entre o Microsoft Teams e. ServiceNow AI Platform A instância foi estabelecida com sucesso.

Crie um modelo de canal de bate-papo

Configure Equipes de bate-papo e Modelos de canal para criar equipes de bate-papo e canais para colaborar, rastrear as conversas de bate-papo e adicionar usuários e grupos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de usuários a esses Canais de bate-papo. Esses modelos de canal são criados no Microsoft Teams quando um incidente de segurança grave é promovido.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

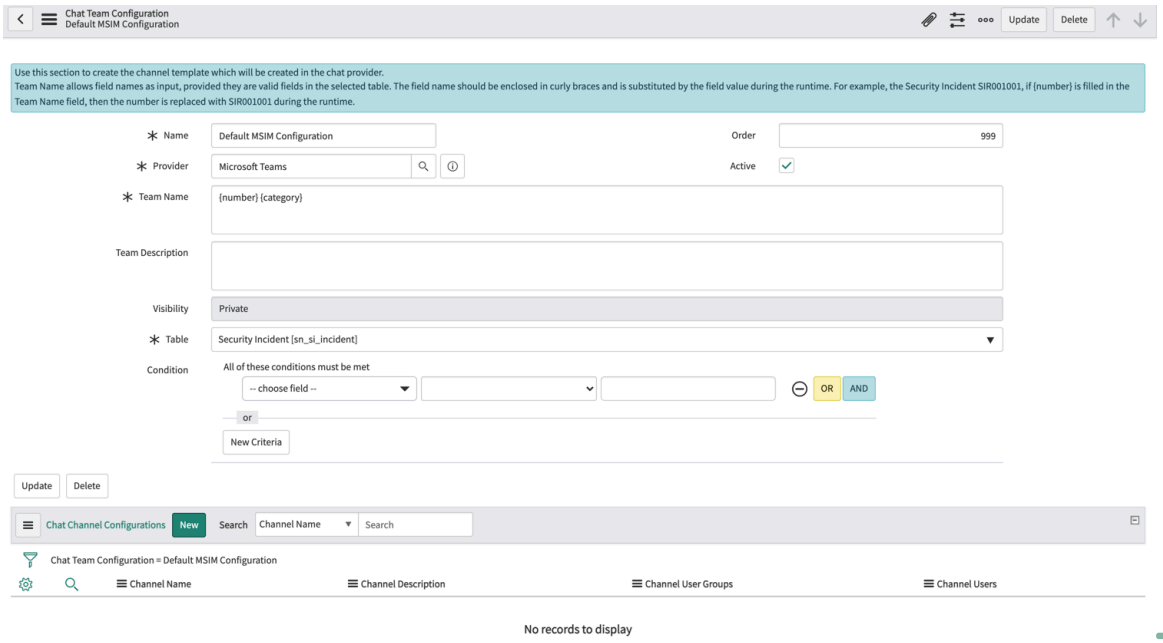
1. Navegar até **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Modelos de canal**.
2. No formulário Configuração do canal de bate-papo, clique em **Novo** no cabeçalho do formulário.
3. No formulário, preencha os campos.

Formulário Configuração da equipe de bate-papo

Campo	Descrição
Nome	Nome da pasta.
Provedor	Microsoft Teams.
Nome da Equipe	Nome da equipe, por exemplo, no formato "número"-"categoria". **Nota:** O nome da equipe fornecido aqui será usado em todos os registros de Incidentes de segurança graves. Para garantir que o Nome real da equipe da Microsoft seja exibido na aplicação MS Teams e tenha um valor de nome exclusivo para diferentes incidentes de segurança graves, é recomendável que você use um valor de campo de incidente exclusivo, como o número do incidente - (número). Como mostrado no exemplo de captura de tela, o "número" seguido por um separador "-" e a variável de campo "categoria" forneceriam um número exclusivo e uma descrição do incidente de segurança grave para o qual o Microsoft Teams foi criado, por exemplo "número" - "categoria".
Descrição da equipe	Descrição opcional da equipe.
Tabela	Incidente de segurança grave (sn_msi_incident).

Tradução automática

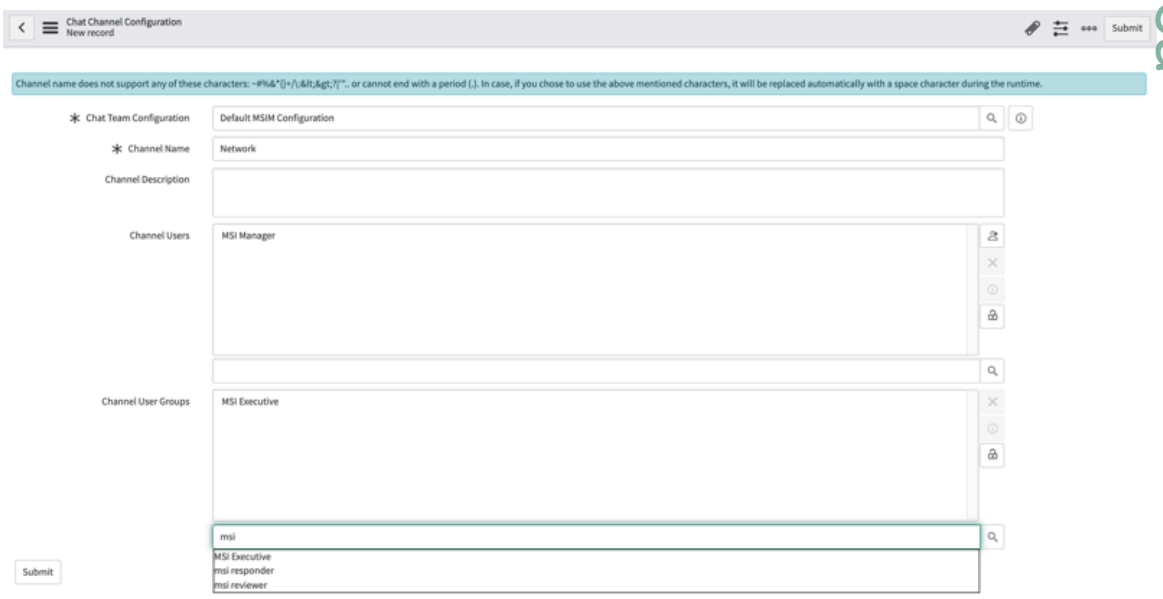
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Enviar**.
5. Navegue até a seção Configuração do canal de bate-papo.
6. Clique **Novo(a)** Para criar uma nova Configuração de canal de bate-papo.
7. Insira **Configuração da equipe de bate-papo** e **Nome do Canal**.

> **Nota:** O novo canal que você criou aqui também será o nome do seu canal no Microsoft Teams. Você pode pesquisar o mesmo canal e adicionar suas conversas.

8. Adicione **Usuários do canal** e **Grupos de usuários do canal** na lista de pesquisa.
9. **Enviar** novo registro de configuração do canal de bate-papo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

Agora, o canal de bate-papo foi criado e os usuários foram atribuídos a esses grupos de canal de bate-papo. Você pode exibir as atividades de bate-papo de colaboração em Microsoft Teams E no fluxo de atividades Colaboração do Espaço do MSIM com a estrutura de hierarquia de canal de bate-papo organizado, conforme configurado na configuração do provedor de canal de bate-papo.

Exibir atividade de mensagem de bate-papo

A atividade de mensagem de bate-papo é registrada e exibida na guia Colaboração do espaço Gestão de incidentes de segurança graves.

A atividade de mensagem de bate-papo inclui todas as conversas de bate-papo ocorridas entre os participantes, diferentes grupos de usuários.

Solução de problemas do Conector de bate-papo do MS Teams para MSIM

Consulte a seção de solução de problemas do conector de bate-papo do Microsoft Teams sobre trabalhos agendados, propriedades do sistema e subfluxos do Flow Designer do Microsoft Teams.

Processe trabalhos agendados do conector de bate-papo em qualquer caso se você não vir que as mensagens de bate-papo de colaboração são publicadas no Microsoft Team e no fluxo de atividades de colaboração externa do espaço MSIM.

Trabalhos agendados para Microsoft Teams

Trabalhos agendados são trabalhos automatizados executados para processar as notificações do Microsoft Teams Conector de bate-papo e renove as assinaturas do Microsoft Teams em uma programação recorrente.

Função necessária: administrador

- **Conector de bate-papo do MS Teams: Notificação de processo**

  Para cada evento de mensagem de bate-papo, será recebida uma notificação que terá o ID do recurso e a notificação que serão armazenadas em uma tabela. Um trabalho de programação é executado a cada 30 segundos para selecionar notificações não processadas e consultar a API do Microsoft Teams para obter o conteúdo real da mensagem, que é armazenado em uma tabela diferente.

- **Conector de bate-papo do MS Teams: Renovar assinaturas**

  Para cada canal na equipe, as assinaturas são criadas para ser notificado sobre os eventos criados, atualizados e excluídos. Esta assinatura fica ativa somente por 60 minutos. As assinaturas são renovadas a cada 25 minutos por meio do trabalho de programação do Conector do Microsoft Teams: Renovar notificação.

Microsoft Teams Fluxo funcional do conector de bate-papo

Exiba esta seção para entender Microsoft Teams Subfluxos do Flow Designer relacionados usados para administrar a criação do(s) canal(s) de bate-papo e o acesso do usuário do incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

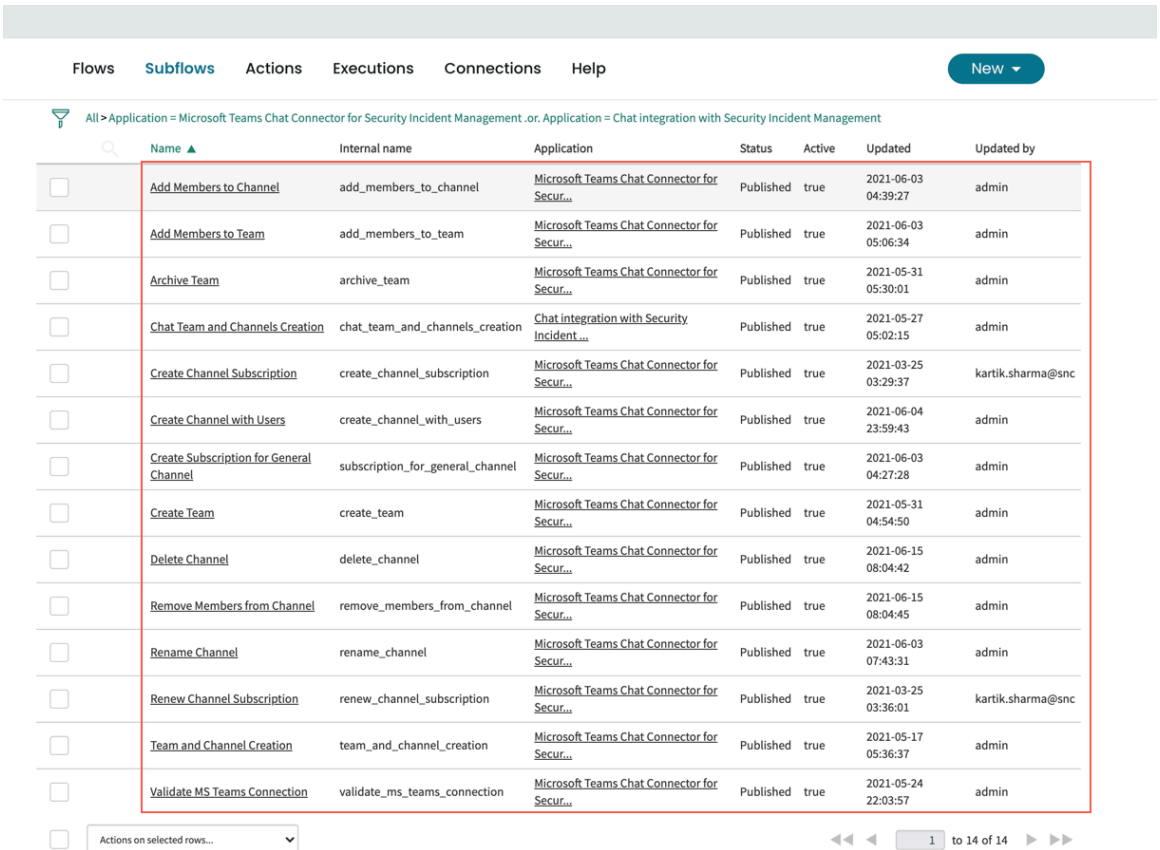
Procedimento

1. Navegar até **Tudo** > **Flow Designer**.
2. Adicionar membros ao canal

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicionar membros à equipe
4. Arquivar equipe
5. Criação de equipe de bate-papo e canais
6. Criar assinatura de canal
7. Criar canal com usuários
8. Criar assinatura para o canal geral
9. Criar Equipe
10. Excluir canal
11. Remover membros do canal
12. Renomear canal
13. Renovar assinatura do canal
14. Criação de equipe e canal
15. Validar conexão do MS Teams



Configure o conector de bate-papo do Slack para incidentes de segurança graves

Integre e colabore com Slack Para resolver Incidente de segurança grave para exibir e filtrar atividades de bate-papo de colaboração.

Configurar e assinar um Slack O ambiente de bate-papo, a recuperação de conversas de bate-papo de canais especificados e o arquivamento do Slack e dos canais associados estão incluídos como parte do processo de fechamento do incidente. Designado Slack ambiente e relacionado Slack A configuração da API é necessária para criar canais individuais específicos de um Incidente grave de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para configurar o Slack, ative o Slack como o provedor de bate-papo. Em seguida, você pode criar canais de bate-papo para as várias partes interessadas e grupos que se comunicam sobre atividades e rastrear conversas de bate-papo para resolver o. Incidente grave de segurança. . Slack e. Slack A configuração de API inclui:

- Comece a usar a configuração do conector de bate-papo do Slack
- Ative o Slack como um provedor de canal
- Crie um modelo de canal de bate-papo para o Slack
- Exibir atividades de mensagens de bate-papo no Slack

Comece a usar a configuração do conector de bate-papo do Slack

Revise as informações a seguir antes de começar a trabalhar com Slack como uma aplicação de conector.

Certifique-se de que os plug-ins a seguir estejam instalados antes de começar a estabelecer, ativar e validar Slack configurar conexões.

Plug-ins necessários

Nome	Descrição
Slack Conector de bate-papo para Gestão de incidentes de segurança	Usar **sn_slack_connector** ID do plug-in para pesquisar e instalar Slack Conector para Gestão de incidentes de segurança graves. Instalar este plug-in permite rastrear as atividades de bate-papo usando o componente de colaboração específico para Slack.
Slack spoke	A instalação deste plug-in estabelece uma conexão do spoke com Slack. Para obter mais informações, consulte Slack Spoke .

Crie um modelo de canal de bate-papo para o Slack

Configure Equipes de bate-papo e Modelos de canal para criar equipes de bate-papo e canais para colaborar, rastrear as conversas de bate-papo e adicionar usuários e grupos de usuários a esses Canais de bate-papo. Esses modelos de canal são criados em Slack quando um incidente de segurança grave é promovido.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa

O novo canal que você criar será o nome do canal em Slack também. Você pode pesquisar o mesmo canal e adicionar suas conversas.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Modelos de canal**.
2. Selecione **Configuração do canal do Slack** Para exibir os detalhes da configuração do Slack.
3. Selecione **Ativo** Caixa de seleção para ativar a configuração do canal de bate-papo do Slack.
4. No campo Nome da equipe, forneça o número MSI e o nome do código.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, todos os canais do Slack serão prefixados com o número do incidente. Por exemplo, MSI0000000 - [nome do canal] . Você pode mudar o prefixo para qualquer campo de sua escolha neste formato: (field_name) .

Nota: O nome da equipe fornecido aqui será usado em todos os registros de Incidentes de segurança graves. Para verificar se o real Slacké exibido em Slack E tem um valor de nome exclusivo para diferentes incidentes de segurança graves, é recomendável que você use um valor de campo de incidente, que é exclusivo, como MSI0000000 - [nome do canal] .

5. Clique com o botão direito do mouse na configuração e selecione **Salvar** .
6. Navegue até a seção Configuração do canal de bate-papo.
7. Selecionar **Novo(a)** Para criar uma nova Configuração de canal de bate-papo.
8. No formulário, preencha os campos.

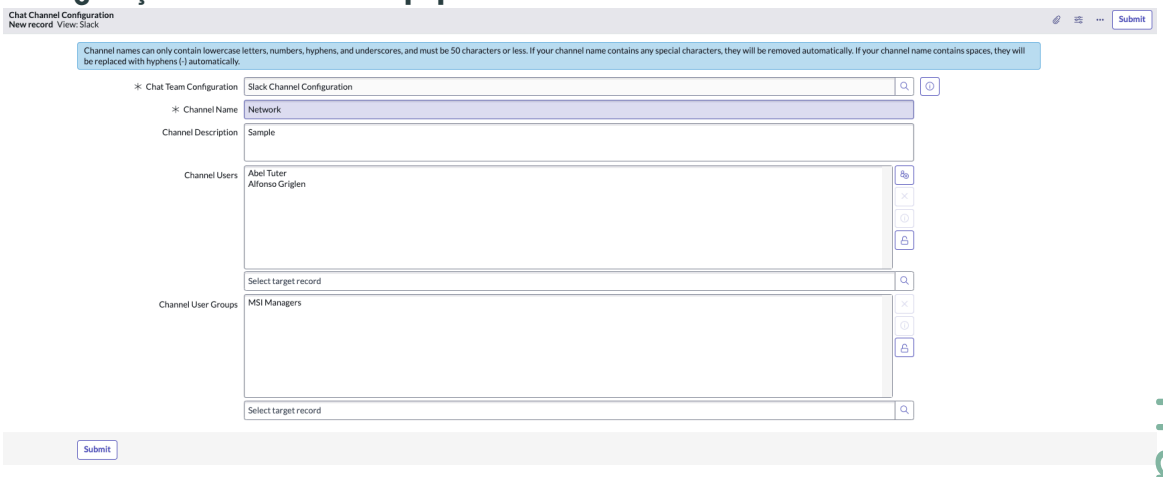
Campo	Descrição
Configuração da equipe de bate-papo	Nome da configuração da equipe de bate-papo. Por exemplo, configuração do canal do Slack.
Nome do Canal	Nome do canal. Por exemplo, jurídico. **Nota:** ○ Nomes de canal só podem conter letras minúsculas, números, hifens e sublinhados e devem ter 50 caracteres ou menos. Se o nome do canal contiver caracteres especiais, eles serão removidos automaticamente. Se o nome do canal contiver espaços, eles serão substituídos automaticamente por hifens (-). ○ O novo canal que você cria aqui será o nome do seu canal em Slack também. Você pode pesquisar o mesmo canal e adicionar suas conversas.
Descrição do Canal	Descrição exclusiva do canal.
Usuários do canal	Selecione **Desbloquear usuários do canal** e adicione os usuários que podem acessar este canal na lista de pesquisa. Selecione **Bloquear usuários do canal** ícone para bloquear a lista selecionada de usuários do canal.
Grupos de usuários do canal	Selecione **Desbloquear grupos de usuários do canal** e adicione os grupos de usuários que podem acessar este canal na lista de pesquisa. Você também pode usar **Adicionar-me** ícone para adicionar a si mesmo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Selecione **Bloquear grupos de usuários do canal** ícone para bloquear a lista seleciona–da de grupos de usuários do canal.

Configuração do canal de bate-papo do Slack



9. Selecione **Enviar**.

Resultado

Agora, o canal de bate-papo foi criado e os usuários foram atribuídos a esses grupos de canal de bate-papo. Você pode exibir as atividades de bate-papo de colaboração em Slack E no fluxo de atividades Colaboração do Espaço do MSIM com a estrutura de hierarquia de canal de bate-papo organizado, conforme configurado na configuração do provedor de canal de bate-papo.

Ative o Slack como um provedor de canal

Ativar Slack validando o. Slack conexão.

Antes de Iniciar

Função necessária:

- sn_msi.workspace_admin - Gravação
- sn_msi.chat_collab_provider - Ler

Quando a conexão é ativada e validada, uma mensagem informativa é exibida informando que a conexão do provedor foi validada com sucesso. Você pode modificar a configuração do canal adicionando e removendo usuários e, possivelmente, adicionando mais canais ou renomeando os canais existentes.

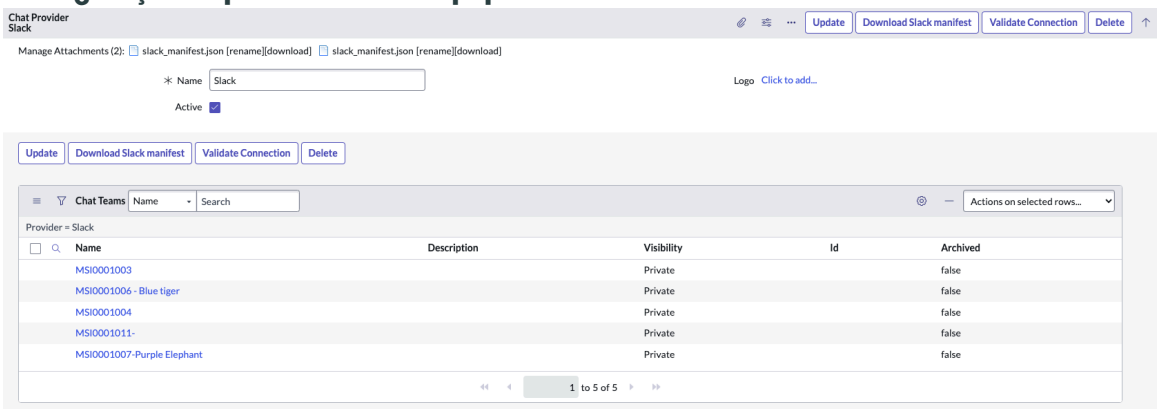
Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Configuração do provedor de bate-papo**.
2. Selecione **Slack** Para abrir a configuração do provedor de bate-papo do Slack.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do provedor de bate-papo do Slack



3. Selecione **Baixar manifesto do Slack** para baixar o. `slack_manifest.json` arquivo.
. `slack_manifest.json` O arquivo contém a configuração completa da configuração do Slack e permite que você configure o Slack automaticamente. Você precisa carregar este arquivo JSON na configuração do Slack.
4. Abra o. `slack_manifest.json` e execute as seguintes etapas:
   a. Vá para `api.slack.com/apps` URL no navegador da Web.
   b. Selecione **Criar novo app** ação.
   c. No pop-up Criar um app, escolha **De um manifesto do app** opção.
   d. No pop-up Escolha um espaço para desenvolver seu app, escolha um espaço na lista e selecione **Próximo** .
   Por exemplo, Espaço do Slack do MSIM.
   e. No pop-up Inserir manifesto do app abaixo, selecione **JSON** e copie e cole o código do `slack_manifest.json` arquivo.
   f. Selecione **Avançar**.
   g. No pop-up Revisar resumo e criar seu app, selecione **Criar** .
   Seu app foi criado.
   h. Na página Informações básicas, selecione **Instalar no espaço** .
   O bot de integração do Slack solicita sua permissão para acessar o Espaço do Slack do MSIM.
   i. Selecionar **Permitir**.
   j. Na seção Credenciais da aplicação, preencha os detalhes navegando de volta para a instância da ServiceNow.
   k. Selecionar **Tudo** > **Configurações do Slack**.
   Você precisa da função sn_msi.workspace_admin para esta ação.
   l. Selecione um **Segredo da assinatura** propriedade.
   m. Copie o segredo de assinatura e cole-o na seção Credenciais do app do Slack.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

n. Na instância da ServiceNow, navegue até **Tudo** > **Flow Designer**.

o. Navegar até **Conexões** > **Slack** > **Exibir detalhes** > **Configurar**.

p. No formulário, preencha os campos.

Campo	Descrição
Nome da Conexão	Nome desta conexão. Por exemplo, Slack.
URL de conexão	URL desta conexão. Por exemplo, https://slack.com
Nome da Credencial	Nome das credenciais. Por exemplo, credenciais do Slack.
Nome do OAuth	Nome do OAuth. Por exemplo, Slack OAuth.
ID do cliente do OAuth	O ID do cliente gerado para a conta que você criou no Slack.
Segredo do cliente do OAuth	O segredo do cliente da conta que você criou no Slack.
URL de redirecionamento do OAuth	Nome da instância de redirecionamento do OAuth. Por exemplo, msimslack.service-now.com/oauth_redirect.do

q. Selecione **Configurar e obter token do OAuth**.
O bot de integração do Slack solicita sua permissão para acessar o Espaço do Slack do MSIM.

r. Selecionar **Permitir**.
O token de acesso OAuth está disponível e expirará no <YYYY-MM-DD> <HH:MM:SS>.

5. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Configuração do provedor de bate-papo**.
6. Selecione **Ativo** Caixa de seleção para ativar o registro Provedor de bate-papo.
7. Selecione **Validar conexão** para testar a conexão.
Uma mensagem de confirmação é exibida informando que a conexão do provedor foi validada com sucesso.
8. Clique com o botão direito do mouse no registro e selecione **Salvar** .
Depois disso, a conexão entre Slack e ServiceNow AI Platform a instância foi estabelecida com sucesso.
9. Navegar até **api.slack.com/apps** > **Recursos** > **OAuth e Permissões**.

a. Verifique se todos os escopos estão corretos.

b. Navegar até **Recursos** > **Assinaturas de evento**.

c. No campo URL da solicitação, selecione **Tente novamente** .
Você pode ver uma mensagem verificada.

d. Selecione **Save** (Salvar).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir atividades de mensagens de bate-papo no Slack

A atividade de mensagem de bate-papo é registrada e exibida na guia Colaboração do espaço Gestão de incidentes de segurança graves.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa

A atividade de mensagem de bate-papo inclui todas as conversas de bate-papo ocorridas entre os participantes, diferentes grupos de usuários. Para obter mais informações, consulte Gerencie as comunicações dos canais de bate-papo usando o Slack.

Administração do Gestão de incidentes graves de segurança

Planeje e configure a sua implementação do Gestão de incidentes graves de segurança.

Você pode configurar os seguintes aspectos de Gestão de incidentes graves de segurança administração:

Habilitar proposta, promoção e vinculação de incidentes de segurança graves

Permita que os usuários decidam propor ou promover incidentes como incidentes de segurança graves. Rastreie facilmente todos os incidentes relacionados a um incidente de segurança grave, permitindo que os incidentes de segurança sejam vinculados ao incidente primário ou secundário.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Permita que os usuários proponham um incidente de segurança a um incidente de segurança grave selecionando **Propor incidente de segurança grave** Caixa de seleção na seção Ações do Espaço SIR/VR.
3. Permita que os usuários promovam um incidente de segurança a um incidente de segurança grave selecionando **Promover a incidente de segurança grave** caixa de seleção.
4. Habilitar a vinculação de um incidente de segurança a um incidente de segurança grave para que eles possam ser rastreados juntos selecionando **Link para Incidente de segurança grave** caixa de seleção.
5. Selecione **Atualizar**.

Marque incidentes de segurança como incidentes de segurança graves

Marque ou rotule os incidentes de segurança ou registros vulneráveis a um incidente de segurança grave quando o incidente é proposto ou promovido. Se um incidente de segurança for proposto, o registro do incidente será referido como candidato a incidente de segurança grave. Quando uma segurança é promovida, o registro do incidente é chamado de Incidente de segurança grave com o estado Aceito.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilitar **Rótulos de exibição** marque a caixa para rotular o candidato a incidente proposto como incidente de segurança grave selecionando **Nome do rótulo - Propor como candidato** Campo de pesquisa e selecione Candidato a incidente de segurança grave em **Rótulos do espaço SIR/VR** seção.
3. Habilitar **Rótulos de exibição** marque a caixa para rotular o candidato a incidente promovido como incidente de segurança grave selecionando **Nome do rótulo - Promoção a incidente de segurança grave** Campo de pesquisa e selecione Incidente de segurança grave em **Rótulos do espaço SIR/VR** seção.
4. Selecione **Atualizar**.

Configure rótulos para incidentes de segurança graves

Configure rótulos na Gestão de incidentes de segurança graves para criar rótulos personalizados e filtrar as atividades e tarefas de colaboração externas no fluxo de atividades. Os diferentes tipos de rótulos implementados são rótulos de estado e rótulos de linha do tempo.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilitar **Rótulos de exibição** Caixa de seleção para habilitar a rotulagem de diferentes estados de incidente, como Análise, Conter, Erradicar, Recuperar, Revisar, evento da linha do tempo no **Rótulos do espaço do MSIM (Exibir em atividades e tarefas de colaboração)** seção.
3. Selecione **Atualizar**.

Configure rótulos para incidentes de segurança graves

Configure diferentes tipos de rótulos para filtrar melhor e também indicar os estados do incidente. Os rótulos de incidentes de segurança graves fornecem flexibilidade para rotular as atividades de colaboração e tarefas dos registros de incidentes.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Você pode marcar ou desmarcar os rótulos usando o ícone de rótulos que está disponível na seção Fluxo de atividades da seção do organizador de colaboração e tarefas do espaço do MSIM.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Rótulos do ISG**.
2. Clique em **Novo** para criar um novo rótulo.
3. Preencha o formulário com **Nome do rótulo** e. **Cor do rótulo** .
4. Clique em **Criar rótulo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Como parte do sistema de base, a seguir estão os rótulos configurados para cada estado de incidente e você não pode modificar o nome ou a cor do rótulo:
   - Análise
   - Contém
   - Erradicar
   - Revisão
   - Recuperar
   - Evento da linha do tempo

Nota: Você pode modificar os rótulos personalizados e suas propriedades.

Configure categorias da linha do tempo para incidentes de segurança graves

Configure e atribua categorias da linha do tempo, como Ameaça, Resposta ou Personalizada, aos seus incidentes de segurança graves usando a seção Linha do tempo na guia Visão geral.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Categorias da linha do tempo**.
   As seguintes categorias de linha do tempo são fornecidas como parte do sistema de base:
   - **Personalizado** .
   - **Resposta** .
   - **Ameaça** .
2. Para modificar uma categoria de evento da Linha do tempo existente, execute as seguintes etapas:
   a. Selecione uma categoria de evento da Linha do tempo na lista.
   b. Você pode modificar o nome da categoria de evento da Linha do tempo.
   c. Você pode modificar a Cor do evento e selecionar outra cor para sua categoria de evento da Linha do tempo.
   d. Selecione **Atualizar**.
3. Para criar uma nova categoria de evento da Linha do tempo, execute as seguintes etapas:
   a. Selecione **Novo**.
   b. No campo Nome, insira um nome para a categoria de evento da Linha do tempo.
   c. No campo Cor do evento, escolha uma cor para a categoria da linha do tempo do evento usando a lista suspensa.
   d. Selecione **Enviar**.

Definir preferências de notificação para MSIM

Automatize o processo de notificação por e-mail e notifique os usuários quando um incidente de segurança for proposto ou promovido a candidato a incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_msi.workspace_admin.

As notificações são acionadas somente quando um incidente de segurança é proposto e enviado a todos os usuários e grupos configurados para a lista de notificações. Por padrão, a notificação por e-mail é recebida pelo usuário que propôs o incidente de segurança como candidato a incidente de segurança grave.

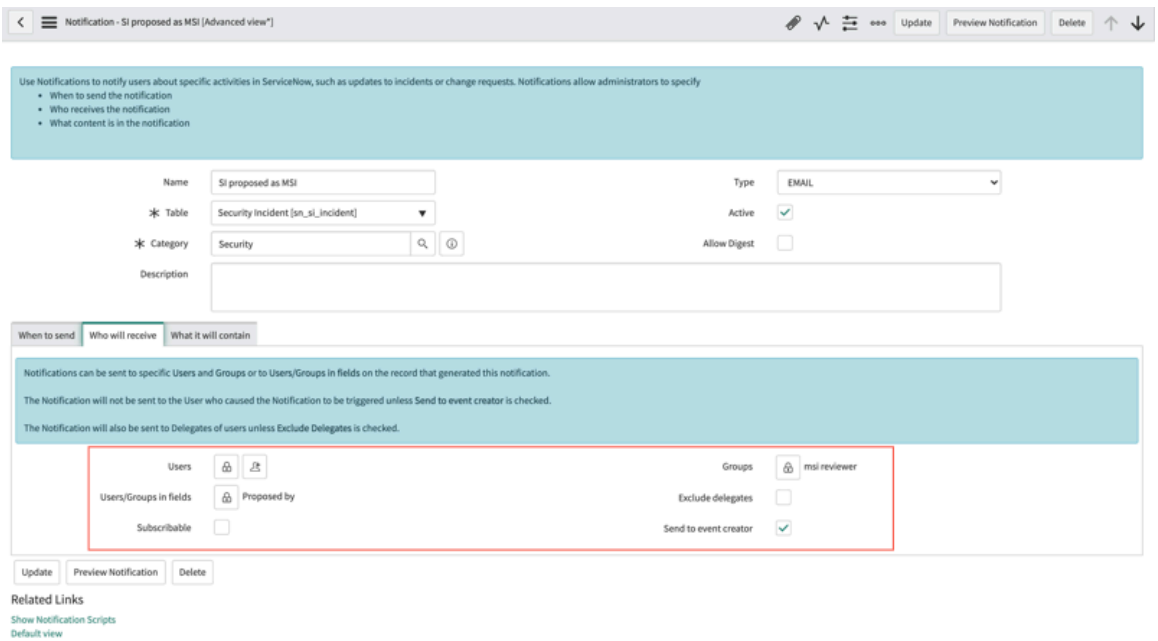
Notificação: Incidente de segurança proposto (SI) como incidente de segurança grave (MSI)

Quem receberá:

- Por padrão, **Revisores MSI** o nome do grupo é criado e qualquer usuário adicionado a este grupo terá o privilégio de ser um **MSIM Manager** e os usuários que estão nesse grupo receberão os e-mails de notificação.
- Qualquer usuário específico que é adicionado ao **Usuários** a lista também receberá os e-mails de notificação.

O que ele conterá:

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail, que inclui o assunto ou a mensagem HTML, você deve ter acesso à função de administrador do sistema ou atribuído como administrador do sistema e não como administrador MSI.



Incidente de segurança promovido (SI) como incidente de segurança grave (MSI)

Esta notificação é acionada quando um incidente de segurança é promovido e quando o Explorador de arquivos e Microsoft Teams a estrutura base foi criada. Por padrão, esta notificação é recebida pelo usuário que promoveu o incidente de segurança a um incidente de segurança grave.

Quem receberá

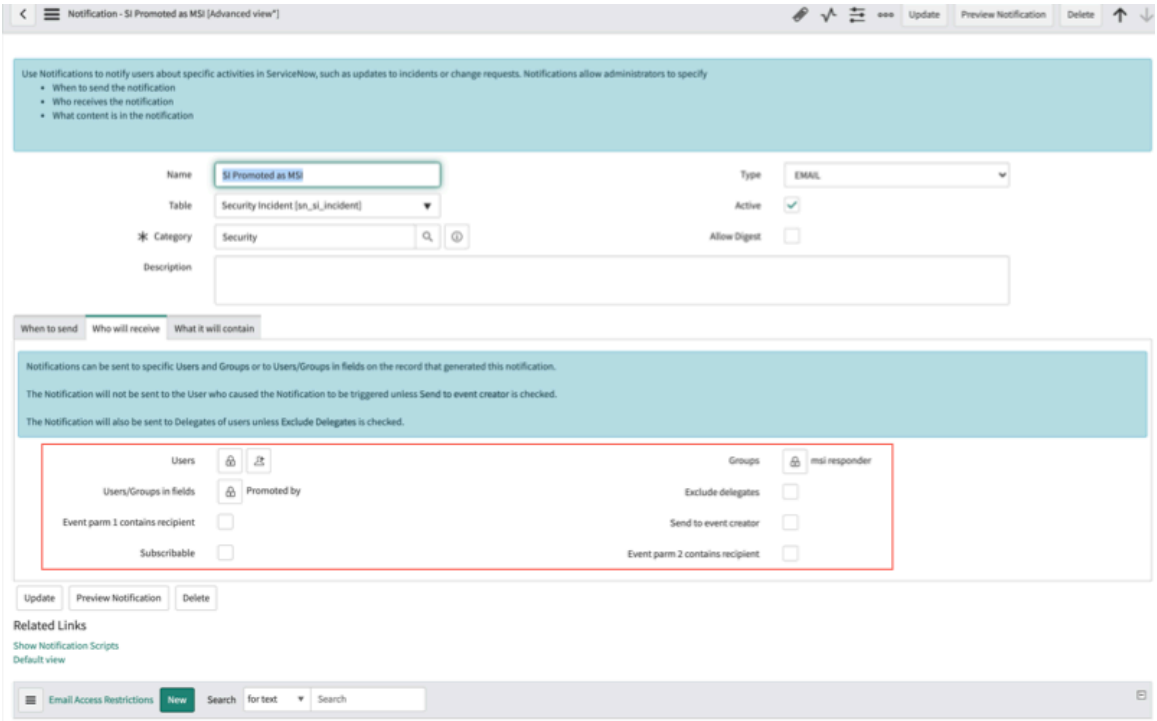
- Por padrão, um **Grupo** por nome **Respondente MSI** é criado e qualquer usuário que for adicionado a este grupo terá o privilégio de ter **Respondente do MSIM** e todos os usuários que estão nesse grupo receberão o e-mail de notificação.
- Qualquer usuário específico que é adicionado ao **Usuários** a lista também receberá os e-mails de notificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que ele conterá

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail, que inclui o assunto ou a mensagem HTML, você deve ter acesso à função de Administrador do sistema ou atribuído como Administrador do sistema e não como Administrador MSI.



Configurar atividades de fechamento MSI

Estabeleça ações que ocorrerão automaticamente quando um incidente de segurança grave for encerrado. Aumente a segurança arquivando e removendo automaticamente o acesso a pastas que contêm informações de resolução.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Arquive comunicações de bate-papo relacionadas à resolução do incidente selecionando **Arquivar canais de colaboração** Caixa de seleção na seção Ações de fechamento automatizadas.
3. Remova pastas que contenham material relacionado à resolução do incidente selecionando **Remover pastas de colaboração** caixa de seleção.
4. Selecione **Atualizar**.

Gestão de incidentes graves de segurança espaço

Gestão de incidentes graves de segurança fornece um espaço dedicado para gerenciar incidentes de segurança graves especificamente projetados para o. Incidente grave de segurança gerente.

Colabore facilmente em atividades que ajudam a resolver incidentes de segurança graves compartilhando e exibindo arquivos e pastas, exibindo e atualizando tarefas de incidente e se comunicando com aqueles que trabalham no incidente por meio de canais de bate-papo dedicados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Gestão de incidentes de segurança graves (MSIM) fornece um mecanismo para rastrear e resolver incidentes de segurança graves. O MSIM funciona em conjunto com os recursos de produto de resposta a vulnerabilidades e incidentes de segurança existentes e melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves, projetado especificamente para a função de usuário do gerenciador de incidentes de segurança graves.
- Organize tarefas de resposta a incidentes de segurança graves, incluindo tarefas rastreadas em incidentes de segurança vinculados e grupos de vulnerabilidade.
- Automatizar a criação de pastas de colaboração e canais de comunicação de bate-papo depois que um incidente de segurança grave é criado, bem como o arquivamento como parte do fechamento do incidente.
- Componente explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de um Microsoft SharePoint integração.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, DE TI e DE segurança por meio de um Microsoft Teams integração.
- Relatório resumido do impacto de incidentes de segurança graves e métricas de andamento, incluindo acúmulo de ativos, usuários, locais e recursos de equipe afetados, bem como linha do tempo de marcos de incidentes significativos.

Use o Espaço do MSIM para rastrear e resolver incidentes de segurança graves:

1. Exiba os gráficos de tendências e o andamento do incidente de segurança grave.
2. Rastreie e organize a atividade Arquivos do Microsoft SharePoint por meio do Espaço do MSIM.
3. Rastreie e organize a atividade de bate-papo do Microsoft Teams por meio do Espaço do MSIM.
4. Exiba e atualize detalhes do incidente por meio do Espaço do MSIM.
5. Filtre as atividades de colaboração no fluxo de atividades do Espaço do MSIM.

Como usar o Gestão de incidentes graves de segurança

Os gerentes podem usar Gestão de incidentes graves de segurança espaço para exibir os registros de incidentes propostos, promovidos, vinculados e rejeitados e rastrear suas atividades relacionadas.

Propor, promover e vincular registros de incidentes

Propor ou promover incidentes de segurança como incidentes de segurança graves quando os incidentes forem identificados como ameaça crítica para a organização.

Depois que a Gestão de incidentes de segurança graves estiver instalada em seu ServiceNow, você pode lidar com a transição de incidentes de segurança para incidentes graves da seguinte forma:

- Propor um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem um processo de revisão.
- Rejeitar um incidente de segurança proposto como incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode vincular um incidente de segurança como incidente secundário ao incidente de segurança grave para que todos os incidentes de segurança relacionados possam ser rastreados juntos.

Propor como um Incidente grave de segurança

Propor um incidente de segurança a um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Listas**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja propor como incidente de segurança grave.
3. Selecione **Mais ações** e selecione **Propor como incidente de segurança grave** .
4. Na caixa de diálogo Propor como incidente de segurança grave, preencha os campos.
   a. **Data de detecção** : Data em que o incidente de segurança grave foi criado ou proposto pela primeira vez.
   b. **Justificativa** : Forneça a justificativa para propor o incidente.
   c. **Possível impacto** : Indica o impacto do incidente.
5. Selecione **Propor** .

Resultado

O incidente é proposto e ocorrem as seguintes ações:

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador Incidente de segurança grave definido é exibido.
- O registro aparece na lista relacionada Incidente de segurança grave no registro do incidente, com o estado listado como Proposto e na lista Candidatos ao Espaço MSIM.
- A seção Atividade no Espaço do MSIM mostra que o incidente de segurança foi proposto para ser promovido como um incidente de segurança grave.
- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.

Promover para um Incidente grave de segurança

Promova um incidente de segurança a um incidente de segurança grave ou rejeite propostas promovidas por meio do Gestão de incidentes graves de segurança(MSIM) Workspace.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Listas**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja promover como incidente de segurança grave.
   Revise os detalhes do incidente de segurança na seção Detalhes ou exiba detalhes estendidos no registro do incidente em uma guia separada clicando em **Exibir mais detalhes** .
3. Selecione **Mais ações** e selecione **Promover a incidente de segurança grave** .
4. Na caixa de diálogo Promover incidente de segurança grave, preencha os campos.
   a. **Data de detecção** : Data em que o incidente de segurança grave foi criado ou proposto pela primeira vez.
   b. **Data de resolução estimada** : A data de resolução estimada até quando o incidente de segurança grave é estimado para ser resolvido.
   c. **Nome do código** : Selecione o nome do código do incidente de segurança grave.
   Por exemplo, Blue Tiger.
   d. **Categoria** : Selecione a categoria do incidente de segurança grave.
   Por exemplo, Configuração incorreta.
   e. **Justificativa** : Forneça a justificativa para propor o incidente.
   f. **Possível impacto** : Indica o impacto do incidente.
5. Selecione **Propor** .
6. Promova o incidente de segurança ou rejeite a proposta de promoção.
   - Para promover o incidente, clique em **Promover a incidente de segurança grave** .
   - Para rejeitar a proposta de promoção, clique em **Rejeitar como incidente de segurança grave** .
7. Selecione **Save** (Salvar).

Resultado

- Se você rejeitou a proposta de promoção, o incidente não será promovido e a entrada do incidente será movida para a guia Rejeitado.
- Se você promoveu o incidente, a entrada do incidente será movida para a guia Abrir e o registro de segurança exibirá um marcador indicando que é um incidente de segurança grave.
- A decisão é listada na seção Atividade do Espaço do MSIM.

Quando um incidente é promovido, a configuração padrão é aplicada.

- Uma estrutura de pastas é criada com base na configuração do modelo de pasta.
- Os canais de bate-papo são criados com base na configuração de canais.
- Uma mensagem de e-mail é enviada para os usuários designados. A notificação padrão contém um link para o incidente de segurança grave e os detalhes do incidente. Agora,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os usuários designados também têm acesso aos recursos de colaboração, portanto, a notificação também inclui o nome do Microsoft Team e um link para as pastas do Microsoft SharePoint relacionadas ao incidente.

Vincular a Incidente grave de segurança

Vincular incidentes de segurança a um incidente de segurança grave.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja vincular ao incidente de segurança grave.
3. Selecione **Ações adicionais** e selecione **Link para Incidente de segurança grave** .
4. Selecione o incidente de segurança grave ao qual você deseja vincular.
   a. Na caixa de diálogo, selecione o ícone Pesquisar usando lista.
   b. Selecione o incidente de segurança grave ao qual você deseja vincular.
   c. Selecione **OK**.
5. Selecione **Propor** .

Resultado
A proposta é enviada e ocorrem as seguintes ações:

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador Incidente de segurança grave definido aparece ao lado de **Selecione marcador de segurança** campo.
- Em **Detalhes** guia do incidente de segurança grave em Gestão de incidentes graves de segurança, a lista suspensa de número de registro inclui ambos os incidentes.
- O registro aparece na lista relacionada Incidente de segurança grave do registro do incidente, com o estado listado como Proposto.
- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.
- . **Atividade** A seção no Espaço do MSIM mostra que o incidente de segurança foi adicionado como um incidente de segurança secundário ao incidente de segurança grave com um link.

Usando a exibição de lista MSI no espaço do MSIM

Com a exibição de lista no espaço do MSIM, você pode exibir incidentes de segurança graves propostos, promovidos e rejeitados.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

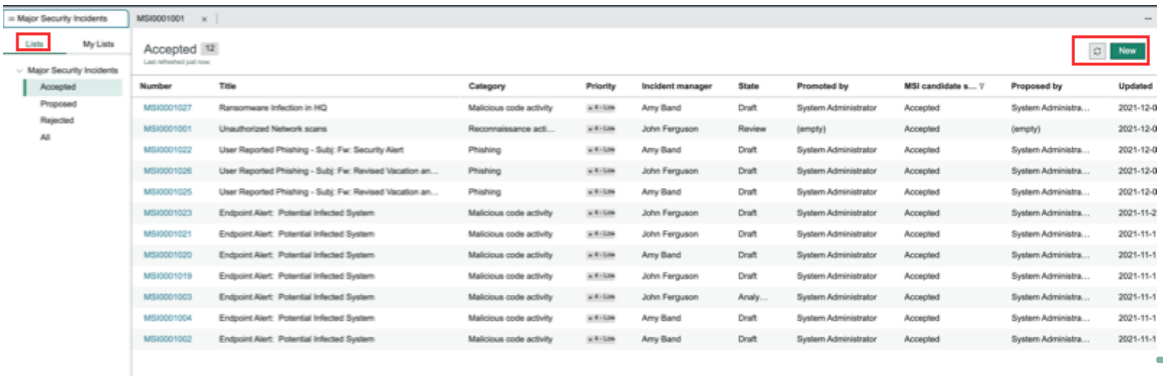
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode criar novos incidentes usando **Novo** botão disponível no canto superior direito do espaço.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Espaço do MSIM**.
2. Selecione a guia Listas para exibir a exibição de listas.



3. Selecione **Minhas listas** para criar sua própria lista de incidentes de segurança graves.
4. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista:

Tarefa	Descrição
Minhas listas	Crie novas listas de registros MSI e exiba as listas que você criou.
Defina filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna.
Filtre itens ou corresponda itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ○ Mostrar correspondência - Exibe somente itens que correspondam ao item selecionado na coluna. ○ Descartar - Filtre os itens da coluna que correspondem ao item selecionado na respectiva coluna.
Atualizar lista	Atualize as listas e exiba as listas completas que foram atualizadas.
Novo(a)	Crie um novo registro MSI.

Exibir Incidente grave de segurança métricas de impacto

Fornece relatórios resumidos atualizados do impacto e do andamento de incidentes de segurança graves, que é um aspecto importante do gerenciamento de um incidente de segurança grave usando o novo espaço.

. **Visão geral** fornece as métricas relevantes para gerenciar o escopo e o andamento do incidente, incluindo um acúmulo de ativos, usuários, locais e recursos de equipe afetados, bem como a linha do tempo de marcos significativos do incidente.

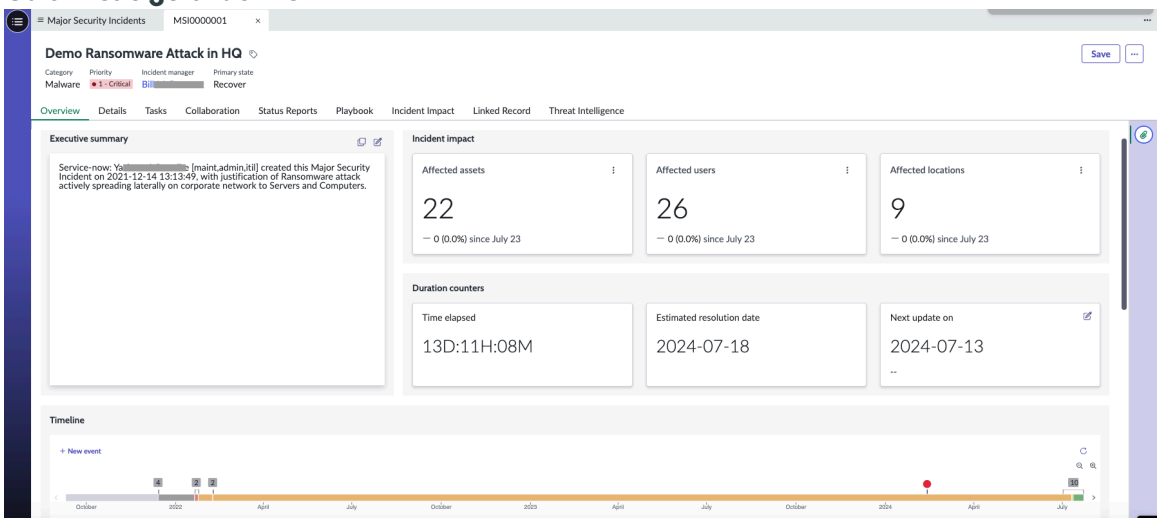
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A linha do tempo fornece uma exibição horizontal dos principais eventos e marcos que ocorreram como parte da resolução de incidente de segurança grave específico. O componente da linha do tempo é exibido na parte superior de todas as guias do espaço Gestão de incidentes de segurança graves com a capacidade de recolher e expandir para exibição conforme necessário. Os dados de eventos representados serão atualizados e atualizados sempre que eventos de marco designados ou marcos forem adicionados ou atualizados.

Cada evento ou marco é indicado com uma opção de tipo de evento de linha do tempo diferente para identificar o número e o tipo de eventos ou marcos. AGORA, registrar atualizações, atividades de colaboração. Além disso, o período de intervalo de tempo para os diferentes estados de incidente de segurança grave é rastreado automaticamente e exibido usando intervalos codificados por cores exibidos junto com a duração de cada estado de incidente.

Guia Visão geral do MSIM



Resumo executivo e Impacto do incidente

Tarefa	Descrição
Resumo executivo	Um breve resumo do incidente de segurança grave junto com o nome do usuário, a função do usuário e os detalhes do carimbo de data/hora. • Você pode modificar o Resumo executivo selecionando **Editar** ícone. Depois de fazer as mudanças necessárias, selecione **Atualização** opção. • Para copiar o Resumo executivo e colá-lo em um incidente de segurança grave, selecione **Cópia** e cole o resumo no incidente de segurança grave necessário.
Impacto do incidente	Esses componentes exibem os recursos afetados com base em um acúmulo de todas as tarefas ativas e incidentes vinculados com ativos, usuários, locais e membros da equipe atribuídos identificados. Os recursos afetados são:

Tradução automática

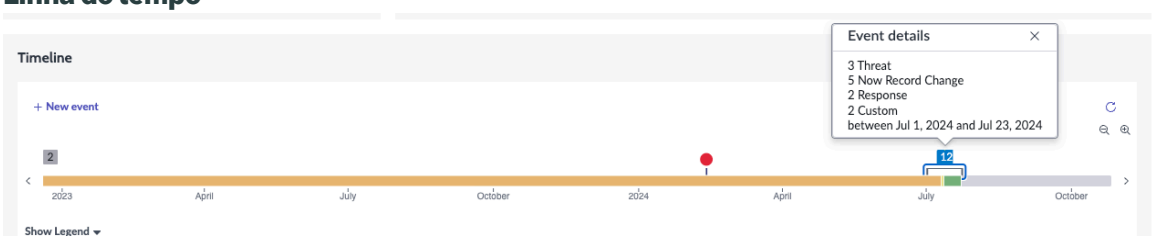
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo executivo e Impacto do incidente

Tarefa	Descrição
	• **Ativos afetados** • **Usuários afetados** • **Locais afetados** Selecionar os valores numéricos permite detalhar e navegar até os ativos afetados, usuários e detalhes do local e exibe as tarefas relacionadas no **Impacto do incidente** do espaço. Com base no link do tipo de impacto de incidente selecionado, os detalhes do incidente relacionado, como tipo de tarefa e sua descrição, grupo de atribuição e estado do incidente, são exibidos em **Impacto do incidente** Do espaço do MSIM.
Contadores de duração	Esses componentes exibem a duração do incidente de segurança grave. Os recursos afetados são: • **Tempo decorrido** : Exibe o tempo decorrido a partir do momento em que o incidente de segurança grave é detectado. • **Data de resolução estimada** : Exibe a data estimada de resolução até quando o incidente de segurança grave é estimado para ser resolvido. • **Próxima atualização em** A data e a hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 5:00 pm EST em 25 de março de 2024. Você pode modificar **Próxima atualização em** selecionando **Editar** ícone. Selecione a nova data e hora e selecione **Atualização** .

Você pode habilitar ou desabilitar a exibição de determinados tipos de evento para indicadores de linha do tempo e intervalos de linha do tempo de acordo usando os botões de alternância de filtro.

Linha do tempo



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte a tabela a seguir para obter recursos adicionais disponíveis com o componente de linha do tempo.

Recursos adicionais do componente da linha do tempo

Tarefa	Descrição
Novo evento	Cria novos eventos personalizados e associa esses eventos ao registro MSI. Isso ajuda na criação de eventos para datas passadas e futuras que podem não ser capturados por meio de uma tarefa rotulada, mudança de estado de registro ou atividade de colaboração rotulada, que são exibidas por padrão na linha do tempo.
Atualização	Atualiza os eventos da Linha do tempo para exibir as atualizações mais recentes.
Indicadores da linha do tempo	Lista os vários tipos de eventos, como mudanças no campo Now Record, atividades de colaboração rotuladas e outros (personalizados), junto com os ícones e o número total de eventos que ocorreram em relação a cada indicador de tipo de evento. O indicador de slide permite habilitar ou desabilitar todos os eventos de um tipo de evento específico.
Mostrar legenda	Selecione para exibir a legenda suspensa com diferentes tipos de indicadores de linha do tempo.
Barra de andamento da linha do tempo	Exibe o andamento geral do incidente por meio de eventos de linha do tempo designados ou marcos que ocorreram nos diferentes intervalos de linha do tempo exibidos. Você também pode vincular um tipo de evento a uma categoria de evento. Depois de vinculá-lo, os detalhes do evento serão atualizados em ambos os lugares na linha do tempo.
Intervalos de linha do tempo	Exibe vários tipos de estado de incidentes e duração conforme o incidente progride durante todo o ciclo de vida do incidente de segurança grave. Habilite ou desabilite um evento específico com base no estado do incidente.

Crie um evento de linha do tempo

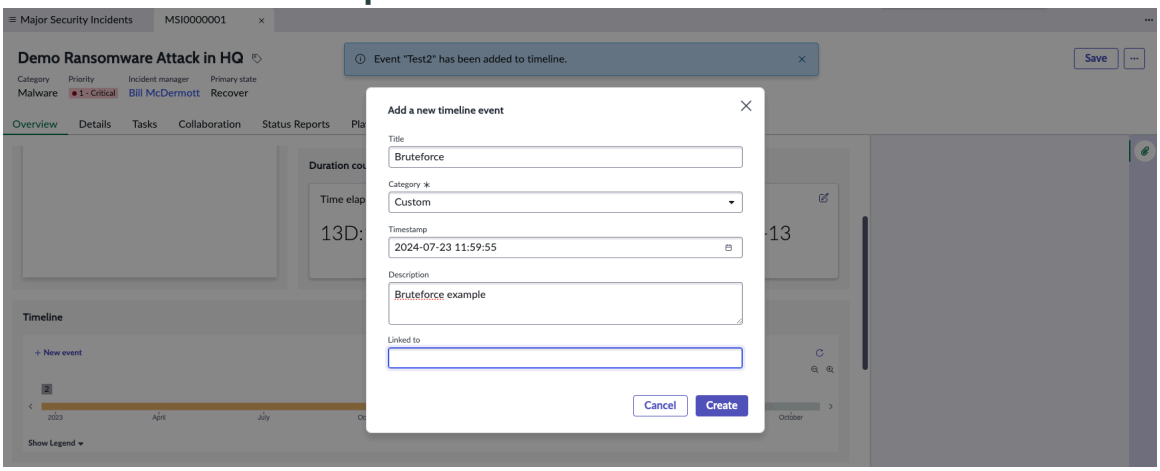
Para criar um novo evento de Linha do tempo, execute as seguintes etapas:

1. Na guia Visão geral, navegue até **Linha do tempo** seção.
2. Selecionar **Novo evento**.
3. No pop-up Adicionar um novo evento de linha do tempo, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Novo evento de linha do tempo



Tarefa	Descrição
Título	Insira o título do evento da linha do tempo.
Categoria	Selecione uma categoria para o evento da linha do tempo. As categorias a seguir são fornecidas como parte do sistema de base e você pode escolher uma com base em seus requisitos. ○ **Personalizado** . ○ **Resposta** . ○ **Ameaça** . Para adicionar ou configurar uma categoria de evento da Linha do tempo, consulte Configure categorias da linha do tempo para incidentes de segurança graves.
Carimbo de data/hora	Selecione a data e a hora do evento da linha do tempo usando o calendário Carimbo de data e hora. Você pode adicionar eventos à Linha do tempo antes e depois da data de início.
Descrição	Forneça uma breve descrição sobre o evento da linha do tempo.
Vinculados a	Opção para vincular o evento da linha do tempo a um registro de incidente de segurança grave.

4. Selecionar **Criar**.
5. Você pode usar **Ampliar** e. **Reduzir** ícones para ampliar ou reduzir a barra de andamento da linha do tempo, o que inclui a exibição de eventos individuais quando os números são exibidos para representar vários eventos próximos.

   Você também pode adicionar o nível de zoom padrão para mostrar todos os eventos.
6. Selecione **Atualizar** ícone para exibir os eventos mais recentes da linha do tempo.

Exibir Incidente grave de segurança gráficos de tendências

Exiba as métricas de andamento do impacto do incidente de segurança grave visualizadas como gráficos de barras e gráficos.

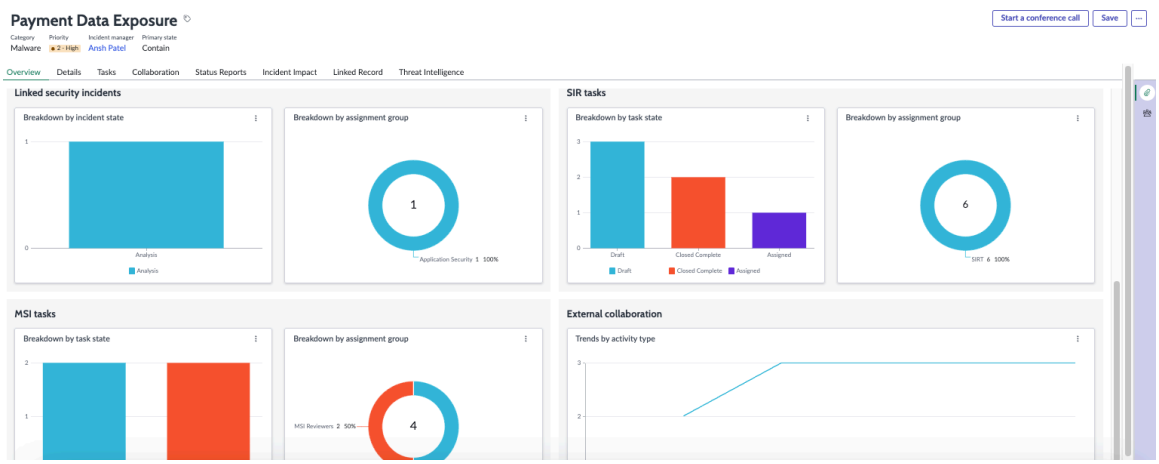
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Além das visualizações da linha do tempo do incidente e do gráfico de tendências de andamento, o **Visão geral** fornece métricas de impacto relevantes para gerenciar o escopo em mudança do incidente, incluindo acúmulo de ativos, usuários, locais e recursos de equipe afetados.

As contagens exibidas nos componentes de visualização são baseadas em tarefas ativas em incidentes de Resposta de incidente de segurança vinculada (SIR). À medida que as tarefas são abertas e encerradas, essas contagens mudam em termos da natureza e do volume da atividade restante planejada para o incidente de segurança grave para representar as tendências mostradas nos componentes de visualização do gráfico de tendências.

Métricas de impacto da guia Visão geral do MSIM



Consulte a tabela a seguir para obter as ações de IU que você pode executar no **Visão geral** seção:

Visão geral das seções de IU

Título	Descrição
Tempo	Exibe o período no número total de dias a partir do momento que o incidente de segurança grave está ativo. O tempo é calculado com base em **Data de detecção** inserido em **Detalhes** do espaço. A Data de detecção é geralmente capturada inicialmente quando o incidente de segurança grave foi criado ou proposto pela primeira vez. Sempre que esta data for modificada, a hora será calculada, atualizada e exibida automaticamente no formato dias: Horas: Minutos, por exemplo, 20D: 13H: 58M. **Data de resolução estimada**A data em que a data de resolução do incidente é estimada para ser resolvida. Essa data é geralmente capturada inicialmente quando o incidente de segurança grave foi criado ou promovido pela primeira vez.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral das seções de IU

Título	Descrição
	A data é atualizada e atualizada com base na data estimada fornecida em **Detalhes** do espaço. Se a data estimada não for fornecida na seção Detalhes, esta seção exibirá "hífen" sem nenhum valor de data.
Equipe ativa	Exibe as diferentes equipes de resposta e membros da equipe de cada equipe que estão trabalhando ativamente no incidente de segurança grave e suas tarefas relacionadas. **Equipe ativa** Tendência: Exibe o gráfico de tendências de cada equipe e seus membros de equipe que estão trabalhando ativamente no incidente de segurança grave e nas tarefas relacionadas em intervalos regulares. **Nota:** Exiba os grupos ativos atribuídos no **Detalhes** do espaço.
Incidentes DE SIR vinculados	**Por estado do incidente**: Exiba a distribuição de incidentes de segurança vinculados com base em um estado de incidente, como Análise, Conter, Erradicar, Recuperar ou Revisar. **Tendências por estado do incidente**Indica ainda a exibição de tendência de como o número de incidentes vinculados está progredindo com base no estado do incidente. Selecionar cada link de estado de incidente permite navegar e exibir os detalhes do incidente de segurança vinculado diretamente no **SI/VI vinculado** do espaço. Esta seção é atualizada e atualizada automaticamente sempre que ocorrem mudanças nos incidentes subjacentes.
Tarefas SIR	Exibe os totais de tarefas ativas que estão vinculados ao registro MSI por meio de incidentes SIR. • **Por estado da tarefa**: Exiba as tarefas de resposta do incidente com base no estado do incidente, como Rascunho, Atribuído, Trabalho em andamento, Encerrado concluído. Este gráfico de distribuição permite um detalhamento de distribuição adicional por grupos de atribuição. Selecionar cada estado de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral das seções de IU

Título	Descrição
	tarefa permite exibir uma lista filtrada por estado de tarefa de incidente no **Tarefas** do espaço. A exibição filtrada permite exibir e atualizar detalhes da tarefa individual. • **Tarefas em andamento por rótulo do estado do incidente**: Exibe tarefas e grupos ativos com base no rótulo de estado do incidente que deve ser aplicado nos componentes do Organizador de tarefas. Esses rótulos padrão têm valores como Análise, Conter, Erradicar, Recuperar ou Revisar para indicar a natureza da tarefa envolvida. • **Atrasados(as)**: Exibe as tarefas de resposta do incidente de segurança, que estão ativas e excederam a data de vencimento. Você pode exibir os detalhes de todas as tarefas atrasadas selecionando a contagem total de atrasos e fazendo com que ela navegue automaticamente até a guia Tarefas. • **Tendências por estado da tarefa**: Exiba a tendência de andamento do trabalho em andamento e das tarefas de resposta encerradas durante a duração do incidente. **Nota:** O gráfico do gráfico de tendências recupera os dados mais recentes com base no trabalho agendado. Você pode configurar ou modificar o intervalo de tempo de recuperação de dados conforme necessário.
Tarefas do MSI	Exibe tarefas ativas no total, que foram criadas diretamente no registro MSI (e estas não são tarefas de resposta vinculadas): **Por estado da tarefa:** Exiba as tarefas criadas pelo incidente de segurança grave, as tarefas atribuídas e suas informações relacionadas. Selecionar cada estado de tarefa permite exibir uma lista filtrada por estado de tarefa de incidente no **Tarefas** do espaço. A exibição filtrada permitirá exibir e atualizar detalhes da tarefa individual.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral das seções de IU

Título	Descrição
Colaboração externa	Exibe atividades de colaboração no total para todas as atividades de colaboração rotuladas do Fluxo de atividades de colaboração: • **Por rótulo de estado de incidente:**Exiba os dados de atividades de colaboração de incidentes com os quais estão coordenados Microsoft Teams e. Microsoft SharePoint Arquivos e pastas e são rotulados usando rótulos de estado de incidente, como Análise, Conter, Erradicar ou Recuperar do **Colaboração** do espaço. • **Tendências por tipo de atividade**: Exiba o gráfico de tendências para o número de Microsoft Teams e. Microsoft SharePoint atividades de arquivos e pastas durante a duração do incidente.

Atualização Incidente grave de segurança detalhes

Exiba e atualize detalhes específicos relacionados ao incidente de segurança grave, como Detalhes do registro do incidente, Participantes da equipe ativa e o log de atividades correspondente.

Todos os detalhes relacionados do incidente de segurança grave são exibidos com várias seções de formulário no **Detalhes** do espaço. Exibe os detalhes, como Detalhes do registro do incidente, Participantes da equipe ativa e o log de atividades correspondente. Você também pode exibir os Incidentes SIR vinculados, os detalhes do registro do Grupo de vulnerabilidades e a capacidade de transmitir uma publicação de atividade para todos os registros de incidentes vinculados.

Principalmente, a guia Detalhes contém:

1. Campos do formulário Incidente de segurança grave e seções de IU relacionadas a incidentes.
2. Fluxo de atividades

A tabela a seguir fornece os detalhes dos campos do formulário de incidente de segurança grave:

Seções do formulário Incidente de segurança grave

Campo	Descrição
Incidente	
Número	Número do registro de incidente de segurança grave.
Estado principal	O estado primário do registro de incidente de segurança grave.
Data de detecção	A data em que o incidente de segurança grave foi criado ou proposto pela primeira vez.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções do formulário Incidente de segurança grave

Campo	Descrição
	Sempre que você modifica a Data de detecção na guia Detalhes, a data e a hora do MSI são calculadas, atualizadas e exibidas automaticamente no **Hora** > **Tempo desde o início do incidente** . **Visão geral** do espaço.
Título	Título do incidente de segurança grave.
Nome do código	Nome do código do incidente de segurança grave. Por exemplo, Blue Tiger.
Próxima atualização em	A data e a hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 5:00 pm EST em 25 de março de 2024.
Categoria	Categoria do incidente de segurança grave.
Subcategoria	Tipo de subcategoria do incidente de segurança grave.
Data de resolução estimada	A data estimada até quando o incidente deve ser resolvido. O valor padrão é 7 dias a partir do momento da criação do incidente de segurança grave.
Prioridade	Prioridade do incidente de segurança grave.
Sensor de alerta	Sensor de alerta do incidente de segurança grave. Por exemplo, Usuário relatado como phishing.
Origem	Origem do incidente de segurança grave.
Equipe ativa	
Gerente de incidentes	Nome do gerente de incidentes.
Grupos designados	Indica as diferentes equipes de resposta e os membros da equipe de cada equipe que estão trabalhando ativamente no incidente de segurança grave.
Candidato	
Estado do candidato a ISG	Indica o estado do candidato a incidente de segurança grave, como Proposto ou Promovido. Se o incidente for promovido, o estado será exibido como Aceito.
Promovido por	Usuário que promoveu o incidente de segurança grave.
Promovido	Data em que o incidente de segurança grave foi promovido.
Justificativa	Justificativa do incidente de segurança grave. A justificativa deve incluir o número MSI e o nome do código.
Impacto potencial	O possível impacto e a gravidade do incidente de segurança grave. O possível impacto deve incluir o número MSI e o nome do código.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções do formulário Incidente de segurança grave

Campo	Descrição
Restrição	
Impor restrição	Selecione esta opção para impor restrições a determinadas restrições de incidentes de segurança graves. Você pode impor restrições para limitar a exibição ou modificar o acesso somente a determinados usuários ou grupos. Para obter mais informações, consulte Restringir o acesso a determinados incidentes de segurança graves.
Membros permitidos	Lista de usuários que podem acessar o incidente de segurança grave.
Grupos permitidos	Lista de grupos que podem acessar o incidente de segurança grave.
Outras ações	
Anexo	Anexos relacionados ao incidente de segurança grave. Selecione **Selecione** opção para adicionar anexos ao incidente.
Chamada em conferência	Use chamadas em conferência com os provedores de serviços terceirizados como um canal de comunicação para se reunir com as partes interessadas para resolver os incidentes de segurança graves. Para obter mais informações, consulte Gestão de incidentes graves de segurança Integração de chamada em conferência.

Atividade :

Use a seção Atividade para adicionar suas anotações de trabalho e comentários, publicar sua atividade de forma privada e também adicionar comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade adicionada ou anotações de trabalho na seção Atividade.

Nota: Selecione **Mostrar mais** link detalhes para exibir os detalhes de um registro de incidente de segurança específico, que estão associados a esse incidente de segurança grave.

Defina suas preferências para exibir as atividades relacionadas, como:

1. **Filtros** : Selecione **Conjuntos de filtros** ícone para definir filtros.

   Defina filtros para exibir as conversas de atividade, como atividades adicionadas nas anotações de trabalho, e-mail, linha do tempo e quaisquer comentários adicionais.

2. **Sinalizado** : Selecione **Sinalizado** ícone para sinalizar as atividades.

   Sinalize todas as conversas de atividade importantes para que você as mantenha à mão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restringir o acesso a determinados incidentes de segurança graves

Gerencie quem pode exibir ou modificar incidentes de segurança graves que contêm informações confidenciais. Você pode impor restrições de incidentes de segurança graves para determinar quem tem acesso para exibir ou modificar determinados registros de incidentes de segurança graves e listas relacionadas e limitar o acesso de leitura ou gravação somente a determinados usuários ou grupos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

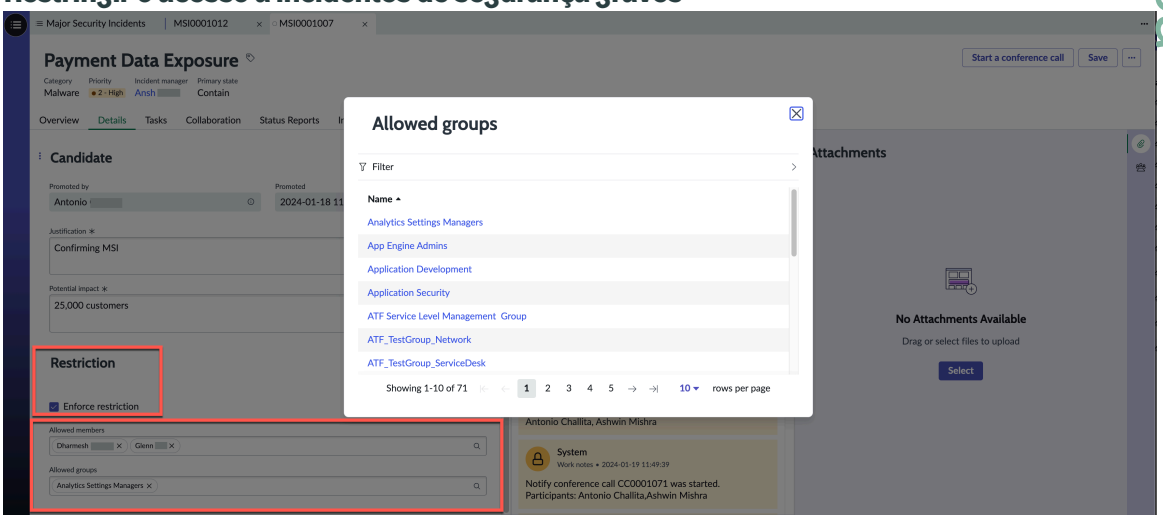
As restrições de incidentes de segurança graves permitem ocultar que os incidentes de segurança graves críticos sejam acessados ou modificados por todos os usuários ou grupos em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança graves que um usuário ou grupo pode exibir ou modificar. Você pode impor uma restrição de incidente de segurança grave selecionando **Impor restrição** e marcando os usuários ou grupos com permissão para exibir ou modificar o incidente de segurança grave específico.

Depois de impor a restrição a incidentes de segurança graves ou listas relacionadas a determinados usuários ou grupos, todos os usuários ou grupos restantes em sua organização não poderão exibir ou modificar esses incidentes de segurança graves ou listas relacionadas.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Detalhes**.
5. Role para baixo e selecione **Restrição** seção.
6. Selecione **Impor restrição** caixa de seleção para habilitar a restrição do incidente de segurança grave.

Restringir o acesso a incidentes de segurança graves



7. No campo Membros permitidos, selecione os usuários que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. No campo Grupos permitidos, selecione os grupos que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.

   Nota: Após **Impor restrição** se a caixa de seleção estiver habilitada para o incidente de segurança grave, somente o sn_msi.workspace_manager e os membros ou grupos permitidos terão acesso para exibir ou modificar o incidente de segurança grave.

9. Selecione **Save** (Salvar).

Vincular registros adicionais a. Incidente grave de segurança

No espaço, use a funcionalidade Vincular registros para vincular todos os registros de Incidente de segurança relacionados e seus incidentes de segurança secundários, tarefas de correção de Resposta a vulnerabilidades e Casos de segurança da Inteligência contra ameaças a um Incidente grave de segurança(MSI).

Antes de Iniciar

Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Procedimento

1. Navegar até **Resposta a incidentes de segurança graves** > **Espaço do MSIM**.
2. Navegue até **Listas** exibição, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Selecione o registro de incidente que deve ser vinculado e que não está no estado Encerrado na lista de registros promovidos.
5. Clique em **Registros vinculados** guia.
   Uma lista suspensa é fornecida para selecionar outras tabelas de registro vinculadas.
   A seção Registros vinculados exibe os registros vinculados e seus registros relacionados, que foram vinculados ao Incidente de segurança grave.
6. Selecione a exibição da tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança na lista.
   Com base na exibição da tabela de registros do tipo de seleção, os registros vinculados vinculados aos registros de incidentes de segurança graves são exibidos.
7. Vincular um registro que não está vinculado a nenhum registro MSI e está em **Aberto** selecione o registro e clique em **Vincular registro** no canto superior direito da página.

   Nota: Você não pode vincular um registro de incidente a um registro MSI se ele estiver em **Encerrado** estado.

8. Selecione o registro a ser vinculado e clique em **Link** .
   Uma mensagem de confirmação exibe que o registro está vinculado com sucesso e o acúmulo de registros relacionados será processado em segundo plano.

   Nota: Depois que um registro é vinculado, a exibição de lista é atualizada automaticamente e lista a lista atualizada de registros de incidentes.

Tópicos relacionados

Desvincular registros de Incidente grave de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desvincular registros de Incidente grave de segurança

Usando o espaço Gestão de incidentes de segurança graves, desvincule os registros de incidentes de segurança graves da seção Registros vinculados.

Antes de Iniciar

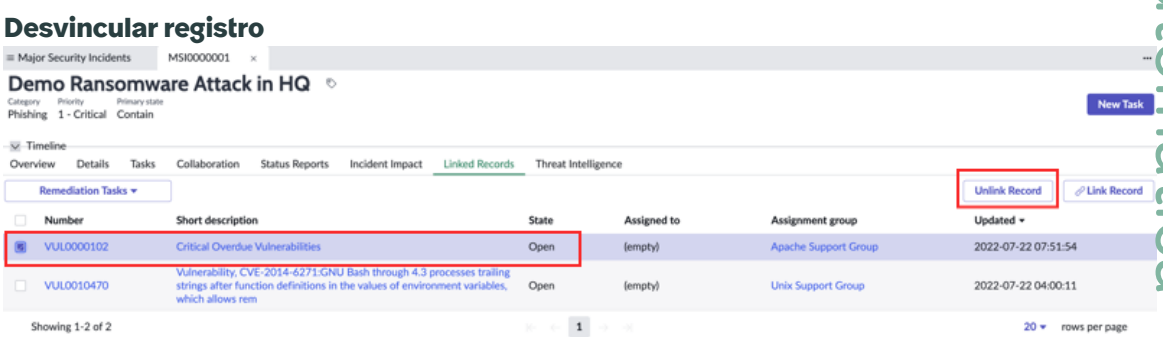
Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Nota: Você só pode desvincular um único registro de cada vez. Depois de desvincular um registro, as informações acumuladas relacionadas serão removidas das seções Impacto do incidente e Inteligência contra ameaças no espaço e a ação não poderá ser desfeita.

Para obter mais informações sobre registros de acúmulo, consulte Rollup Framework para MSIM.

Procedimento

1. Navegar até **Resposta a incidentes de segurança graves** > **Espaço do MSIM**.
2. Navegue até **Listas** exibição, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Clique em **Registros vinculados** guia.
   Esta seção exibe os registros vinculados e seus registros relacionados, que estão vinculados ao Incidente de segurança grave.
5. Selecione a exibição da tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança.
6. Selecione o registro a ser desvinculado da exibição de lista de registros.
7. Clique em **Desvincular registro** .

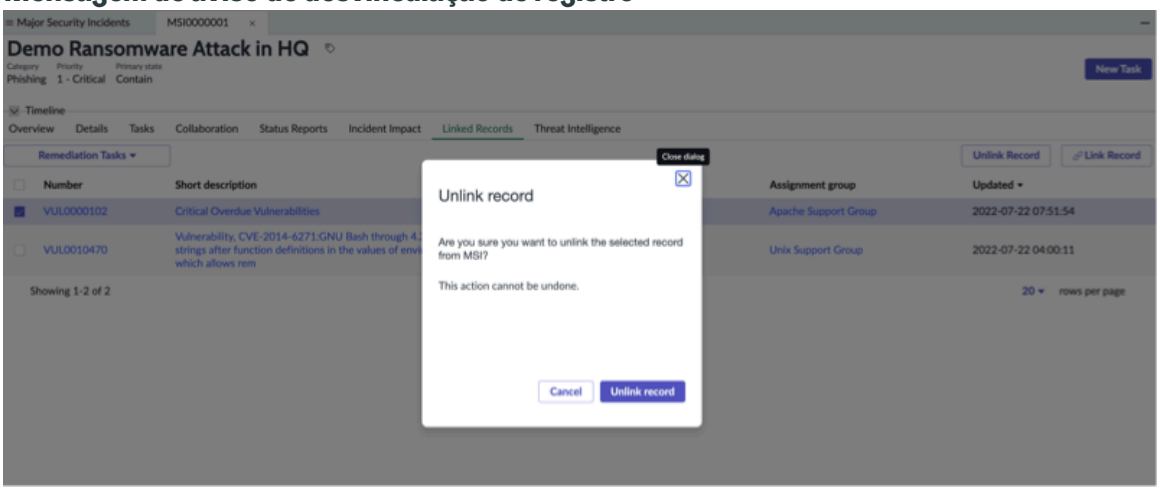


8. Uma mensagem de aviso é exibida perguntando se você deseja desvincular o registro selecionado do MSI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de aviso de desvinculação de registro



9. Clique em **Desvincular registro** .
   O registro é desvinculado e, depois de desvinculado, as mudanças não podem ser revertidas. A exibição de lista de registros vinculados será atualizada após a desvinculação.

Tópicos relacionados

Configure registros vinculados em Gestão de incidentes graves de segurança

Configurar registros de acúmulo em Gestão de incidentes graves de segurança

Gerenciar tarefas em um Incidente grave de segurança

A guia Tarefa permite rastrear e gerenciar todas as tarefas associadas a um incidente de segurança grave no espaço do MSIM. Você pode exibir as várias tarefas usando o Visual Task Board padrão (exibição Kanban) ou a exibição de lista.

O sn_msi.workspace_manager pode fazer o seguinte na guia Tarefas:

- Criar uma tarefa
- Modificar tarefas
- Exiba e atribua tarefas a si mesmo ou a outras pessoas
- Excluir tarefas

Nota: Certifique-se de ter instalado o. **Cartão de tarefa do MSIM VTB: 1,0.1v** Aplicativo separadamente após instalar o aplicativo MSIM.

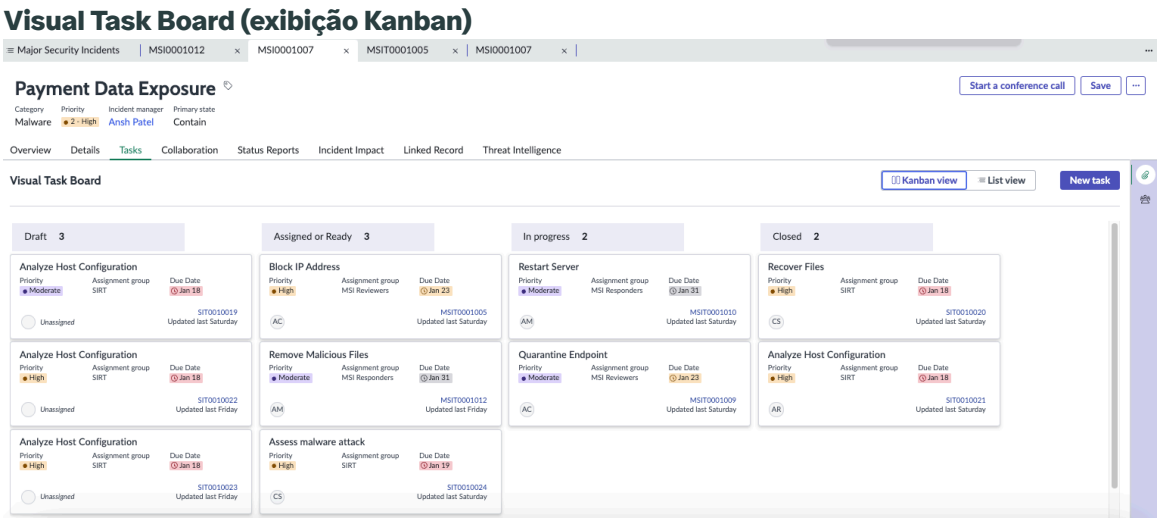
A guia Tarefas exibe os detalhes de todas as tarefas associadas a um incidente de segurança grave. A guia Tarefa oferece suporte a duas exibições:

- **Visual Task Board (exibição Kanban)** :

  Exiba e atualize vários registros de tarefa, que aparecem como cartões no Visual Task Board que podem ser movidos entre raias com base no status das tarefas no incidente de segurança grave.

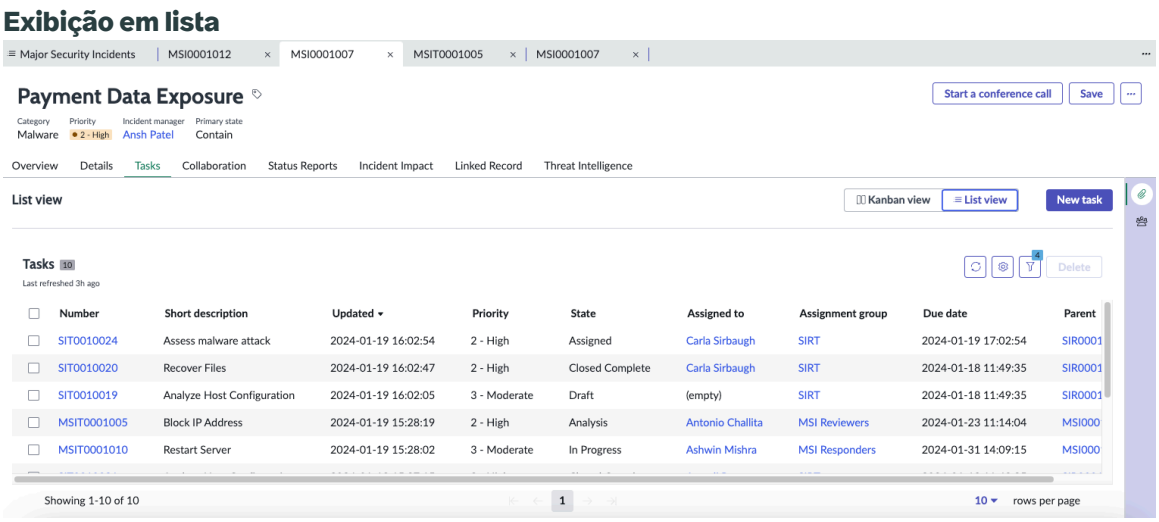
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- **Exibição de lista** :

  Exiba e atualize vários registros de tarefa usando na forma de listas. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas nas quais precisa trabalhar em um incidente de segurança grave.



Tradução automática

As atividades rotuladas são resumidas e exibidas na seção Visão geral do incidente de segurança grave. Um gráfico de gráfico de tendências está disponível na seção Visão geral para exibir o estado consolidado das atividades da tarefa.

Gerencie tarefas usando o Visual Task Board

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando o Visual Task Board (exibição Kanban).

Você pode usar o Visual Task Board para mover os cartões passo a passo entre raias como Rascunho, Atribuído ou Pronto, Em andamento e Encerrado, dependendo do status das tarefas. Um fluxo de atividades no quadro exibe a atividade recente para rastrear mudanças de tarefa com facilidade. Você pode adicionar cartões de tarefa de qualquer tabela que estenda a tarefa para rastrear rapidamente atualizações e editar incidentes de segurança graves diretamente do quadro.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma tarefa usando o Visual Task Board

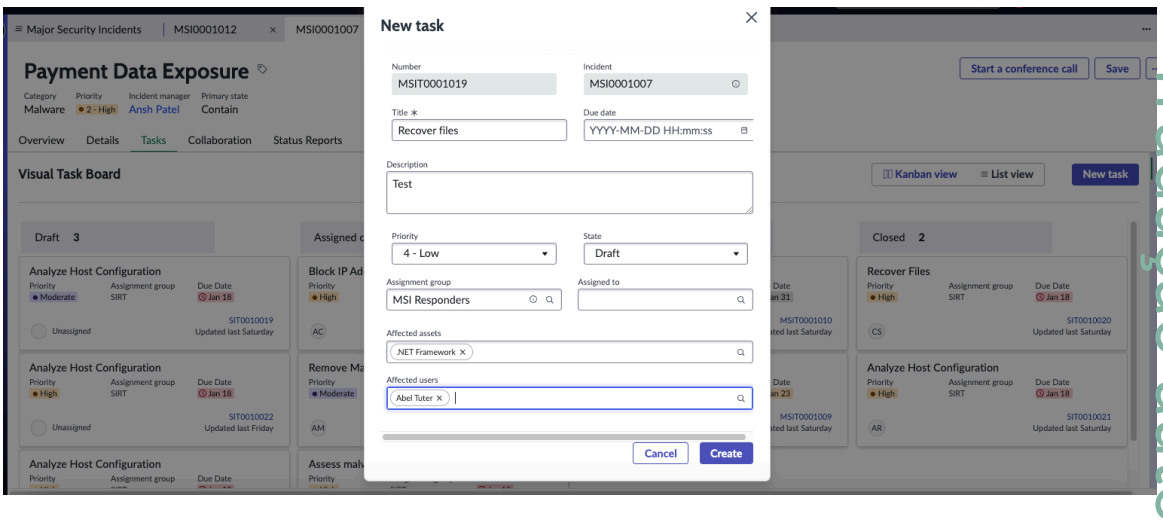
Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o. **Cartão de tarefa do MSIM VTB: 1,0.1v** Aplicativo separadamente após instalar o aplicativo MSIM.

Os gerentes MSI podem criar uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** guia.

Crie uma tarefa usando o Visual Task Board



5. Selecione **Exibição Kanban** e escolha **Nova tarefa** .
6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo gerado automaticamente para a tarefa selecionada. Este campo não é editável.
incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando **Calendário** e especifique a hora no **Selecione Hora** seção.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será executada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **2 - Alta** ○ **3 - Moderado(a)** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho** .
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuição a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione **Criar** para criar a tarefa.

Exiba e modifique uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o. **Cartão de tarefa do MSIM VTB: 1,0.1v** Aplicativo separadamente após instalar o aplicativo MSIM.

Os gerentes MSI podem exibir os detalhes de uma tarefa e as informações de atividade dos respondentes MSI e modificar uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** e escolha **Exibição Kanban** .
5. Escolha o cartão de tarefa desejado em uma das raias para exibir os detalhes da tarefa.

   O cartão de tarefa pode estar em uma das raias: Rascunho, Atribuído ou Pronto, Em andamento ou Encerrado.

6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número	Um número exclusivo gerado automaticamente para a tarefa selecionada. Este campo não é editável.
incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando **Calendário** e especifique a hora no **Selecione Hora** seção.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será executada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderado(a)** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho** .
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuição a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

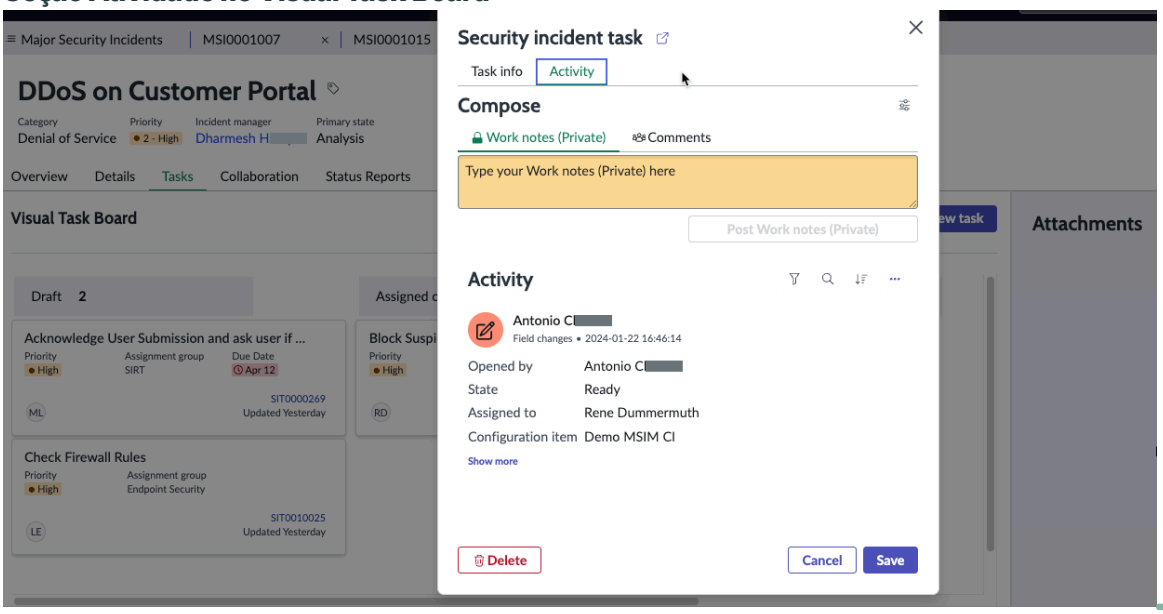
7. Selecione **Atividade** Seção para exibir os detalhes da atividade dos respondentes MSI.

   Use a seção Atividade para adicionar suas anotações de trabalho e comentários, publicar sua atividade de forma privada e também adicionar comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade adicionada ou anotações de trabalho na seção Atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção Atividade no Visual Task Board



Nota: Selecione **Mostrar mais** link detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

Exclua uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o. **Cartão de tarefa do MSIM VTB: 1,0.1v** Aplicativo separadamente após instalar o aplicativo MSIM.

MSI Manager pode excluir uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** e escolha **Exibição Kanban**
5. Escolha o cartão de tarefa que você deseja excluir.
6. No pop-up de tarefa de incidente de segurança grave, selecione **Excluir** opção.

   O pop-up Excluir tarefa é exibido solicitando que você confirme a exclusão da tarefa.

7. Selecione **Excluir**.

Gerencie tarefas usando a exibição de lista

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando a exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A exibição de lista exibe os detalhes de todas as tarefas associadas ao incidente de segurança grave, como Número da tarefa, Prioridade, Estado atual, Atribuído a, Grupo atribuído. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas necessárias nas quais precisa trabalhar em um incidente de segurança grave.

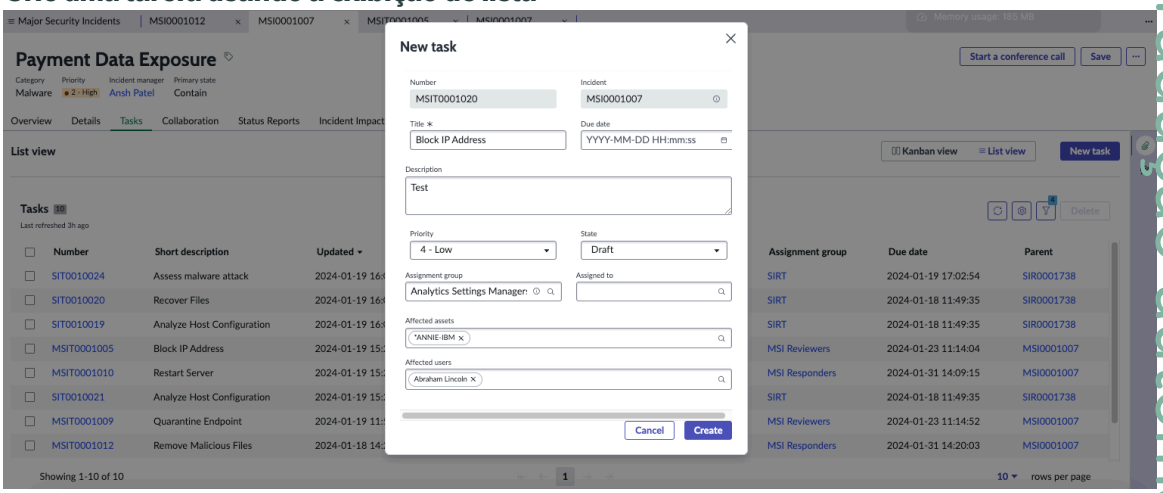
Crie uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Os gerentes MSI podem criar uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** guia.

Crie uma tarefa usando a exibição de lista



5. Selecione **Exibição de lista** e escolha **Nova tarefa** .
6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo gerado automaticamente para a tarefa selecionada. Este campo não é editável.
incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando **Calendário** e especifique a hora no **Selecione Hora** seção.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será executada. A prioridade pode ser um dos seguintes valores:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderado(a)** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho** .
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuição a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione **Criar** para criar a tarefa.

Exiba e modifique uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Os gerentes MSI podem exibir os detalhes de uma tarefa e as informações de atividade dos respondentes MSI e modificar uma tarefa na exibição de lista usando as etapas a seguir

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** e escolha **Exibição de lista** .
5. Escolha a Tarefa desejada na exibição de lista para exibir os detalhes da tarefa.
6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número	Um número exclusivo gerado automaticamente para a tarefa selecionada. Este campo não é editável.
incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando **Calendário** e especifique a hora no **Selecione Hora** seção.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será executada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderado(a)** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho** .
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuição a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

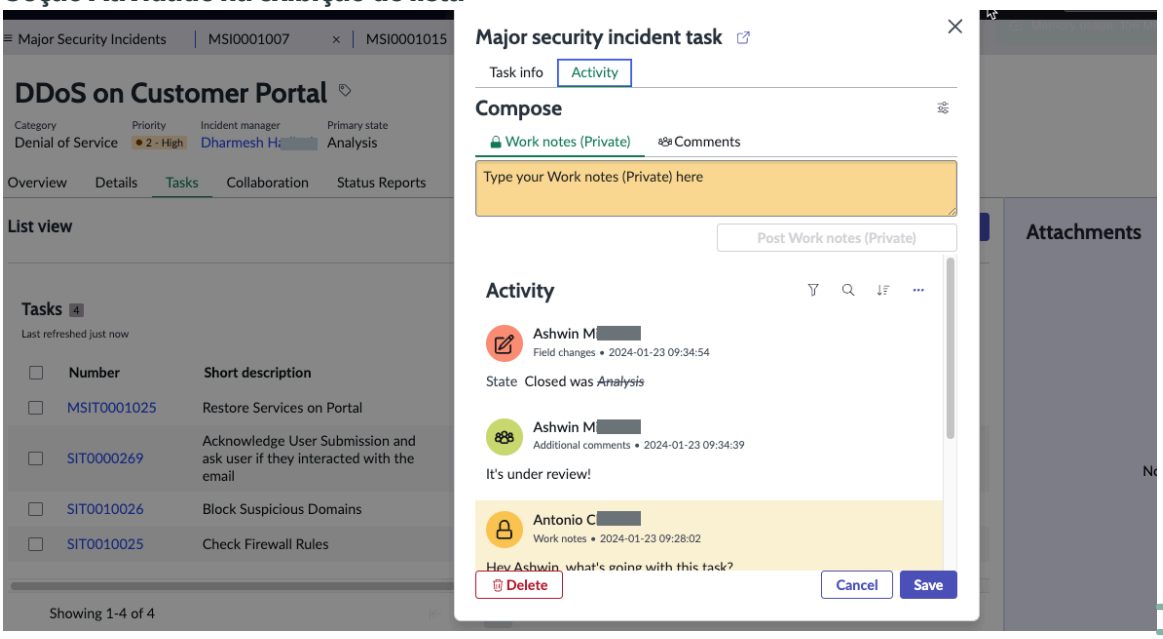
7. Selecione **Atividade** Seção para exibir os detalhes da atividade dos respondentes MSI.

   Use a seção Atividade para adicionar suas anotações de trabalho e comentários, publicar sua atividade de forma privada e também adicionar comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade adicionada ou anotações de trabalho na seção Atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção Atividade na exibição de lista



Nota: Selecione **Mostrar mais** link detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

9. Você também pode executar as seguintes ações na exibição de lista:
   a. Selecione **Atualizar** Ícone para atualizar a lista de tarefas na exibição de lista.
   b. Selecione **Configurações** e use **Editar colunas** Opção para modificar a lista de colunas que aparecem na exibição de lista. Use **Redefinir larguras** opção para redefinir as larguras das colunas.

Exclua uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

MSI Manager pode excluir uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione **Tarefas** guia.
5. Selecione **Exibição de lista** .
6. Escolha uma Tarefa que você deseja excluir da lista.
7. No pop-up de tarefa de incidente de segurança grave, selecione **Excluir** opção.

   O pop-up Excluir tarefa é exibido solicitando que você confirme a exclusão da tarefa.

8. Selecione **Excluir**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rastreie a atividade de colaboração por meio de MSIM espaço

Rastreie atividades de bate-papo e arquivo relacionadas à resolução de incidentes de segurança graves por meio do Espaço do MSIM.

As atividades são coordenadas usando Microsoft Teams bate-papo e. Microsoft SharePoint arquivos e pastas e, em seguida, postados de volta para Incidente grave de segurança por meio de integrações.

Uma vez Microsoft Teams E o Microsoft SharePoint estão integrados ao Gestão de incidentes graves de segurança, você pode usar MSIM Espaço para rastrear a colaboração entre usuários de resposta a incidentes e outros grupos que estão contribuindo para a resolução de um incidente de segurança grave. Todas as atualizações nas pastas de colaboração e arquivos em Microsoft SharePoint são sincronizados com MSIM Espaço File Explorer E também refletidos nos componentes do fluxo de atividades.

Quando um incidente de segurança é promovido como incidente de segurança grave:

1. Uma estrutura de pastas será criada em Microsoft SharePoint com base na configuração do modelo de pasta. A mesma estrutura de pastas será refletida em File Explorer componente do espaço.
2. Uma equipe com vários canais é criada em Microsoft Teams E o mesmo será refletido no componente Gestão de bate-papo do espaço.

Função necessária: sn_msi.workspace_manager.

Interaja com arquivos e pastas

O Explorador de arquivos exibe o sistema de arquivos para que você possa exibir e interagir com arquivos e pastas relacionados à resolução do incidente.

Exibe o arquivo e as pastas que são capturados no Microsoft SharePoint para um incidente de segurança específico. Essas pastas serão criadas automaticamente no Microsoft SharePoint para esse incidente de segurança grave. Você pode usar essas pastas criadas padrão para carregar arquivos de suporte, se necessário. Você pode renomear, mover ou excluir esses arquivos e pastas conforme necessário.

Sempre que você carregar um arquivo em qualquer uma das pastas, a atividade correspondente a essas pastas será associada automaticamente às pastas do Explorador de arquivos na guia Colaboração e a atividade será registrada e exibida na seção Atividade do Espaço de gestão de incidentes de segurança graves.

Nota: Em **Colaboração** , o registro do incidente é anexado ao arquivo primário no sharepoint com um número de incidente exclusivo e uma categoria de incidente.

1. **Exibição do repositório** : Lista os arquivos e pastas listados no Microsoft SharePoint para esse incidente de segurança específico. Para cada arquivo ou pasta, a exibição do repositório exibe o Nome, Modificado por, Modificado pela última modificação e o Tamanho serão exibidos.

Exibição do repositório

Campo	Descrição
Abrir no SharePoint	Selecione esta opção disponível ao lado do incidente de segurança grave. Clique no link para selecionar e exibir a estrutura de pastas no Microsoft SharePoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nova pasta	Selecione esta opção para criar uma nova pasta conforme necessário. Depois de criar uma nova pasta, a mesma nova pasta é criada e associada no Microsoft SharePoint, por padrão.

2. **Recentes** : Exibe todos os logs de atividades recentes. Esses logs incluem suas atividades do SharePoint e do Explorador de arquivos. Geralmente, as atividades recentes são seus arquivos de suporte que incluem a pasta primária.

   A seguir está o procedimento para **Localizar arquivo de log:**

   a. Selecione o respectivo arquivo para exibir os detalhes.

   b. Clique em **Localizar arquivo** .

   Nota: A navegação e os detalhes do arquivo primário e das pastas primárias são exibidos em **Recentes** seção de exibição de lista. Você pode abrir o mesmo arquivo no SharePoint. Sempre que você carregar os arquivos de log relacionados ou qualquer atividade, todos esses arquivos e atividades serão exibidos no SharePoint e no Gerenciador de arquivos.

Gerencie as comunicações dos Canais de bate-papo usando o Microsoft Teams

O Gerenciador de canais de bate-papo exibe o Microsoft Teams com vários canais criados no aplicativo Microsoft Teams com base em uma configuração de modelo.

Esses canais configurados são refletidos no componente Gestão de bate-papo junto com os usuários e grupos de usuários atribuídos a eles. O Gerenciador de canais de bate-papo permite que você execute o seguinte:

- **Gerenciar canais de bate-papo**
- **Renomear equipe**
- **Gerenciar membros da equipe**

A equipe e os canais são criados com base na configuração do Canal de bate-papo no Microsoft Teams.

Gerenciar canais de bate-papo

O Gerenciador de canais de bate-papo permite criar, editar ou excluir canais de bate-papo. Para gerenciar um canal de bate-papo no Microsoft Teams, execute as seguintes etapas:

1. Selecione **Colaboração** guia.
2. Navegar até **Channel Manager de bate-papo** > **Criar novo canal**.
3. Adicionar um novo **Nome do canal** , **Descrição** e selecione **Membros** para o canal.
4. Selecione **Criar**.

   Nota: Um novo registro de canal é criado na seção Canais do Microsoft Teams da aplicação Microsoft Teams e o mesmo registro será refletido no MSIM.

5. Para editar um canal de bate-papo, selecione um canal de bate-papo na lista Gerenciador de canais de bate-papo.
6. Você pode modificar o nome do canal, a lista de membros, a lista de membros do grupo com base em seus requisitos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Save** (Salvar).
8. Para excluir um canal de bate-papo, selecione um canal de bate-papo na lista Gerenciador de canais de bate-papo.
9. Selecione **Excluir canal** .

Renomear equipe

Para renomear uma equipe no Microsoft Teams, execute as seguintes etapas:

1. Selecione **Colaboração** guia.
2. Navegar até **Channel Manager de bate-papo** > **Renomear equipe**.
3. No campo Nome da equipe, renomeie a equipe de acordo com seus requisitos.
4. Selecione **Save** (Salvar).

Nota: Renomear o nome da equipe também renomeará o nome da equipe no Microsoft Teams.

Gerenciar membros da equipe

O Gerenciador de canais de bate-papo permite que você adicione ou remova membros da equipe no Microsoft Teams. Você também pode adicionar membros por meio de grupos. Para gerenciar membros da equipe no Microsoft Teams, execute as seguintes etapas:

1. Selecione **Colaboração** guia.
2. Navegar até **Channel Manager de bate-papo** > **Gerenciar membros da equipe**.
3. No campo Membros, adicione ou remova membros da equipe de acordo com seus requisitos.
4. No campo Adicionar membros por meio de grupos, selecione os grupos que você deseja adicionar no Microsoft Teams.

Nota: Se os membros do grupo já estiverem na equipe, esses membros não serão adicionados.

5. Selecione **Save** (Salvar).

   O Gerenciador de canais de bate-papo exibe os detalhes do total de membros da equipe e o número de novos membros que serão adicionados.

Gerencie as comunicações dos canais de bate-papo usando o Slack

O Gerenciador de canais de bate-papo exibe o Slack com vários canais criados no aplicativo Slack com base em uma configuração de modelo.

Esses canais configurados são refletidos no componente Gestão de bate-papo junto com os usuários e grupos de usuários atribuídos a eles. O Gerenciador de canais de bate-papo permite que você faça isso **Gerenciar canais de bate-papo** . A equipe e os canais são criados com base na configuração do canal de bate-papo no Slack.

Gerenciar canais de bate-papo

O Gerenciador de canais de bate-papo permite criar, editar ou excluir canais de bate-papo no Slack. Para gerenciar um canal de bate-papo, execute as seguintes etapas:

1. Selecione **Colaboração** guia.
2. Navegar até **Channel Manager de bate-papo** > **Criar novo canal**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicionar um novo **Nome do canal** , **Descrição** e selecione **Membros** para o canal.
4. Selecione **Criar**.

> **Nota:** Um novo registro de canal é criado na seção Canais do Slack do aplicativo Slack e o mesmo registro será refletido no MSIM.

5. Para editar um canal de bate-papo, selecione um canal de bate-papo na lista Gerenciador de canais de bate-papo.
6. Você pode modificar o nome do canal, a lista de membros, a lista de membros do grupo com base em seus requisitos.
7. Selecione **Save** (Salvar).
8. Para excluir um canal de bate-papo, selecione um canal de bate-papo na lista Gerenciador de canais de bate-papo.
9. Selecione **Excluir canal** .

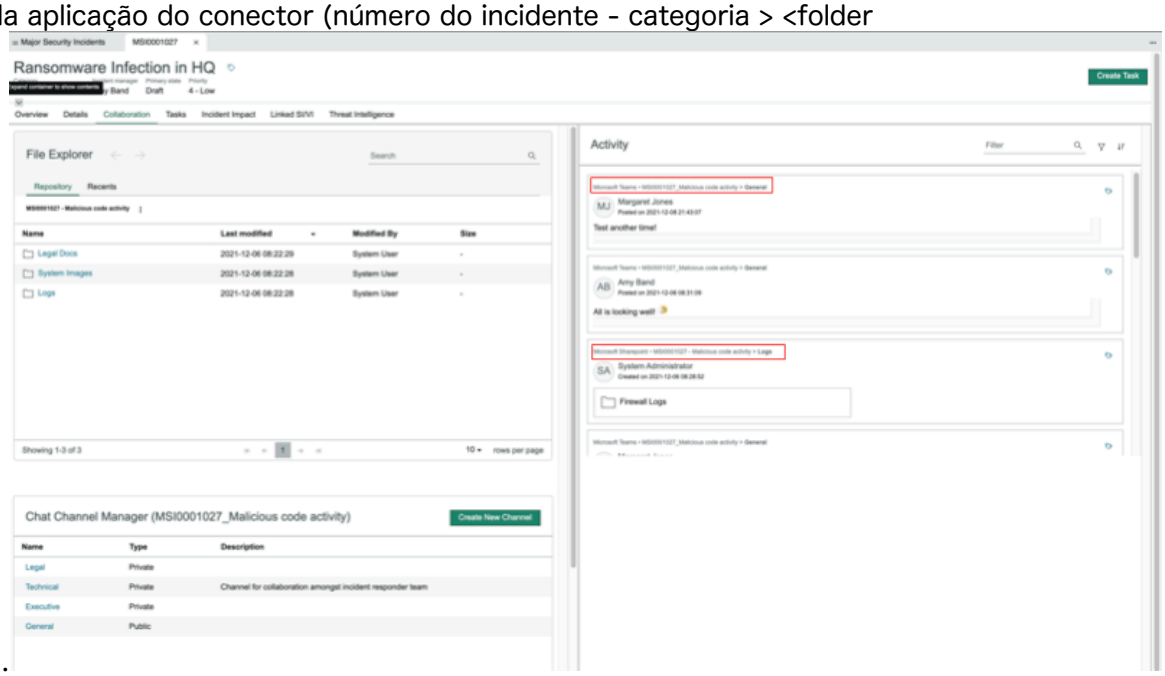
Gerencie conversas do fluxo de atividades

Exibe todas as atividades, logs e status que foram realizados em Microsoft SharePoint, explorador de arquivos e Microsoft Teams.

Se você quiser exibir qualquer atividade específica ou pesquisar os detalhes da atividade de colaboração que foram interagidos entre vários arquivos e pastas e também no Microsoft Teams, poderá usar o recurso de filtro que é exibido no canto superior direito da seção Fluxo de atividades e localizar os detalhes da atividade desejada.

As pastas e conversas de bate-papo compartilhadas com a Gestão de incidentes de segurança graves são refletidas como trilhas com a estrutura:

nome da aplicação do conector (número do incidente - categoria > <folder name>).

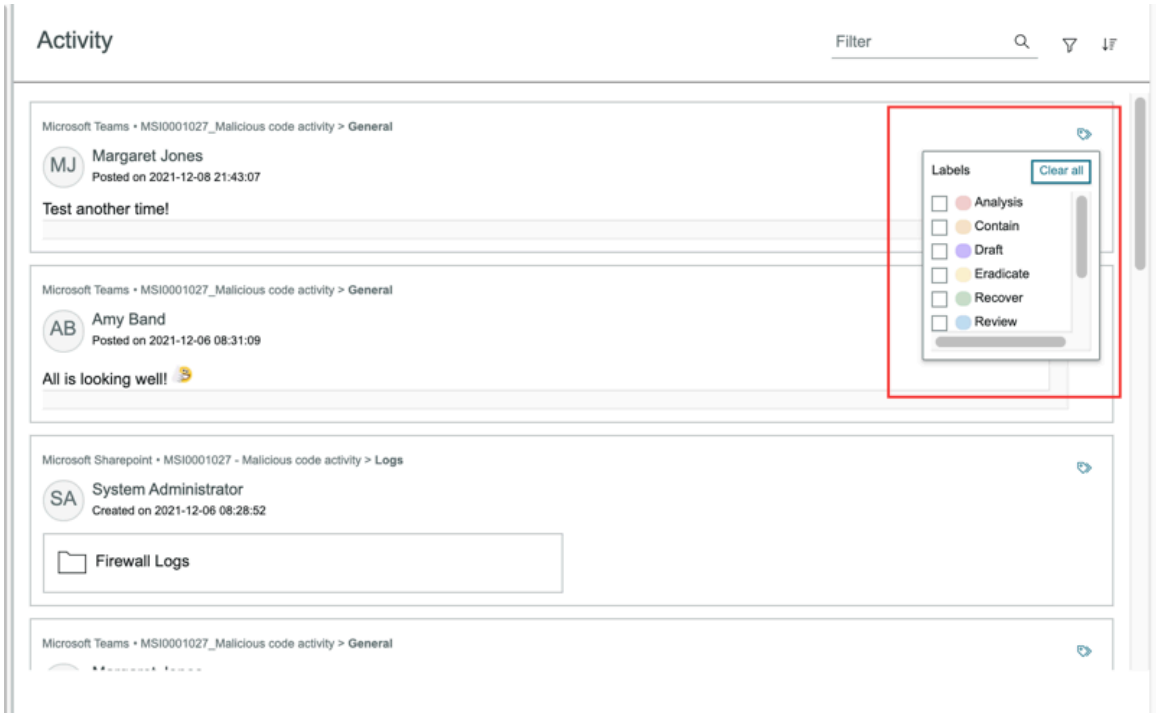


Rotule as atividades :

1. Clique em **Rótulo** ícone.
2. Marque a respectiva caixa de seleção do rótulo de atividade de incidente, conforme mostrado na captura de tela abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. As atividades rotuladas são codificadas por cores e representadas como gráfico de tendência de andamento no **Colaboração externa** do espaço.

Criar e distribuir MSIM Relatórios de status

. Incidente grave de segurança gerente, você pode criar e distribuir os diferentes relatórios de status para diferentes partes interessadas em vários intervalos com base no modelo de relatório configurado ou em um relatório de status anterior durante todo o curso da resolução de incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Você pode visualizar os elementos de dados do relatório resumido configurados anteriormente, adicionar texto ou resumo adicional, remover componentes de relatório individuais conforme necessário e verificar a precisão e a integridade do relatório antes de distribuí-lo para diferentes partes interessadas.

Crie os relatórios de status selecionando o modelo de relatório desejado que foi configurado inicialmente na página Configuração de modelos de relatório MSI.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione **Listas** exibir.
3. Selecione o respectivo registro MSI promovido.
4. Selecione **Relatórios de status** guia.
   A guia Relatórios de status contém três tipos diferentes de subseções, como abaixo.

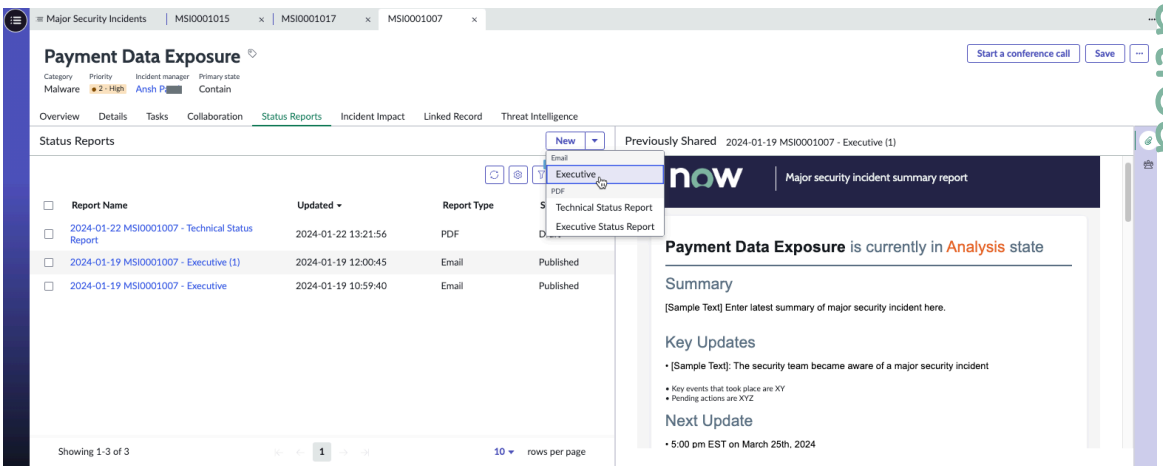
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de relatório	Nome do modelo de relatório de status. **Nota:** A exibição Relatórios de status lista os modelos de relatório predefinidos existentes que estão disponíveis como parte do sistema de base para a persona em questão. Por exemplo, Relatórios de status executivo por e-mail (compatíveis com dispositivos móveis), Relatórios de status técnico e Relatórios de status executivo como PDFs.
Atualização em	A data em que o modelo de relatório foi atualizado pela última vez.
Tipo de relatório	Tipo de relatório de status. O relatório de status pode estar em um dos seguintes tipos: ○ PDF ○ E-mail
Estado	Estado dos relatórios de status. Os relatórios de status podem estar em um dos seguintes estados: ○ Rascunho ○ Em Fila ○ Publicado

5. Selecione o tipo de relatório de status que você deseja exibir ou selecionar **Novo** para criar um relatório de status.

Guia Relatórios de status do MSIM



6. Escolha um dos seguintes tipos de relatório de status na lista.
   - **Executivo** Relatórios de status de e-mail compatíveis com dispositivos móveis.
   - **Relatório de status técnico** PDF
   - **Relatório de status executivo** PDF

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando você seleciona qualquer modelo de relatório desejado, a visualização do relatório selecionado é gerada imediatamente no painel direito. Você pode exibir o relatório de status selecionado do MSI.

7. No modelo Relatório de status de e-mail executivo, preencha as seções com os detalhes do relatório de status.

Seção de relatório	Descrição
Atualizações	Forneça um resumo da atualização de status. Esta seção contém o seguinte: ○ **Resumo MSI** : Forneça um breve resumo do incidente de segurança grave. ○ **Anexar texto do último relatório compartilhado** : Selecione esta opção para anexar o texto do último relatório compartilhado.
Explicação	Adicione uma explicação sobre o que mudou desde que a última atualização de status foi feita. Esta seção contém o seguinte: ○ **Atualizações de chave** : Forneça atualizações de chave, como o que a equipe de segurança deve saber sobre o incidente de segurança grave, nomeie os principais eventos que ocorreram e liste todas as ações pendentes. ○ **Próxima atualização** : Forneça a data e a hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 5:00 pm EST em 25 de março de 2024. ○ **Anexar texto do último relatório compartilhado** : Selecione esta opção para anexar o texto do último relatório compartilhado. ○ **Elementos de filtro** : Selecione os elementos de relatório a serem incluídos no relatório. Por exemplo, Atualizações de chave ou Próximas atualizações.
Informações adicionais	Forneça detalhes específicos relevantes para a atualização de status.
Visualizações	Selecione as visualizações que melhor ajudam a comunicar a atualização de status. ○ **Impacto do incidente** : Selecione as métricas de Impacto do incidente, como Ativos afetados, Local afetado, Usuários afetados relacionados à atualização de status. ○ **Elementos de filtro** : Selecione os elementos de relatório a serem incluídos no relatório. Por exemplo, Impacto do incidente.
Listas	Selecione listas de registros que fornecem contexto para a atualização de status.

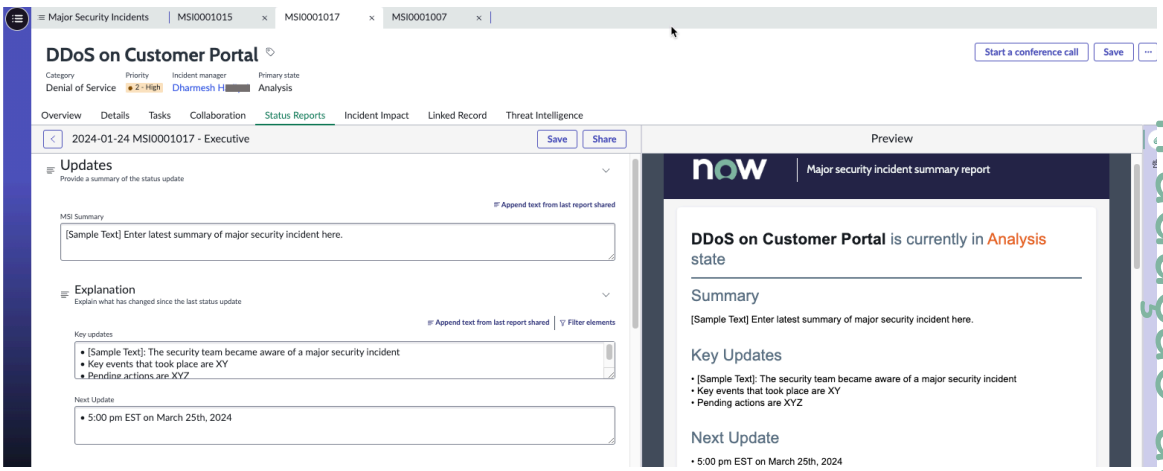
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção de relatório	Descrição
	○ **Registros vinculados** : Selecione os registros vinculados à atualização de status do incidente de segurança grave. Por exemplo, Incidente de segurança vinculado. ○ **Elementos de filtro** : Selecione os elementos de relatório a serem incluídos no relatório. Por exemplo, Registros vinculados.

Nota: As opções que você selecionou na seção Relatórios de status são as mesmas opções renderizadas no relatório Visualizar.

modelo de relatório de status

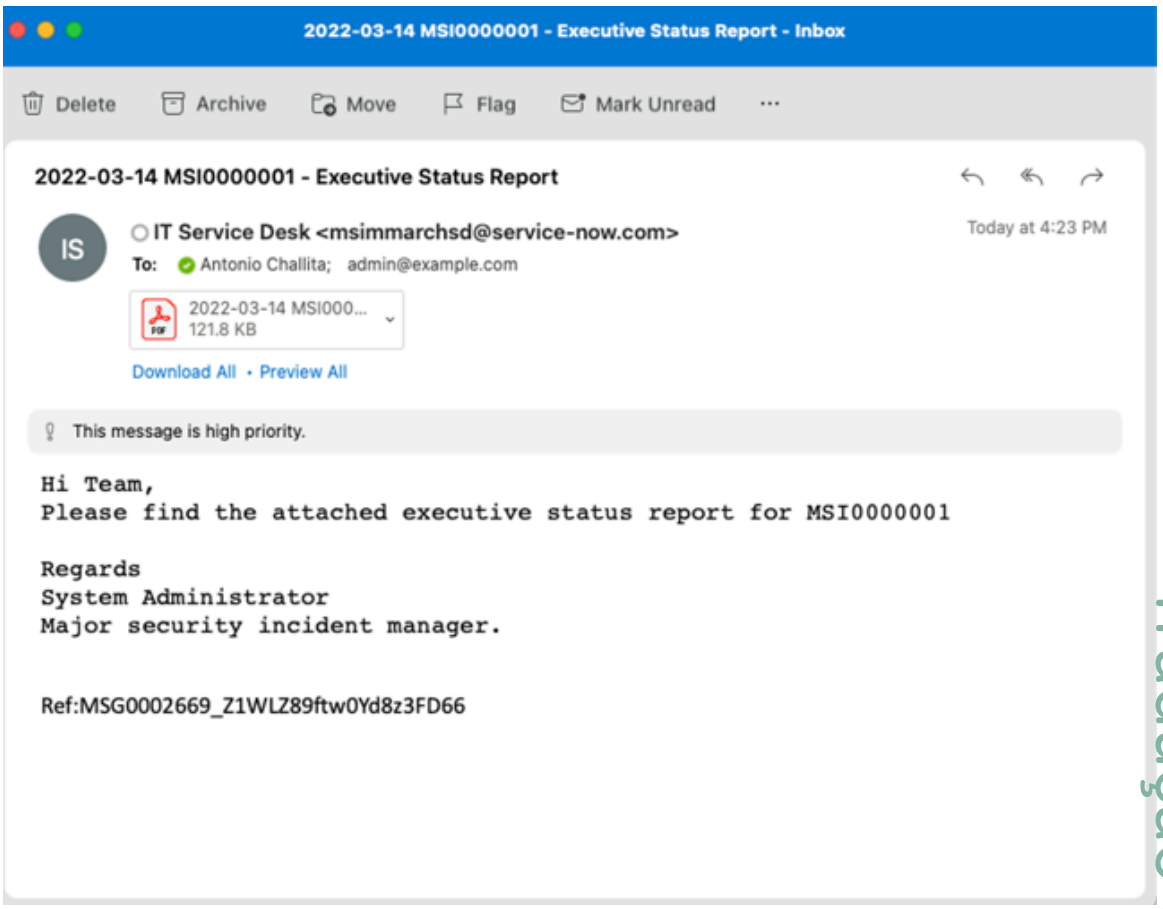


8. Selecione **Salvar** para salvar as atualizações feitas no relatório de status.
9. Selecione **Compartilhar** para compartilhar o relatório de status com partes interessadas internas e externas.
   A caixa de diálogo Compartilhar é exibida.
   a. No campo Assunto, insira o assunto do relatório de e-mail.
   b. No campo Adicionar destinatários internos, digite e selecione os destinatários do relatório de e-mail.
   c. No campo Adicionar destinatários externos, digite o e-mail ou DL dos destinatários para o relatório de e-mail.
   Você pode adicionar vários IDs de e-mail usando vírgula ou ponto-e-vírgula.
10. Selecione **Relatório por e-mail** .
    Um e-mail com o Relatório de status do PDF anexado é enviado com sucesso ao destinatário em questão para que ele verifique.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatório de status - e-mail



11. Você também pode executar as seguintes ações na guia Relatórios de status:
    a. Use **Atualizar** Ação na exibição Relatórios de status para atualizar a lista de relatórios de status.
    b. Use **Listar ações** Ação na exibição Relatórios de status para editar colunas ou redefinir as larguras da lista de relatórios de status.
    c. Use **Filtro** Ação na exibição Relatórios de status para filtrar os relatórios de status com base em determinadas condições.

Tópicos relacionados

Configurar Incidente grave de segurança relatórios de status

Gerenciando MSIM relatórios de status

Os relatórios de status fornecem gráficos de tendências pré-configurados com visualizações de dados acionáveis para melhorar os processos de operações de segurança, medir e analisar a linha do tempo de resolução, a contagem de atrasos e o status de cada tarefa atribuída.

Configurar Incidente grave de segurança relatórios de status

Configure relatórios de incidentes de segurança graves para configurar e baixar os relatórios de acordo com suas necessidades de negócios durante todo o ciclo de vida do processo de correção de registro de incidentes de segurança graves.

Você pode criar os modelos de relatório com um formato e layout específicos e personalizar esses relatórios de acordo com seus requisitos específicos usando o recurso Relatórios de status do Gestão de incidentes graves de segurança espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um usuário com a função sn_msi.workspace_manager pode criar e configurar os modelos de relatório que descrevem o tipo de informações de relatório que podem ser usadas para gerar todos os relatórios de status, que podem ser compartilhados com usuários específicos, como partes interessadas executivas, departamentos jurídicos e mapear esses modelos para os registros de incidentes de segurança graves.

Para personalizar seus relatórios de status MSI, você deve primeiro configurar os modelos de relatório usando **Modelos de relatório** . Com a ajuda dos Modelos de relatório, você pode criar os tipos de modelo de relatório, definir os componentes de relatório para esses modelos de relatório, adicionar informações adicionais, criar dados visualizados para rastrear o escopo e as métricas de andamento, adicionar dados de lista relacionada e gerar os relatórios de status.

A seguir descreve os campos padrão fornecidos em todos os tipos de modelo de relatório. Você pode configurar e formatar o modelo de relatório com base em seus requisitos usando seções, subseções e seus elementos:

Componentes do relatório de status

Tipo de componente	Descrição
Título do relatório	Título do tipo de relatório. Por exemplo, o formato padrão do tipo de relatório é: [Número MSI] - Relatório de parte interessada executiva descrito como MSI0001001: Relatório de parte interessada executiva.
Nome	Exibe o nome do usuário que gerou o relatório usando a seção Relatórios de status do espaço Gestão de incidentes de segurança graves.
Resumo	Exibe um breve resumo do relatório.
Data	Exibe a data em que o relatório é compartilhado com o destinatário em questão.
Andamento	Exibe o escopo e as métricas de andamento, como incidentes DE SIR vinculados, tarefas de resposta, tarefas suplementares, colaboração externa, componentes da linha do tempo, e Eventos de linha do tempo recentes.
Desafios	Esta seção exibe uma breve descrição dos desafios envolvidos durante todo o processo de correção de incidente de segurança grave.
Próximas etapas	Esta seção exibe uma breve descrição das próximas etapas envolvidas na resolução do incidente de segurança grave. Por exemplo, a subseção Equipe ativa no relatório da parte interessada executiva fornece as informações com a próxima etapa na atribuição da equipe que está envolvido na análise mais detalhada do registro de incidente de segurança grave.
Outras personalizações	O modelo de relatório também fornece a capacidade de carregar o logotipo e personalizar os cabeçalhos e rodapés no relatório.

A seguir estão os tipos de categorias de relatório que podem ser configurados e exibidos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Executivo** E-mail
- **Relatório de status técnico** PDF
- **Relatório de status executivo** PDF

Os relatórios acima estão configurados e disponíveis para o usuário selecionar, exibir e gerar o relatório no espaço Gestão de incidentes de segurança graves.

Relatórios de status executivo compatíveis com dispositivos móveis - E-mail

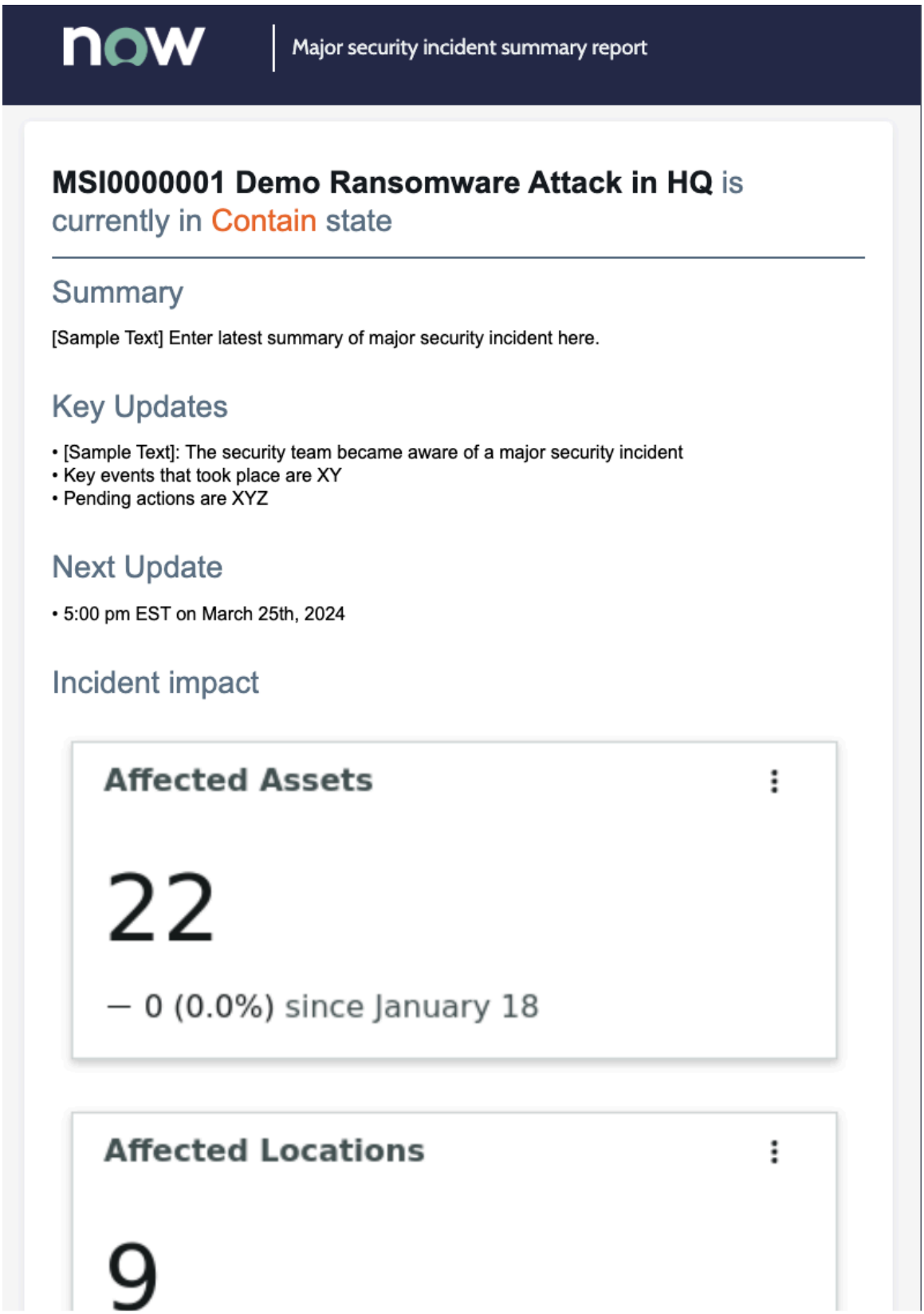
Relatórios de status executivo - E-mail são relatórios de status compatíveis com dispositivos móveis gerados em formato de e-mail. A seção de relatório inclui um resumo do relatório, coluna de duração MSI, escopo/impacto do incidente, métricas de equipe ativa, métricas de andamento, e Componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos do modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório de status de e-mail executivo é mostrado abaixo para sua referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail do relatório de status executivo



Tradução automática

Relatórios de status executivo - PDF

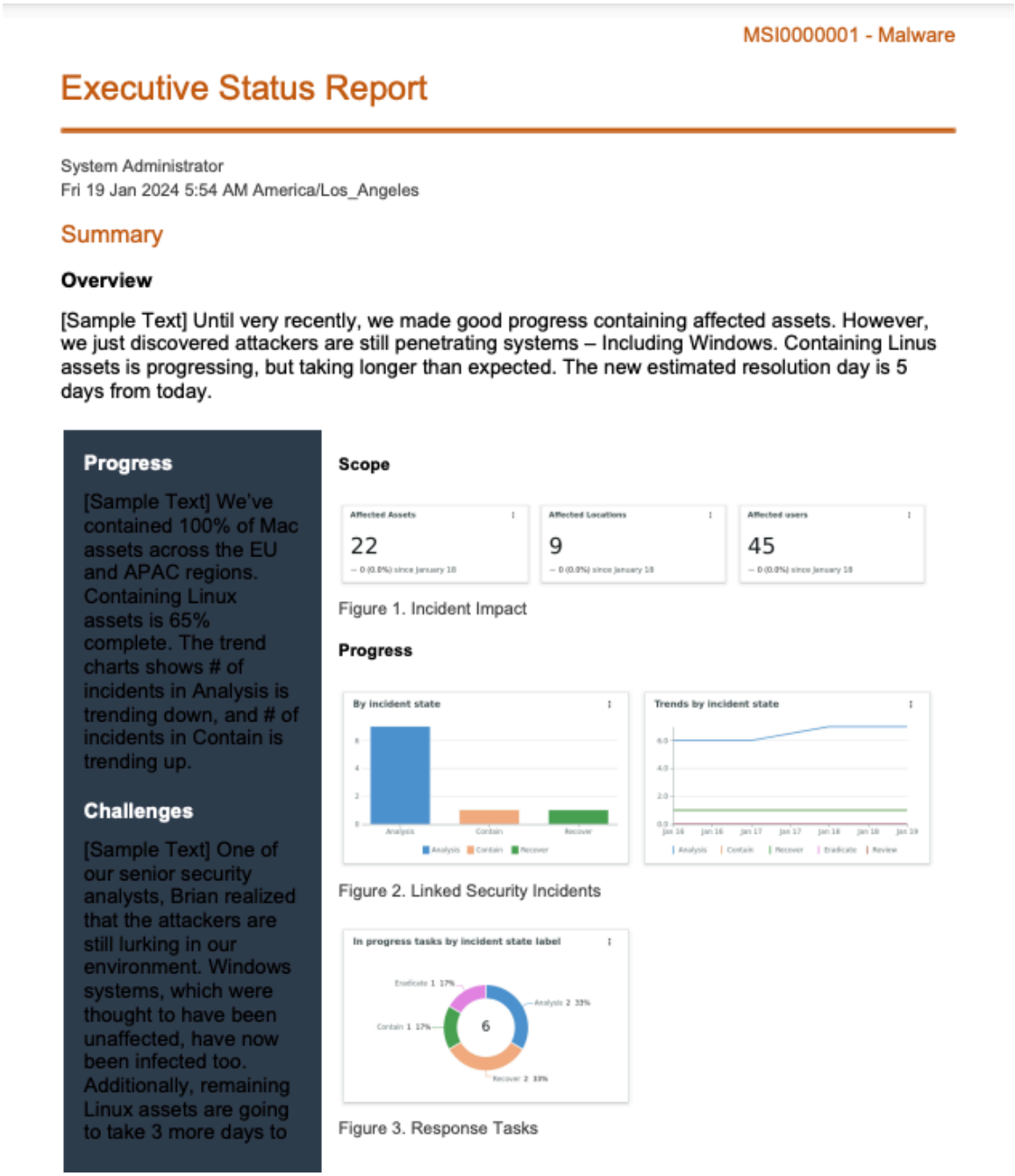
Os Relatórios de status executivo - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, coluna de duração MSI, escopo/impacto do incidente, métricas de equipe ativa, métricas de andamento, e Componentes da linha

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos do modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório executivo é mostrado abaixo para sua referência.

Relatório de status executivo PDF



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Figure 1. Incident Impact

Progress

Figure 2. Linked Security Incidents

Figure 3. Response Tasks

Relatórios de status técnico - PDF

Os Relatórios de status técnico - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, coluna de duração MSI, escopo/impacto do incidente, métricas de equipe ativa, métricas de andamento, e Componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico, atualizações de tarefa rotuladas e atividades rotuladas, com base no grupo de atribuição e no rótulo do marcador selecionado desde quando o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

último relatório de status é gerado e informações adicionais, como impacto do incidente e incidentes vinculados.

Personalize e configure o modelo de relatório para adicionar informações adicionais ao relatório. Um relatório técnico de amostra que mostra as informações adicionais, como o impacto do incidente, é ilustrado abaixo para sua referência, e a parte restante das informações do relatório é semelhante aos relatórios executivos.

Relatório de status técnico - PDF



As seções de modelo de relatório contêm várias subseções, que descrevem como você pode construir as subseções de relatório e seus elementos, como:

1. Identidade visual: Adicione Identidade visual aos seus Modelos de relatório
2. Scripts de Modelo: Use scripts de modelo em seus modelos de relatório

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Use Visualizações em Modelos de relatório
4. Use Listas de relatórios em Modelos de relatório

Criar um Modelo de Relatório

Crie vários modelos de relatório, que podem ser aplicados aos incidentes de segurança graves e gerar um relatório de status. Você pode adicionar campos de formulário de Resposta de incidente de segurança grave padrão e personalizados ao modelo de relatório que podem ser verificados com pontos. Além disso, você pode formatar e configurar o relatório com base em seus requisitos usando seções, subseções e seus elementos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode definir componentes de relatório para seus modelos de relatório e fornecer informações adicionais. Crie dados visualizados para rastrear o escopo e as métricas de andamento, adicionar dados de lista relacionada, visualizar e gerar ou compartilhar os relatórios de status.

Procedimento

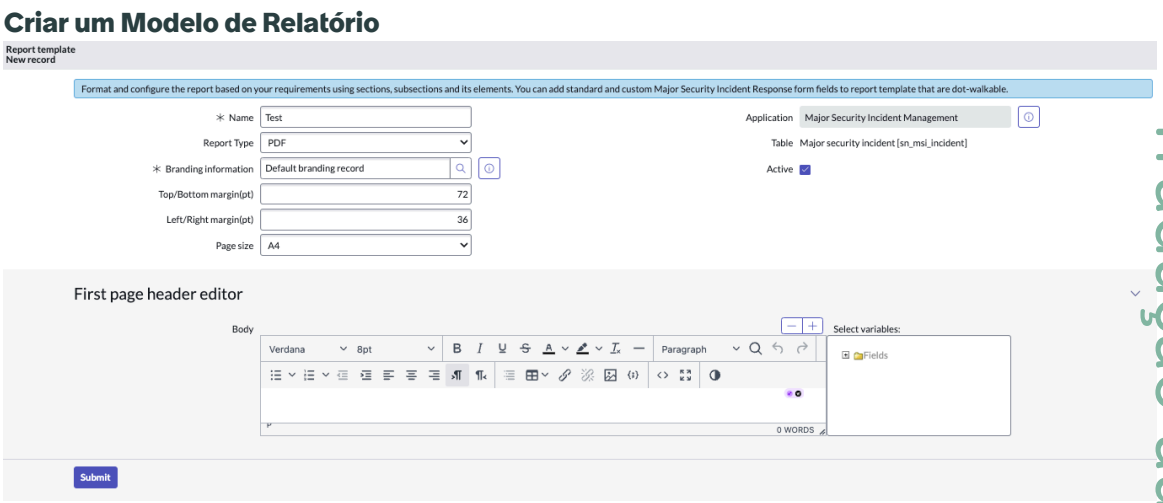
1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Selecione **Novo** para criar um modelo de relatório.
4. No formulário Modelo de relatório, preencha os campos.

Campo	Descrição
Nome	Nome do modelo de relatório.
Informações de identidade visual	Selecione as informações de identidade visual do seu modelo de relatório, como logotipo, cabeçalho e texto do rodapé. Por exemplo, Registro de identidade visual padrão.
Tipo de relatório	Tipo de relatório de status. O relatório de status pode estar em um dos seguintes tipos: ○ PDF ○ E-mail
Tabela	Nome da tabela de modelo de relatório.
Margem superior/inferior	Defina os recuos de margem superior e inferior necessários ao gerar o relatório.
Margem esquerda/direita	Defina os recuos de margem esquerda e direita necessários ao gerar o relatório.
Tamanho da Página	O tamanho da página do seu modelo de relatório. Por exemplo, o tamanho padrão é A4.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Marque a caixa de seleção do MSI Manager para gerar um relatório a partir do modelo que foi criado a partir do **Modelo de relatórios** seção. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar um relatório para esse tipo de modelo de relatório específico no espaço MSIM.
Editor de cabeçalho da primeira página	Permite definir o corpo do modelo. Selecione as variáveis necessárias para adicionar à seção do editor de modelos.



5. **Enviar** novo registro de modelo de relatório.
   Um novo modelo de relatório é criado na página Modelos de relatórios.

Tópicos relacionados

Criar e distribuir MSIM Relatórios de status

Adicione Identidade visual aos seus Modelos de relatório

Adicione identidade visual aos seus relatórios. Você pode adicionar imagem de cabeçalho e rodapé, texto de cabeçalho e rodapé. Você pode incluir essas informações de identidade visual em qualquer um dos tipos de modelo de relatório que você deseja criar, exceto os dois relatórios predefinidos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

As principais considerações ao adicionar identidade visual aos seus modelos de relatório são as seguintes:

- Carregue a imagem do cabeçalho e do rodapé e alinhe a posição da imagem.
- O limite de tamanho máximo para a imagem de cabeçalho e rodapé é de 5 MB. Se o tamanho exceder mais do que o limite especificado, uma mensagem de erro "O formato da imagem não pode ser reconhecido" será exibida no incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ajuste a altura da imagem do cabeçalho e do rodapé.
- O comprimento do texto do rodapé é limitado a 100 caracteres.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
2. Detalhar até **Modelo de relatório** > **Identidade visual**.
3. Selecione **Configurar**.
4. Selecione **Novo** para adicionar uma identidade visual ao seu modelo de relatório.
5. No formulário Modelo de identidade visual, preencha os campos.

Campo	Descrição
Nome	Nome do modelo de identidade visual.
Imagem do cabeçalho	Adicione uma imagem de cabeçalho para o modelo de identidade visual executando as seguintes etapas: **a.** Selecione **Clique para adicionar** . **b.** Selecione **Escolha Arquivo** **c.** Escolha uma imagem do seu sistema e selecione **OK** .
Imagem do rodapé	Adicione uma imagem de rodapé para o modelo de identidade visual executando as seguintes etapas: **a.** Selecione **Clique para adicionar** . **b.** Selecione **Escolha Arquivo** **c.** Escolha uma imagem do seu sistema e selecione **OK** .
Posição da imagem do cabeçalho	Selecione uma posição de imagem de cabeçalho para o modelo de identidade visual. Você pode escolher **À esquerda** , **Central** ou **Certo** .
Posição da imagem do rodapé	Selecione uma posição de imagem de cabeçalho para o modelo de identidade visual. Você pode escolher **Superior esquerdo** , **Centro superior** , **Superior direito** , **Inferior esquerdo** , **Inferior central** ou **Inferior direito** .
Altura da imagem do cabeçalho	Forneça um valor de altura (em pt) para a imagem do cabeçalho do modelo de identidade visual.
Altura da imagem do rodapé	Forneça um valor de altura (em pt) para a imagem de rodapé do modelo de identidade visual.
Texto do rodapé	Forneça um texto de rodapé para o modelo de identidade visual. Você pode incluir informações de classificação ou confidencialidade. Por exemplo, este e-mail é classificado como Confidencial, Somente Interno ou Advogado do Cliente Privilegiado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Posição do texto do rodapé	Selecione uma posição do texto do rodapé para o modelo de identidade visual. Você pode escolher **Superior esquerdo** , **Centro superior** , **Superior direito** , **Inferior esquerdo** , **Inferior central** ou **Inferior direito** .

6. Selecione **Enviar**.
   Um novo modelo de identidade visual é criado na página Modelos de identidade visual.

Use Visualizações em Modelos de relatório

Use widgets de relatório para definir e incluir elementos do Construtor de interface do usuário (UIB), como visualizações de dados nos relatórios de status do MSIM.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Visualizações**.
3. Selecione **Configurar**.
   As Visualizações UIB predefinidas como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Nome do widget	Descrição
Equipe ativa	Exibe a lista de equipes ativas envolvidas na resolução do MSI.
Ativos afetados	Exibe a lista de ativos afetados.
Locais afetados	Exibe a lista de locais afetados.
Usuários afetados	Exibe a lista de usuários afetados.
Gráfico de pizza da colaboração	Inclui as atividades de colaboração no gráfico de pizza.
Gráfico de tendência de colaboração	Exibe as atividades de colaboração como um gráfico de tendências.
Data de resolução estimada	Exibe a data de resolução estimada até quando o MSI está estimado para ser resolvido.
Gráfico de barras dos incidentes vinculados	Exibe o gráfico de barras Incidentes vinculados.
Gráfico de tendências de incidentes vinculados	Exibe o gráfico de tendências de incidentes vinculados.
Gráfico de barras das tarefas de resposta do ISG	Exibe o gráfico Tarefas de resposta MSI.
Gráfico de barras das tarefas de resposta	Exibe o gráfico de barras Tarefas de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do widget	Descrição
Tarefas de resposta em andamento por rótulos	Exibe as tarefas de resposta em andamento por rótulos.
Tarefas de resposta atrasadas	Exibe o total de tarefas de resposta atrasadas para fechamento.
Gráfico de tendências de tarefas de resposta	Exibe o gráfico de tendências de tarefas de resposta.
Tempo decorrido desde a detecção do incidente	Exibe o tempo decorrido a partir do momento em que o incidente é detectado.
Linha do tempo	Exibe a linha do tempo dos principais eventos e marcos que ocorreram como parte do incidente de segurança grave.

Tópicos relacionados

Crie um elemento de Tipo de visualização

Use Listas de relatórios em Modelos de relatório

Use listas de relatórios para definir e incluir os artefatos de lista relacionados para gerar listas no PDF com base nos registros de lista MSI configurados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Listas**.
3. Selecione **Configurar**.
   A seção Listas de relatórios de status MSI descreve como cada lista relacionada específica é afetada desde que o incidente é criado. A seguir estão as listas de relatórios MSI predefinidas como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Listas de relatórios do ISG	Descrição
Ativos afetados	A lista relacionada de ativos afetados é exibida no relatório de status.
Locais afetados	A lista relacionada de locais afetados é exibida no relatório de status.
Usuários afetados	A lista relacionada de usuários afetados é exibida no relatório de status.
Indicadores	A lista relacionada de indicadores é exibida no relatório de status.
Incidente de segurança vinculado	A lista relacionada de exibição de incidentes de segurança vinculados no relatório de status.
Observáveis	A lista relacionada de exibição de observáveis no relatório de status.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Crie um elemento de tipo de lista

Use scripts de modelo em seus modelos de relatório

Crie um script para incluir os dados das listas relacionadas, as operações de data e quaisquer outros dados que não sejam diretamente identificáveis com pontos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este script de modelo predefinido em seus modelos de relatório para incluir quaisquer dados relacionados depois que os modelos de relatório forem configurados e personalizados.

Construa um script de modelo para exibir os dados da lista relacionada no modelo de relatório. Se você quiser utilizar e preencher qualquer script de modelo, adicione o marcador de script de modelo de marcador como: `template_script:nome do script` .

Exemplo: `template_script:msi_collab_cards`

Nota: Não é possível excluir os scripts de modelo predefinidos. Uma mensagem de erro será exibida se um usuário com função de administrador tentar excluir um registro de script de modelo se ele estiver mapeado com qualquer modelo de relatório.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Scripts do Modelo**.
3. Selecione **Configurar**.
   Estes são os Scripts de modelo predefinidos como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Nome do script do modelo	Descrição
formatted_current_date	Retorna a data e a hora locais atuais no formato DDMMYAYYY 00,00 AM ou PM. Por exemplo, 21 de janeiro de 2021 3:51 PST.
msi_active_team	Gere HTML para cartões de equipe ativos.
msi_collab_cards	Gerar HTML para cartões de atividade de colaboração.
msi_task_activities	Gerar HTML para cartões de tarefa.
msi_timeline_events	Gere HTML para cartões de evento da linha do tempo.
si_affected_users	Retorna os usuários afetados da lista relacionada em um formulário tabular.
si_assessments	Retorna os resultados da avaliação pós-incidente em um formulário tabular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do script do modelo	Descrição
si_associated_phish_emails	Retorna os e-mails de phishing associados da lista relacionada em um formulário tabular.
si_associated_phish_headers	Retorna os cabeçalhos de phishing associados da lista relacionada em um formulário tabular.
si_business_criticality	Retorna o valor de criticalidade comercial codificado por cores.
si_malicious_observables	Retorna os observáveis mal-intencionados da lista relacionada em um formulário tabular.
si_observables	Retorna os observáveis da lista relacionada em um formulário tabular.
si_priority	Retorna um valor de prioridade codificado por cores.
si_response_tasks	Retorna as tarefas de resposta da lista relacionada em um formulário tabular.
si_time_to_identify	Retorna a duração gasta no estado Rascunho e Análise.
si_time_to_resolve	Retorna o tempo para resolver o incidente.

Nota: Você também pode criar seu próprio script de modelo para incluir os dados das listas relacionadas, as operações de data e quaisquer outros dados que não sejam diretamente identificáveis com pontos, além dos scripts de modelo listados.

Visualize o Modelo de Relatório

Use a funcionalidade Visualizar para visualizar seu modelo de relatório de tempo de design para gerar e compartilhar o relatório com outras partes interessadas durante o tempo de execução do Gestão de incidentes graves de segurança espaço.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Selecione o Modelo de relatório desejado.
4. Selecione o Tipo de relatório como **E-mail** ou **PDF** baseado em sua exigência.
5. Selecione **Salvar e visualizar relatório** ação.

   A caixa de diálogo Visualizar relatório é exibida.
6. Selecione um incidente de segurança grave usando a opção Pesquisar para visualizar um relatório com o modelo selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Visualizar relatório** .
   O relatório gera uma visualização de acordo com a configuração do modelo selecionado. Se você selecionou o Tipo de relatório como **E-mail** , em seguida, a visualização está no formato de modelo de e-mail. Os relatórios de status no formato de e-mail são compatíveis com dispositivos móveis.

Crie um modelo de seção de relatório

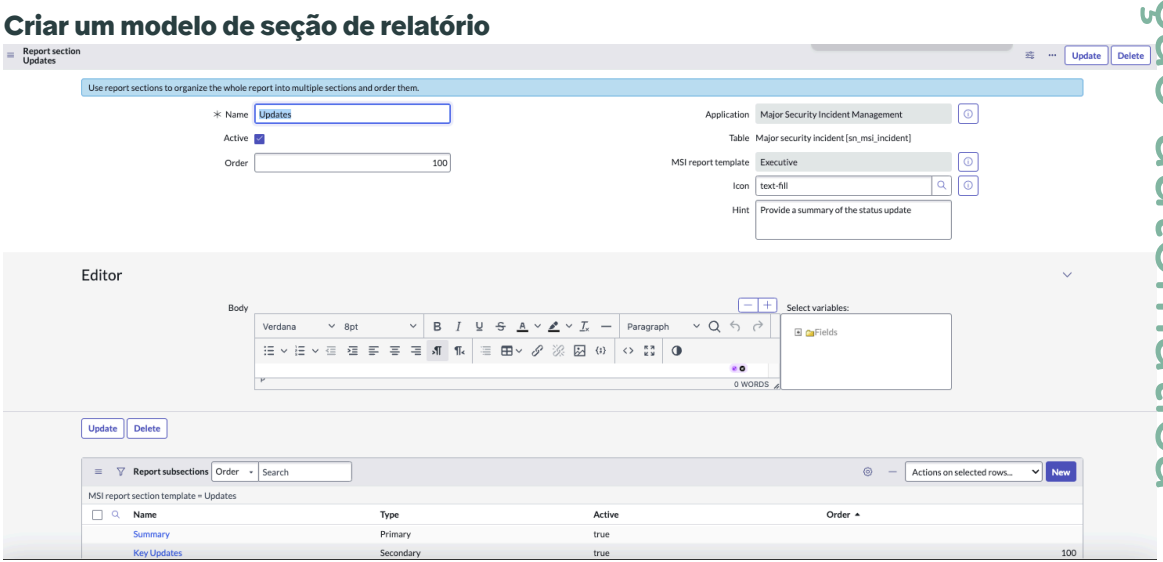
Um relatório pode ser dividido em várias seções. Use a seção Relatório para dividir o relatório em várias seções e reorganizá-las em ordem.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente.
4. Navegar até **Seções de relatório** > **Novo(a)**.
   A nova página da seção de relatório é exibida.



5. No formulário Modelo de seção Relatório, preencha os campos.

Campo	Descrição
Nome	Nome da seção Modelo de relatório. Por exemplo, Resumo.
Tabela	Nome da tabela de modelo de relatório.
Ativo	Marque a caixa de seleção para criar uma seção de relatório para o modelo selecionado no espaço do MSIM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma seção de relatório para este modelo no espaço MSIM.
Modelo de relatório do ISG	O nome do modelo de relatório MSI para o qual o relatório é dividido em seções.
Ordem	A ordem na qual as seções do relatório serão renderizadas.
Ícone	Use o ícone para exibir ícones do sistema no relatório.
Dica	Use o texto de dica para orientar a criação do relatório. No relatório, o texto da dica é exibido abaixo do título da seção.
Editor - Corpo	Defina o corpo da seção do modelo. Você pode definir o corpo da seção selecionando os tokens ou variáveis personalizados no editor.

6. Salve e. **Enviar** a nova seção de modelo de relatório.

Crie um modelo de subseção de relatório

Use a subseção do relatório para organizar ainda mais a seção em várias subseções e configurar o alinhamento e a posição usando os tipos disponíveis, como Painel lateral de texto, Primário e Secundário.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

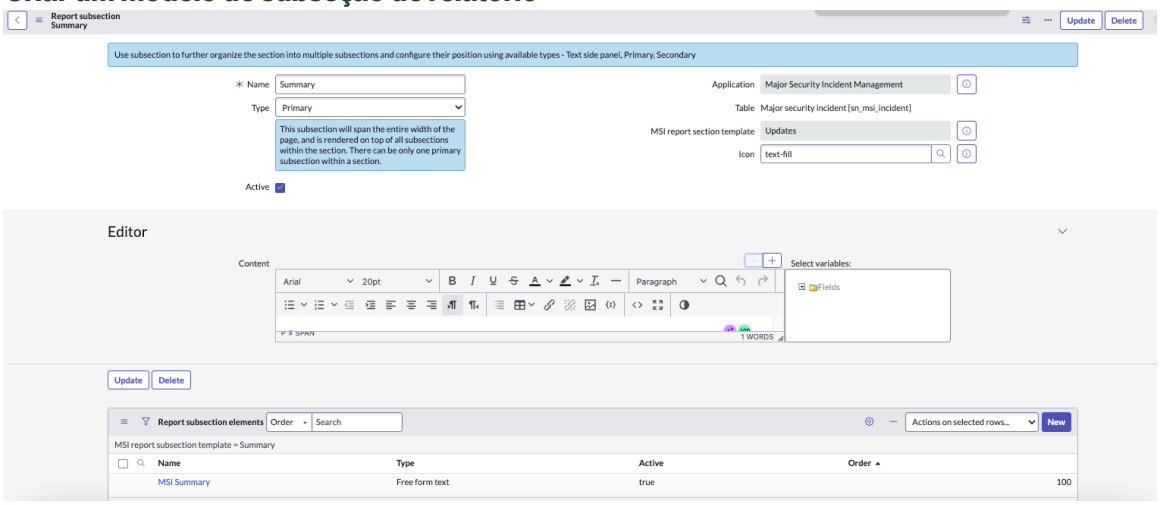
Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Navegar até **Subseções de relatório** > **Novo(a)**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um modelo de subseção de relatório



6. No formulário de subseção Relatório, preencha os campos.

Campo	Descrição
Nome	Nome da subseção Modelo de relatório. Por exemplo, escopo. **Nota:** As subseções existentes para os relatórios predefinidos são: Visão geral, escopo, andamento, explicação. ○ **Visão geral** : Exibe a visão geral como uma subseção no relatório. ○ **Escopo** : Exibe os elementos de visualização no relatório, como contadores de duração, impacto do incidente, equipes ativas e tendência de equipes ativas. ○ **Andamento** : Exibe os elementos de visualização no relatório, como Gráficos de incidentes de segurança vinculados, Gráfico de tarefas de resposta e Gráficos de colaboração.
Tipo	O tipo de subseção do relatório. Os tipos disponíveis são: ○ **Primário** : Esta subseção abrange toda a largura da página e é renderizada em cima de todas as subseções na seção. Só pode haver uma subseção primária em uma seção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Secundário** : Esta subseção abrange toda a largura da página, a menos que seja usada com o painel lateral de texto. ○ **Painel lateral de texto** : Esta subseção acompanha o painel secundário e oferece suporte somente ao texto.
Tabela	Nome da tabela de modelo de relatório.
Modelo de seção de relatório do ISG	O nome do modelo de relatório MSI para o qual você está dividindo o relatório em seções.
Ordem	A ordem na qual as subseções do relatório serão renderizadas.
Ícone	Use o ícone para indicar ou realçar o contêiner de seção no formulário de configuração de tempo de execução do relatório.
Ativo	Marque a caixa de seleção para criar uma subseção de relatório para o modelo selecionado no espaço do MSIM. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma subseção de relatório para este modelo no espaço MSIM.
Editor - Conteúdo	Defina o conteúdo da subseção do modelo.

7. Salve e. **Enviar** a nova seção de modelo de relatório.

Criar modelo de elemento de subseção de relatório

Use elementos de subseção para organizar ainda mais uma subseção em vários elementos. Os elementos de subseção ajudam a definir visualizações, listas e texto de formato livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

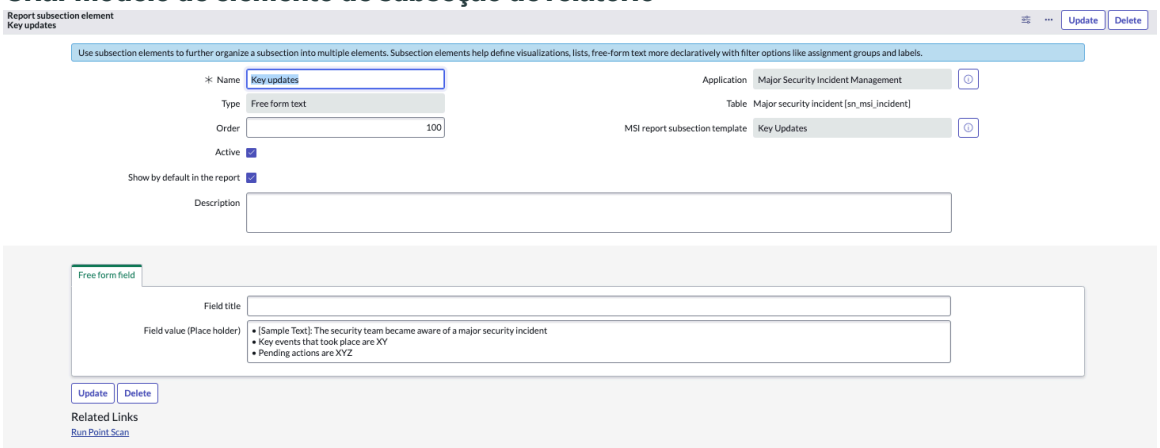
Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo(a)**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar modelo de elemento de subseção de relatório



7. No formulário Elementos da subseção Relatório, preencha os campos.

Campo	Descrição
Nome	Nome do elemento da subseção do modelo de relatório. Por exemplo, escopo. **Nota:** As subseções existentes para os relatórios predefinidos são: Contadores de duração, Impacto do incidente, Equipe ativa, Tendência da equipe ativa. ○ **Contadores de duração** : Exibe o contador de duração como um elemento de subseção, como Tempo estimado para resolver o incidente no relatório de status. ○ **Impacto do incidente** : Exibe os elementos de visualização no relatório, como os ativos afetados, os locais afetados e os usuários afetados. ○ **Equipe ativa** : Exibe os elementos de visualização no relatório, como o número de equipes ativas envolvidas no fechamento do incidente de segurança grave. ○ **Tendência de equipe ativa:** Descreve a tendência de equipes ativas em uma representação gráfica.
Tipo	O tipo de elemento da subseção do relatório. Os tipos disponíveis são: ○ Texto de forma livre ○ Visualização ○ Personalizado ○ Lista

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela	Nome da tabela de modelo de relatório.
Ativo	Marque a caixa de seleção para criar uma seção de relatório para o modelo selecionado no espaço do MSIM. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma seção de relatório para este modelo no espaço MSIM.
Mostrar por padrão no relatório	Marque esta caixa de seleção se quiser incluir a seção no relatório para renderizar rapidamente os elementos.
Modelo de relatório MSI	O nome do modelo de relatório MSI para o qual você está dividindo o relatório em seções.
Ordem	A ordem na qual as seções do relatório serão renderizadas.
Descrição	Forneça uma descrição para o tipo de elemento da subseção.

8. Salve e. **Atualização** a nova seção de modelo de relatório.

Crie um elemento de tipo de formulário livre

Crie um tipo de elemento de formulário livre para definir o texto de formulário livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo(a)**.
7. Preencha o formulário de elementos da subseção do relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione **Campo de formulário livre** opção.
   Exibe **Campo de formulário livre** seção.
9. Na guia Formulário livre, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Título do campo	Nome do título do campo. Por exemplo, Visão geral.
Valor do campo (espaço reservado)	Insira a descrição do valor do campo. Este é um exemplo de texto de Visão geral. Fizemos um bom progresso com os ativos afetados. No entanto, acabamos de descobrir que os invasores ainda estão penetrando nos sistemas, incluindo o Windows. O conteúdo de ativos Linus está em andamento, mas es–tá demorando mais do que o esperado. O novo dia de resolução estimado é de 5 dias a partir de hoje.

Crie um elemento de Tipo de visualização

Crie um tipo de elemento de visualização para definir os elementos de visualização de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo(a)**.
7. Preencha o formulário de elementos da subseção do relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione **Visualização** opção.
   Exibe **Visualização** seção.
9. No formulário Visualização, preencha os campos.

Campo	Descrição
Legenda do conjunto de visualizações	Insira o nome da legenda do Conjunto de visualizações. Por exemplo, Contadores de duração.
Visualizações	Selecione o tipo de Visualizações. Por exemplo, selecione Tempo decorrido desde a detecção do incidente, Data de resolução estimada para o tipo de subseção: Contadores de duração.

Tradução automática

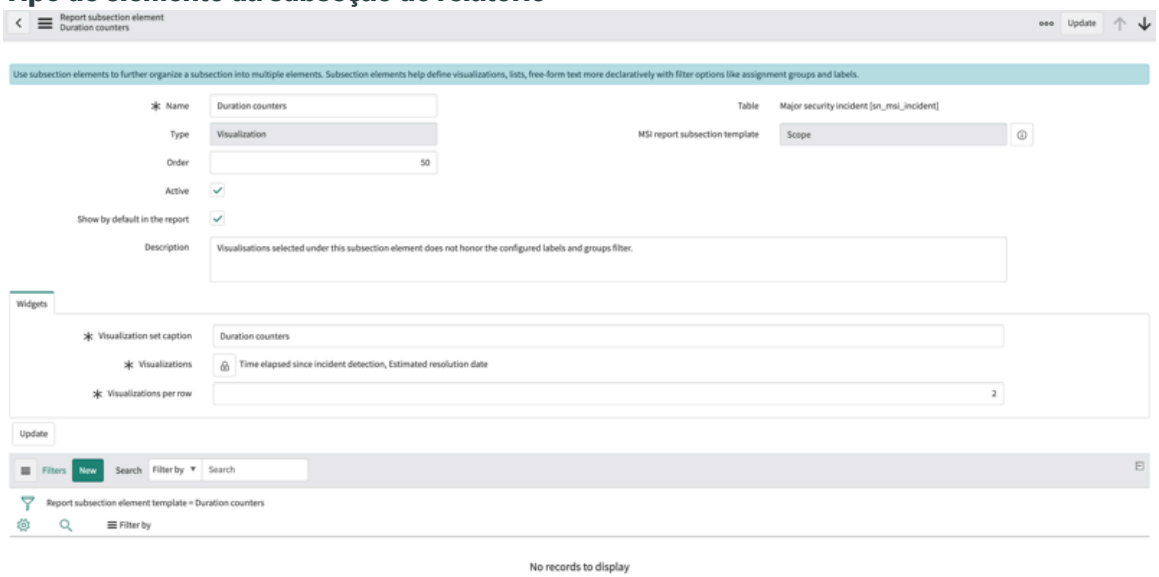
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visualizações por linha	Selecione o número de Visualizações exibidas de acordo com cada linha.

10. Selecione **Enviar**.

Example: Tipo de elemento de subseção do modelo de relatório para um Relatório de status técnico

Tipo de elemento da subseção do relatório



Crie um elemento de tipo de lista

Crie um elemento de tipo de lista, que define os elementos de lista relacionados de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo(a)**.
7. Preencha o formulário de elementos da subseção do relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione **Lista** opção.
   Exibe **Listas** seção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. No formulário Lista, preencha os campos.

Campo	Descrição
Listas	Nome das listas relacionadas associadas ao MSI. Por exemplo, observáveis, indicadores. Selecione uma lista usando a opção de pesquisa.

Crie um elemento de tipo personalizado

Crie um elemento de tipo de lista, que define os elementos de lista relacionados de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar** .
3. Abra um modelo de relatório existente e navegue até a respectiva lista Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo(a)**.
7. Preencha o formulário de elementos da subseção do relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione **Personalizado** opção.
   Exibe **Conteúdo personalizado** seção.
9. No formulário Conteúdo personalizado, preencha os campos.

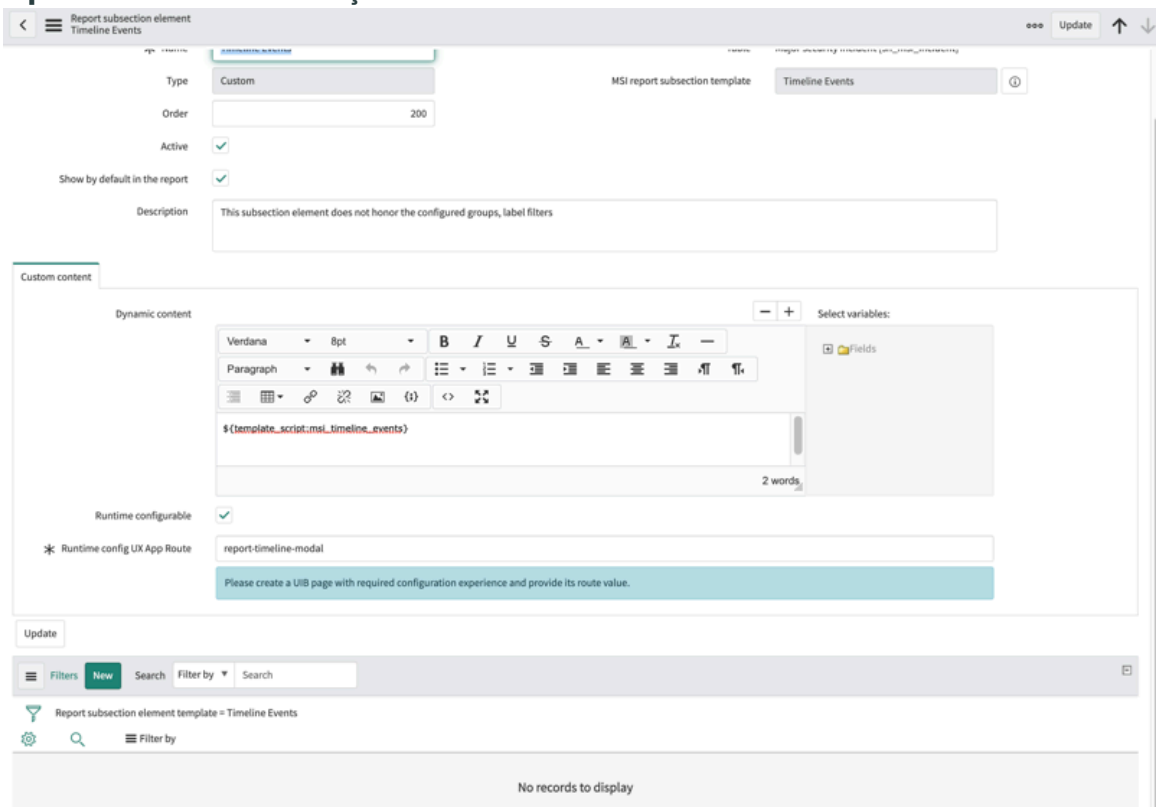
Campo	Descrição
Conteúdo dinâmico	Insira o conteúdo dinâmico, como os scripts do modelo.
Tempo de execução configurável	Marque esta caixa de seleção se o tipo de elemento personalizado for configurável para tempo de execução.
Rota da aplicação UX de configuração de tempo de execução	Insira o valor Rota da aplicação de UX da configuração do tempo de execução quando uma página do UIB for criada com a experiência de configuração necessária. **Nota:** Este campo aparece somente quando **Tempo de execução configurável** a opção está selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: A seguir está um exemplo do tipo de elemento de subseção do modelo de relatório para um Relatório de status técnico

Tipo de elemento da subseção do relatório



Adicione propriedades do sistema

Adicione propriedades do sistema para controlar o comportamento da aplicação MSIM. A seguir estão as propriedades do sistema padrão que são introduzidas como parte do Gestão de incidentes graves de segurança relatórios de status.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.export_img	Use esta propriedade para controlar a exportação de imagens. O valor padrão é definido como ATIVADO.
sn_msi.export_img_log	Use esta propriedade para habilitar o login no console do navegador. O valor padrão é definido como DESLIGADO.
sn_msi.export_img_parallel_threshold	Use esta propriedade para controlar o número máximo de solicitações paralelas para gerar as imagens a partir das configurações do widget de relatório. O valor padrão é definido como 14.
sn_msi.img_export_log	Use esta propriedade para habilitar os logs do console no navegador.
sn_msi.img_export_poll_interval	Use esta propriedade para controlar o intervalo de tempo entre pesquisas que verifica se a imagem foi gerada ou não. O tempo de intervalo de pesquisa padrão é definido como 3000 milissegundos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.export_poll_request_timeout	Use esta propriedade para controlar o tempo máximo que o sistema pode pesquisar a imagem exportada. O valor padrão é 120000 milissegundos.
sn_msi.msi_report_uib_element_js_path	Use esta propriedade para controlar o caminho genérico para capturar a imagem da parte da página do UIB.
sn_msi.report_default_style_objects	Use esta propriedade para mudar o CSS dos PDFs gerados, como tamanho da fonte, cor da fonte ou valor do campo. Por exemplo, se sn_msi.workspace_manager preferir mudar a cor da fonte do painel esquerdo do relatório de status do PDF gerado, o gerenciador do espaço poderá modificar a cor da fonte da propriedade do sistema e renderizar o PDF em uma exibição desejada.

Playbooks da Gestão de incidentes de segurança graves

Você pode invocar o fluxo do playbook da Gestão de incidentes de segurança graves automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook é compatível somente com o Designer de automação de processos (PAD) criado. A Gestão de incidentes de segurança graves fornece o playbook de solicitação jurídica com o sistema de base.

Playbook para solicitação jurídica

O playbook de solicitação jurídica fornece orientação passo a passo sobre como você pode informar o jurídico sobre o resumo mais recente de um MSI para que eles possam notificar a SEC no intervalo de tempo de 4 dias necessário para violações materiais.

Visão geral

Como gerente de incidentes, você pode usar o playbook de solicitação jurídica para informar a equipe jurídica sobre o resumo mais recente de um MSI para que eles possam notificar a SEC sobre violações materiais. Você pode usar os modelos do Designer de automação de processos (PAD) para executar as etapas no playbook de solicitação jurídica e informar a equipe jurídica adequadamente.

Este playbook pode ser usado se um incidente de segurança grave for criado ou atualizado. Você precisa ativar o playbook de Solicitação jurídica no PAD e executar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança grave:

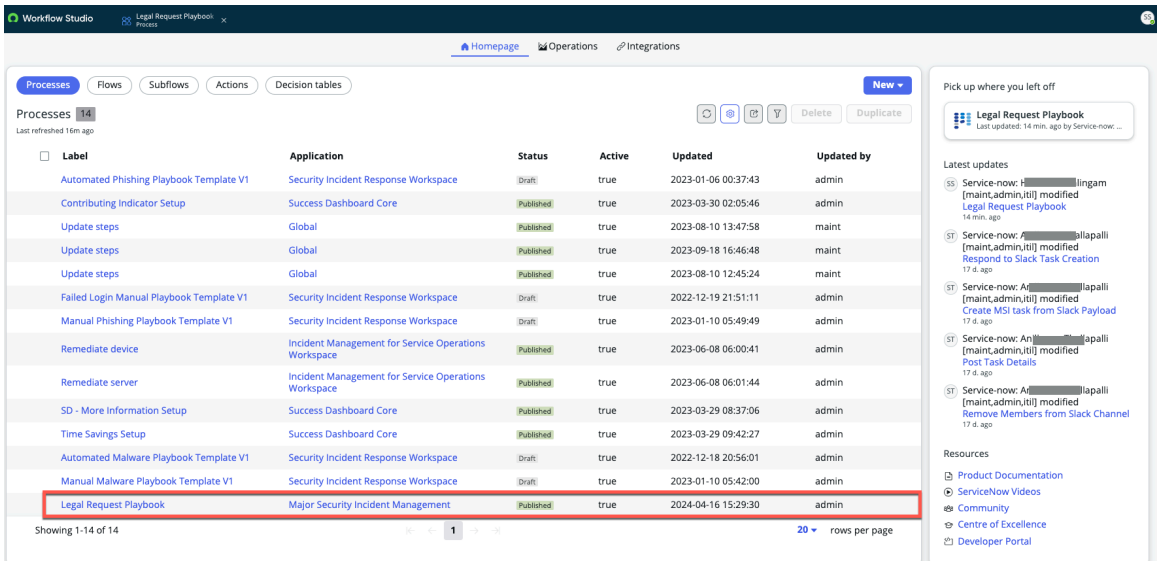
- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem determinadas atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook para solicitação jurídica



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você continua concluindo tarefas e raias. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou selecionar **Concluir** para concluir o processo de criação do direito.

Criar processos para playbook de solicitação jurídica

Use estas etapas para criar processos para playbook de solicitação jurídica no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_msi.workspace_manager.

Procedimento

1. Clique **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

   Por exemplo, Playbook de solicitação jurídica.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique em **Selecione um gatilho** .
4. Selecione **Defina suas próprias condições para quando o processo for executado** e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique em **Defina as condições do gatilho** .
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
7. Clique em **Vá para o Designer** .
   A página Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicione uma nova raia** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O painel Propriedades da raia é aberto no lado direito da IU.

9. No painel Propriedades da raia, insira os seguintes detalhes: **Nome** , **Descrição** , **Condição de execução** e **Indicar quando começar** .
. **Condição de execução** e. **Indicar quando começar** os campos indicam quando a raia seria executada.

10. Clique em **Salve e feche** .

11. Para adicionar outra raia, clique em **Adicione outra raia** .
Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, **Análise** raia começa imediatamente e não tem condição de execução. **Conter** a raia começa após a conclusão da raia anterior e tem uma condição de execução baseada no resultado de uma atividade na raia anterior.
Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.

12. Clique em **Adicione outra atividade de processo** Em uma raia específica (por exemplo, raia de análise).
O pop-up Adicionar atividade é aberto.

    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.

13. Clique em **Crie uma nova atividade** .
Uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.

15. Adicione uma condição de execução e indique quando iniciar.
Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.

16. Clique em **Exibir todas as propriedades** e habilitar **Propriedades avançadas** alterne para exibir todos os campos de experiência de atividade da definição de atividade.

Usando o playbook de solicitação jurídica

Use estas etapas para saber como você pode usar o playbook de solicitação jurídica no Espaço do MSIM e seus recursos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager.

Procedimento

1. No espaço do MSIM, abra um incidente de segurança grave.

2. Selecione **Playbook** guia.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança grave.

   Nota: Se você não vir os playbooks listados, será necessário acessar o PAD e habilitar eles para vê-los no **Playbook** guia.

3. Selecione **Playbook de solicitação jurídica** .

4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.

5. Clique em **Análise** Para ver a lista de atividades realizadas na fase Análise.
Você tem a opção de mudá-lo de acordo com seus requisitos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de mudá-los de acordo com seus requisitos. Se houver alguma atividade restante ou ação do usuário que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Rollup Framework para MSIM

Estende a capacidade de vincular os registros de origem do Gestão de incidentes graves de segurança espaço.

Visão geral

O Rollup Framework torna o fluxo de rollup configurável e extensível. Use este modelo de estrutura para configurar as informações, que podem ser acumuladas em um Incidente de segurança grave.

Anteriormente, sn_msi.workspace_manager era capaz de vincular os incidentes de segurança e os itens vulneráveis que foram propostos ou promovidos como MSI. Depois de vincular o incidente de segurança ou o item vulnerável, as informações foram acumuladas para um incidente de segurança grave. O tipo de informação necessária a ser acumulada foi codificado nos scripts.

Você pode usar o modelo de estrutura para configurar o fluxo de rollup, que oferece suporte aos seguintes recursos e também aborda os problemas existentes na aplicação:

O modelo de estrutura de rollup habilita o sn_msi.workspace_manager com os seguintes benefícios para:

- Adicione ou remova o link, propor ou promover MSI capacidades de registro em qualquer tabela, o que estende a tabela de tarefas.
- Controle o tipo de informação a ser acumulada MSI ao executar ações como vincular/propor/promover nos registros de incidentes.
- Ofereça suporte a vinculação, proposta ou promoção para incidentes de segurança, tarefas de correção e casos de segurança prontos para uso (OOTB) do ambiente clássico e Gestão de incidentes graves de segurança espaço.

A estrutura de acúmulo exibe as configurações conforme explicado na tabela a seguir.

Configurações da Estrutura de acúmulo

Nome	Descrição
Configuração de registro vinculada	Armazena as informações de tabelas de tarefas que podem ser usadas para vincular/promover/propor Incidente grave de segurança.
Acumular configuração de registro	Captura as informações que podem ser acumuladas da tabela de tarefas quando ações de link/promover/propor são executadas.
Configuração de layout de lista	Controla os rótulos e o layout da lista para várias tabelas, conforme mostrado em Gestão de incidentes graves de segurança Guias do espaço, como Impacto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações da Estrutura de acúmulo

Nome	Descrição
	do incidente, Registros vinculados e Inteligência contra ameaças.

Configure registros vinculados em Gestão de incidentes graves de segurança

Use a Configuração de registros vinculados para armazenar as informações de tabelas de tarefas que podem ser usadas para vincular/promover/propor Incidente grave de segurança.

Função necessária: admin e sn_msi.workspace_admin.

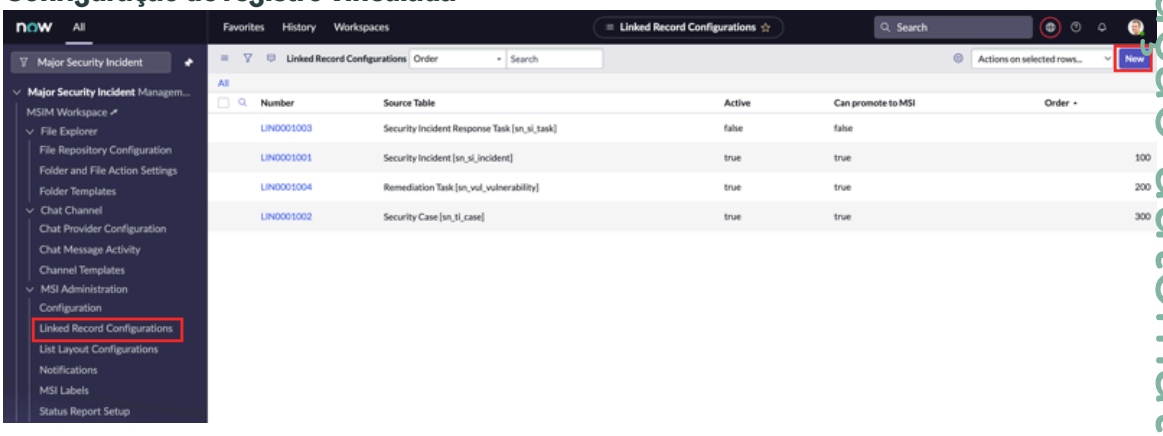
Nota: O administrador pode criar o registro e. MSIM o administrador do espaço pode atualizar o registro.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Configurações de registro vinculadas**.

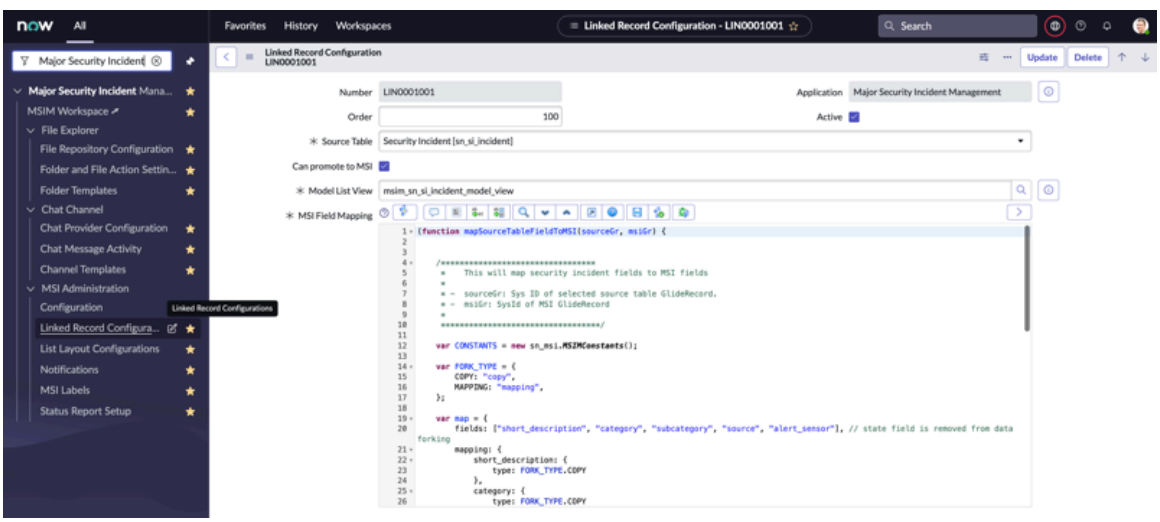
   A página Configuração de registro vinculado é exibida.

   Configuração de registro vinculada



2. Na página Configuração de registro vinculado, clique em **Novo**

   Nota: Certifique-se de que a aplicação esteja em Gestão de incidentes graves de segurança escopo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário de configuração de registro, preencha os campos.

Descrições do campo de registros vinculados

Campo	Descrição
Tabela de origem	Indica a tabela de tarefas que deve ser vinculada e acumulada Incidente grave de segurança.
Ordem	Permite controlar a ordem da tabela de origem atual no menu suspenso do espaço do MSIM. Abaixo está um exemplo de **pedido** . Consulte a imagem 1 abaixo, que é fornecida após esta tabela.
ListView do modelo	Selecione uma exibição que possa controlar o layout da lista mostrado na Lista modal de registros vinculados.
Pode promover para MSI	Marque esta caixa de seleção para confirmar se o registro é um registro primário. Abaixo está um exemplo de **Pode promover para MSI** seleção de opção. Consulte a imagem a seguir 2, que é fornecida após esta tabela. Se esta caixa de seleção estiver marcada e o valor for verdadeiro , em seguida: ○ você pode propor e promover diretamente um registro de origem para Incidente grave de segurança usando as ações de ambiente clássicas com configurações adicionais. ○ você pode vincular registros de origem a incidentes de segurança graves do ambiente clássico e MSIM espaço. ○ Gestão de incidentes graves de segurança a página de registro vinculado do espaço exibe os registros da tabela de origem vinculada. **Nota:** Se um registro puder ser proposto/promovido diretamente como um Incidente grave de segurança, em seguida, esse registro é um registro primário. Por exemplo, na configuração da tabela de tarefas Resposta de segurança, o valor de **Pode promover para MSI** É falso, pois você não pode promover diretamente a tarefa de Resposta de segurança para Incidente grave de segurança. Por isso, ele não aparece em MSIM lista suspensa da guia de registro vinculado do espaço.
MSI Mapeamento de campo	Grave um script para mapear os campos de registro de origem para um incidente de segurança grave

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	recém-criado quando o registro das tabelas de origem estiver em processo de ser proposto ou promovido. Este script é executado somente quando **Pode promover para MSI** o valor é verdadeiro.

Imagem 1: Ordem de exibição da lista de registros vinculados

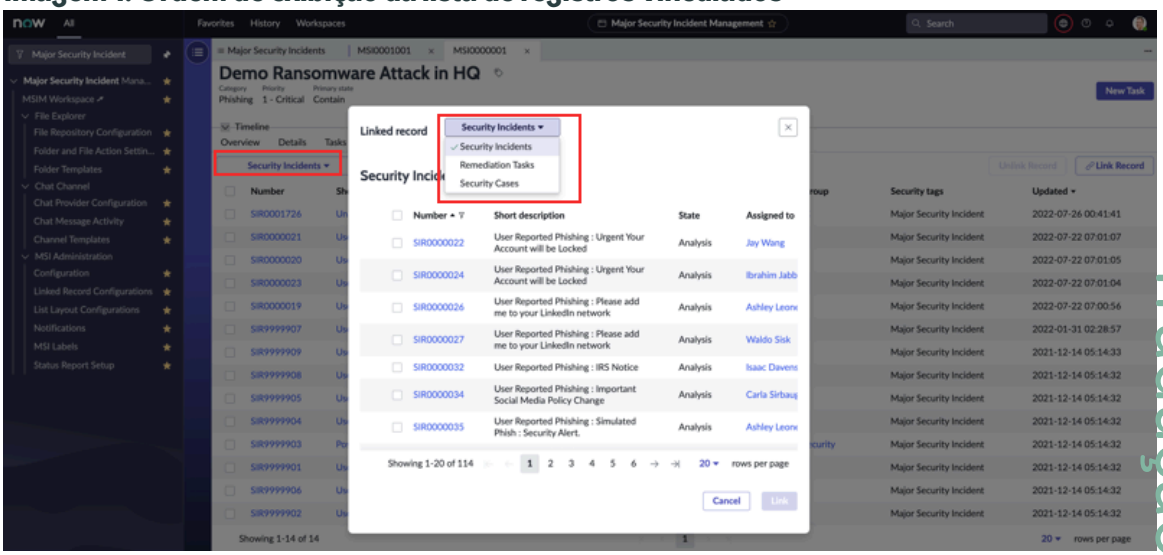
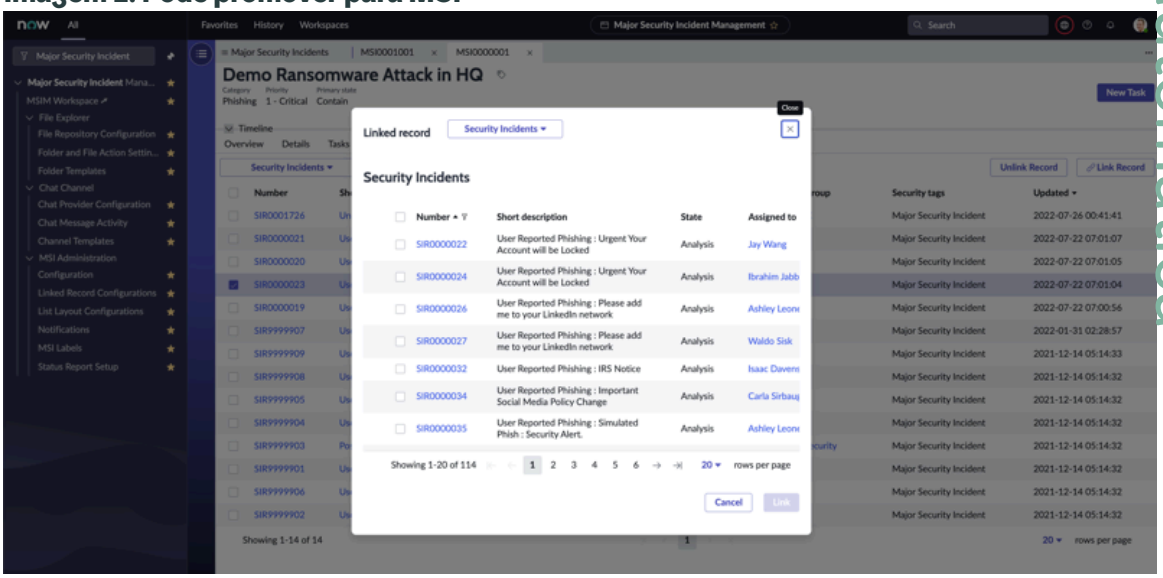


Imagem 2: Pode promover para MSI



Tradução automática

Configurar registros de acúmulo em Gestão de incidentes graves de segurança

Configurar registros de acúmulo em Gestão de incidentes graves de segurança Controlar as informações, que serão acumuladas quando o registro de origem for vinculado/proposto/promovido como Incidentes de segurança graves.

Função necessária: admin e sn_msi.workspace_admin.

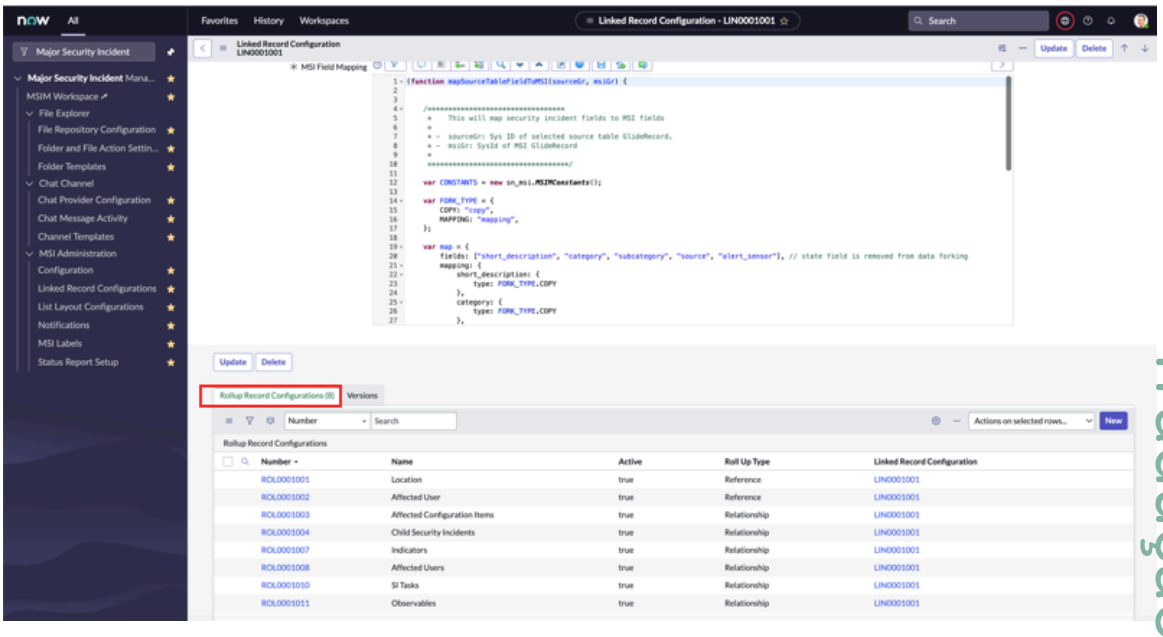
Nota: O administrador do sistema pode criar o registro e o administrador do espaço MSI pode atualizá-lo.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

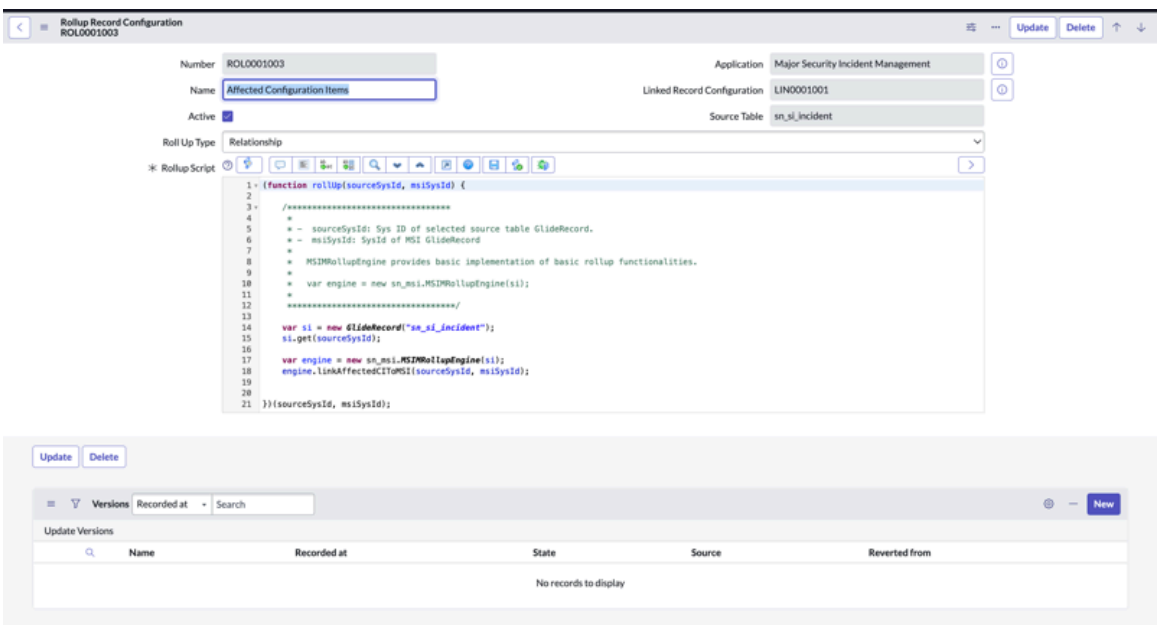
Procedimento

1. Navegar até **Resposta a incidentes de segurança graves** > **Configuração de registros vinculados**. A página Configurações de registro vinculado é exibida.
2. Selecione ou crie um novo registro vinculado e navegue até **Acumular configuração de registro** da mesma página.

Seção Configuração de registro de acúmulo



3. Clique em **Nova**.



4. Na página de configuração, preencha os detalhes.

Acumular configuração de registro

Nome do Campo	Descrição de Campo
Nome	Indica o nome do registro de acúmulo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição de Campo
Ativo	Marque esta caixa de seleção para implementar a configuração atual quando ocorrer o rollup do registro de origem.
Configuração de registro vinculada	Indica um número exclusivo, que se refere à configuração de registros vinculados primários e somente leitura.
Tabela de origem	O nome da tabela de origem usado na configuração de Registro vinculado, que é somente leitura.
Tipo de Rollup	Descreve o tipo de informação que deve ser acumulada. ○ **Relacionamento** : Selecione esta opção se os dados precisarem estar presentes como uma lista relacionada. ○ **Referência** : Selecione esta opção se os dados estiverem presentes como um campo de referência no formulário da tabela de origem.
Script de Acúmulo	Se o tipo de rollup for: **Relacionamento** . **Rollup script** o campo está habilitado, o que permite gravar script e pode ser usado para acumular informações. Aqui, o script receberá as entradas que contêm informações do registro de origem e do incidente de segurança grave. O script deve ser capaz de encontrar as informações das tabelas de relacionamento e do rollup para a tabela Registro vinculado (sn_msi_m2m_child).
Campo de origem	Se o tipo de rollup for: **Referência** . **Campo de origem** está disponível. Isso permite que você selecione o campo de referência da tabela de origem que contém as informações que precisam ser acumuladas.
Campo de destino	Se o tipo de rollup for: **Referência** . **Campo de destino** está disponível. Isso permite que você faça referência ao campo da tabela Registro vinculado (sn_msi_m2m_child) e armazene os dados presentes no Campo de origem selecionado e no registro da Tabela de origem.

Escrevendo script para rollup

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

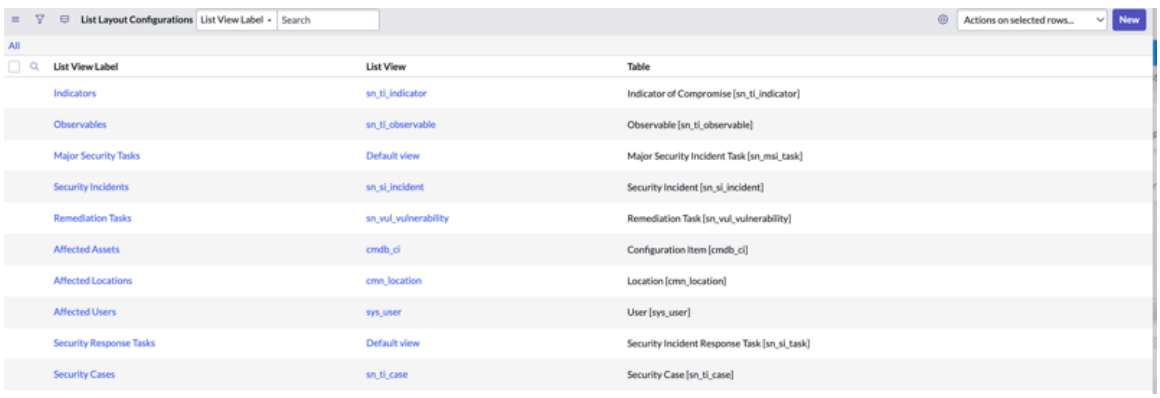
Nome	Descrição
Entradas	• SourceSySID: Sys ID do registro da tabela de origem que está sendo vinculado/proposto/promovido. • MsiSysId: Sys ID do incidente de segurança grave ao qual o registro de origem está sendo vinculado/proposto/promovido.
Saída	Nenhum valor de retorno de saída.
Responsabilidade	O script deve acumular informações para a tabela Registro vinculado (sn_msi_m2m_child). • Usar SourceSySID para consultar dados ServiceNow tabelas de relacionamento. • Depois que os dados forem obtidos, acumule-os em um Registro vinculado (sn_msi_m2m_child) usando MSIRollupEngine utilitário para acumular dados.

Configure o Layout da lista em Gestão de incidentes graves de segurança

Configure o layout da lista para personalizar o layout e os rótulos usados em Gestão de incidentes graves de segurança Espaço como Impacto do incidente, Registros vinculados e Inteligência contra ameaças.

Função necessária: admin e sn_msi.workspace_admin.

Nota: O administrador do sistema pode criar o registro e o administrador do espaço MSI pode atualizá-lo.



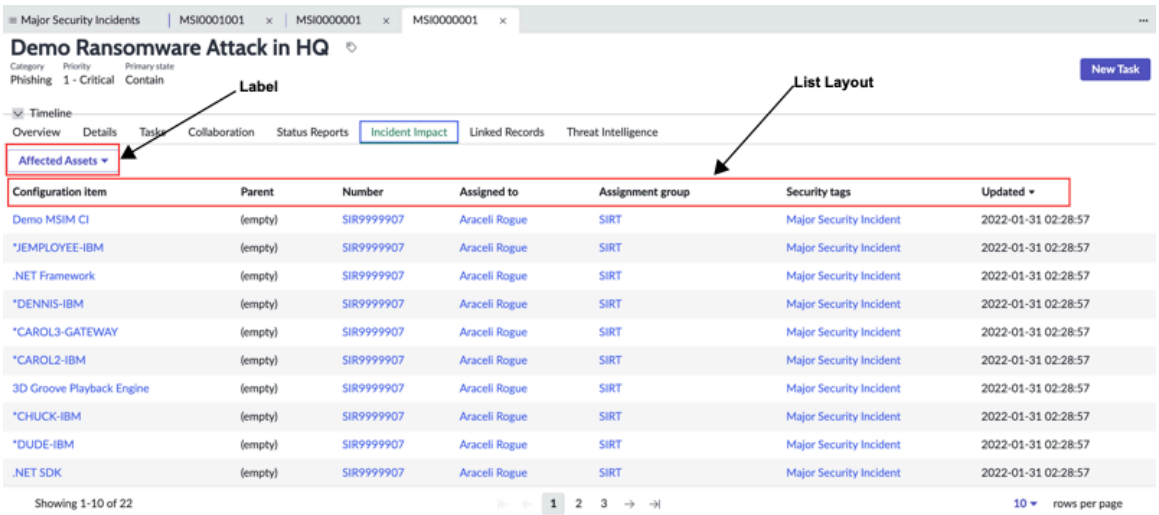
As configurações de layout de lista já foram enviadas para as tabelas conhecidas existentes mostradas em Gestão de incidentes graves de segurança espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se você quiser renderizar a exibição personalizada para as tabelas existentes, atualize o respectivo registro da tabela na configuração de layout de lista com a exibição de lista personalizada.
- Para novas tabelas de tarefas, você pode criar uma nova configuração de Layout de lista para renderizar a exibição de lista personalizada e os rótulos. Para obter um procedimento mais detalhado, consulte Como fazer Etapa 4. Crie uma exibição para uma nova guia Registro vinculado para um Caso de segurança



Exemplo de implementação de caso de uso de acúmulo para um caso de segurança

As etapas a seguir explicam um exemplo de caso de uso sobre como adicionar suporte para vincular/propor/promover a Incidente de segurança grave para uma tabela de Caso de segurança.

- Etapa 1. Criar configuração de registro vinculado para um caso de segurança
- Etapa 2. Criar uma exibição para a janela modal para um Caso de segurança
- Etapa 3. Crie ações de IU para a tabela de origem para um caso de segurança
- Etapa 4. Crie uma exibição para uma nova guia Registro vinculado para um Caso de segurança
- Etapa 5. Adicione ACLs (Access Control Lists, listas de controle de acesso) para Gestão de incidentes graves de segurança usuários do espaço
- Etapa 6. Crie regras de negócio para um caso de segurança
- Etapa 7. Criar configurações de registro de acúmulo

Etapa 1. Criar configuração de registro vinculado para um caso de segurança

Crie uma configuração de registro vinculado para um caso de segurança.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

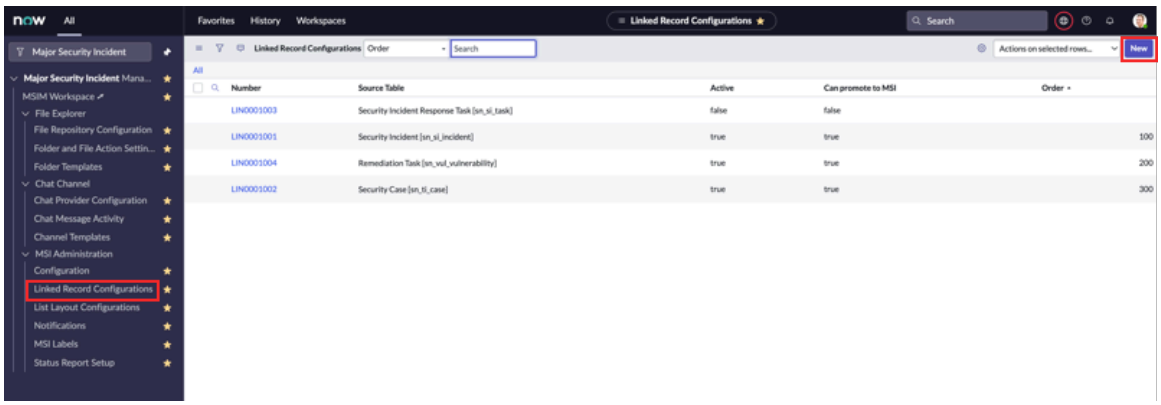
Nota: O administrador do sistema pode criar o registro e o administrador do espaço MSI pode atualizá-lo.

Tradução automática

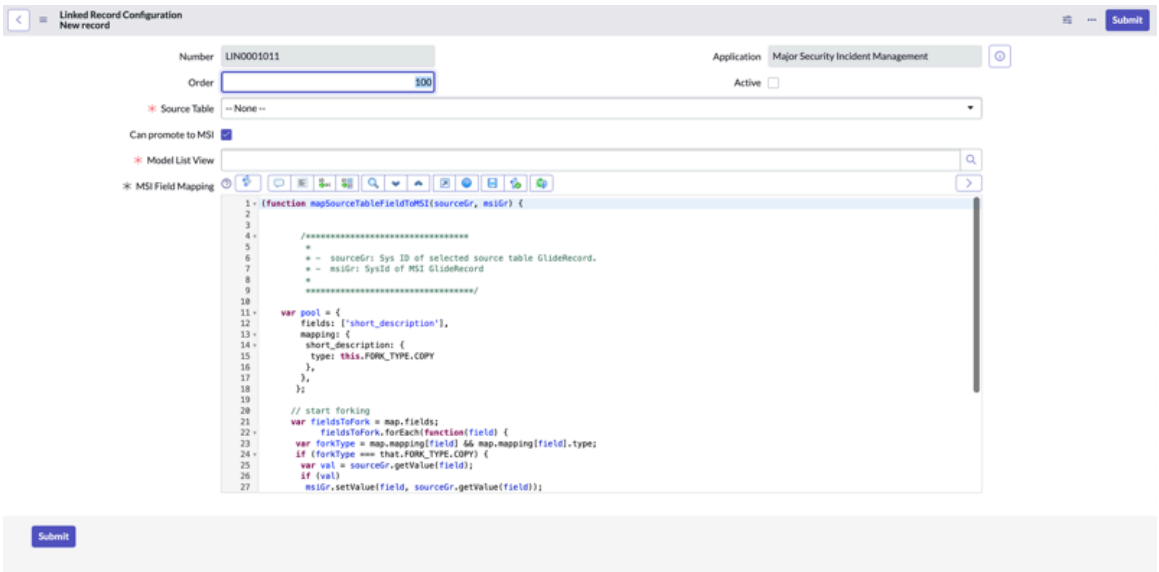
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. PESQUISE a Configuração de registro vinculado na navegação à esquerda.
2. Clique em **Nova**.



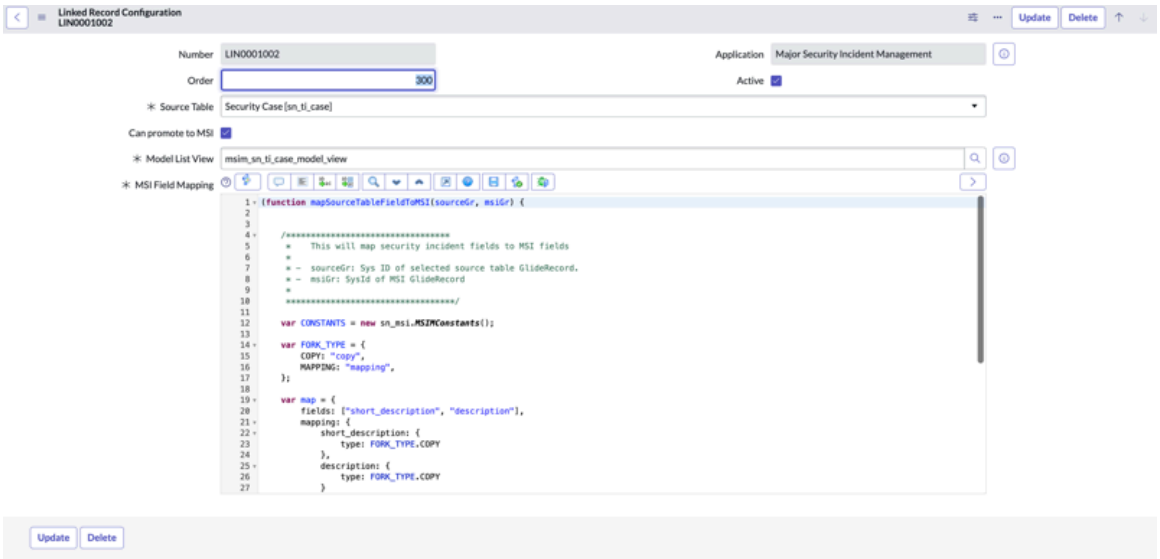
3. Preencha o formulário com as colunas necessárias e escreva um script de mapeamento de campo.



4. Agora, você criou uma configuração de registro vinculado para o Caso de segurança adicionando os valores conforme descrito na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nome	Descrição
Tabela de origem	Caso de segurança (sn_ti_case). Neste exemplo, vincule/promova/proponha um caso de segurança como MSI.
Ordem	Valor de entrada: 300 **Nota:** Menor A ordem tem precedência sobre as ordens mais altas. Como um Caso de segurança tem uma ordem maior do que o Incidente de segurança e a Tarefa de correção, ele aparecerá na última sequência.
Pode promover para MSI	Verdadeiro, marque esta caixa de seleção para promover o caso de segurança para MSI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: ◦ Vincular e desvincular registros de casos de segurança a incidentes de segurança graves do Gestão de incidentes graves de segurança espaço. Além disso, a funcionalidade Desvincular registro está visível somente para os registros vinculados. ▪ Isso habilitará o link, a promoção e a proposta de Caso de segurança para Incidente de segurança grave usando ações de ambiente clássicas, mas essas ações de IU não estarão disponíveis prontas para uso. Cada ação de IU precisa ser criada manualmente. Para obter mais informações, consulte Etapa 3. Crie ações de IU para a tabela de origem para um caso de segurança. ▪ A ação de IU Vincular/Promover/Propor estão disponíveis para Incidente de segurança, Tarefa de correção e Caso de segurança prontos para uso. ◦ A página de registro vinculado do espaço do MSIM mostrará os registros de caso de segurança vinculados. Consulte a imagem abaixo 1 para exibir as opções disponíveis depois de marcar esta caixa de seleção.
Exibição de lista modal	msim_sn_ti_case_model_view **Nota:** Esta exibição contém campos e ordem de campos mostrados na exibição de lista no modal de registro de link no espaço MSIM. Para obter mais informações, consulte Etapa 2. Criar uma exibição para a janela modal para um Caso de segurança. Consulte a imagem abaixo 2 para exibir a partir do **Registros vinculados** página.
Script de mapeamento de campo	Este script descreve os campos do registro de tabelas de origem que serão mapeados para o incidente de segurança grave recém-criado quando o registro de tabelas de origem for proposto ou promovido. que receberá entradas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	○ SourceGr: Objeto de registro do Glide caso de segurança ○ MsiGr: Objeto de registro do Glide incidente de segurança grave O script lerá a descrição resumida do caso de segurança e o copiará como título para o incidente de segurança grave.

Imagem 1: Pode promover para MSI

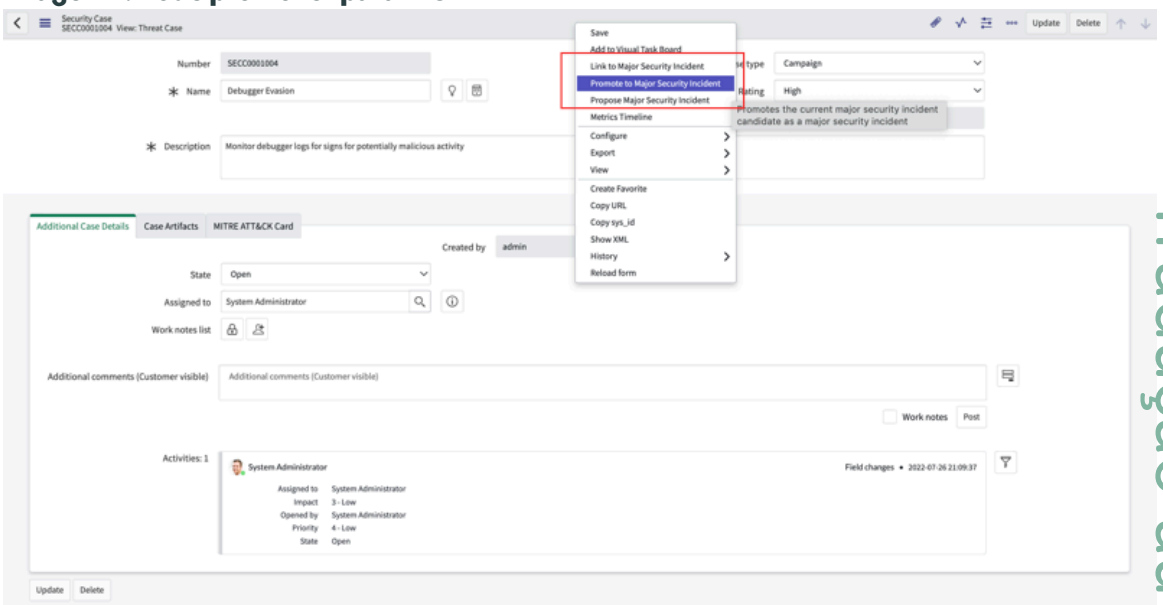
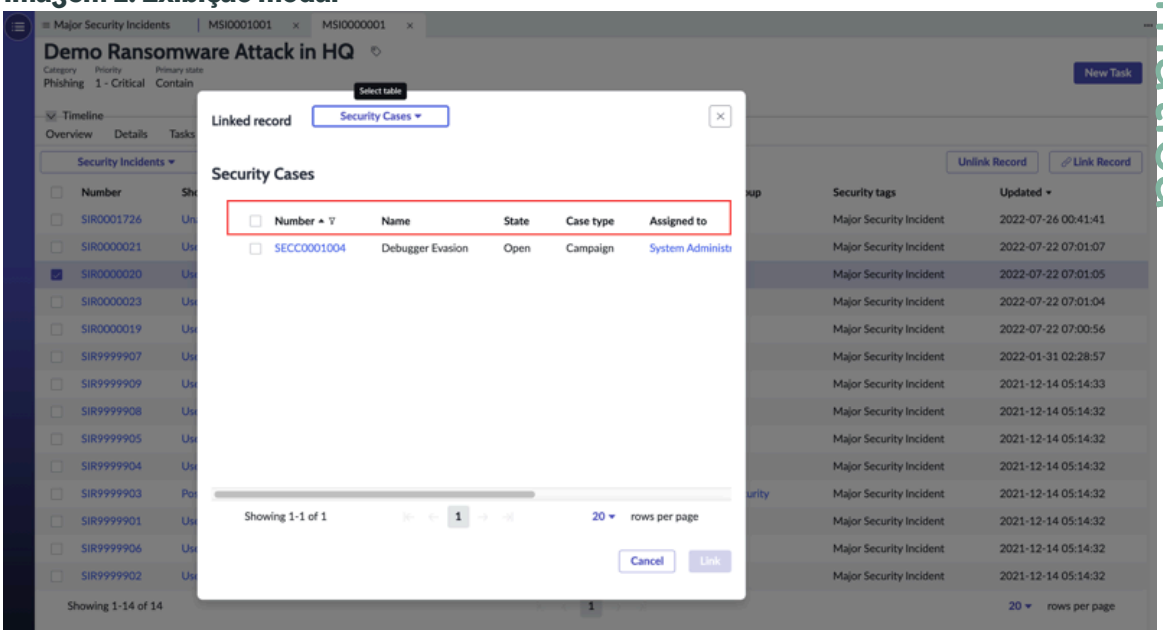


Imagem 2. Exibição modal



Etapa 2. Criar uma exibição para a janela modal para um Caso de segurança

Criar uma exibição para a janela modal para um Caso de segurança.

Tradução automática

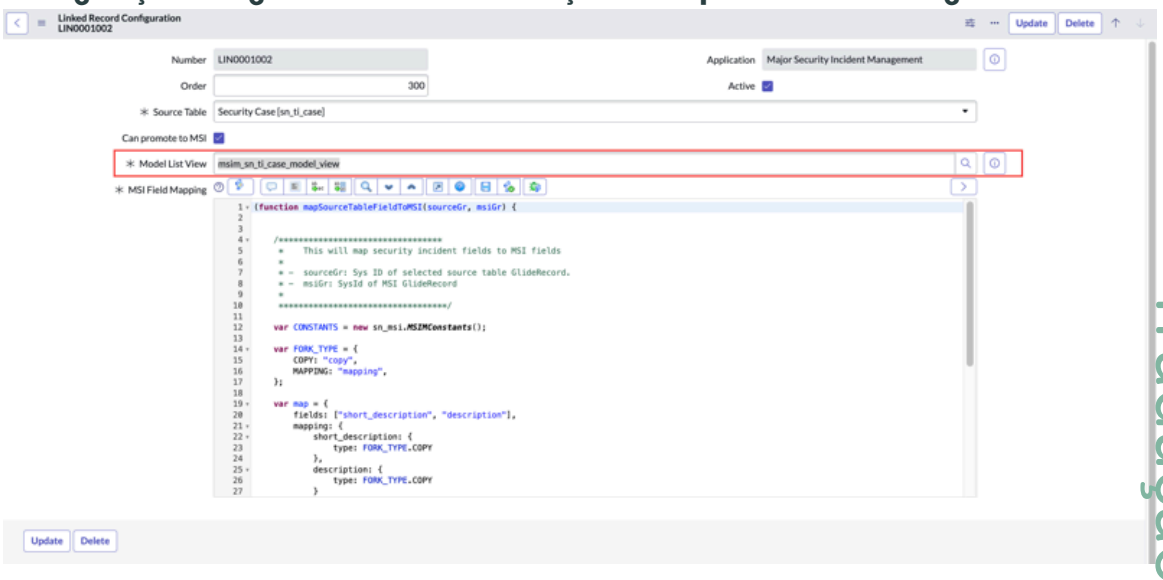
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Principal consideração:

- Por padrão, a lista modal de registro vinculado mostrará somente o. **Padrão** layout da lista. Se você quiser personalizar o layout da lista, poderá fazer isso usando **Exibição personalizada** Na Tabela de origem.
- Se você quiser renderizar a exibição personalizada, a exibição personalizada também deverá ser selecionada na Configuração de registro vinculado para a tabela de origem.

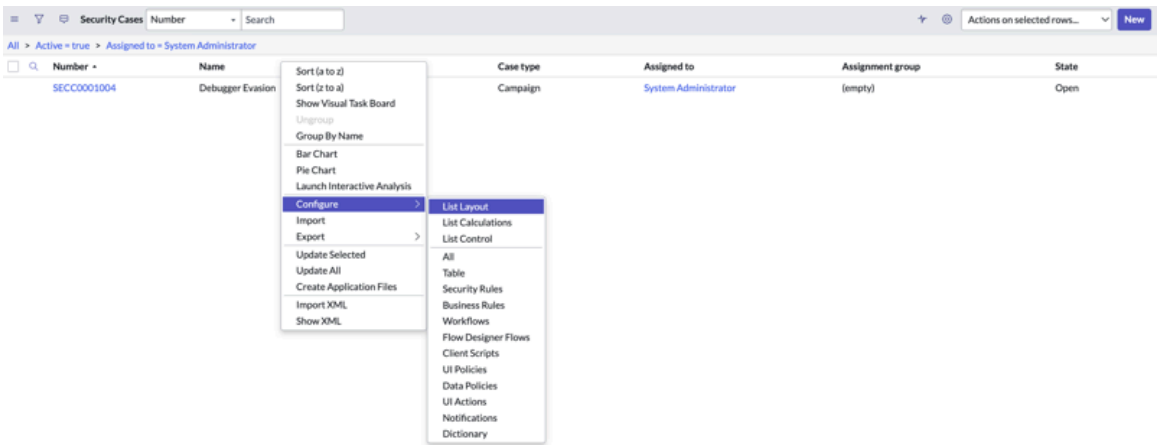
Configuração de registro vinculado da exibição modal para a tabela de origem



Função necessária: administrador

Procedimento

1. Vá para a tabela de origem e clique em **Configurar** > **Layout de Lista**.



2. Ir para **Exibição em lista** > **Nome de exibição**.
3. Clique em **Novo** Na lista suspensa Nome da exibição e crie uma nova exibição, por exemplo, msim_sn_ti_case_modal_view.
4. Selecione a exibição recém-criada.
   Uma vez selecionado, você pode escolher os campos obrigatórios na lista Disponível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Salvar**.
6. Navegar até **Menu** > **Visualizações** para verificar se a exibição foi renderizada corretamente.

Etapa 3. Crie ações de IU para a tabela de origem para um caso de segurança

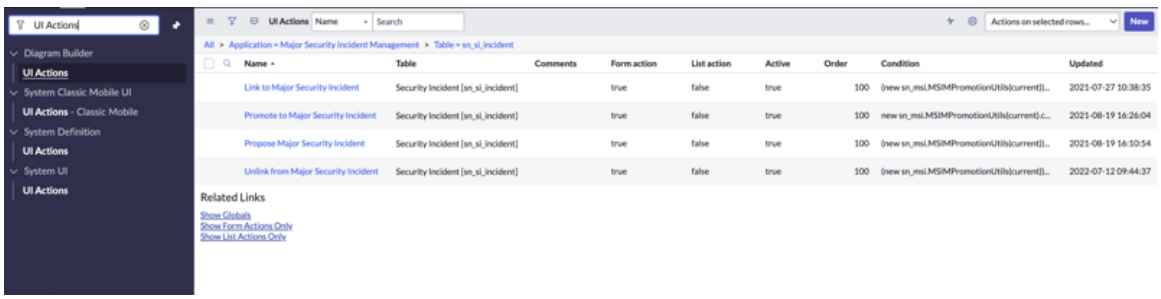
Crie ações de IU para a tabela de origem para um caso de segurança.

Antes de Iniciar

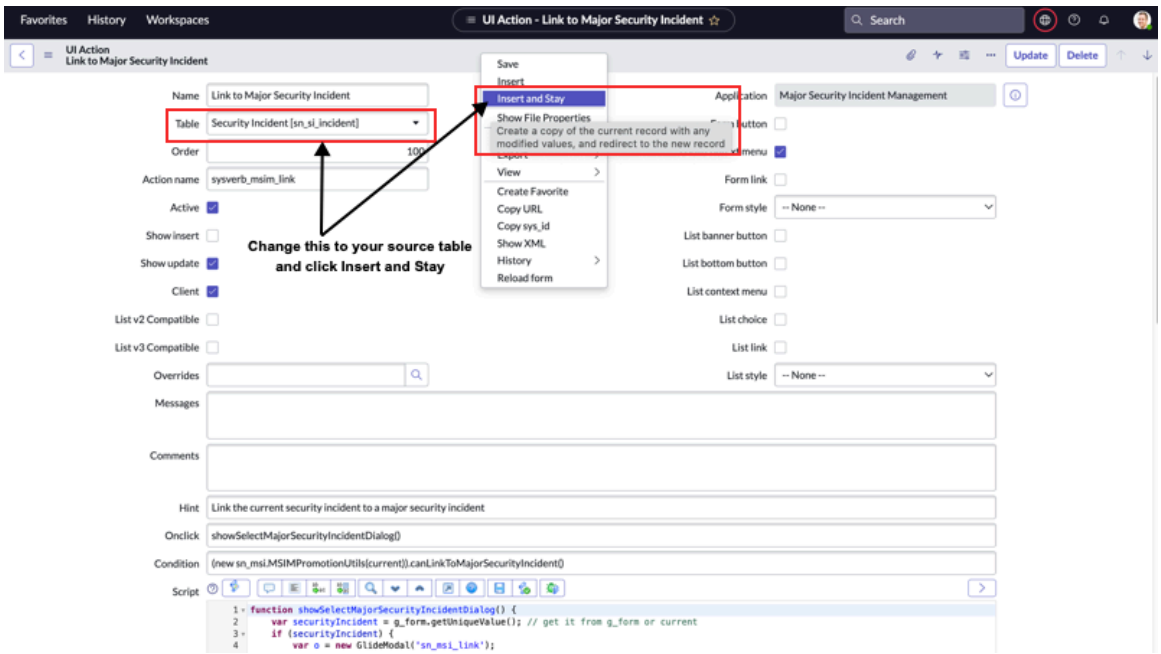
Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Ações de IU**.
2. Execute a opção Filtro para filtrar a lista **Aplicação** Gestão de incidentes de segurança graves e. **Tabela** : sn_si_incident.



3. Selecione cada ação de IU uma por uma e salve os detalhes da tabela de origem.



4. Repita as mesmas etapas acima para as seguintes ações de IU:
   - Link para Incidente de segurança grave
   - Incidente grave de segurança proposto
   - Desvincular de um incidente de segurança grave
   - Promover a incidente de segurança grave

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

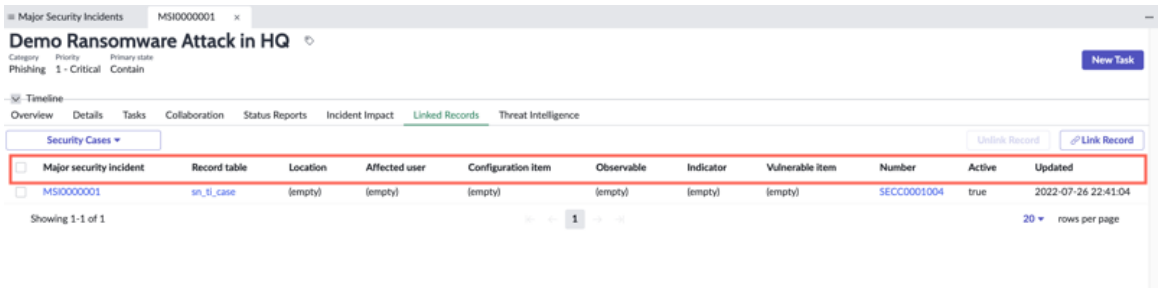
Etapa 4. Crie uma exibição para uma nova guia Registro vinculado para um Caso de segurança

Personalize o layout de Lista para uma tabela de Caso de segurança quando ele for exibido na página Vincular registros com Gestão de incidentes graves de segurança espaço.

Antes de Iniciar

Pré-requisitos:

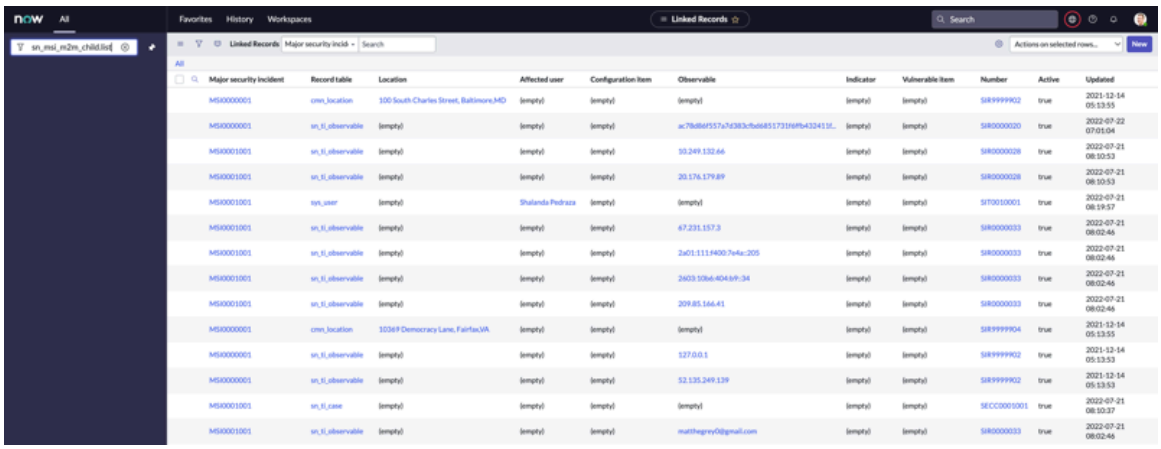
- Escolha a coluna que deve estar visível quando uma lista for renderizada para uma tabela de Caso de segurança.
- Escolha a ordem dos campos a serem exibidos na lista suspensa.



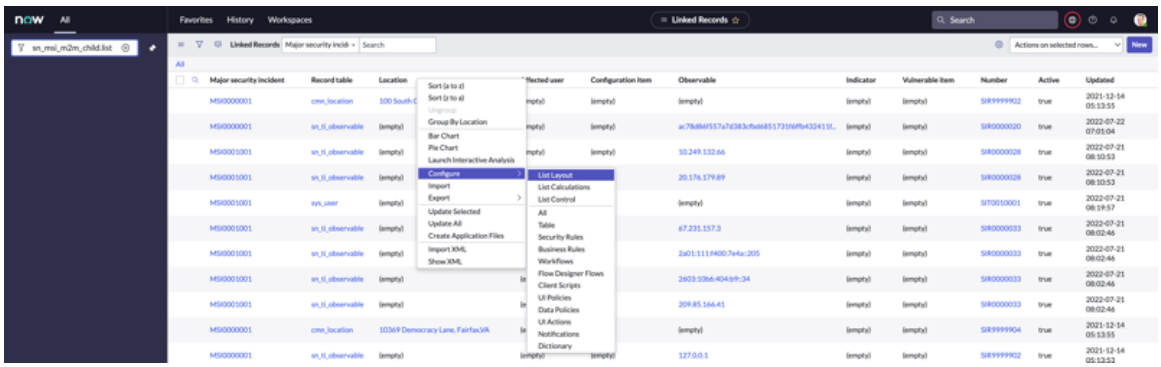
Função necessária: administrador

Procedimento

1. Pesquisar **sn_msi_m2m_child.list** usando a navegação à esquerda.
   A tabela Registros vinculados é exibida.



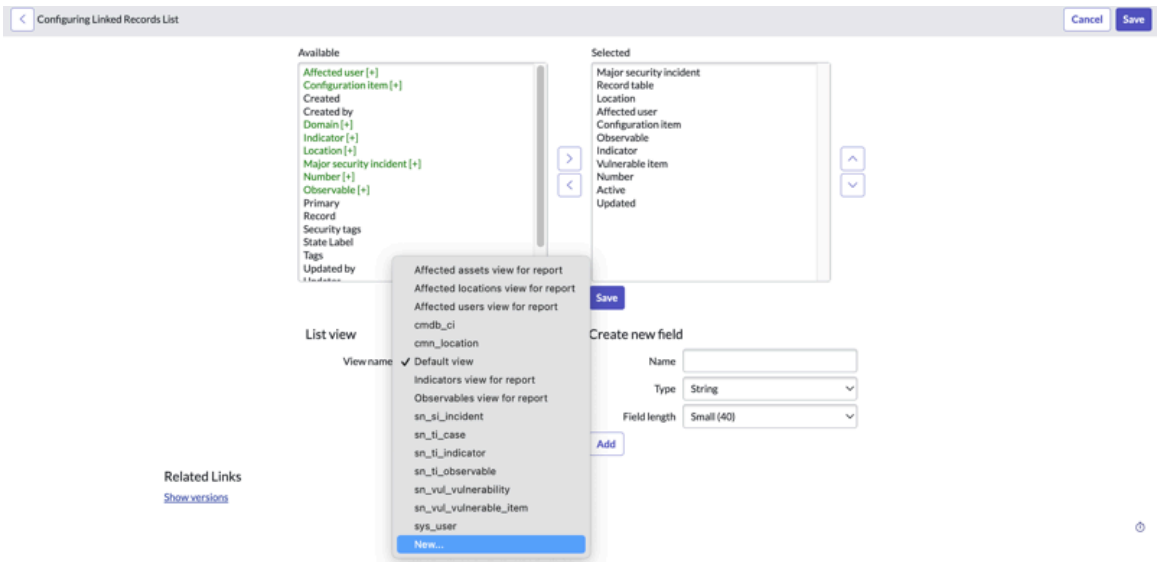
2. Clique com o botão direito do mouse no cabeçalho e selecione **Configurar** > **Layout de Lista**.
   A página Configuração da lista de registros vinculados é exibida.



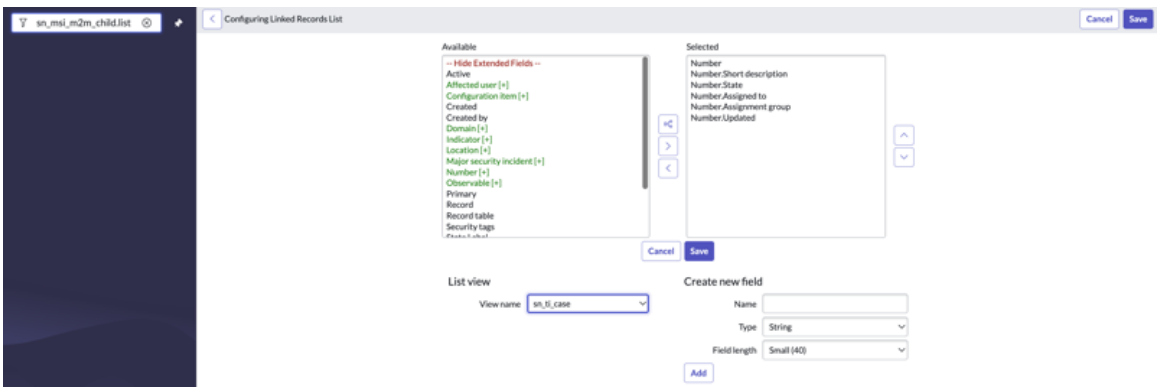
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

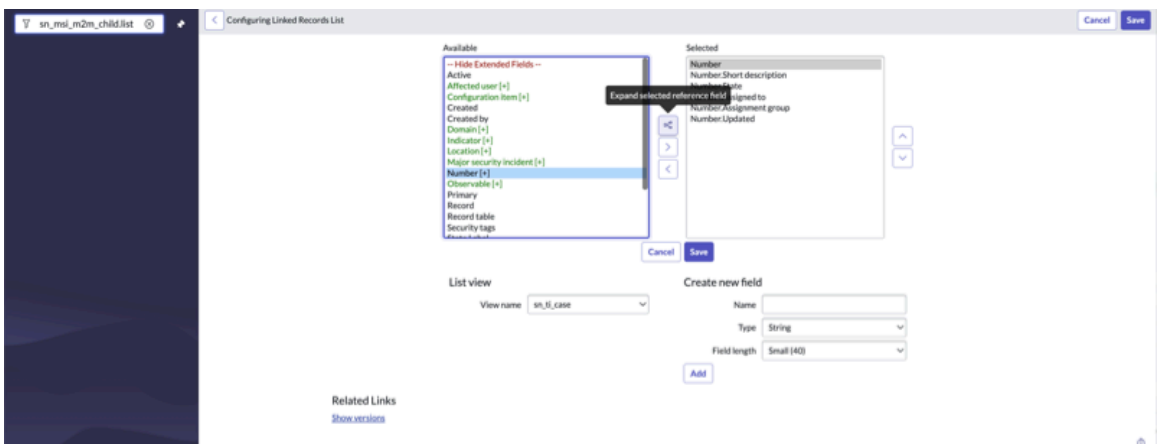
3. Ir para **Exibição da lista** > **Nome de exibição**.
4. Selecione **Novo** Na lista suspensa Nome da exibição.



5. Selecione as colunas que serão renderizadas na exibição de lista do espaço.
   O registro do caso de segurança é armazenado no **Número** coluna. Para renderizar informações de um caso de segurança, você deve colocar pontos no **Número** coluna.



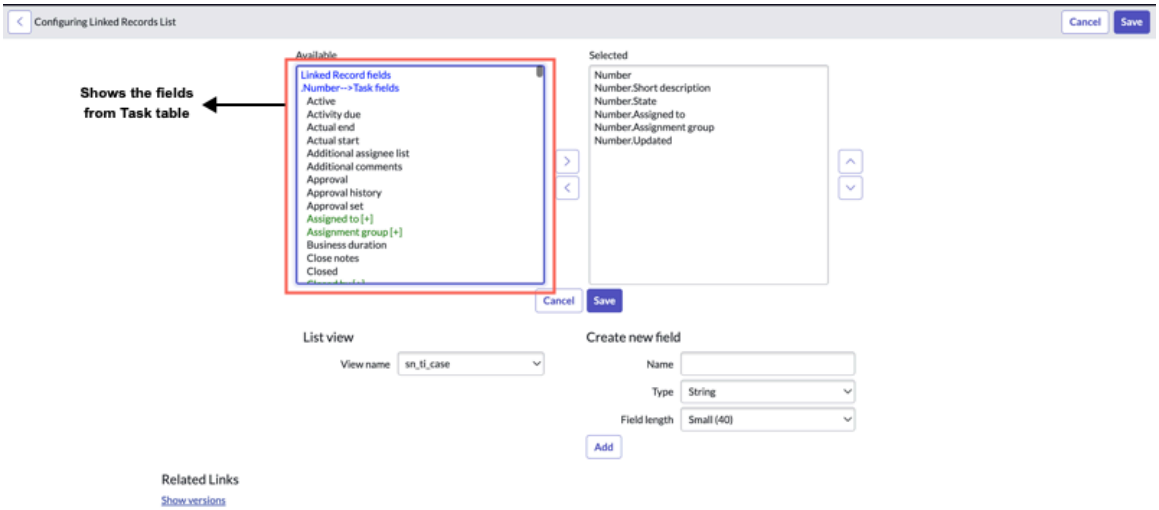
   a. Para referência com pontos, primeiro selecione **Número** Na lista Disponível e clique em **Expandir Campo de referência selecionado** .



   b. Expanda as colunas de **Número** Para selecioná-los e movê-los para a lista Selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Clique em **Salvar** para salvar e criar uma exibição.

6. A próxima etapa é renderizar a exibição criada em Gestão de incidentes graves de segurança, você precisa criar um **Configuração de Layout de Lista** .

a. PESQUISE **Configuração de Layout de Lista** usando a navegação à esquerda.

b. Clique **Administração do MSI** > **Configurações de Layout de lista**.

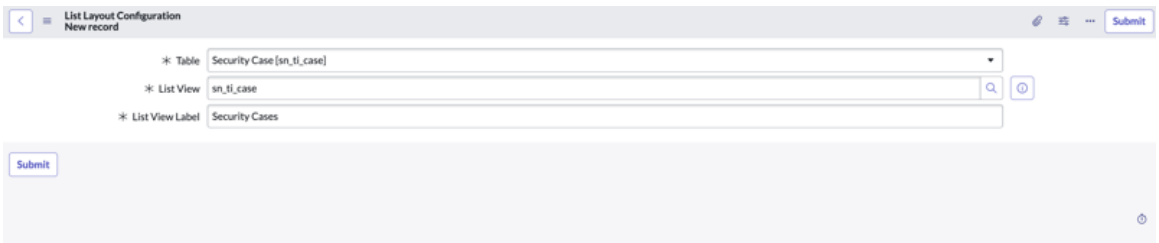
c. Clique em **Novo** para criar uma nova configuração.

d. Selecione a tabela de origem na coluna Tabela e selecione a exibição recém-criada no campo Exibição de lista.

e. . **Exibição de lista** rótulo permite que você controle rótulos quando a mesma tabela de origem é renderizada no Gestão de incidentes graves de segurança espaço.

f. Salvar o registro.

Nota: Depois que o registro for salvo, navegue até Gestão de incidentes graves de segurança espaço para exibir a exibição de lista renderizada e o rótulo no espaço.



Etapa 5. Adicione ACLs (Access Control Lists, listas de controle de acesso) para Gestão de incidentes graves de segurança usuários do espaço

Adicione ACLs (Access Control Lists, listas de controle de acesso) para Gestão de incidentes graves de segurança usuários do espaço.

Antes de Iniciar

Função necessária: administrador

Nota: As permissões necessárias para vincular e desvincular recursos são controladas pelo sn_msi.linkedsivi_read função.

Gestão de incidentes graves de segurança a persona contém a função sn_msi.linkedsivi_read.

Tradução automática

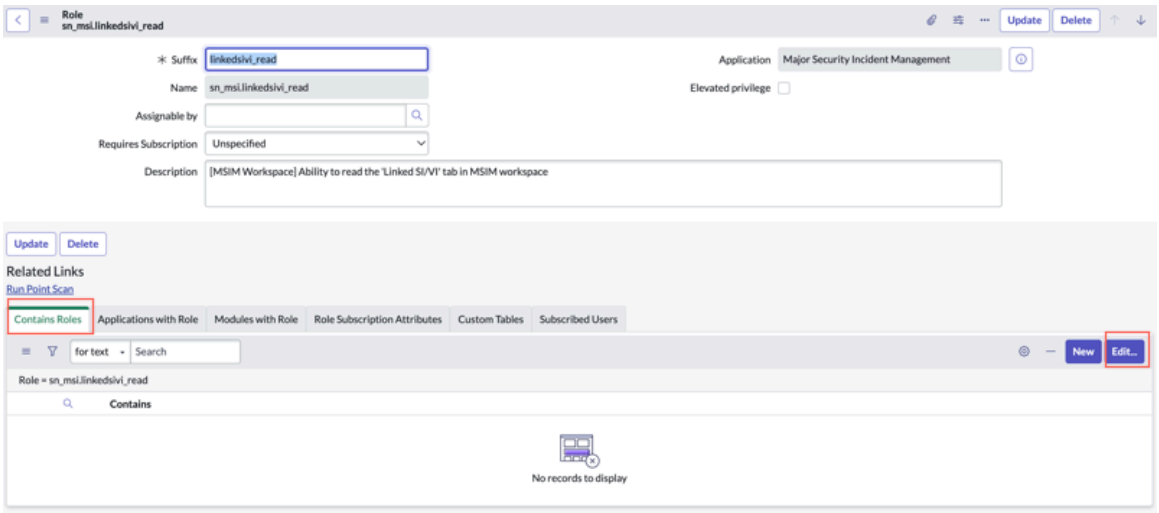
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. sn_msi.workspace_admin (administrador do Espaço do MSIM)
2. sn_msi.workspace_manager (gerenciador do Espaço do MSIM)
3. sn_msi.workspace_responder (respondente do Espaço MSIM)

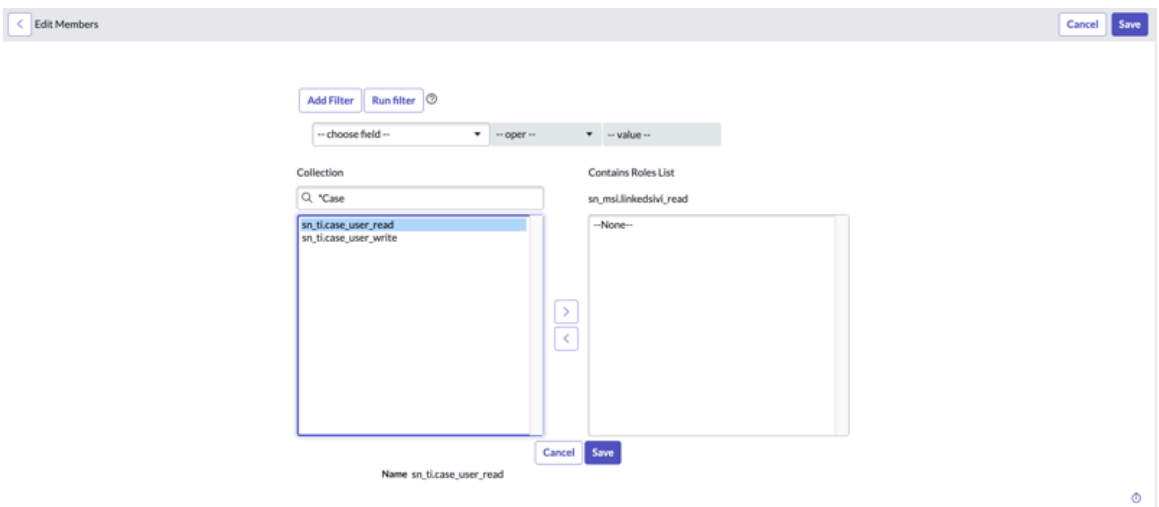
Nota: Para qualquer tabela de origem, certifique-se de que as funções necessárias sejam adicionadas ao sn_msi.linkedsivi_read função.

Procedimento

1. Navegar até **Administração de Usuários** > **Funções** e pesquise **sn_msi.linkedsivi_read** função.
2. Clique em **Editar** Na seção Lista relacionada Contém funções.



3. Certifique-se de que as funções da tabela de origem sejam adicionadas na seção Contém funções.
   A página Editar membros é exibida para configurar as funções necessárias para um caso de segurança.



4. PESQUISE as funções da tabela de origem na seção Coleções.
   Selecione as funções necessárias que permitem acesso de leitura e gravação na tabela de origem para um caso de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Para um caso de segurança, duas funções separadas para leitura e gravação são necessárias.
- Acesso de gravação em tabelas para a capacidade de selecionar o registro de origem Gestão de incidentes graves de segurança Modal de registro vinculado ao espaço.

5. Clique em **Salvar** para adicionar funções.
6. Verifique se as funções foram adicionadas com sucesso ao **Contém funções** seção de lista relacionada.

Etapa 6. Crie regras de negócio para um caso de segurança

Crie regras de negócio necessárias para um caso de segurança.

Antes de Iniciar
Função necessária: administrador

Crie as três regras de negócio a seguir para o novo Caso de segurança da tabela de origem (sn_ti_case). Essas regras de negócios são necessárias para manter a consistência no comportamento com a tabela de origem fornecida pronta para uso, como Incidente de segurança (sn_si_incident).

Regras de negócio para a nova tabela de origem:

1. **Desativar link quando inativo** : Depois que o caso de segurança for encerrado, as informações relacionadas não serão mais mostradas em Gestão de incidentes graves de segurança página do espaço.
2. **Sincronize as informações da equipe na atualização** A guia Detalhes do incidente de segurança grave mostra as informações sobre todas as equipes e usuários ativos que trabalham em diferentes tarefas. Depois que atualizamos Atribuído ao usuário ou grupo de atribuição é alterado no caso de segurança, precisamos atualizar as informações da equipe do caso de segurança na seção Equipe ativa de incidente de segurança grave. Essas regras de negócios atualizarão o novo usuário atribuído a e grupo de atribuição na seção Equipe ativa.
3. **Sincronize as informações da equipe ao excluir** A guia Detalhes do incidente de segurança grave mostra as informações sobre todas as equipes e usuários ativos que trabalham em diferentes tarefas. Depois de encerrarmos o caso de segurança, não precisamos mais mostrar as informações da equipe do caso de segurança na seção Equipe ativa de incidente de segurança grave. Essas regras de negócios removerão o usuário atribuído a e o grupo de atribuição da equipe ativa.

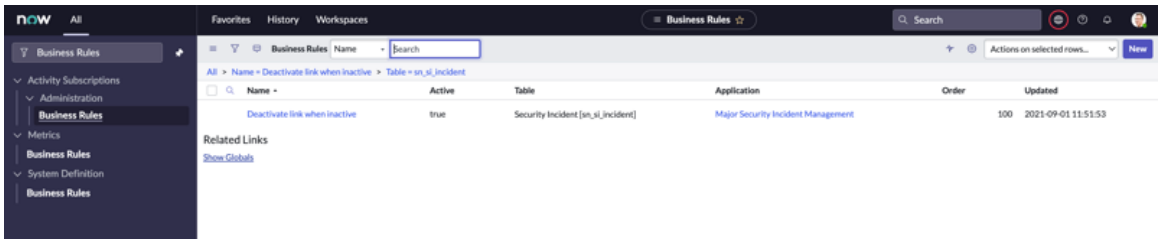
Criar regras de negócio para a nova tabela de origem:

Procedimento

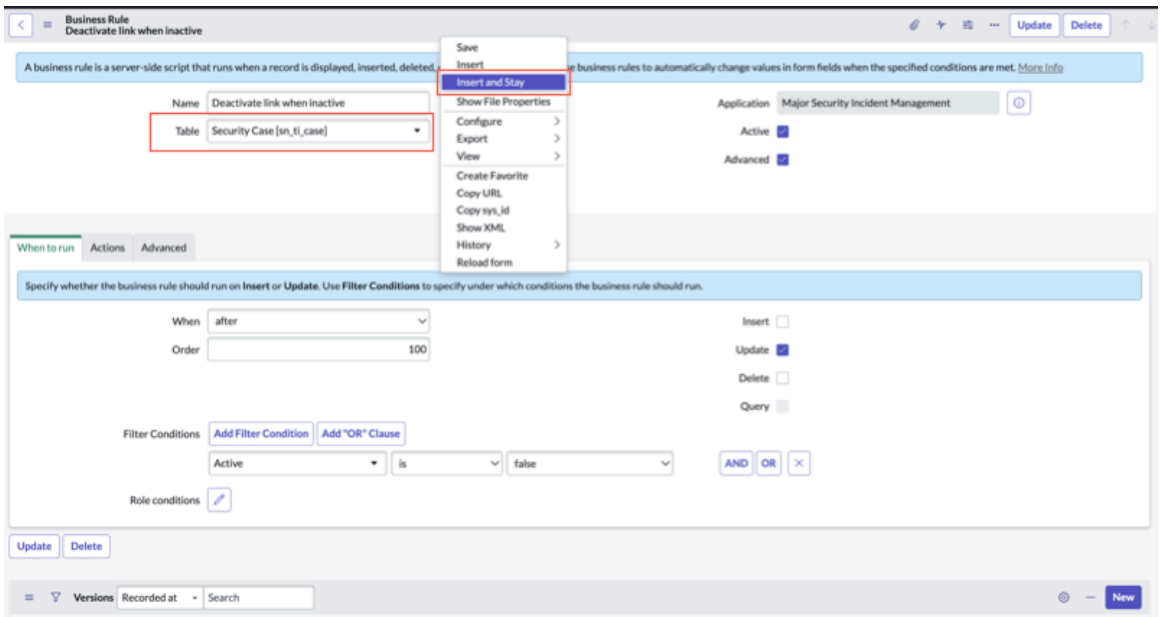
1. Navegar até **Definição do sistema** > **Regras de negócio**.
2. Execute a opção de filtro para filtrar os critérios de regras de negócio com as informações abaixo:
   - **Nome** Desativar link quando inativo
   - **Tabela** : sn_si_incident

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Abra o registro e mude o nome da tabela para uma nova tabela de origem: sn_ti_case .
4. Clique com o botão direito do mouse no menu na página e clique em **Inserir e permanecer** para criar o registro.



5. Repita o procedimento para outras duas regras de negócios também.
   - Sincronize as informações da equipe ao excluir
   - Sincronize as informações da equipe na atualização

Etapa 7. Criar configurações de registro de acúmulo

Crie configuração de registro de acúmulo para vincular e desvincular registros adicionais ao MSI.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

Nota: O administrador do sistema pode criar o registro e o administrador do espaço MSI pode atualizá-lo.

Para acumular informações, como itens de configuração, observáveis e indicador de comprometimento relacionado a um caso de segurança, crie uma configuração de registro de acúmulo.

Procedimento

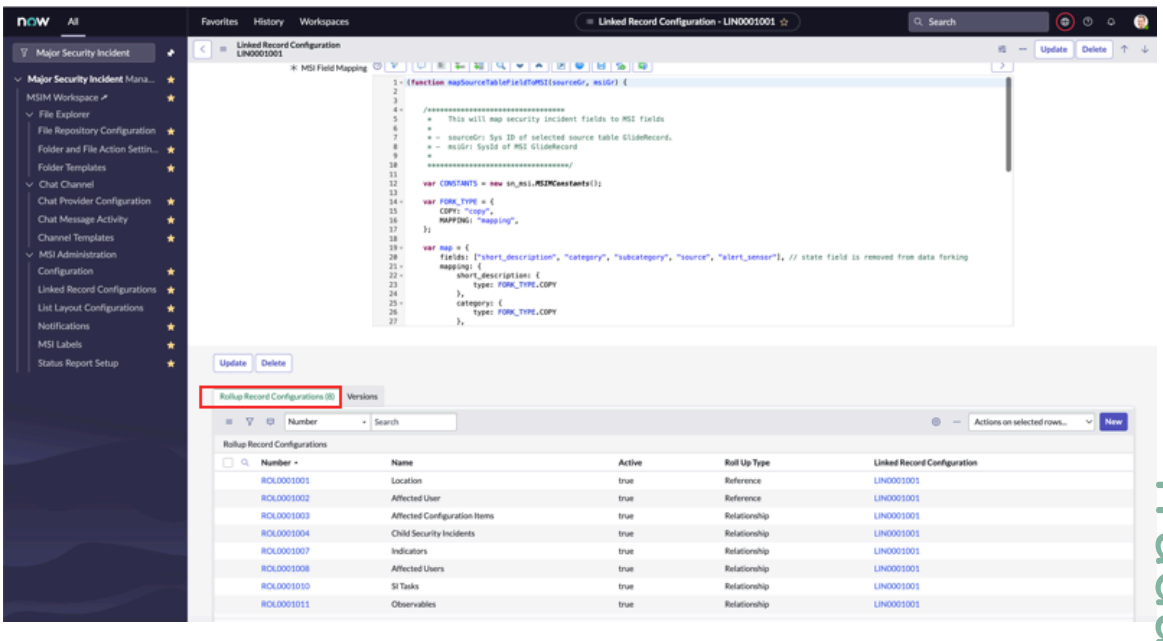
1. Navegar até **Resposta a incidentes de segurança graves** > **Configuração de registros vinculados**.
   A página Configurações de registro vinculado é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Selecione ou crie um novo registro vinculado e navegue até **Configuração de registro de acúmulo** da mesma página.

Seção Configuração de registro de acúmulo



O que Fazer Depois

- Para obter informações mais detalhadas, consulte Configurar registros de acúmulo em Gestão de incidentes graves de segurança
- Para obter informações de exemplo de caso de segurança, consulteEscrevendo script para um caso de segurança

Escrevendo script para um caso de segurança

Gravando um script para um Caso de segurança para acumular a configuração de registro.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

Nota: O administrador do sistema pode criar o registro e o administrador do espaço MSI pode atualizá-lo.

Procedimento

1. PESQUISE as configurações de registro vinculado usando a navegação à esquerda.
2. Navegar até **Administração do MSI** > **Configuração de registro vinculada**.
3. Abra o registro de configuração que foi criado para um caso de segurança.
4. A configuração do registro de acúmulo será exibida na seção Lista relacionada.
5. Clique em **Novo** para criar uma nova configuração de registro de acúmulo.

   Abaixo está um exemplo de registro criado para acumular dados de observáveis relacionados ao Caso de segurança que estamos tentando acumular com os valores de campo como:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
Tipo de acúmulo	Relacionamento **Nota:** As informações do observável estão disponíveis em um formato de lista relacionada.

Script de Acúmulo	A entrada sourceSySID contém o sys ID do caso de segurança e o msiSysId contém o sys ID do incidente de segurança grave.
	
	Rollup Script
	`(function rollUp(sourceSysId, msiSysId) {`
	`  var caseGr = new GlideRecord("sn_ti_case");`
	`  caseGr.get(sourceSysId);`
	
	`  var engine = new sn_msi.MSIMRollupEngine(caseGr);`
	
	`  var m2m = new GlideRecord("sn_ti_m2m_task_observable");`
	`  m2m.addQuery("task", sourceSysId);`
	`  m2m.query();`
	`  while (m2m.next()) {`
	`  var observable = m2m.observable.getRefRecord();`
	`  engine.linkToMSI(observable, sourceSysId, "observable", msiSysId, false);`
	`  }`
	
	`})(sourceSysId, msiSysId);`
	
	○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table.
	
	○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case.
	
	○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method:
	
	`MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkRecordTable", "msiSysId", "isPrimaryRecord")`

Tradução automática

Executar rollup atômico sob demanda

A estrutura de acúmulo não pode lidar com atualizações nos registros vinculados existentes. Nesses casos, o rollup atômico sob demanda deve ocorrer para registros vinculados, o que pode ser obtido por meio de regras de negócios.

Para capturar atualizações nos registros vinculados, regras de negócio devem ser criadas na tabela de origem.

Essas regras de negócio funcionam em operações de inserção, atualização e exclusão. Ao executar inserção ou atualização, você precisa adicionar ou atualizar informações acumuladas para MSI. Se você excluir, as informações acumuladas serão removidas de MSI.

Por exemplo, depois que um incidente de segurança é vinculado a. MSI, as informações relacionadas serão acumuladas automaticamente MSI. Mais tarde, se você adicionar um

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

novo observável a um MSI, em seguida, o observável recém-adicionado também será acumulado para MSI. Aqui, **Observável acumulado de sincronização** a regra de negócio captura a atualização e o acúmulo do registro atualizado MSI. Da mesma forma, a mesma regra de negócio também lida com a remoção dos observáveis acumulados existentes, se forem removidos do incidente de segurança.

Regras de negócios predefinidas

A seguir estão algumas regras de negócios predefinidas que ajudam você a entender como lidar com rollups atômicos

Regra	Descrição
Indicador acumulado de sincronização (sn_ti_m2m_task_indicator)	Use esta regra de negócio para lidar com o acúmulo e a remoção de indicador de comprometimento de Incidente de segurança, Caso de segurança e Tarefa de correção.
Observável acumulado de sincronização (sn_ti_m2m_task_observable)	Usar Esta regra de negócio lida com o acúmulo e a remoção de observáveis vinculados de Incidente de segurança, Caso de segurança e Tarefa de correção.
Usuário afetado acumulado de sincronização (sn_si_m2m_task_affected_user)	Usar Esta regra de negócios lida com o acúmulo e a remoção de usuários afetados vinculados do incidente de segurança, do caso de segurança e da tarefa de correção.
IC afetado acumulado de sincronização (task_ci)	Usar Esta regra de negócio lida com o acúmulo e a remoção de itens de configuração associados do Incidente de segurança, Caso de segurança e Tarefa de correção.

Integrações do Resposta a incidentes de segurança

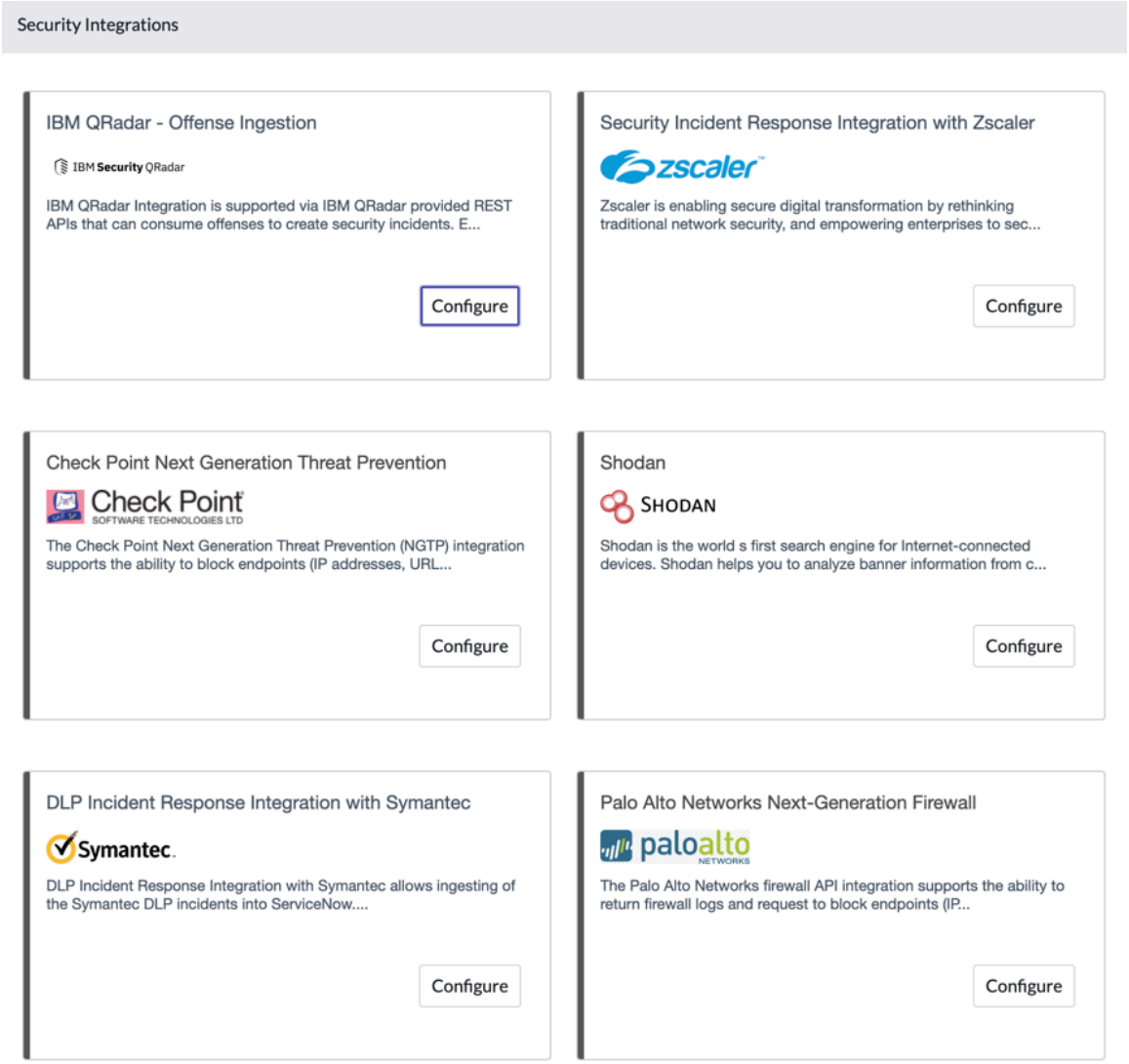
. Operações de segurança as principais aplicações e integrações de terceiros não principais estão disponíveis no ServiceNow Store. Esta seção fornece instruções para ativar as integrações e configurar ambas ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema de base inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências em Operações de segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode filtrar as integrações visíveis usando **Categoria** menu suspenso. . **Mostrar Configurações** o menu suspenso permite que você veja várias instâncias de implementações que permitem sua criação.

Botões nos cartões de integração

Os cartões de integração exibem botões diferentes dependendo do estado atual da integração e da origem do cartão.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar** .
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos do site da integração de terceiros.
Novo(a)	Determinadas integrações, como Carbon Black e IBM QRadar, permitem definir várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in é ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Botão	Descrição
Abrir página	No sistema de base, sua instância executa uma consulta à ServiceNow Store para todas as aplicações que têm dependências em Operações de segurança plug-ins. Quando essas aplicações são encontradas e os plug-ins de aplicações associados são ativados, os cartões de integração para elas são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o **Abrir página** o botão muda para **Configurar** .

ArcSight ESM Integração de ingestão de evento

. ArcSight ESM integração de ingestão de evento com Resposta a incidentes de segurança o produto permite que os analistas de incidentes de segurança coletem eventos correlacionados e automatizem a criação de incidentes de segurança com o. ServiceNow plataforma. Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados por analistas para identificar e responder a possíveis ameaças à segurança cibernética.

Com essa integração, eventos correlacionados que são candidatos a incidentes de segurança podem ser ingeridos periodicamente. Você pode mapear campos em eventos correlacionados para campos de incidente de segurança, visualizar a configuração de um evento como um incidente de segurança e configurar a ingestão programada de eventos para criar incidentes de segurança automaticamente continuamente.

Visão geral de ArcSight ESM Integração de ingestão de evento

Esta integração fornece a um analista do SOC (Security Operations Center, centro de operações de segurança) visibilidade para eventos de correlação em ArcSight ESM. Esses dados podem ser integrados ao ServiceNow AI Platform Incidentes de segurança de Resposta a incidentes de segurança (SIR) para investigação e correção adicionais. Os perfis são criados em seu ServiceNow AI Platform instância para lidar com diferentes tipos de evento de correlação que são criados e disponibilizados por meio de visualizadores de consulta de correlação em ArcSight ESM. Esses perfis personalizam a diferença ArcSight ESM Campos de evento correlacionados são exibidos em incidentes de segurança SIR.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de eventos para criar SIR incidentes de segurança para tipos específicos de ameaças, como malware e tentativas de acesso não autorizado.
- Mapeamento de arrastar e soltar de ArcSight ESM valores de campo de evento de correlação a associados SIR campos de incidente de segurança.
- Uma visualização do SIR layout de incidente de segurança com base em exemplos de eventos de correlação para validar detalhes de mapeamento de eventos.
- Ingerir eventos de correlação históricos, bem como novos eventos notáveis em intervalos configuráveis.
- Filtre eventos de correlação que não atendem SIR critérios de geração de incidentes, por exemplo, eventos de baixa prioridade
- Agregar eventos aos existentes SIR incidentes de segurança com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualizar eventos de correlação com base em SIR criação de incidentes e/ou condições de fechamento por meio de uma interface bidirecional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões da ServiceNow AI Platform compatíveis

Esta integração é compatível com o New York Patch 6 e Orlando ServiceNow AI Platform versões.

As seguintes aplicações de Operações de segurança devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila:

1. Framework de integração de segurança
2. Security Support Common
3. Resposta a incidentes de segurança
4. Ingestão de evento e alerta para operações de segurança
5. Plug-ins do Hub de integração
   a. Tempo de execução do hub de integração da ServiceNow
   b. Etapa de ação do hub de integração da ServiceNow - REST

Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

ArcSight ESM versões compatíveis

Esta integração foi testada com a versão 7.0.0.2436 do ArcSight ESM Gerente. A integração oferece suporte a ambos ArcSight ESM Ambientes de serviço no local e em nuvem/ hospedado.

MID Server

Esta integração requer um MID Server instalado e configurado em seu ServiceNow AI Platform® instância para se conectar ao ArcSight ESM serviço quando ArcSight ESM o servidor está implantado em sua rede corporativa. Se você estiver usando ArcSight ESM Um MID Server não é necessário. Consulte Site de documentação do produto da ServiceNow Para obter mais informações sobre MID Servers.

Referências

Referência	Identificador do documento	Título do documento
1	ArcSight ESM documentação do produto	Documentação do produto ArcSight .
2	ServiceNow Site de documentação do produto	Site de documentação do produto da ServiceNow

Configure seu ServiceNow AI Platform® instância do ArcSight ESM integração de ingestão de evento

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform® E Resposta a incidentes de segurança (SIR).	As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform® instância. • Um usuário com ServiceNow AI Platform® a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no ServiceNow AI Platform®: ◦ Cria e edita perfis de evento. ◦ Seleciona e mapeia valores de ArcSight ESM eventos de correlação com incidentes de segurança. ◦ Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração. ◦ Ingestão de eventos correlacionados em andamento. ◦ Habilita atualizações de evento correlacionado quando um incidente SIR é criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no Site de documentação do produto ServiceNow .
Verifique se você está usando a versão 7.0.0.2436 ou posterior do ArcSight ESM Gerente. Versões anteriores não são compatíveis.	Se você tiver acesso ao ArcSight ESM Visualizador de consulta, você tem acesso à API necessária para esta integração. Não há outra configuração especial necessária para a API.
Configure o Visualizador de consulta em ArcSight ESM.	Antes de ingerir eventos de correlação, você deve configurar o Visualizador de consulta no ArcSight ESM console. Consulte Configure o. ArcSight ESM Visualizador de consultas para obter detalhes.
Opcional Criar fases personalizadas em ArcSight ESM para atualizações de evento de correlação.	Um evento de correlação passa por muitas fases em seu ciclo de vida antes de ser encerrado. ArcSight ESM Fornece fases padrão, como Inicial, Monitoramento, Em fila e Encerrado. Algumas dessas fases exigem entradas do usuário, mas outras fases são aplicadas automaticamente ao evento sem qualquer intervenção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	do usuário (o. **Usuário obrigatório** o campo está desmarcado em ArcSight ESM console. Você pode criar fases personalizadas que não exigem nenhuma intervenção do usuário e usá-las em seu ServiceNow AI Platform® instância. Consulte Opções adicionais: Automatizar atualizações de eventos correlacionados e fechamento com base em SIR status do incidente para obter detalhes.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação DO MID Server configurada Um MID Server em seu ServiceNow AI Platform® a instância é necessária para se conectar ao ArcSight ESM se o ArcSight ESM o servidor está implantado em sua rede corporativa. Consulte Instale e configure a aplicação ServiceNow para ArcSight ESM Integração de ingestão de evento Para obter instruções sobre como configurar uma aplicação DO MID Server. Consulte MID Server Para obter informações sobre MID Servers. Se você estiver usando um serviço hospedado ou em nuvem, que seja acessível pela Internet, um MID Server não será necessário.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Ingestão de evento e alerta para operações de segurança: Esta aplicação requer: ○ Tempo de execução do IntegrationHub da ServiceNow com.glide.hub.integration.runtime ○ Etapa de ação do ServiceNow IntegrationHub - REST **5.** Threat Core Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você configurou com sucesso seu ServiceNow AI Platform® instância da integração. A próxima etapa é instalar o. ArcSight ESM Ingestão de evento de segurança para a aplicação Operações de segurança do ServiceNow Store para a integração.

Configure o. ArcSight ESM Visualizador de consultas

Crie um visualizador de consulta e defina filtros que incluirão eventos de correlação criados recentemente que serão ingeridos ServiceNow.

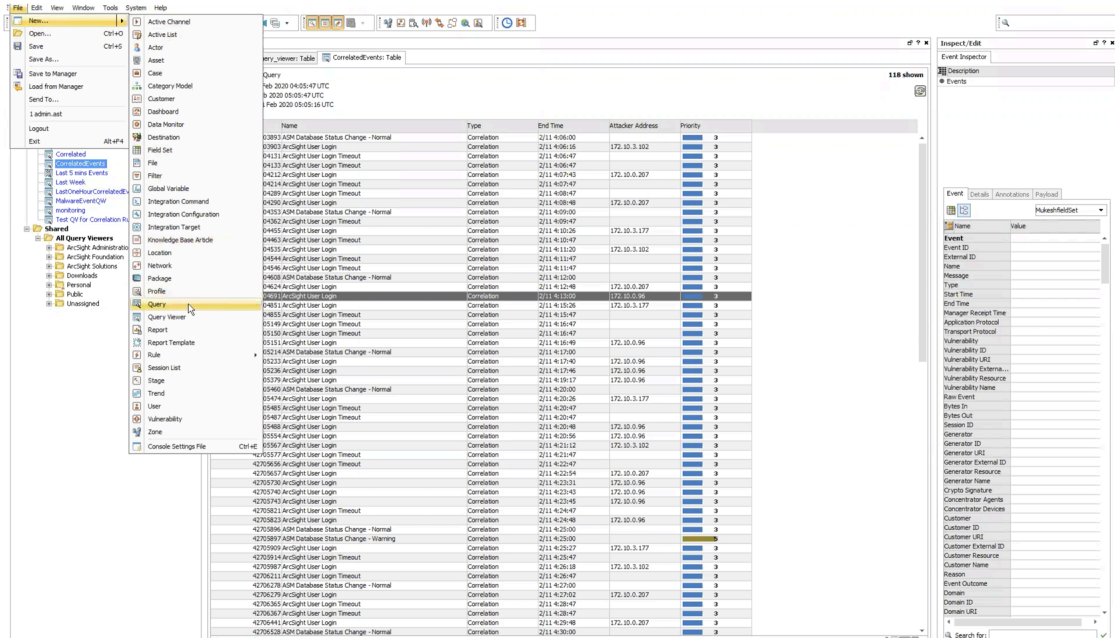
Antes de Iniciar

Função necessária: Administrador do ArcSight

Procedimento

1. Faça login no ArcSight ESM console para criar um visualizador de consulta.

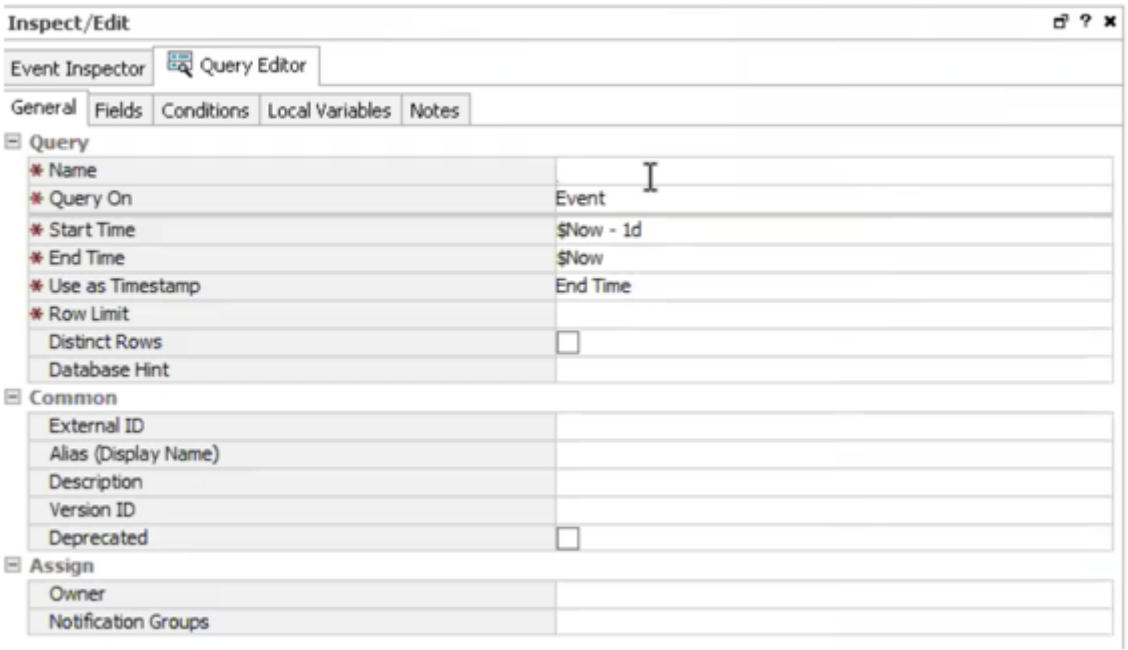
2. Para criar uma nova consulta, navegue até **Arquivo** > **Novo(a)** > **Consulta**.



3. Defina condições para o Visualizador de consulta no **Inspecionar/Editar** painel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

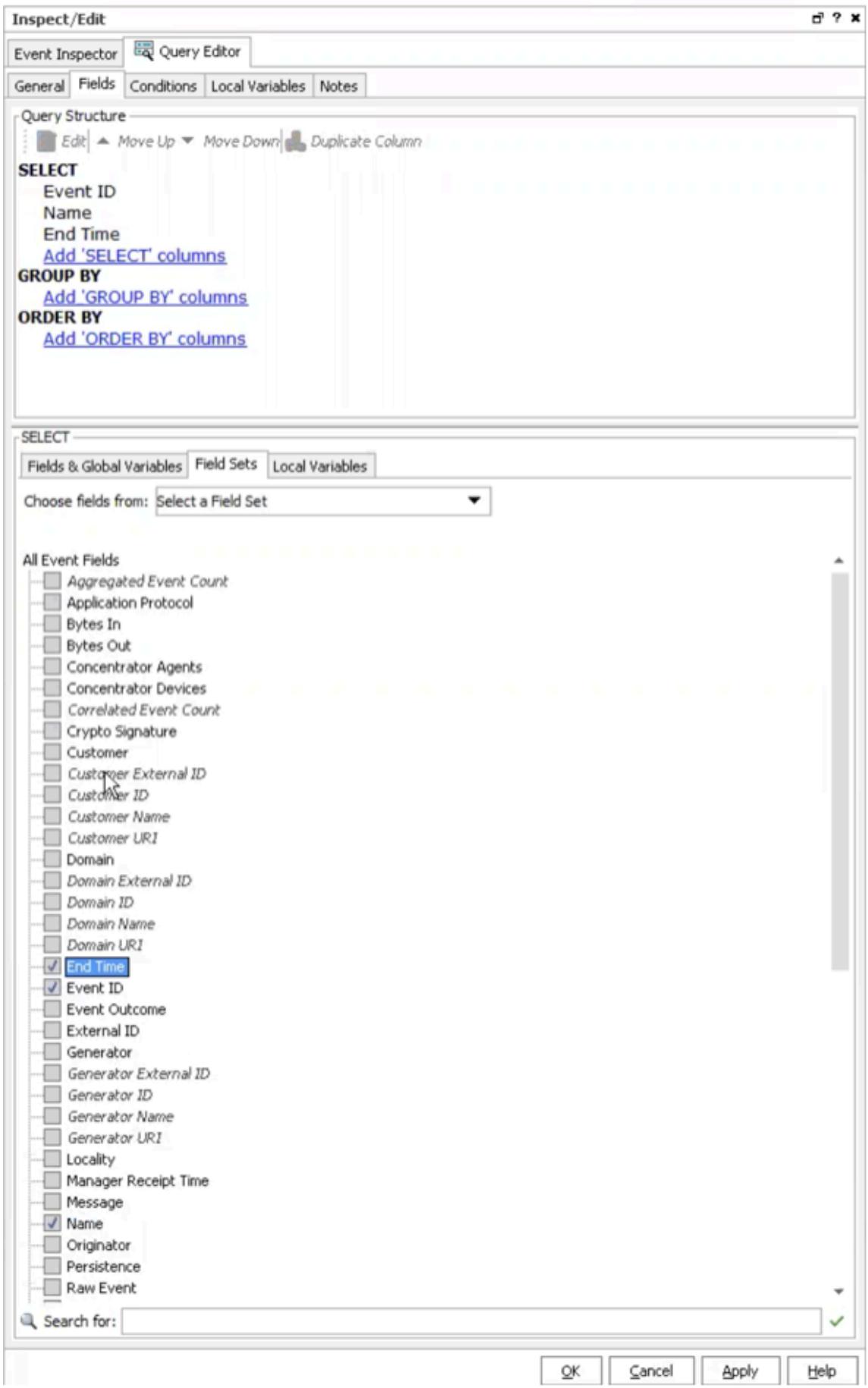


Nome do Campo	Descrição
Nome	Insira um nome para a consulta.
Consulta em	Selecione **Evento** na lista suspensa.
Hora de início	Para ingerir os dados mais recentes, selecione a data dos eventos a serem ingeridos. Especifique uma data que seja um dia ou alguns dias antes da data atual. **Nota:** Não é possível especificar uma data que seja mais de 7 dias anterior à data atual. Se você estiver ingerindo um grande número de eventos, deverá especificar uma data 1 ou 2 dias mais antiga do que a data atual.
Hora de término	Esta é a data atual.
Limite de linhas	O número máximo de eventos que podem ser ingeridos por vez. Especifique um valor menor que 5000 aqui.

4. Clique em **Campos** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

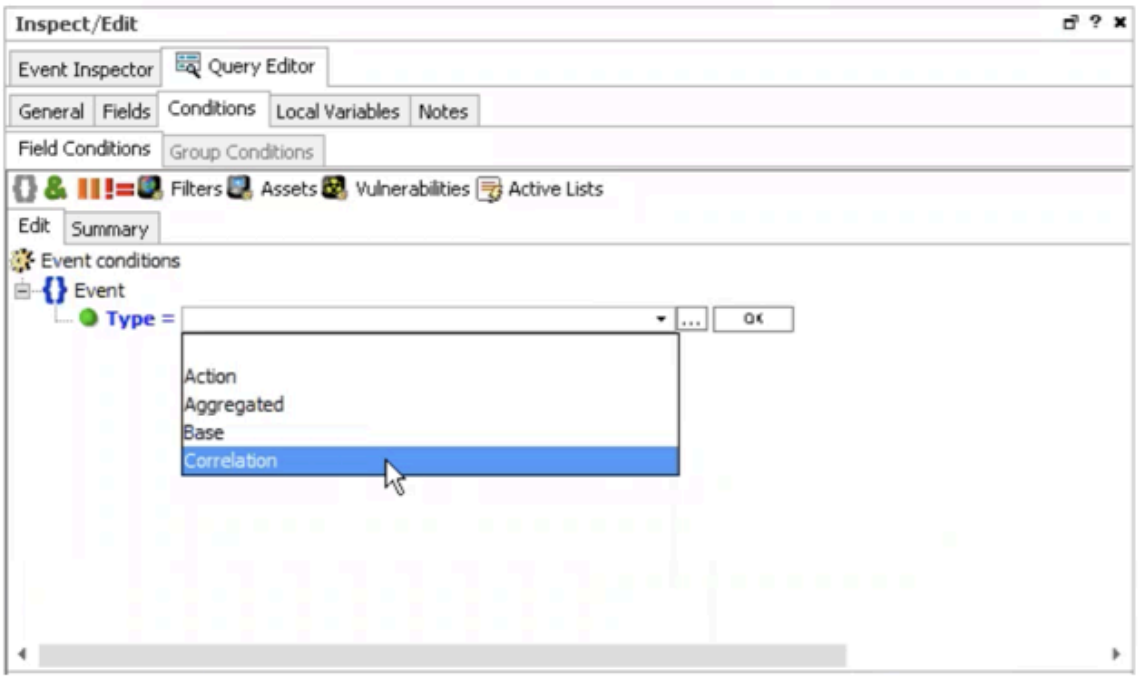


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os campos que devem ser incluídos durante a ingestão.
   Você deve selecionar `ID do evento` , `Nome` e `Hora de término` campos para que a ingestão seja bem-sucedida.
6. Clique em **Adicione colunas "ORDENAR POR"** link e selecione **ID do evento** e especifique a ordem de classificação como **Decrescente** para garantir que os eventos mais recentes sejam ingeridos.
7. Clique em **Condições** guia.
8. Clique com o botão direito **Evento** em **Condições do evento** em **Resumo** seção.
9. Clique **Nova condição** > **Raiz** > **Tipo** E selecione o Tipo de evento como **Correlação** .

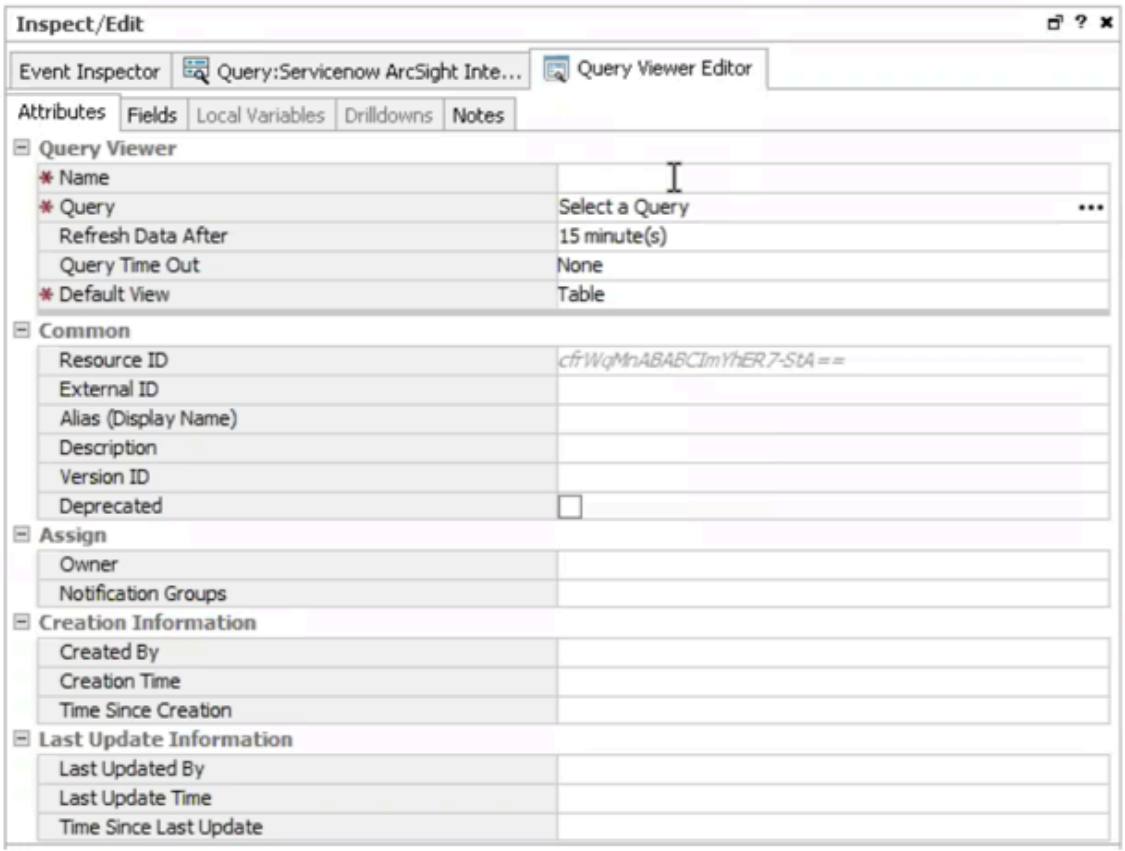
Importante: Somente eventos de correlação serão recuperados; os eventos de base para correlações não serão recuperados.



10. Clique em **OK** para salvar a consulta.
    A próxima etapa é criar um Visualizador de consulta para esta consulta.
11. Navegar até **Arquivo** > **Novo(a)** > **Visualizador de consultas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



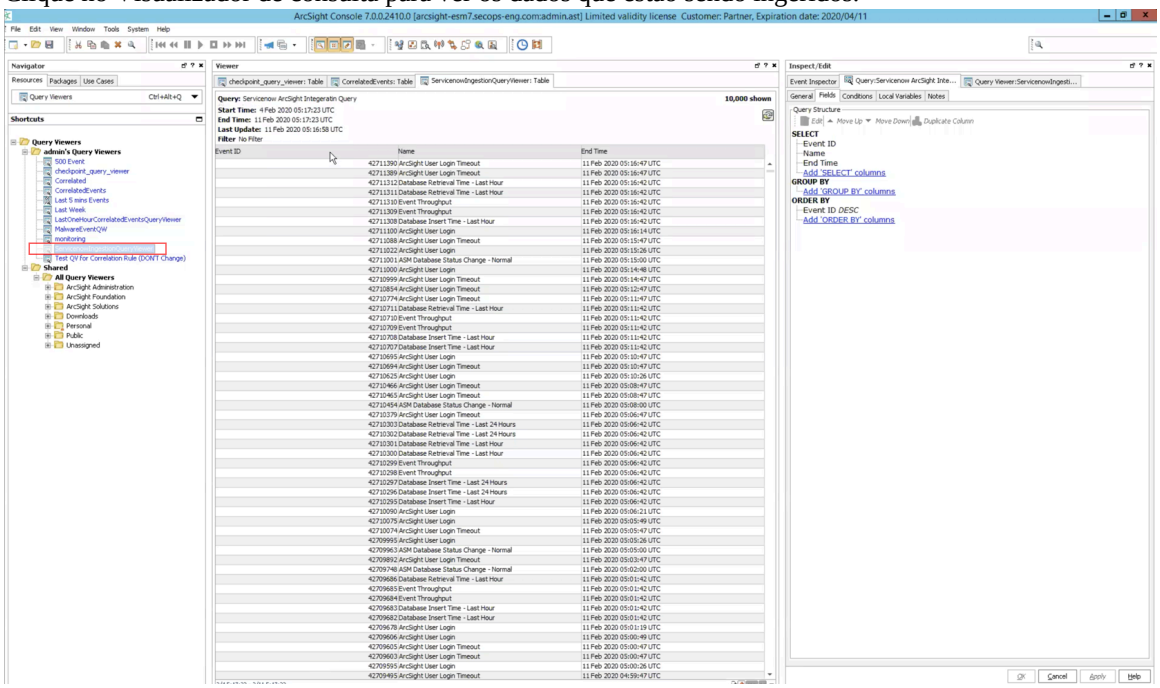
Nome do Campo	Descrição
Nome	Insira um nome para o Visualizador de consulta.
Consulta	Selecione a consulta que você acabou de criar.
Atualizar dados após	Especifique a frequência na qual os dados serão atualizados.

12. Clique em **Campos** e certifique-se de que os campos obrigatórios (*`ID do evento`*, *`Nome`*, *`Hora de término`* que você especificou em sua consulta estão selecionados.
13. Clique em **Aplicar** Para salvar o Visualizador de consulta.
    O novo Visualizador de consulta que você criou está listado na seção Visualizadores de consulta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

14. Clique no Visualizador de consulta para ver os dados que estão sendo ingeridos.



Instale e configure a aplicação ServiceNow para ArcSight ESM Integração de ingestão de evento

Antes de executar a integração no seu ServiceNow AI Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se você não instalou o. ArcSight ESM aplicação do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize ArcSight ESM lado a lado.
3. Para configurar a aplicação, clique em **Novo** .
4. Como alternativa, se for um **Configurar** é exibido em um bloco, clique nele para editar uma configuração existente.
5. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome exclusivo para ArcSight ESM Gerenciador que será usado na configuração do perfil de integração para distinguir entre vários ArcSight ESM Origens do gerente, se necessário. Espaços são compatíveis com nomes, mas parênteses não são compatíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

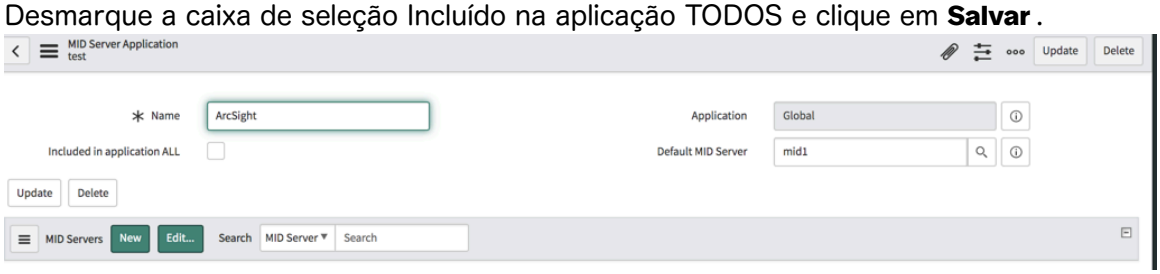
Campo	Descrição
URL do endpoint da API ArcSight	URL do ArcSight ESM Servidor do gerenciador. Observe que o URL deve incluir a porta da API, por exemplo: https://arcsight-esm.com:8443
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário da API no ArcSight ESM Console do gerente.
Senha da API	Senha que você criou para sua conta de usuário de API no ArcSight ESM Console do gerente.
Implantação no Local	O padrão é desmarcado. Se você estiver usando a versão baseada em nuvem de ArcSight ESM Que tenha acesso direto à Internet, verifique se a caixa de seleção está desmarcada. Para uma implantação no local, marque esta caixa de seleção e especifique a aplicação do MID Server.
Aplicação do MID Server	Especifique um nome de aplicação DO MID Server aqui. Esta aplicação DO MID Server pode apontar para qualquer um dos MID Servers que foram configurados e qualquer MID Server disponível será usado. Se você não tiver uma aplicação do MID Server configurada, deverá criar uma nova aplicação DO MID Server para esta integração. **Nota:** A aplicação MID Server pode ser configurada somente por usuários com função de administrador do sistema.

Para criar uma nova aplicação DO MID Server, siga estas etapas:

a. Navegar até **MID Server** > **Aplicações** e clique em **Novo** .

b. Insira um nome para a aplicação DO MID Server e selecione um MID Server a ser usado como padrão.

c. Desmarque a caixa de seleção Incluído na aplicação TODOS e clique em **Salvar** .

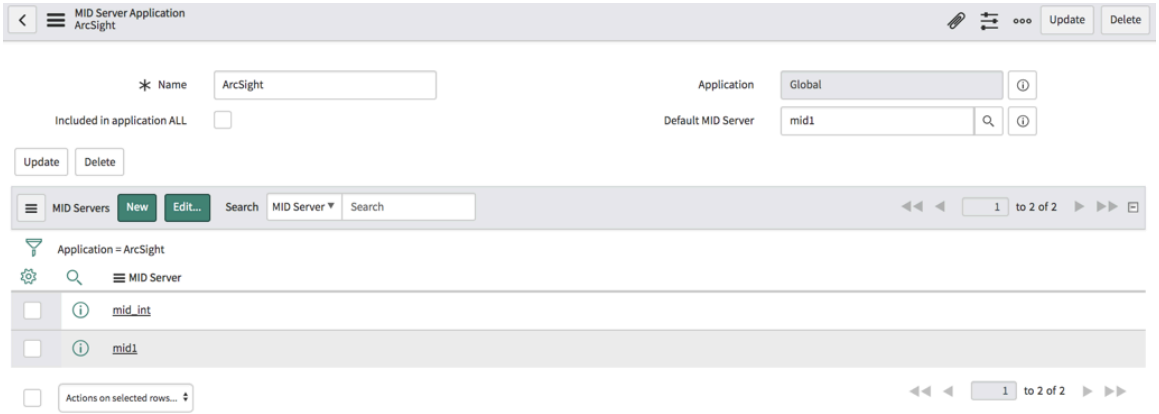


d. Clique em **Editar**. Em **Editar membros** , selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar** .

Tradução automática

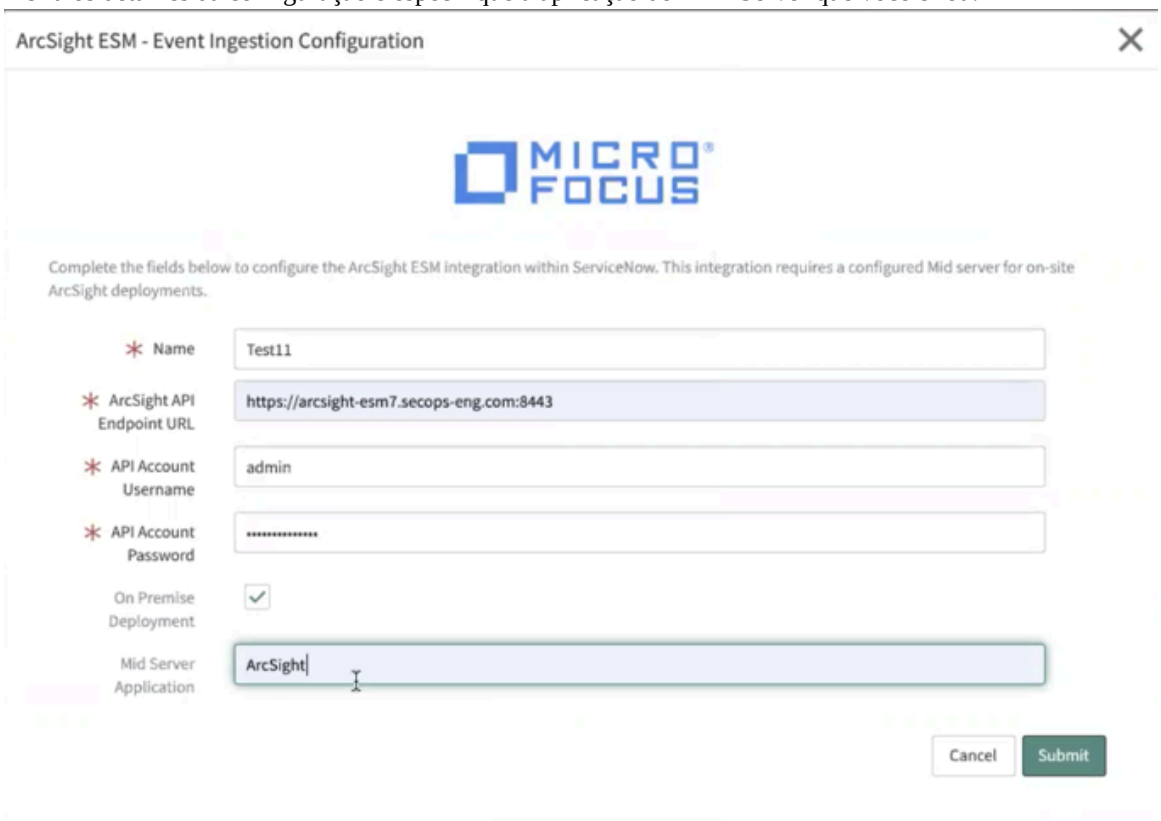
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Os MID Servers selecionados serão listados conforme mostrado abaixo.



Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.

6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.



Cada evento de correlação que você ingerir do seu ArcSight ESM O console do gerenciador requer um perfil de evento exclusivo em sua instância. No entanto, o ArcSight ESM A origem que você configura no formulário Configuração de ingestão de evento pode ser reutilizada para vários perfis, desde que cada perfil ingere tipos de evento de correlação exclusivos.

7. Clique em **Enviar**.
Cada um deles é validado e enviado com sucesso ArcSight ESM A configuração do servidor é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim** .

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um perfil

Como um usuário com a função sn_si.admin, você cria um perfil em seu ServiceNow AI Platform e determinar quais eventos de correlação criam incidentes de segurança. Antes ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança são criados a partir de eventos de correlação, os valores de campo de eventos são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Eventos de correlação são automaticamente ingeridos no Operações de segurança do seu ServiceNow AI Platform instância dependendo do tipo de perfil definido. Um perfil é um encapsulamento de um tipo de evento de correlação, como tentativas de acesso não autorizado ou malware.

Depois que um evento de correlação é ingerido, você pode mapear campos de evento de correlação individuais para os campos correspondentes no incidente de segurança. Você pode filtrar eventos de correlação para especificar quais eventos criam incidentes de segurança. Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para eventos de correlação identificados como de alto risco. Você também pode definir critérios de agregação de eventos adicionais para que os eventos de correlação duplicados de entrada sejam agregados a um incidente de segurança em aberto. Por fim, você pode definir uma programação de ingestão e ativar o perfil.

Nomes dos perfis de evento em seu ServiceNow AI Platform a instância deve ser exclusiva e só pode ser mapeada para um perfil de evento ativo a qualquer momento.

Crie e nomeie o perfil para ArcSight ESM integração de ingestão de evento

Você pode configurar um perfil para ingerir eventos de correlação.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil de evento para um evento de correlação em seu ServiceNow AI Platform instância, navegue até **Integração do ArcSight ESM** > **Perfil de evento do ArcSight ESM**.
2. Clique em **Nova**.
3. Preencha os campos.

Um exemplo de um formulário preenchido segue a tabela.

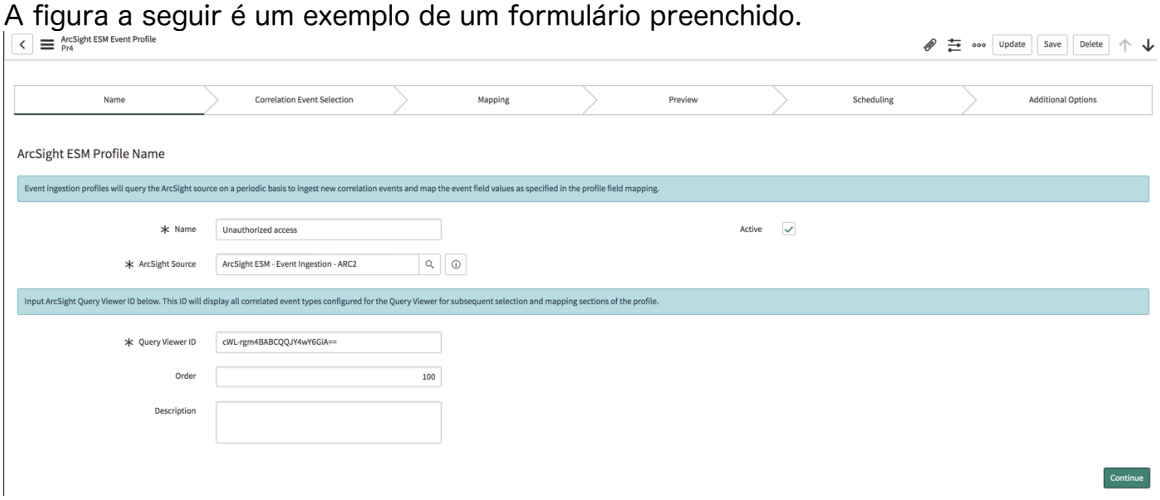
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e os nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.
Ativo	a caixa de verificação está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo e a ingestão não ocorrerá.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você deve concluir todas as seções no perfil antes de ativá-lo.
Origem do ArcSight	. ArcSight ESM servidor configurado durante a etapa de autenticação inicial. Se você tiver vários ArcSight ESM servidores configurados, selecione o servidor apropriado para os tipos de evento de correlação que serão ingeridos para o perfil. Você deve selecionar um valor.
ID do visualizador de consulta	Insira o ID do recurso do Visualizador de consulta configurado no ArcSight ESM Console. O ID do recurso é um identificador exclusivo para qualquer Visualizador de consulta configurado no servidor ArcSight ESM. Depois que o ID do recurso for enviado, o nome da Exibição de consulta será retornado para garantir que o Visualizador de consulta correto tenha sido selecionado. Consulte a seção abaixo para obter uma captura de tela de como determinar o ID do recurso para o Visualizador de consulta selecionado em ArcSight ESM.
Ordem	O padrão é 100. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido.

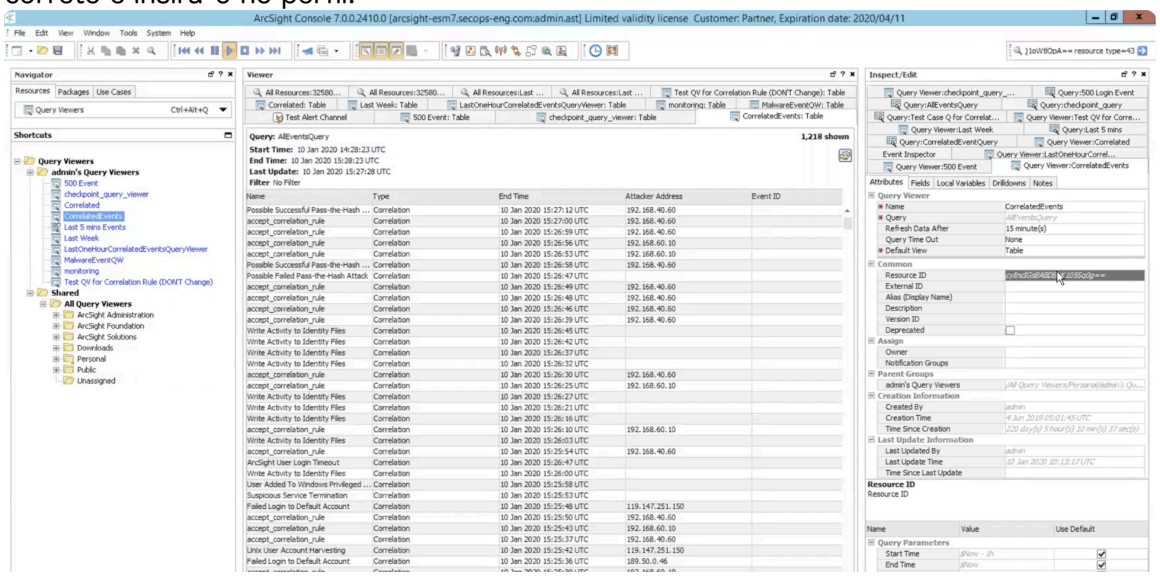


Depois de inserir os detalhes do perfil, clique em **Continuar** . O ID do visualizador de consulta será validado e se um ID de recurso correspondente estiver presente no ArcSight ESM Visualizador de consulta, o nome do Visualizador de consulta será retornado conforme mostrado abaixo. Se a validação falhar, verifique se o ID do recurso existe no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ArcSight ESM console. Se o ID do recurso não for encontrado, encontre o ID do recurso correto e insira-o no perfil.



O que Fazer Depois

A próxima etapa é selecionar os tipos de evento de correlação para ingestão no Visualizador de consulta que foi selecionado na etapa anterior.

Selecione eventos de correlação para ArcSight ESM integração de ingestão de evento

Com base em ArcSight ESM E o Visualizador de consulta configurado, selecione uma regra de evento de correlação para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba os eventos de correlação disponíveis listados na Seleção de evento de correlação em seu ServiceNow AI Platform para que você possa determinar quais eventos de correlação deseja ingerir e criar incidentes de segurança. Você só pode selecionar um tipo de regra de correlação na lista para cada perfil.

O ID do visualizador de consulta e o Nome do visualizador de consulta conforme especificado no formulário Visualizador de consulta são exibidos. Selecione um evento de correlação na lista que você pode usar para criar um mapeamento de configuração para o evento correlacionado ingerido.

Clique na lista suspensa no campo Lista de eventos de correlação. Uma lista de eventos de correlação presentes no ArcSight ESM O Console do Visualizador de Consultas é exibido.

Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

Campos de evento de correlação de mapeamento para ArcSight ESM integração de ingestão de evento

Depois de identificar a regra de evento de correlação específica na lista, a próxima etapa é mapear os campos de evento de correlação para os campos no formulário de incidente de segurança.

Visão geral dos campos de evento de correlação de mapeamento

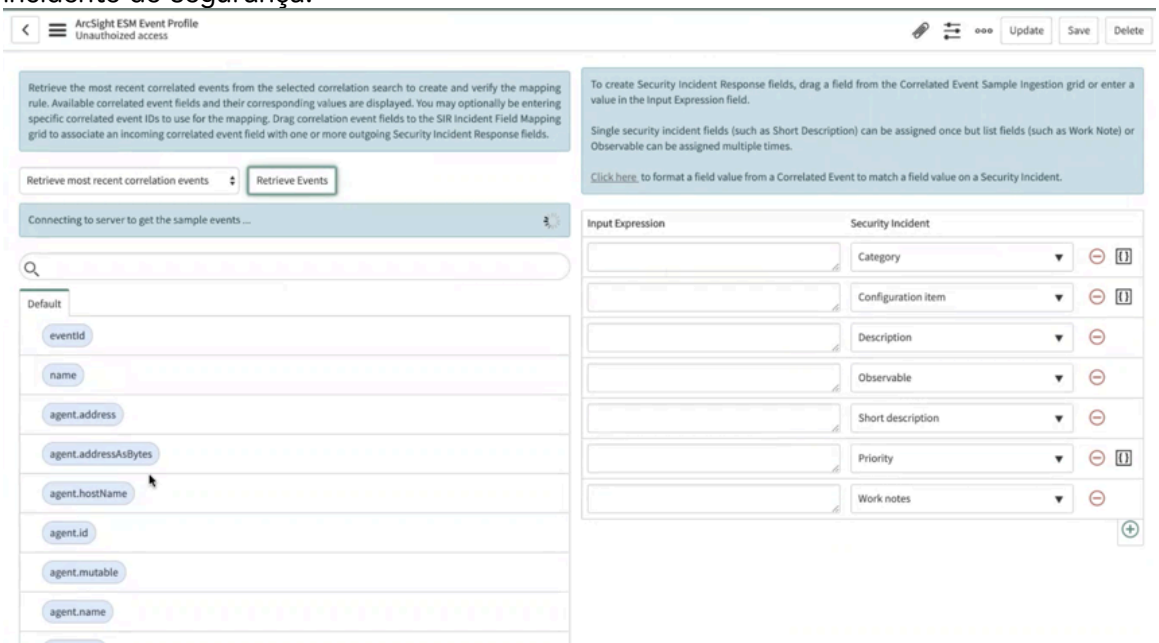
Para a etapa de mapeamento, você pode ingerir eventos de correlação de amostra para a regra de correlação selecionada. Durante esta fase de mapeamento, você pode garantir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que todos os dados de campo de evento de correlação relevantes sejam mapeados para o local apropriado no SIR formulário de incidente e visualize o. SIR incidente na seção de visualização.

A figura a seguir mostra a configuração de mapeamento padrão fornecida para criar o perfil de evento de correlação. Você pode personalizar os campos que preenchem o incidente de segurança.



Ao clicar em **Recuperar eventos** , os nomes dos campos do evento de correlação e os valores correspondentes são preenchidos no lado esquerdo do formulário. . ArcSight ESM campos de evento de correlação que estão disponíveis para mapear para os campos de incidente de segurança.

Você pode preferir revisar alguns eventos de correlação de amostra em seu console para ingerir a etapa de configuração de mapeamento de campo. Esta etapa é rotulada Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos de correlação de amostra do ArcSight ESM Gerente da regra de correlação selecionada para ajudar no processo de mapeamento de campo. Há opções para ingerir os cinco eventos de correlação mais recentes para o evento de correlação selecionado ou ingerir até cinco eventos de correlação específicos com base nos IDs de evento.

Abaixo está um resumo das etapas necessárias para mapear eventos de correlação:

- Mapeamento de campo: Edite a configuração de mapeamento arrastando os campos de evento de correlação do lado esquerdo e soltando-os no SIR seção de mapeamento de incidentes à direita. O mapeamento à direita associa o campo Evento de correlação de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: Personalize a grade de mapeamento adicionando ou removendo campos usando o ícone de adição na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou mapeados anteriormente com a codificação de cores fornecida (os campos mapeados ficam esmaecidos, os campos azuis não estão mapeados).
- Condições de geração de incidente: Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para filtrar quais eventos de correlação devem criar incidentes de segurança versus eventos de correlação que devem ser filtrados, por exemplo, eventos de correlação de baixa prioridade. Isso é feito na seção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de geração de incidentes localizada abaixo da seção Ingestão de amostra de evento de correlação.

- Critérios de agregação de evento: Defina critérios de agregação de evento adicionais que agreguem um evento de correlação de entrada a um existente SIR incidente de segurança em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, esse recurso de agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de eventos notáveis de segurança relacionados em um único incidente de segurança.
- Tradução de campo de formato: Em determinados casos, valores de campo de evento no ArcSight ESM o evento de correlação pode não ser traduzido diretamente para os campos no SIR incidente de segurança. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos.

  Por exemplo, com o editor de script, um valor de categoria Alerta de malware e infecção por vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser traduzidos em uma Atividade de código mal-intencionado comum no campo Categoria no SIR Incidente de segurança usando a funcionalidade Formatar tradução de campo.

A próxima etapa é ingerir eventos de correlação de amostra e mapear valores para SIR campos de incidente de segurança.

Criar mapeamentos para ArcSight ESM integração de ingestão de evento

Nesta etapa, você ingira eventos de correlação de amostra e mapeia valores para os campos de incidente de segurança SIR.

Antes de Iniciar

Função necessária: admin, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, você pode revisar até cinco eventos de correlação de amostra na coluna Ingestão de amostra de evento de correlação à esquerda do formulário para ajudar no mapeamento e na tradução dos valores do campo de evento para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos exibidos por padrão geralmente são campos importantes a serem preenchidos no formulário de resposta a incidentes de segurança. Esses campos podem ser removidos e todos os campos adicionais podem ser exibidos usando os botões mais e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear ArcSight ESM campos que não são exibidos na grade de mapeamento padrão no incidente de segurança.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os eventos de correlação de amostra mais recentes para a regra de correlação selecionada ou fornecer os IDs de evento de correlação exclusivos para os eventos de correlação específicos que você deseja usar para sua experiência de mapeamento de evento de correlação.
3. Na lista suspensa, selecione uma das seguintes opções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

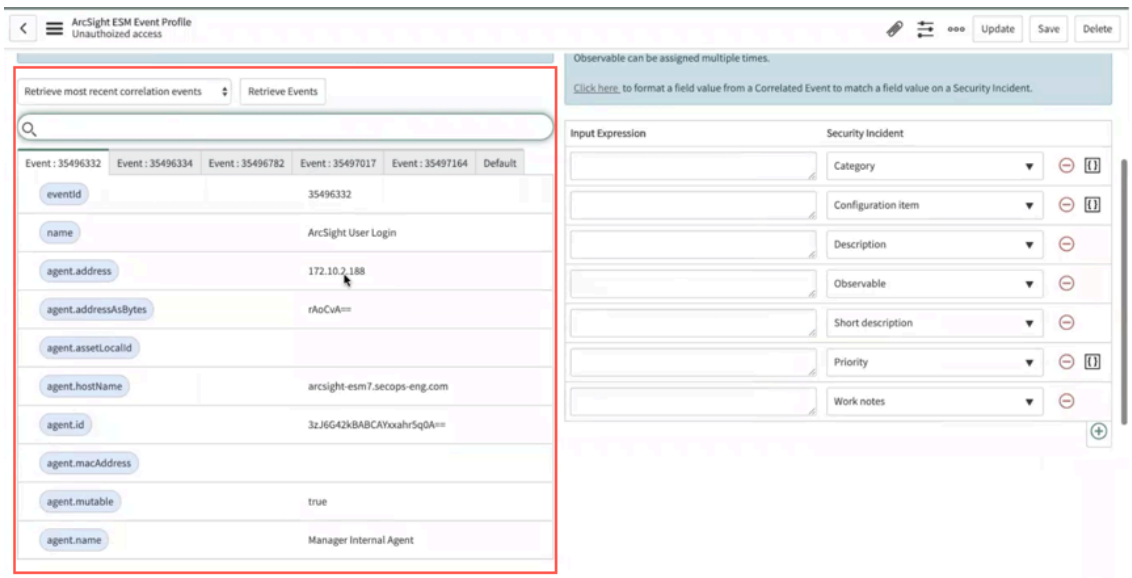
- Recuperar os eventos de correlação mais recentes
- Selecione eventos de correlação com base no ID do evento

Clique em **Recuperar eventos** para extrair os eventos de correlação de amostra mais recentes do ArcSight ESM console para a regra de pesquisa de correlação selecionada.

Os campos de evento de correlação e resultados de valores são exibidos como guias individuais.

A extração de eventos de correlação de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Na figura a seguir, os pares de valor de nome de campo para o evento de correlação ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário depois que a extração de ingestão é concluída. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



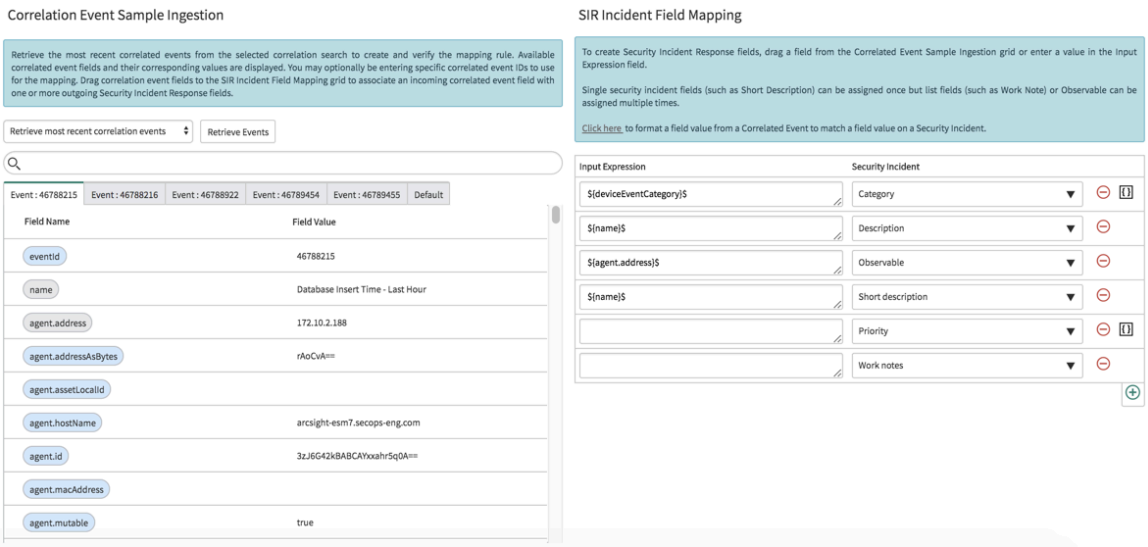
4. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
5. Arraste o nome do campo, por exemplo, agent.hostname E solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   Para ajudar você a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Campos azuis claros à esquerda indicam que um campo de evento de correlação ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de correlação de entrada a mais de um campo em um incidente de segurança.

   Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Esta codificação por cores ajuda a rastrear quais campos de evento já foram utilizados para mapeamentos de campo de incidente de segurança futuros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

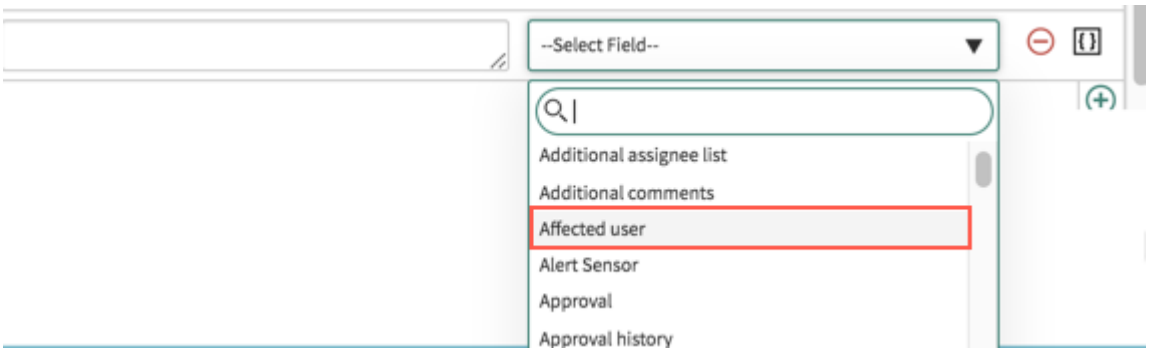


6. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

Na lista de seleção expandida do novo campo, alguns campos são sombreados. Na figura a seguir, Usuário afetado tem um fundo cinza, porque foi mapeado no incidente de segurança. Semelhante à codificação por cores dos campos de eventos de correlação no lado esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente DE SIR já mapeados.



Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o. Observável o campo pode ser mapeado várias vezes com valores diferentes. Da mesma forma, o Item de configuração e. Anotações de trabalho os campos são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista de seleção, o campo não será preenchido no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar **ID do evento** que você deseja no **Expressão de entrada** campo.
Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

7. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de scripts, consulte Use o editor de scripts para formatar valores de evento de correlação.**Condições de filtragem de geração de incidentes**

8. Opcional: Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um evento de correlação de entrada deve atender para criar um SIR incidente de segurança.
Para definir condições de geração de incidentes, siga estas etapas.

a. Role até a seção Condições de geração de incidentes no formulário e selecione **Filtro com base em condições** marque a caixa para habilitar a opção.

(Optional) O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

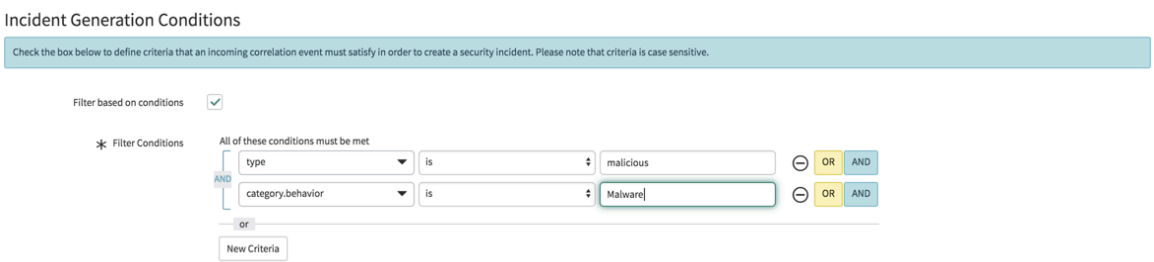
As opções nas listas de seleção do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de evento de correlação para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo dos eventos de correlação que você ingerir. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores de ArcSight ESM evento de correlação.

Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.

b. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
Se **E.** selecionado, todas as condições devem ser correspondidas. Se **OU** está selecionado, qualquer condição pode ser correspondida.

c. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando as duas condições de filtragem inseridas forem correspondidas.

Este tipo de filtragem de condição de geração de incidentes ajuda a restringir os eventos de segurança e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou filtrar eventos em ArcSight ESM. Se critérios de filtragem adicionais forem definidos, somente os eventos de correlação que corresponderem a todos os critérios serão mapeados para incidentes.

Nota: Se qualquer um dos nomes de campo de evento tiver caracteres especiais, como aspas ("), hifens ("), sublinhados (-) ou ampersands ("), esses caracteres talvez precisem ser substituídos para fins de tradução de mapeamento e, possivelmente, criar um nome de evento duplicado. O mapeamento pode ser feito corretamente, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `events.event` e o segundo campo de evento é `events.event` esses campos não podem ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `eventos no evento(1)` .

Critérios de agregação de eventos para lidar com eventos de correlação semelhantes e evitar incidentes duplicados

9. **Opcional:** Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos de correlação de entrada sejam agregados a um incidente de segurança em aberto.
   Para definir os critérios, siga estas etapas abaixo:

   a. Role até **Critérios de agregação de evento** No formulário e marque a caixa de seleção Condições de agregação para habilitar esta opção.

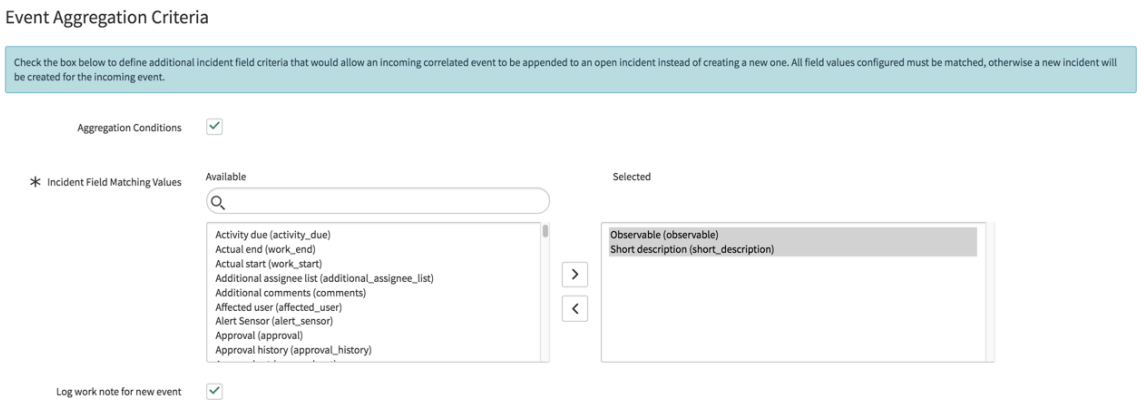
   (Optional) As colunas Valores de correspondência do campo do incidente são exibidas. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.

   b. Na lista Disponível, selecione os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform E mova-os para a lista Selecionado.

   (Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este evento de correlação de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de evento de correlação mapeados para eles. Todos os valores devem corresponder. Se somente um subconjunto dos valores for correspondido, as condições de agregação de evento não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para obter o mapeamento de campos de vários valores.

Tradução automática

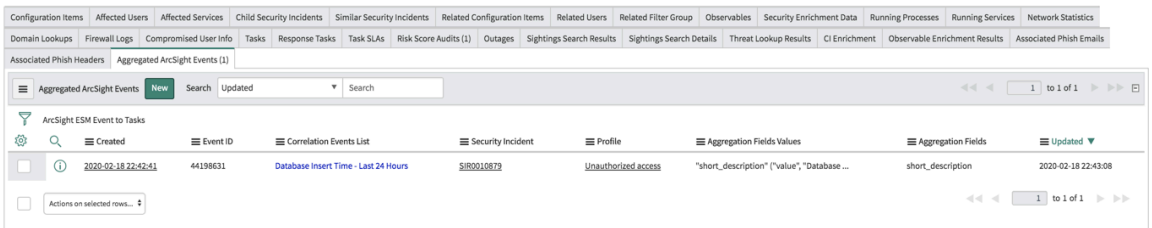
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se um novo evento de correlação corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo evento de correlação será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como analista de SOC que trabalha com incidentes de segurança, você pode exibir todos os eventos de correlação agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os eventos de correlação agregados em um incidente de segurança são exibidos no **Eventos agregados do ArcSight** lista relacionada. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam a entender por que esses eventos de correlação estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em **Links relacionados** e clique em **Mostrar todas as listas relacionadas** link.

Nota: Se você não vir esta lista relacionada, siga estas etapas:

- Clique com o botão direito do mouse no cabeçalho do formulário Incidente de segurança e clique em **Configurar** > **Listas relacionadas**.
- Selecione **Eventos agregados do ArcSight** Na lista Disponível, mova-o para a lista Selecionado e clique em **Salvar** .
- Clique em **Mostrar listas relacionadas** . Agora você verá **Eventos agregados do ArcSight** Na seção Lista relacionada.



c. Opcional: Para registrar em log uma anotação de trabalho para cada vez que um evento for agregado no incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra em log que um novo evento correlacionado foi adicionado junto com um link para os detalhes do evento correlacionado.

Valores mapeados de um evento de correlação para campos em um foram mapeados com sucesso SIR incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também agregou eventos de correlação aos existentes SIR incidentes de segurança quando os valores do campo de evento correspondem aos critérios de agregação configurados.

10. Escolha um para continuar com a configuração do perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido. **Visualização** está selecionado na barra de andamento. A próxima etapa é visualizar os campos mapeados em um SIR incidente de segurança.
Atualizar	Seus dados são salvos e ArcSight ESM A lista Perfis de evento é exibida.
Anterior	O formulário Seleção de evento de correlação é exibido.
Excluir	Exclua este perfil de evento e a lista Perfis de evento será exibida.

Visualize o incidente de segurança do ArcSight ESM Integração de ingestão de evento

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um ServiceNow AI Platform Resposta a incidentes de segurança Incidente de segurança (SIR). Esta etapa de visualização permite que você verifique se mapeou todos os campos de correlação que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin.

Por Que e Quando Desempenhar Esta Tarefa

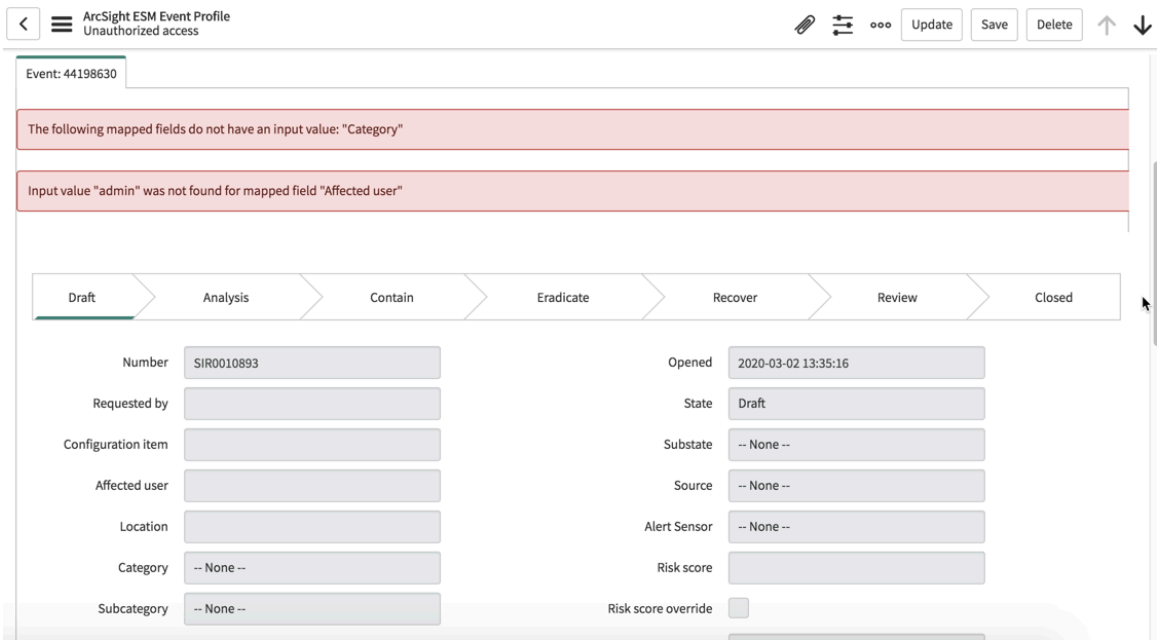
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de incidentes de segurança não são salvas como incidentes reais no Resposta a incidentes de segurança produto.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
2. Na lista de seleção IDs de evento de amostra, selecione um item.
   O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores do evento de correlação no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento de correlação não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para Categoria campo que é um campo de referência com um conjunto específico de valores. Como resultado, este valor de campo mapeado não aparecerá em SIR formulário de incidente de segurança sem modificações adicionais.

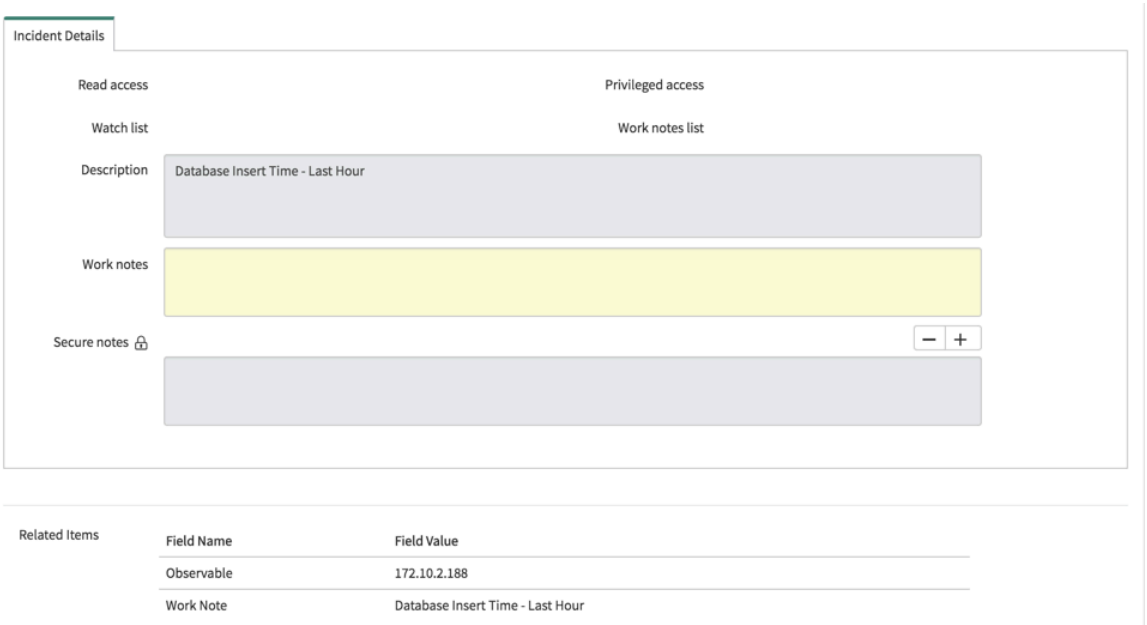
4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são preenchidos com os valores dos pares de valores extraídos do ArcSight ESM amostras de evento de correlação.



O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será definir a programação.

Crie uma programação para ArcSight ESM ingestão de evento

Você pode definir a pesquisa ou a programação de extração para novos eventos correlacionados. Durante esta etapa, você pode verificar as configurações existentes para recuperação de evento de correlação ou modificar a programação conforme necessário. Esta etapa também permite recuperar eventos de correlação históricos usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin.

Por Que e Quando Desempenhar Esta Tarefa

Você pode escolher se deseja ingerir eventos de correlação históricos durante a etapa Programação. Você também escolhe a frequência com que pesquisará novos eventos de correlação futuros que correspondam à configuração do perfil.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho do ArcSight ESM a integração de ingestão de evento de correlação pode ser afetada pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no ArcSight ESM servidor contra o desejo de ser notificado o mais rápido possível quando um evento é criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo eventos de correlação novos e atualizados

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando os eventos de correlação são extraídos do console do <ArcSight>.

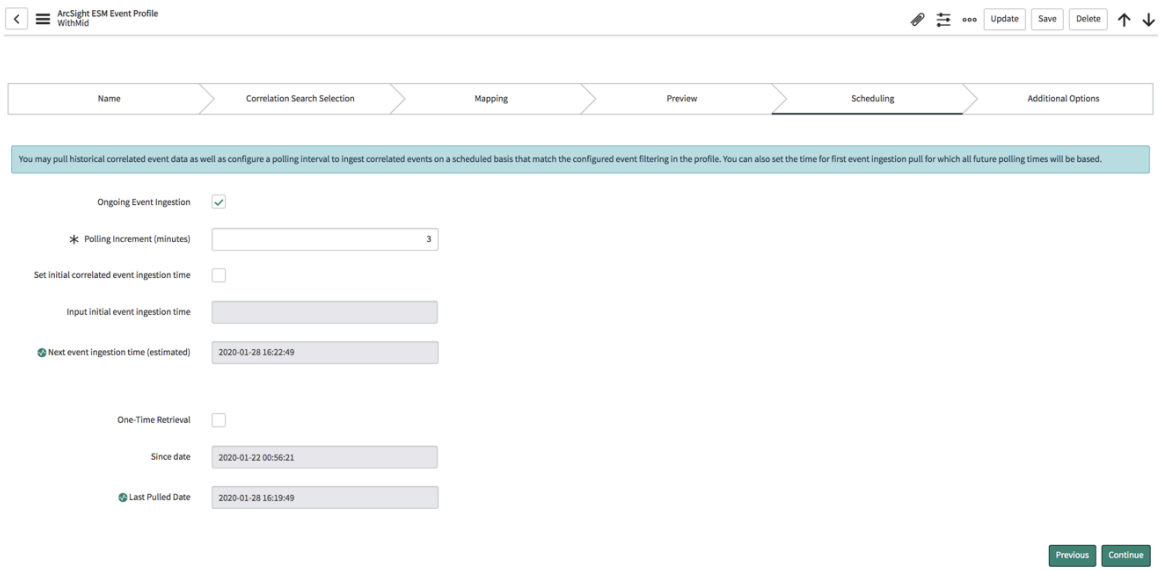
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
◦ Campo Ingestão de evento contínuo selecionado ◦ Campo Recuperação única limpo	Evento em andamento Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do ArcSight ESM servidor para novos eventos de correlação a cada cinco minutos. Os incidentes de segurança serão criados se eventos de correlação forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar o desejo de sobrecarga de pesquisa de ingestão de obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, esse valor pode ser modificado para um minuto, se necessário.
◦ Campo Ingestão de eventos em andamento limpo ◦ Campo Recuperação única selecionado	Recuperação Única Use esta configuração se quiser uma extração única para ingerir eventos de correlação históricos. Quando esta configuração é definida, um perfil é usado uma vez para recuperar eventos de correlação de eventos históricos baseados em um intervalo de datas. À direita do campo Desde data, clique no ícone de calendário. No calendário exibido, selecione a data em que você deseja começar a extrair alertas. A partir do valor da data Desde, os eventos de correlação são recuperados até a data atual. Observe que você pode recuperar eventos de até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de eventos históricos por motivos de arquivamento, mas sim uma quantidade mínima de eventos em andamento que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os eventos de correlação forem extraídos, esta configuração não recuperará mais eventos de correlação para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os eventos de correlação encontrados para o intervalo inserido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como exemplo para programar um tempo de ingestão de evento de correlação inicial, se você tiver um diário ArcSight ESM Verificação de segurança que é executada uma vez por dia às 4 hora local, você pode configurar o perfil de evento de correlação correspondente em seu ServiceNow AI Platform Instância a ser executada às 4:05 hora local para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` No campo Ingestão de evento inicial. No campo Incremento (minutos), insira `1440` (24 horas) para programar a próxima ingestão de evento para 24 horas a partir da ingestão de evento inicial. A hora de ingestão do evento inicial e a hora de ingestão do próximo evento são exibidas nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, selecione **Ingestão de eventos em andamento** marque a caixa para habilitar esta opção.

   b. No campo Incremento (minutos), insira `1440` (24 horas).

   c. Clique em **Defina o tempo de ingestão do evento correlacionado inicial** Caixa de seleção para habilitar a edição dos campos Ingestão de evento inicial e Ingestão de próximo evento.

   d. No campo Tempo de ingestão do evento inicial, insira `04 05 00` .
   No campo Tempo de ingestão do próximo evento (estimado), a hora da próxima ingestão do evento é exibida.

4. Clique em **Continuar** Para navegar até a página Opções adicionais.

> **Nota:** O número padrão de incidentes de segurança que podem ser criados e agregados em um dia e o período de tempo do fluxo são definidos em ArcSight ESM Configurações de integração. Você pode modificar essas configurações, se necessário. Consulte ArcSight ESM Configurações de integração para integração de ingestão de evento para obter detalhes.

Opções adicionais: Automatizar atualizações de eventos correlacionados e fechamento com base em SIR status do incidente

. ArcSight ESM a integração tem uma interface bidirecional que permite que eventos de correlação criem incidentes de segurança, bem como a capacidade de atualizar os eventos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de correlação depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como número do incidente de segurança, grupo de atribuição, SIR URL do incidente e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais** .
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos correlacionados quando o incidente de segurança for criado.

Opção ou Campo	Descrição
Atualize eventos correlacionados após a criação de incidentes SIR	Selecione esta opção se quiser atualizar a fase do evento de correlação em ArcSight ESM e atualizam o evento com comentários adicionais quando um incidente de segurança é criado a partir do evento de correlação. Isso pode ocorrer para eventos de correlação que podem criar um novo incidente de segurança, bem como agregar incidentes de segurança existentes. **Nota:** Se esta opção não estiver selecionada, a fase do evento não será atualizada quando o incidente de segurança for criado.
Atualização da fase do evento correlacionado	Selecione uma opção de fase na lista de seleção Atualização de fase de evento correlacionado que exibe todas as fases disponíveis recuperadas do ArcSight ESM servidor.

Fase de evento correlacionado não configurada Se você não configurou nenhuma fase de evento correlacionada em seu ServiceNow AI Platform, você verá somente o. **Atribuir fase - Configuração inicial** Na lista de seleção Atualização da fase do evento correlacionado. Para configurar a fase, siga estas etapas:

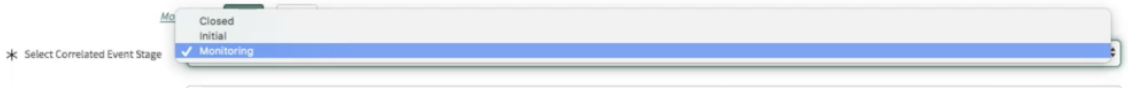
- Insira um ID de recurso no campo Inserir ID de recurso de fase e clique em **Enviar** . O ID do recurso é validado no ArcSight ESM e a tela a seguir são exibidos.



- Clique em **Salvar** para salvar a nova fase (**Monitoramento**).
- Clique na lista suspensa Selecionar fase de evento correlacionado.

Tradução automática

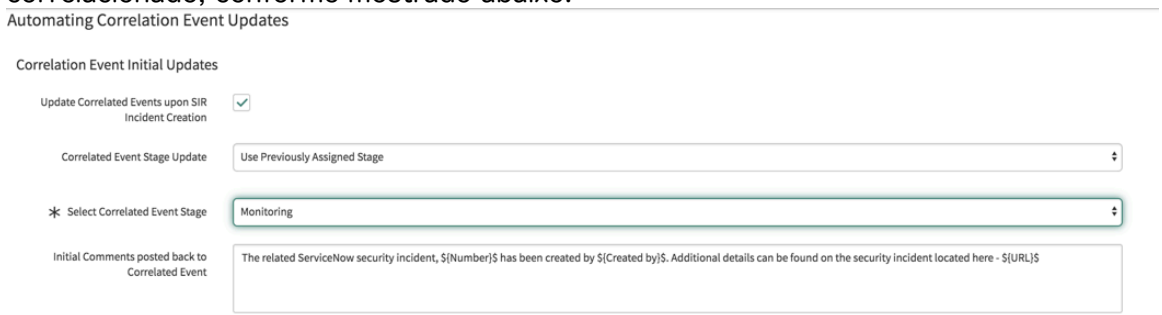
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Você pode selecionar a fase recém-criada na lista.

Fase de evento correlacionado já configurada : Se você já configurou a fase de evento correlacionado, siga estas etapas:

- Selecione **Usar fase atribuída anteriormente** Na lista de seleção Atualização da fase do evento correlacionado.
- Selecione uma fase existente na lista de seleção Selecionar fase de evento correlacionado, conforme mostrado abaixo.



- Comentários iniciais publicados novamente no evento correlacionado: Além de atualizar o valor da fase do evento de correlação, você também pode publicar comentários nas anotações da fase de correlação. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato"nome do campo" para qualquer campo no formulário de incidente de Resposta a incidentes de segurança.

Nota: Você pode usar as fases padrão definidas em ArcSight ESM console ou crie suas próprias fases personalizadas. Para criar uma nova fase, siga estas etapas:

- Em ArcSight ESM console, selecione **Arquivo** > **Novo(a)** > **Fase**. A guia Inspecionar/ Editar é exibida.
- Defina a nova fase e não selecione **Usuário obrigatório** caixa de seleção. Certifique-se de que a fase esteja definida corretamente e na posição correta no ciclo de vida do evento.

3. Na seção Automatizando fechamento de evento correlacionado, você pode definir como atualizar o incidente de segurança quando ele for encerrado.

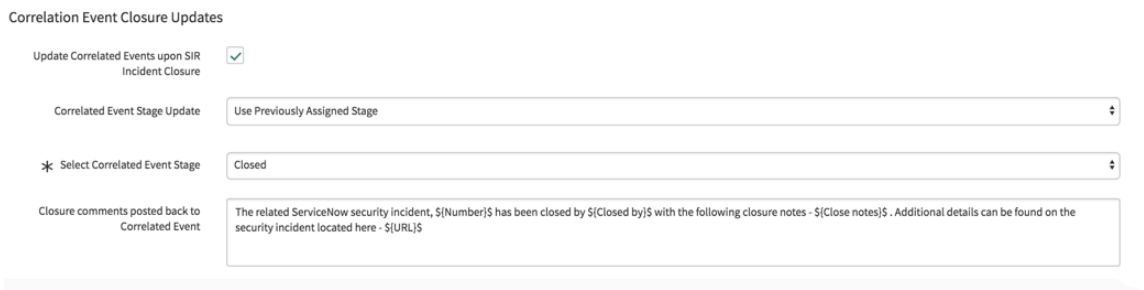
4. No formulário, preencha os campos.

Opção ou Campo	Descrição
Atualize eventos correlacionados após o fechamento do incidente SIR	Selecione esta opção se quiser atualizar o status do evento de correlação e adicionar comentários adicionais quando um incidente de segurança for encerrado a partir do evento correlacionado. Isso ocorrerá para os eventos notáveis de gatilho iniciais que criam o incidente de segurança, bem como eventos agregados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou Campo	Descrição
	Nota: Se esta opção não estiver selecionada, a fase do evento não será atualizada quando o incidente de segurança for encerrado.
Atualização da fase do evento correlacionado	Selecione uma opção de fase no menu que exibe todas as fases disponíveis recuperadas do ArcSight ESM servidor. Selecione o valor da fase a ser definido para todos os eventos de correlação quando um incidente de segurança for encerrado. **Nota:** As fases exibidas aqui são baseadas nas fases configuradas na seção Atualizações iniciais do evento de correlação.
Selecionar fase do evento correlacionado	Selecione um status apropriado aqui.
Comentários de fechamento publicados novamente no evento correlacionado	Além de atualizar o valor do status do evento de correlação, você também pode publicar comentários de fechamento nas anotações do evento de correlação. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato"nome do campo" para qualquer campo no formulário de incidente de Resposta a incidentes de segurança.



5. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair eventos de correlação do ArcSight ESM console baseado em sua programação.

ArcSight ESM Configurações de integração para integração de ingestão de evento

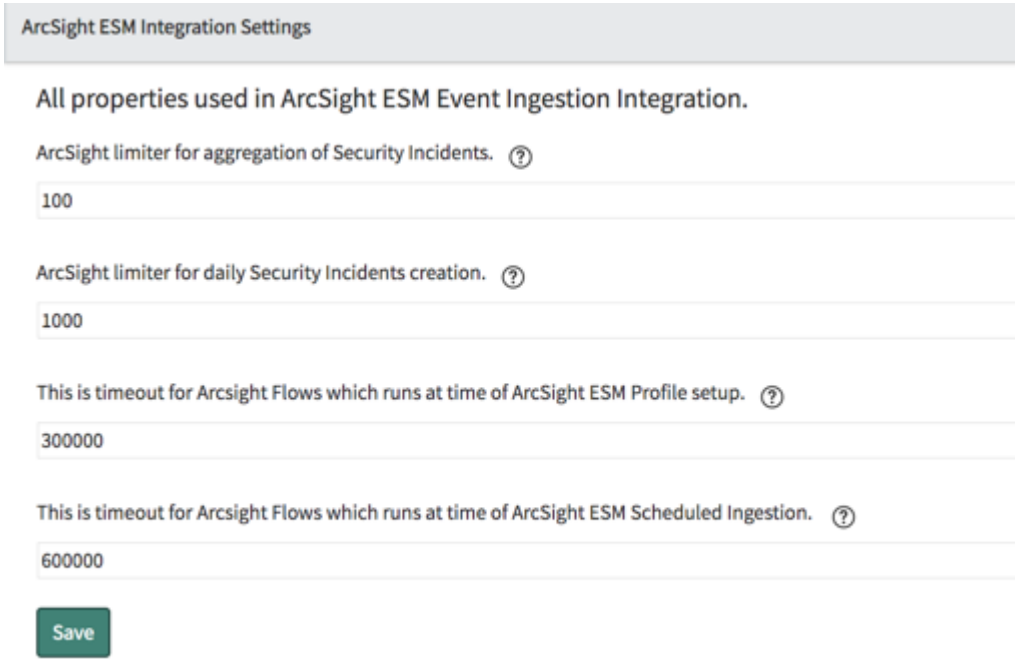
Use esta opção para modificar ArcSight ESM configurações de ingestão padrão.

Para modificar as propriedades do sistema, faça login como um usuário com *sn_si.admin* e navegue até **Integração do ArcSight ESM** > **Configurações de integração do ArcSight ESM**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

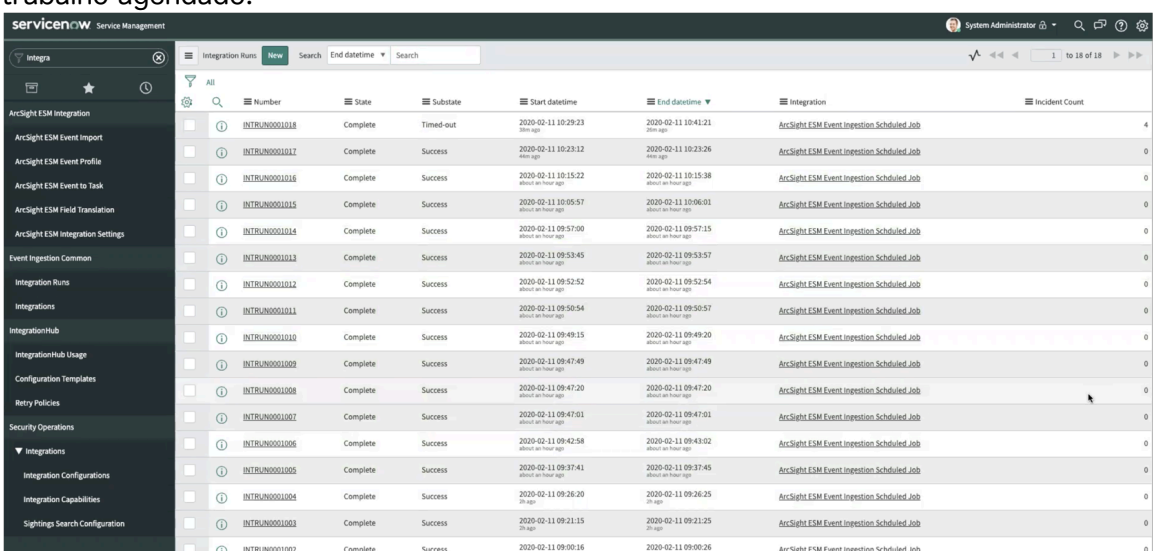


Solução de problemas ArcSight ESM integração de ingestão de evento

Esta seção fornece informações sobre como solucionar problemas de erros que possam ocorrer durante a ingestão de eventos.

Execuções de integração

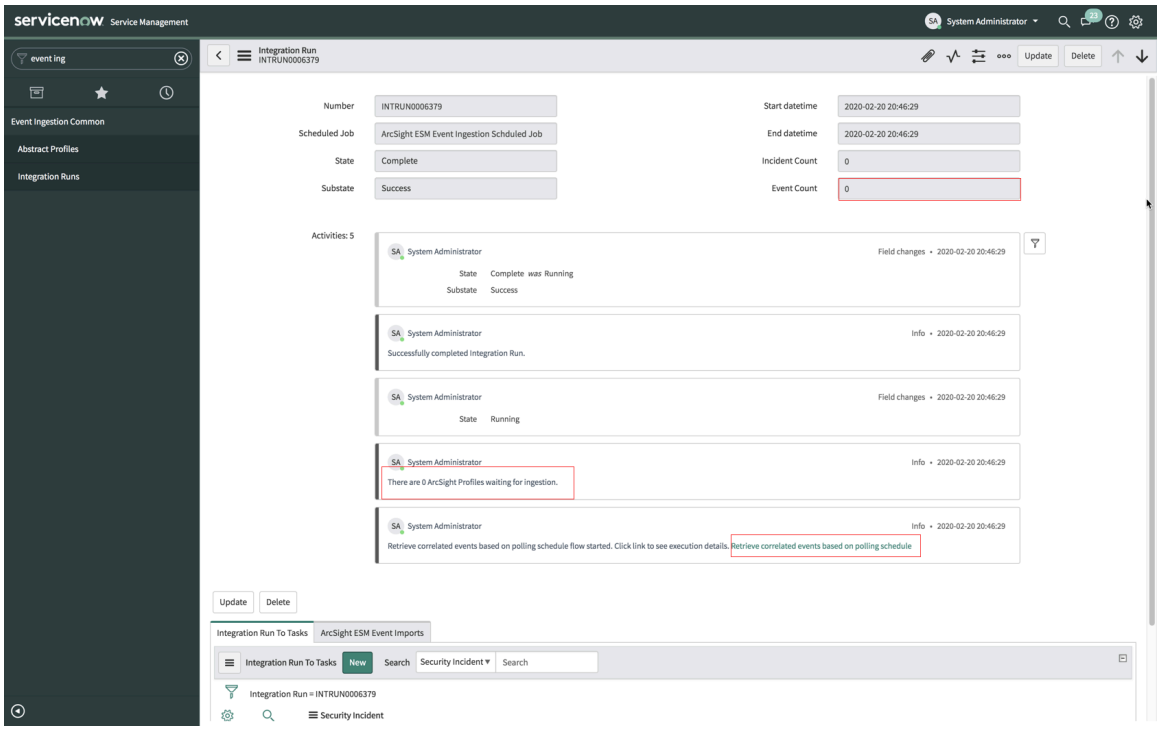
Navegar até **Ingestão de evento comum** > **Execuções de integração**. Uma execução de integração ocorre a cada minuto e captura detalhes sobre os eventos ingeridos durante o trabalho agendado.



Você pode ver a lista de execuções de integração e o status de cada execução (Sucesso, Tempo limite, Aguardando) e o número de incidentes de segurança que foram criados. Clique no link Número para detalhar a página Execução de integração detalhada.

Tradução automática

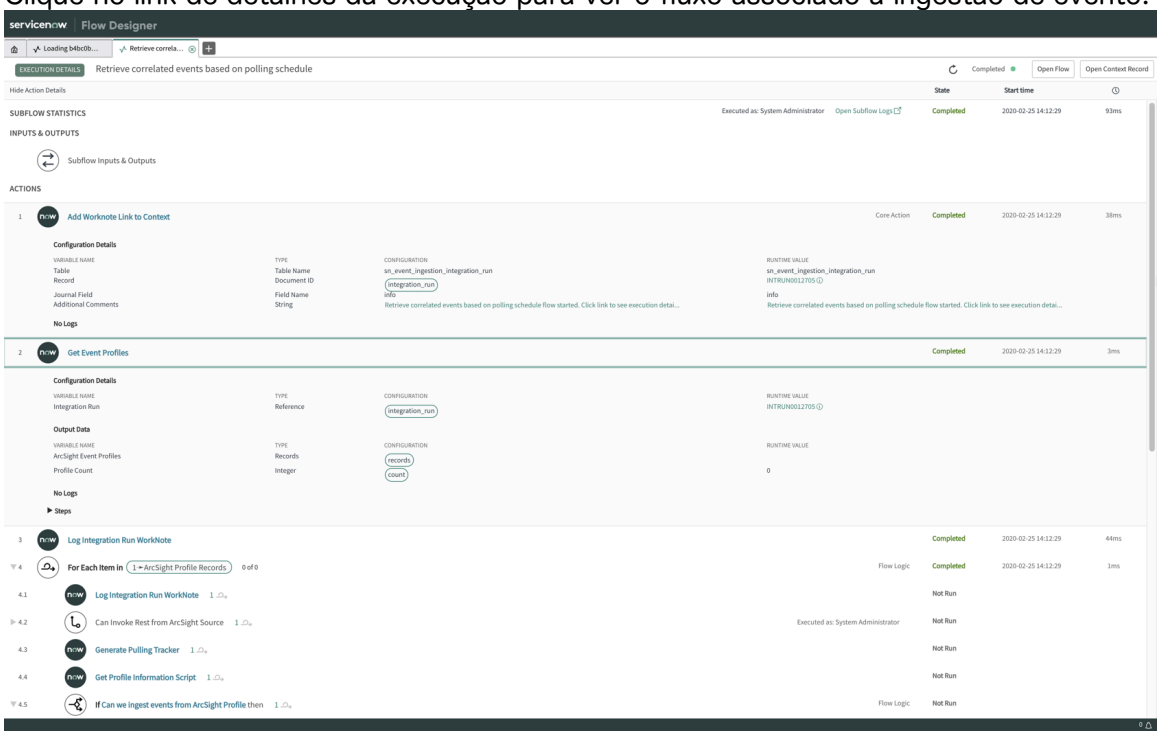
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode exibir detalhes como o número de eventos que foram ingeridos, o status, qual evento foi transformado em um incidente de segurança e as diferentes tarefas realizadas durante a ingestão. Além disso, você pode clicar no link para exibir os detalhes da execução do fluxo.

Detalhes da execução do fluxo

Clique no link de detalhes da execução para ver o fluxo associado à ingestão de evento.



Você pode exibir uma execução passo a passo do fluxo detalhando as várias ações e subfluxos que foram executados como parte do fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cópia ArcSight ESM perfil para integração de ingestão de evento

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis para economizar tempo.

Antes de Iniciar

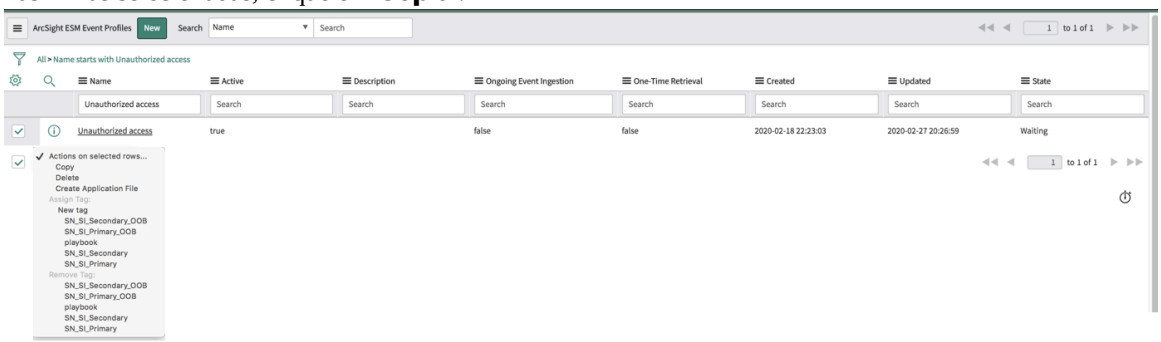
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

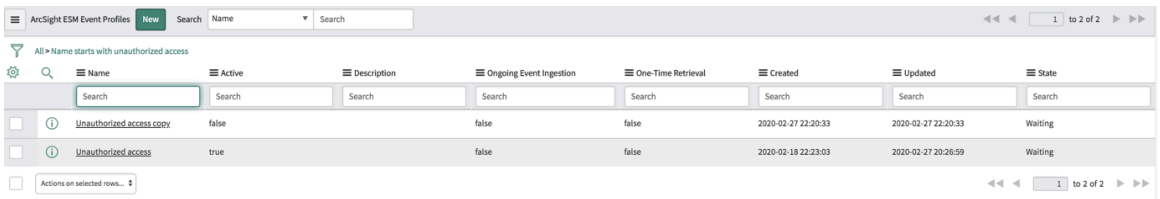
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Tudo** > **Integração do ArcSight ESM** > **Perfil de evento do ArcSight ESM**.
2. Na lista Perfis do ArcSight exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Cópia** .



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que **Ativo** o status da coluna é definido como falso, pois o perfil precisa ser ativado.

Use o editor de scripts para formatar valores de evento de correlação

Além dos campos mapeados diretamente dos valores de evento de correlação ingeridos, use o editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O editor de script muda os valores de um ArcSight ESM campo evento de correlação para que os valores compatíveis com ServiceNow AI Platform SIR Os incidentes de segurança são mapeados para os campos Categoria, Item de configuração (IC), Observável e outros campos de incidente de segurança.

Em determinados casos, ArcSight ESM Os valores de evento de correlação são mapeados para campos de referência, como Categoria, Item de configuração (IC) e campos observáveis no incidente de segurança. Como um usuário com a função sn_si.admin, você pode preferir editar os valores do campo de evento mapeado para traduzir o formato ou os valores de dados para estar em conformidade com os formatos de campo de incidente e os valores esperados. Se você quiser traduzir o valor de um ArcSight ESM evento de correlação com um valor compatível com esses campos no SIR incidente de segurança, use o editor de scripts.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de scripts.
2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete [] ao lado de um campo para abrir o editor de script desse campo.

   Em determinados casos, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento de correlação, por exemplo, um valor para o item de configuração pode não ser correspondido.

   Se não for possível encontrar uma correspondência para um nome de host em ServiceNow AI Platform CMDB Para o campo Item de configuração, você pode editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração.

   O editor é aberto com o campo exibido em Campo de destino.
4. Insira as mudanças no script e clique em **Atualização** para salvar suas mudanças.
   . ArcSight ESM A tabela Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

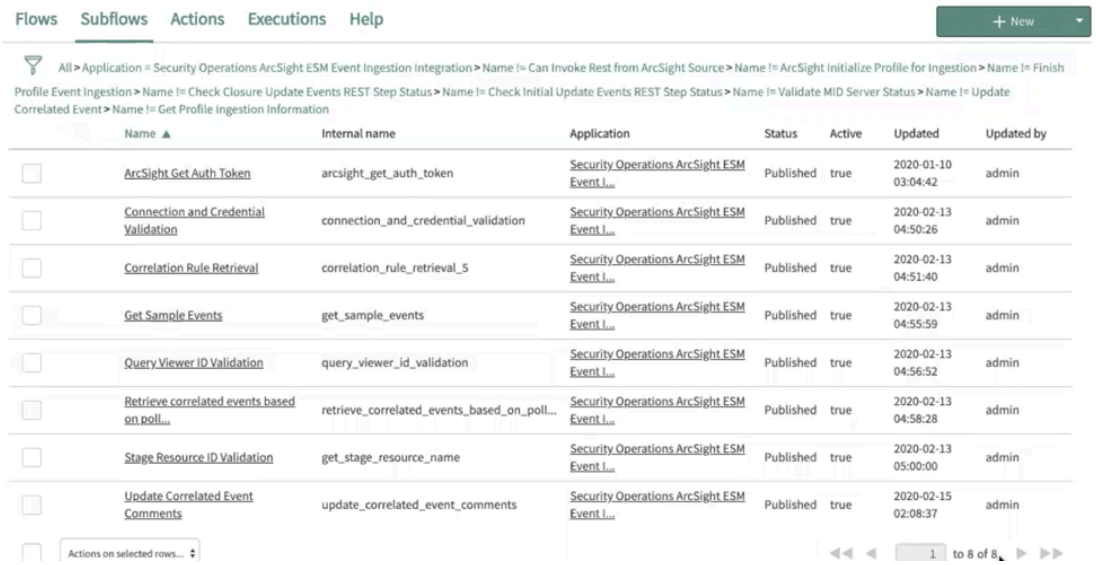
Uso do Flow Designer com ArcSight ESM integração de ingestão de evento

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com o. ArcSight ESM integração.

Para exibir esses subfluxos, navegue até **Flow Designer** > **Designer** e clique em **Subfluxos** guia. A figura abaixo mostra os subfluxos importantes usados durante a criação do perfil e o trabalho de ingestão programada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



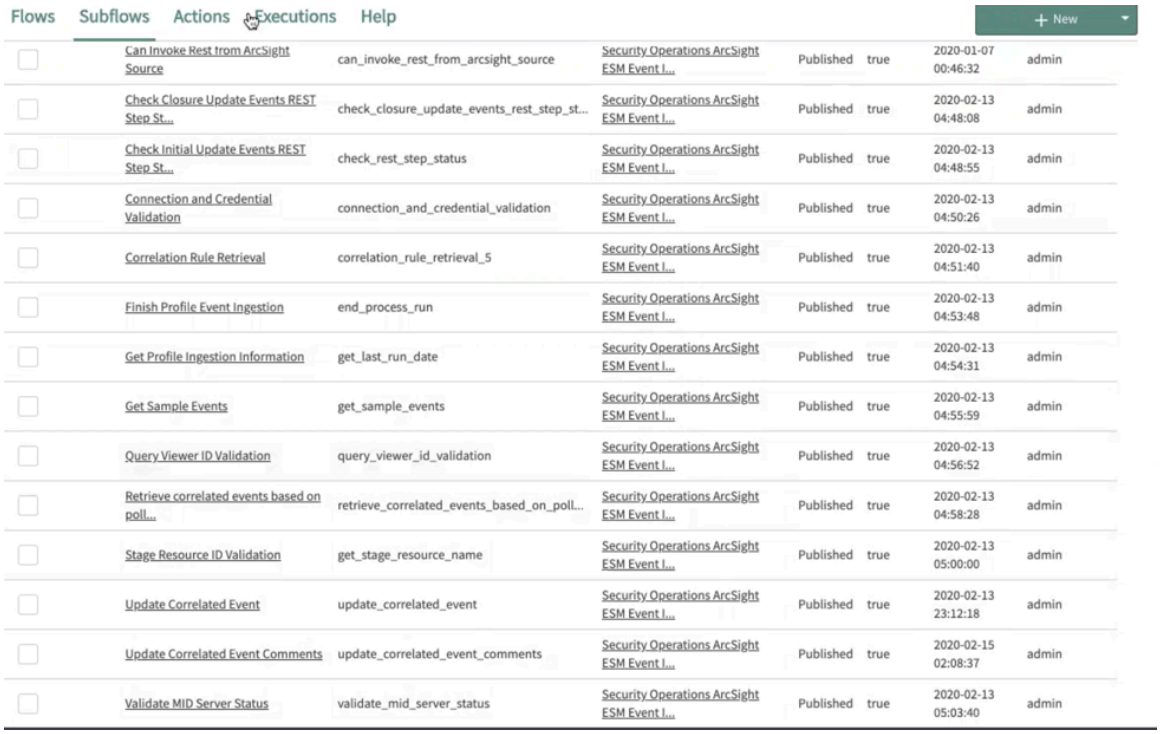
Esses subfluxos são listados na sequência em que são executados abaixo:

- **Validação de conexão e credencial** Este subfluxo valida ServiceNow conectividade com ArcSight ESM e as credenciais especificadas. Este subfluxo é usado quando você clica em **Configurar** botão em **ArcSight ESM - Ingestão de evento** lado a lado no **Operações de segurança** > **Integrações** > **Configuração de integrações** página.
- **ArcSight Obter token de autenticação** : Este subfluxo gera o. ArcSight ESM Token de autenticação do Nome de usuário e Senha usando ArcSight ESM Serviço de login. O Serviço de login fornece o token de autenticação que pode ser usado para chamar qualquer outro ArcSight ESM endpoint. Este subfluxo é usado em todos os outros subfluxos.
- **Validação do ID do visualizador de consulta** : Este subfluxo verifica se o ID do visualizador de consulta especificado durante a criação do perfil está presente no ArcSight ESM servidor.
- **Recuperação de regra de correlação** : Este subfluxo recupera as regras de correlação com base no ID do Visualizador de consulta.
- **Obter evento de amostra** : Este subfluxo busca os eventos de correlação de amostra do ArcSight ESM servidor. Esses eventos de amostra são mapeados para os campos de incidente de segurança na seção Mapeamento do perfil.
- **Validação do ID do recurso da fase** : Este subfluxo valida o ID do recurso de fase especificado no ArcSight ESM E busca o nome do recurso.
- **Atualizar comentários de evento correlacionado** : Este subfluxo atualiza os comentários do evento correlacionado nas seções Inicial e Encerramento do incidente na página Opções adicionais do perfil.
- **Recupere eventos correlacionados com base na programação de pesquisa** : Este subfluxo executa o trabalho agendado que busca os eventos correlacionados com base no intervalo de pesquisa.

Durante a execução, os subfluxos acima também acionam vários outros subfluxos e ações direta ou indiretamente, conforme mostrado abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web Services(AWS) Hub de segurança integração

AWS Security Hub É um serviço de Gestão de postura de segurança na nuvem (CSPM) que fornece verificações de segurança automatizadas e contínuas e verificações de práticas recomendadas em relação aos seus recursos da AWS.

Visão geral do AWS Security Hub integração

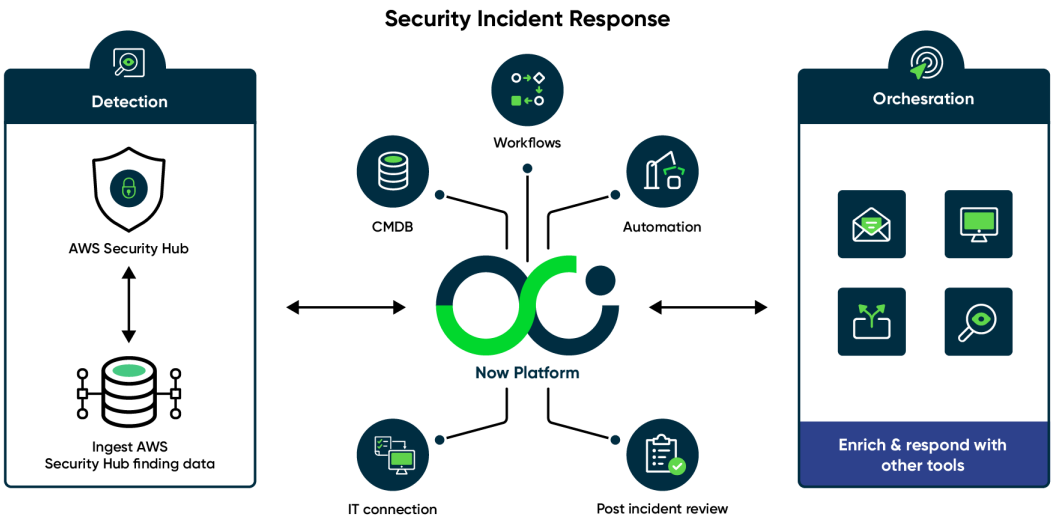
AWS Security Hub permite que você identifique problemas em suas configurações. O Security Hub agrega seus alertas de segurança, que são chamados de descobertas. AWS Security Hub gera essas descobertas em um formato padronizado e as prioriza para que você possa enriquecer, investigar e corrigir com mais facilidade. Você pode usar AWS Security Hub Integração para ingerir descobertas do Hub de segurança e criar automaticamente incidentes de segurança no Resposta a incidentes de segurança.

AWS Security Hub integração no SIR segue uma arquitetura bidirecional. SIR ingere Hub de segurança descobre dados para criar um incidente de segurança e atualiza simultaneamente um Hub de segurança descoberta com atualizações no incidente de segurança correspondente.

Consulte o diagrama a seguir para saber como o AWS Security Hub se integra ao ServiceNow AI Platform Operações de segurança aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Use os principais recursos desta integração para executar as seguintes ações:

- Descubra descobertas do AWS Security Hub que são candidatas a incidentes de segurança e automatize a criação desses incidentes de segurança.
- Mapeie descobertas do AWS Security Hub e campos de entidade para SIR campos de incidente de segurança.
- Filtrar descobertas do AWS Security Hub.
- Agregue descobertas a incidentes de segurança em aberto existentes para que você não precise criar incidentes de segurança duplicados.
- Automatize as atualizações de status das descobertas do AWS Security Hub para Resposta a incidentes de segurança para que você possa criar e fechar incidentes de segurança.

  Nota: ServiceNow Também atualiza o status das descobertas do AWS Security Hub com base na criação, no andamento ou no fechamento do incidente de segurança. Esta atualização também inclui comentários de descobertas agregadas e novas.

- Programe a ingestão de descobertas para criar incidentes de segurança periodicamente.
- Sincronizar comentários de descoberta do AWS Security Hub com SIR Anotações de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça esta integração

Identificador do documento	Título do documento
Site de documentação do produto do AWS Security Hub	AWS Security Hub Documentation
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece com AWS Security Hub integração

Ativar e configurar o. AWS Security Hub Integração de descobertas do plug-in Security Operation para fazer interface com seu ServiceNow® instância e. Resposta a incidentes de segurança produto.

Antes de Iniciar

Função necessária: sn_si.admin

Antes de poder usar AWS Security Hub, você deve baixá-lo do ServiceNow Store.

Por Que e Quando Desempenhar Esta Tarefa

Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração tranquila.

Check-list

Atribua e verifique o necessário ServiceNow® plataforma e. Resposta a incidentes de segurança funções.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria perfis de incidente. ◦ Mapeia o. AWS Security Hub encontrar campos de dados para os campos de incidente de segurança. ◦ Agenda a ingestão de incidentes em andamento. ◦ Habilita atualizações de incidentes quando um Resposta a incidentes de segurança o incidente foi criado ou encerrado.
Atribua o. AWS Security Hub funções necessárias.	As funções a seguir são necessárias em AWS Security Hub para registrar e configurar sua aplicação: • SecurityHubReadOnlyAccess • SecurityHubFullAccess

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Revise AWS Security Hub configurações de integração	Navegar até **Tudo** > **Integração de descobertas do AWS Security Hub** > **Configurações de integração de descobertas do AWS Security Hub**. Revise ou modifique as configurações de propriedades de acordo com seus requisitos.
Configure sua aplicação no AWS portal.	Registre sua aplicação no AWS e conceda aos usuários acesso de leitura e gravação à aplicação . Para obter mais informações, consulte os tópicos a seguir: • Configuração da configuração da AWS com o console • Integrações do Hub de segurança.

Registre e configure o. AWS Security Hub portal

Registre sua aplicação no AWS Security Hub e conceda aos usuários acesso de leitura e gravação à aplicação .

Registrando um ServiceNow® perfil de usuário em AWS portal

Antes de Iniciar

Função necessária: AWSSecurityHubFullAccess

Procedimento

1. Faça login no AWS portal.
2. Navegar até **Gestão de identidade e acesso (IAM)** > **Usuários** > **Criar usuário novo**.
3. A tabela a seguir descreve os campos que você deve configurar para criar um perfil de usuário:

Crie um perfil de usuário

Campo	Descrição
Especifique os detalhes do usuário > **Nome de usuário**	Nome do perfil de usuário.
Definir permissões > **Adicionar usuário ao grupo**	Adicione o perfil de usuário a um grupo com políticas de permissão predefinidas. Você pode criar um grupo de acordo com sua preferência e atribuir políticas de permissão ao grupo. Mais tarde, você pode adicionar perfis de usuário ao grupo e as políticas de permissão atribuídas ao grupo são atribuídas automaticamente aos perfis de usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Copiar permissões	Copie permissões de um perfil de usuário e atribua as mesmas ao novo perfil de usuário.
Anexar políticas diretamente	Adicione AWSSecurityHubFullAccess como a política de permissão para seu perfil de usuário. Atribua uma nova política de permissão ao perfil do usuário de acordo com sua preferência.
Revise e crie	Revise todos os detalhes que você adicionou no perfil de usuário.

4. Selecione **Criar usuário** .
5. Selecione **Exibir usuário** na janela pop-up exibida.
6. Crie uma chave de acesso e uma chave de acesso secreta para o perfil do usuário.
   Essas chaves são necessárias para acessar o. AWS Security Hub integração do seu ServiceNow® instância.
7. Navegar até **Serviços da AWS** > **Pesquisar** > **AWS Security Hub** > **.**
8. Selecione **Vá para** *`Hub de segurança`*.
9. Em Habilitar AWS Security Hub, selecione **Download** para habilitar AWS Configuração.
   Baixe os arquivos e execute-os em sua conta. Isso concede a você permissão para coletar todas as informações de vários serviços de emissão de relatórios da AWS e agregar a. AWS Security Hub.
10. Selecione **Habilitar** *`AWS Security Hub`*na parte inferior da página.
    Leva alguns minutos para *`AWS Security Hub`*Painel para exibir todos os detalhes.
11. Mudar região de **Global** . **Leste DOS EUA (Ohio)** .
    O código para **Leste DOS EUA (Ohio)** . **leste dos eua-2** . Todos ServiceNow® os recursos são atribuídos a este código de região.

Instale e configure o. AWS Security Hub integração

Instale e configure o. AWS Security Hub integração do ServiceNow Store em seu ServiceNow AI Platform instância para iniciar a ingestão AWS Security Hub descobertas.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe o. AWS Security Hub integração do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE AWS Security Hub lado a lado e clique **Configurar** .
4. No formulário, preencha os campos.

AWS Security Hub Formulário de configuração

Campo	Descrição
Nome	Nome do AWS Security Hub configuração da instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome da região	Região que você atribuiu em ServiceNow® perfil de usuário em AWS Security Hub portal.
Chave Secreta	Chave secreta que você criou para ServiceNow® perfil de usuário em AWS Security Hub portal.
Chave de acesso	Chave de acesso que você criou para ServiceNow® perfil de usuário em AWS Security Hub portal.

5. Clique em **Enviar**.

Resultado
Depois de validar e enviar com sucesso a configuração, cada um Hub de segurança A configuração do servidor de ingestão de descobertas é salva na página Integrações de segurança como um bloco.

Crie um perfil para AWS Security Hub integração da descoberta

Crie um AWS Security Hub perfil em seu ServiceNow AI Platform instância da qual você usará para ingerir dados AWS Security Hub e criam um incidente de segurança correspondente em Espaço de resposta a incidentes de segurança.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A integração permite que você crie incidentes de segurança para diferentes tipos de descobertas no AWS Security Hub plataforma, como tentativas de acesso não autorizado e malware. Esses incidentes são criados com base nos perfis que você configura no ServiceNow AI Platform instância. Inicialmente, todos os incidentes são criados para um tipo de descoberta configurado em um perfil. Você pode filtrar ainda mais as descobertas criadas para especificar quais descobertas criam incidentes de segurança.

Todas as descobertas que atendem aos critérios de seleção em seu AWS Security Hub locatário, e estão disponíveis sobre AWS Security Hub Inicialmente, são ingeridas em seu ServiceNow AI Platform instância.

Procedimento

1. Navegar até **Tudo** > **Integração de descobertas do AWS Security Hub** > **Perfil de descobertas do AWS Security Hub**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

AWS Security Hub Formulário Configuração de ingestão de descobertas

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda você a identificar o tipo de perfil e também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Selecione para ativar o perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando o perfil está ativo, isso implica que ServiceNow AI Platform ingere ativamente AWS Security Hub os dados de descobertas e os incidentes de segurança correspondentes são criados em SIR quando as condições de filtragem são correspondidas.
Origem	. AWS Security Hub Locatário de integração que você configurou para ingerir descobertas. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de descoberta que você planeja ingerir para o perfil.
Ordem	Insira um valor para este campo que indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Descrição	Texto extra para ajudá-lo a distinguir este perfil de outros perfis.

Mapeie o. AWS Security Hub campos de descoberta

Mapeie o indivíduo AWS Security Hub campos de descoberta para os campos no SIR incidente de segurança para que você possa criar incidentes com os dados mapeados.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Na página de mapeamento, em AWS Security Hub Seção Mapeamento, selecione um dos métodos de ingestão de amostra.

Métodos de ingestão de amostra

Campo	Descrição
Todos os campos de descoberta padrão	Use este método de ingestão para exibir a lista estática de todos os campos de descobertas. Este método contém somente nomes de campo padrão sem valores. Você pode usar essas informações para mapear com SIR campos.
Recuperar recente AWS Security Hub descobertas	Use este método de ingestão para importar os dados das descobertas mais recentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Você pode ingerir 5 descobertas de amostra por padrão e um máximo de 20 descobertas de amostra. Os valores do campo de descoberta de amostra são preenchidos quando o perfil ingere as descobertas de amostra. Você pode mapear essas descobertas para **Campos de destino do incidente SIR** . Os campos e valores de descoberta aparecem como guias individuais.
Importar dados de amostra	Selecione **Importar dados de amostra** para importar descobertas de amostra AWS Security Hub. Este botão aparece quando você seleciona Recuperar recente AWS Security Hub método de ingestão de descobertas. Recuperando descobertas de amostra de AWS Security Hub o servidor leva alguns momentos. Mapeie essas descobertas para **Campos de destino do incidente SIR** . Os campos e valores de descoberta aparecem como guias individuais.

2. Para adicionar campos aos campos padrão exibidos no incidente de segurança, execute as seguintes ações:

Na seção Campos de destino do incidente SIR, selecione Map another field botão. Mostra uma lista de SIR campos, a partir dos quais você pode selecionar para exibir um novo campo.

a. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Nota: Vários observáveis podem ser exibidos no mesmo incidente de segurança. Por exemplo, o. **Observável** o campo pode ser mapeado várias vezes com valores diferentes. Da mesma forma, o **Item de configuração** e. **Campos de anotações de trabalho** suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, verá uma mensagem de erro informando que este campo não oferece suporte a vários valores. Da mesma forma, se um campo em um incidente de segurança tiver uma lista da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista, o campo não será preenchido no incidente de segurança.

b. Em AWS Security Hub Seção Campos de origem, arraste o campo para mapeá-lo para o novo campo.

c. Quando você marca a caixa de seleção que corresponde a um campo, todas as mudanças novas ou atualizadas feitas em AWS Security Hub São atualizados automaticamente no respectivo SIR com novos dados de incidente.

Nota: No sistema de base, a propriedade do sistema sn_sec_security.finding_updates é definida por padrão como verdadeira para receber o. AWS Security Hub Atualizações relacionadas a novos alertas vinculados ao SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Por padrão, os campos Usuários afetados, Itens de configuração e Observáveis são verificados. Sempre que houver novos observáveis ou itens de configuração associados, ou usuários afetados que são adicionados ao incidente, essas informações serão extraídas e preenchidas automaticamente nas respectivas listas relacionadas na Resposta a incidentes de segurança (SIR) durante esse intervalo de pesquisa.
- Para quaisquer outros campos, você deve marcar a caixa de seleção que corresponde a um campo para todas as mudanças novas ou atualizadas feitas na descoberta em AWS Security Hub. Atualiza automaticamente os respectivos dados do incidente SIR com os novos dados do incidente.

Importante: A due diligence deve ser feita antes de selecionar esta funcionalidade, pois a substituição dos dados existentes pode resultar em dados instáveis para o analista trabalhar e qualquer outra automação definida até mesmo pelos valores de campo do incidente de segurança também pode ser afetada. Portanto, é importante fazer a due diligence antes de selecionar qualquer funcionalidade de substituição.

3. Para remover um campo, use (**Remover item**) Ao lado do campo Expressão de entrada na seção Campos de destino do incidente SIR.
4. Para mapear um valor de campo do AWS Security Hub Para um campo na seção Campos de destino do incidente SIR, use uma das seguintes ações:

   a. Arraste o nome do campo (por exemplo, id) e solte-o ao lado de um nome de campo na coluna Campos de destino do incidente SIR.

   Você pode corresponder a qualquer valor do AWS Security Hub Seção Campos de origem para um campo na seção Campos de destino do incidente SIR. Os campos são codificados por cores para que você não ignore ou duplique os campos de descoberta no processo de mapeamento. Campos azuis claros indicam que um campo de descoberta ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de descoberta de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo de descoberta foi selecionado e mapeado para um campo no incidente de segurança. Dessa forma, você pode visualizar quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de descoberta importante restante permanece não mapeada. No entanto, existem alguns campos no AWS Security Hub Seção Campos de origem que não são compatíveis com os campos na seção Campos de destino do incidente SIR. Se você mapear esses valores, eles não serão exibidos quando o SIR for criado.

   b. Você pode adicionar uma combinação de texto e campo.
   Por exemplo, `O nome da descoberta é .` Aqui, `O nome da descoberta é` pode ser inserido manualmente enquanto `(nome)` é mapeado a partir de AWS Security Hub Seção Campos de origem.

   c. Você pode inserir e mapear manualmente um campo de descoberta de origem para um campo de destino. Use oformato "nome do campo" para mapear manualmente um campo de descoberta de origem. Por exemplo, para mapear a severidade de um campo de descoberta, o formato é `(propriedades(severidade))` .

Esta integração classifica determinados subtipos observáveis. Ao mapear um AWS Security Hub Campo de descoberta com o campo observável SIR, o. ServiceNow AI Platform classifica automaticamente o observável. Se você quiser mapear genericamente a entrada AWS Security Hub observável para o tipo de observável em SIR, em seguida, arraste e solte o. AWS Security Hub Campo no campo Observável. No

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

entanto, se você estiver ciente do tipo de observável para a entrada AWS Security Hub observável em SIR, em seguida, mapeie especificamente para SIR Campo de tipo de observável. Alguns exemplos de tipos de observáveis específicos em SIR Incluir Observable (nome do domínio), Observable (endereço de e-mail), Observable (endereço IP (V4)) e Observable (nome do host).

Às vezes, encontrar valores de campo em AWS Security Hub Não pode ser traduzido diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos.

5. Para formatar uma tradução de campo para um novo campo de um AWS Security Hub Descoberta Para corresponder a um valor de campo em um Incidente de segurança, clique em **Clique aqui** link no **Campos de destino do incidente SIR** cabeçalho.

6. Para modificar os campos compatíveis com a tradução de campo, clique em  ícone de tradução de campo de formato de script.
   Os campos compatíveis com a tradução de campo são **Categoria** , **Item de configuração** e **Prioridade** . Por exemplo, clique em  Ícone ao lado da Categoria. . AWS Security Hub O editor de script Tradução de campo de descobertas é aberto.

7. Insira as mudanças no script e clique em **Atualização** Para salvar as mudanças e retornar à página Mapeamento.
   Por exemplo, para Categoria, defina o seguinte no editor de scripts:

   ```
   "<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
   ```

   Este mapeamento garante que um perfil use somente categorias configuradas.

8. Continue seu mapeamento adicionando ou removendo valores de campo.
   Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que uma descoberta de entrada deve atender para criar um incidente de segurança.

9. Para ir para a seção Filtragem e agregação, clique em **Continuar** .

O que Fazer Depois

Defina e defina condições de filtro para que você possa especificar quais descobertas criam incidentes de segurança. Você pode usar os mesmos valores de campo (definidos na seção Mapeamento) no construtor Condições de geração de incidentes (na seção Filtragem e agregação) para definir critérios adicionais que uma descoberta de entrada deve atender para criar um incidente de segurança.

Defina critérios de filtro e agregação para AWS Security Hub ingestão de descobertas

Você pode definir e definir condições de filtro para especificar quais descobertas de entrada devem criar incidentes de segurança. Você também pode definir critérios de campo de incidente adicionais que permitem que uma descoberta de entrada seja anexada a um incidente de segurança em aberto em vez de criar outro incidente de segurança para a mesma descoberta.

Defina as condições de filtragem para AWS Security Hub descobertas para criar incidentes de segurança

Defina as condições de filtragem para que os incidentes de segurança sejam criados somente quando as condições de filtragem corresponderem.

Antes de Iniciar

Função necessária: sn_si.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda você a isolar incidentes de segurança e limita o número de incidentes de segurança que você cria. Se você definir critérios de filtragem adicionais, somente as descobertas necessárias serão ingeridas sem precisar mudar a consulta ou a configuração do incidente acionado.

Execute as etapas a seguir para definir os critérios de entrada AWS Security Hub a descoberta deve satisfazer para que um incidente de segurança seja criado:

Procedimento

1. Selecione **Aplicar pré-filtro** Na seção Pré-filtragem.

   Você pode usar esta opção para filtrar descobertas específicas e reduzir a carga de ingestão de descobertas.

   Em **Filtro de API** Insira uma condição JSON de acordo com seu requisito que filtra descobertas específicas com base na condição. Por exemplo, insira o seguinte valor para filtrar descobertas que têm Status de fluxo de trabalho como Resolvido no Hub de segurança:

   ```
   {"Filters"{
    "WorkflowStatus":[{
    "Comparison":"NOT_EQUALS",
    "Value": "RESOLVED"}]
   }
   }
   ```

   Com base na condição fornecida, AWS Security Hub as descobertas são ingeridas e exibidas no AWS Security Hub tabela bruta de descobertas.

   Navegar até **Tudo** > **Integração de descobertas do AWS Security Hub** > **Descobertas brutas do AWS Security Hub** para exibir os dados brutos das descobertas.

2. Na seção Selecionar campos de descoberta para condições de filtro, selecione **Exiba os campos de descoberta disponíveis** para exibir uma lista de todos os campos disponíveis em um AWS Security Hub descoberta.
   De **Todos os campos de descoberta** Selecione os campos de descoberta que você deseja exibir na seção Condições de geração de incidentes de segurança.

   Nota: Uma descoberta do AWS Security Hub contém vários campos e valores. Em **Todos os campos de descoberta** , você pode pesquisar um campo de descoberta de acordo com seu requisito e selecioná-lo.

3. Na seção Condições de geração de incidentes de segurança, selecione **Filtro com base em condições** para definir os critérios que um de entrada AWS Security Hub a descoberta deve satisfazer para que um incidente de segurança seja criado.

   O primeiro campo em Condições de filtro contém uma lista padrão de duzentas campos que estão disponíveis em um AWS Security Hub Descoberta e os campos de descoberta selecionados na seção Selecionar campos de descoberta para condições de filtro.

   O segundo campo nas Condições de filtro contém operadores condicionais. A opção escolhida determina a condição que deve ser atendida para ingerir uma descoberta.

   O terceiro campo nas Condições de filtro contém valores compatíveis com os campos de descoberta disponíveis. Verifique se o campo de descoberta inserido corresponde aos valores das descobertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, use a condição de filtro *contém* para os seguintes campos com vários valores:

- Workflow(Status)
- WorkflowState

4. Usando as listas e os campos do construtor de condições, defina os filtros para a primeira linha.
5. Para adicionar mais condições, clique em **E.** ou **OU** .
   - Se **E.** selecionado, todas as condições devem ser correspondidas.
   - Se **OU** está selecionado, qualquer condição pode ser correspondida.
6. Para definir uma segunda condição de filtro, clique em **Novos critérios** .

Resultado

Com base nas condições de filtragem, AWS Security Hub as descobertas são importadas para SIR. Navegar até **Tudo** > **Integração de descobertas do AWS Security Hub** > **Importação de descobertas do AWS Security Hub** para exibir as descobertas importadas.

Defina condições a serem agregadas AWS Security Hub descobertas de um incidente de segurança

Defina critérios de agregação de incidentes adicionais que agreguem uma entrada AWS Security Hub Encontrar um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Quando você usa critérios de valor de correspondência de campo para cada perfil, essa agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de incidentes relacionados em um único incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Se um novo incidente corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o incidente será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os incidentes agregados adicionados em uma lista relacionada em um incidente de segurança.

Agregados AWS Security Hub as descobertas em um incidente de segurança são exibidas no AWS Security Hub lista relacionada. Esta lista detalha os carimbos de data/hora associados e os valores de campo agregados. Essas informações ajudam você a entender o motivo AWS Security Hub as descobertas são adicionadas aos incidentes de segurança existentes.

Procedimento

1. Para definir critérios de campo de incidente adicionais que permitem uma entrada AWS Security Hub descoberta a ser anexada a um incidente de segurança em aberto em vez de criar um novo incidente, selecione **Condições de agregação** opção.
2. Em **Campos de incidente com valores correspondentes** campo, insira os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform instância. Todos os valores de campo selecionados no campo de entrada de seleção múltipla devem corresponder para que os critérios de agregação sejam atendidos e que este incidente de entrada possa ser anexado a um incidente de segurança existente. Esta seleção implica que é um *E.* Condição em que campos, como Observáveis e Itens de configuração que podem ter vários valores de campo, são mapeados para eles. Se somente um subconjunto dos valores for correspondido, o AWS Security Hub as condições de agregação de descobertas não foram atendidas e um novo incidente de segurança é criado.
3. Para adicionar várias condições de correspondência de campo, clique em **Adicionar novos critérios** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A agregação ocorrerá se qualquer uma das condições do campo de seleção múltipla que você definir for atendida. Esta seleção implica *OU* condição.

4. Para atualizar a anotação de trabalho de uma nova descoberta quando ela for adicionada a um incidente de segurança, selecione **Anotação de trabalho em log para nova descoberta** .

   A anotação de trabalho registra em log que uma nova descoberta foi adicionada e inclui um link para os detalhes da descoberta. A anotação de trabalho de log também atualiza mais detalhes que você adiciona ao campo de anotação de trabalho na seção de mapeamento.

5. Para configurar a programação, clique em **Continuar** .

Resultado

Com base nas condições de agregação, AWS Security Hub as descobertas são agregadas para criar um para criar um SIR incidente. Navegar até **Tudo** > **Integração de descobertas do AWS Security Hub** > **Descobertas do AWS Security Hub para tarefa** para exibir a lista de incidentes de segurança que foram criados.

O que Fazer Depois

Defina uma programação para recuperar os dados da descoberta e os incidentes da descoberta que correspondem aos critérios no perfil.

Programe o. AWS Security Hub recuperação da descoberta

Defina uma programação para recuperar os dados da descoberta e ingerir o. AWS Security Hub descobertas que correspondem aos critérios no perfil.

Antes de Iniciar

Função necessária: sn_sni.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que deseja pesquisar para o futuro AWS Security Hub descobertas que correspondem a. AWS Security Hub configuração do perfil de descoberta.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho do AWS Security Hub integração de descobertas. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente. Um valor padrão de um minuto é definido para todos os perfis. Você pode modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Todos os alertas adicionados ao incidente em um intervalo de pesquisa específico são processados e anexados ao AWS Security Hub alertas e listas relacionadas e comentários.

Procedimento

1. No formulário de programação, preencha os campos.

   Configure a programação para definir como e quando você extrai descobertas do AWS Security Hub locatário.

Formulário de programação

Campo	Descrição
Ingestão de descoberta contínua	Ingestão de descoberta contínua que o ServiceNow AI Platform a instância extrai do AWS Security Hub locatário para novos incidentes. Os incidentes de segurança serão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	criados se descobertas acionadas forem encontradas e os critérios de filtragem de geração de incidentes de segurança corresponderem.
Descobertas encerradas de pesquisa	Descobertas de pesquisa que foram resolvidas. Essas descobertas são ingeridas durante a ingestão de incidentes em andamento.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos.
Defina o tempo de ingestão da descoberta inicial	Ingestão de descobertas baseada na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Tempo de ingestão da descoberta inicial de entrada	Data e hora especificadas para a ingestão do incidente.
Recuperação Única	Marque esta caixa de seleção para permitir a recuperação única do histórico AWS Security Hub e, em seguida, fazer a reconciliação dos dados. Quando você marca esta caixa de seleção, a aplicação extrairá todos os abertos e encerrados AWS Security Hub descobertas para o período de até 90 dias aproximadamente. Ao processar os dados, as descobertas em andamento e os dados históricos são extraídos, mas o processamento das descobertas em andamento tem precedência sobre a extração histórica. Caso contrário, a extração histórica pode levar algum tempo com base na duração, bem como no número de descobertas ingeridas. **Nota:** O histórico recuperado AWS Security Hub as descobertas passam por verificações de desduplicação para evitar duplicatas no Resposta a incidentes de segurança aplicação.
Desde a data	A data desde a qual as descobertas históricas são ingeridas AWS Security Hub. **Nota:** Os dados das descobertas são extraídos aproximadamente dos últimos 90 dias.

A página de programação permite que você defina como e quando as descobertas são extraídas do AWS Security Hub locatário.

2. Para navegar até a página Opções adicionais, clique em **Continuar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Automatizar o. AWS Security Hub localizando atualizações e fechamentos pelo SIR status do incidente

Automatize as atualizações e fechamentos de descobertas em AWS Security Hub de acordo com SIR status do incidente. . AWS Security Hub a integração tem uma interface bidirecional que permite a ingestão de descobertas para criar incidentes de segurança e atualizar o status das descobertas de acordo com as mudanças no SIR incidente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. No formulário, preencha os detalhes.
   Siga as instruções para concluir a configuração para atualização AWS Security Hub descobertas quando você cria ou fecha um incidente de segurança em SIR.

Formulário Automatizando atualizações de incidentes

Categoria	Campo	Descrição
Atualizar Estado	SIR Estado do incidente	Exibe uma lista de SIR estados do incidente. Selecione uma opção desta lista para mapeá-la para um Hub de segurança Estado da descoberta.
	Hub de segurança Estado da descoberta	Exibe uma lista de Hub de segurança status do fluxo de trabalho. O status do fluxo de trabalho de uma descoberta é atualizado em AWS Security Hub Quando o estado de incidente do estado SIR correspondente muda.
Atualizar prioridade	SIR Prioridade do incidente	Exibe uma lista de SIR níveis de prioridade do incidente. Selecione uma opção desta lista para mapeá-la para um Hub de segurança nível de prioridade da descoberta.
	Hub de segurança Prioridade da descoberta	Selecione uma opção na lista de Hub de segurança níveis de gravidade. A gravidade de uma descoberta é atualizada em AWS Security Hub quando a prioridade do incidente de segurança correspondente muda.
Atualizar anotações de trabalho	Selecione esta opção para atualizar a seção de anotações de um Hub de segurança quando uma anotação de trabalho é atualizada para o correspondente SIR incidente. A seção Anotações de trabalho em SIR tem um limite de 512 caracteres como a seção de anotações de um Hub de segurança a descoberta oferece suporte ao mesmo.	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
Atualizar comentários adicionais	Selecione para atualizar AWS Security Hub seção de comentários de localização com os comentários adicionais fornecidos em SIR incidente.	
Atualizar anotações de resolução	Selecione para atualizar AWS Security Hub encerramento da seção de comentários com as anotações de resolução fornecidas quando SIR o incidente foi resolvido.	

Nota: Cada atualização das anotações de trabalho substitui a última atualização na seção de anotações de um Hub de segurança descoberta. Recomendamos que você adicione anotações de trabalho relevantes em um SIR incidente.

2. Selecione **Concluir**.

O que Fazer Depois

O perfil é movido para o estado Aguardando. Quando a mensagem de confirmação mostrar que a instalação e a configuração estão concluídas, você pode ativar o perfil.

SIR formulário após um AWS Security Hub ingestão da descoberta

Após ServiceNow AI Platform ingere o. AWS Security Hub um incidente de segurança é criado e as atualizações são feitas nesse registro de incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada quando um incidente é agregado e se você configurou o. **Anotação de trabalho em log para nova descoberta** . Defina critérios de filtro e agregação para AWS Security Hub ingestão de descobertas.

Você também pode exibir o registro de importação de descoberta interna que contém os dados brutos do incidente.

Ao clicar em **Clique aqui** , você pode exibir o registro no AWS Security Hub ambiente. O exemplo a seguir mostra o registro no AWS Security Hub ambiente.

Agregado AWS Security Hub descobertas

Exibição agregada AWS Security Hub descobertas: Exiba os incidentes agregados ao incidente de segurança. Navegar até **Mostrar todas as listas relacionadas** > **Descobertas agregadas do AWS Security Hub**.

Criar incidente de segurança: Selecione um incidente na lista e clique em **Ações** e, em seguida, clique em **Criar incidente de segurança** . Esta opção cria um novo incidente de segurança para o incidente e este incidente é desagregado do incidente de segurança primário.

Carbon Black - Integração de aprimoramento de incidentes

Use a integração Carbon Black para investigar e responder a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Encontre recursos de integração de aprimoramento de incidentes Carbon Black-Incident

- Comece a usar a integração Carbon Black - Aprimoramento de incidentes
- Integração Carbon Black de operações de segurança - Obter fluxo de processos em execução

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração Carbon Black de operações de segurança - isolar fluxo de host
- Operações de segurança Carbon Black Integration - Remover fluxo de isolamento de host

Entenda os conceitos de integração

- Tipos de ServiceNow integrações fornecidas
- Operações de segurança gatilhos de fluxo de trabalho

Obtenha ajuda de recursos ServiceNow

- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente
- Upgrade para Madri

Comece a usar a integração Carbon Black - Aprimoramento de incidentes

O aprimoramento de incidentes Carbon Black facilita a investigação de um incidente de segurança consultando logs para indicadores potencialmente mal-intencionados. Para usar a integração Carbon Black - Aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicione o URL base do endpoint apropriado e o MID Server.

Antes de Iniciar

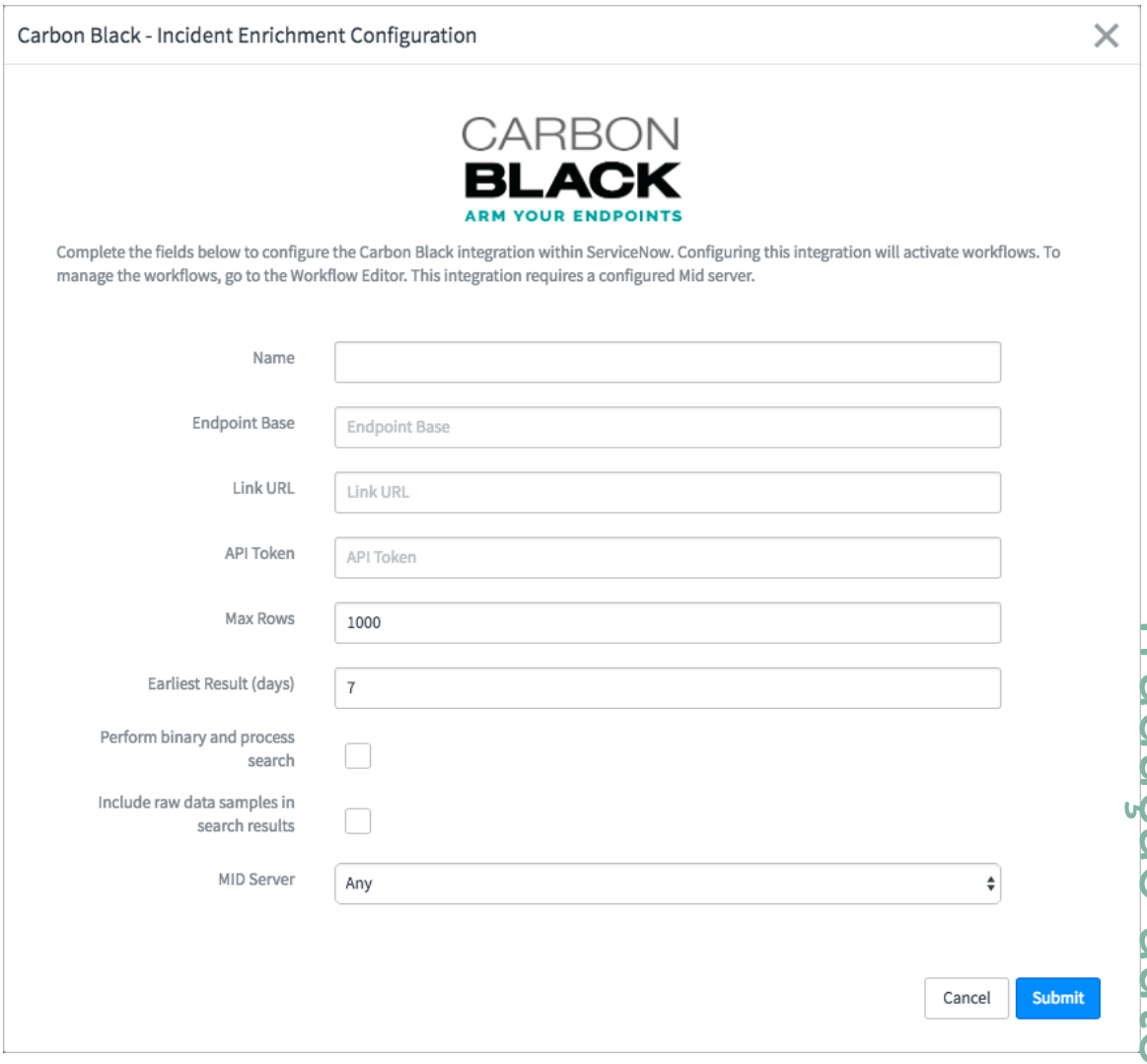
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando o download estiver concluído, acesse Carbon Black E obtenha o URL base do endpoint e o token de API em seu perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
4. No cartão Carbon Black - Aprimoramento de incidentes, clique em **Configurar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	O URL do endpoint que você adquiriu no site Carbon Black.
URL do Link	O URL do link que vincula a uma instância do Carbon Black, quando disponível.
Token de API	O token de API adquirido no site Carbon Black.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar. O padrão é 1000 linhas.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Executar pesquisa binária e de processo	Selecione esta opção para executar pesquisas binárias para encontrar arquivos binários, como hashes de arquivo, e pesquisas de processo para processos .exe que podem ter sido executados.
Incluir amostras de dados brutos	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
nos resultados da pesquisa	**número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Integração do Carbon Black

A integração Carbon Black permite que você investigue e responda a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Explorar

- Integrações do Resposta a incidentes de segurança
- Carbon Black - Integração de aprimoramento de incidentes

Configurar

Comece a usar a integração Carbon Black

Usar

- Operações de segurança gatilhos de fluxo de trabalho
- Exibir itens afetados para um incidente de segurança
- Operações de segurança - Obter fluxo de processos em execução
- Integração Carbon Black de operações de segurança - Obter fluxo de processos em execução
- Exibir itens afetados para um incidente de segurança
- Executar bloqueio de solicitação
- Integração de operações de segurança - Bloquear fluxo de solicitação
- Execute Isolar host

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração Carbon Black de operações de segurança - isolar fluxo de host
- Operações de segurança Carbon Black Integration - Remover fluxo de isolamento de host

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Comece a usar a integração Carbon Black

Carbon Black é um sistema de segurança avançado que se integra facilmente ao Operações de segurança. Antes de usar a integração Carbon Black, você deve baixar a integração do ServiceNow Store E adicione a base de endpoint apropriada e o token de API.

Antes de Iniciar

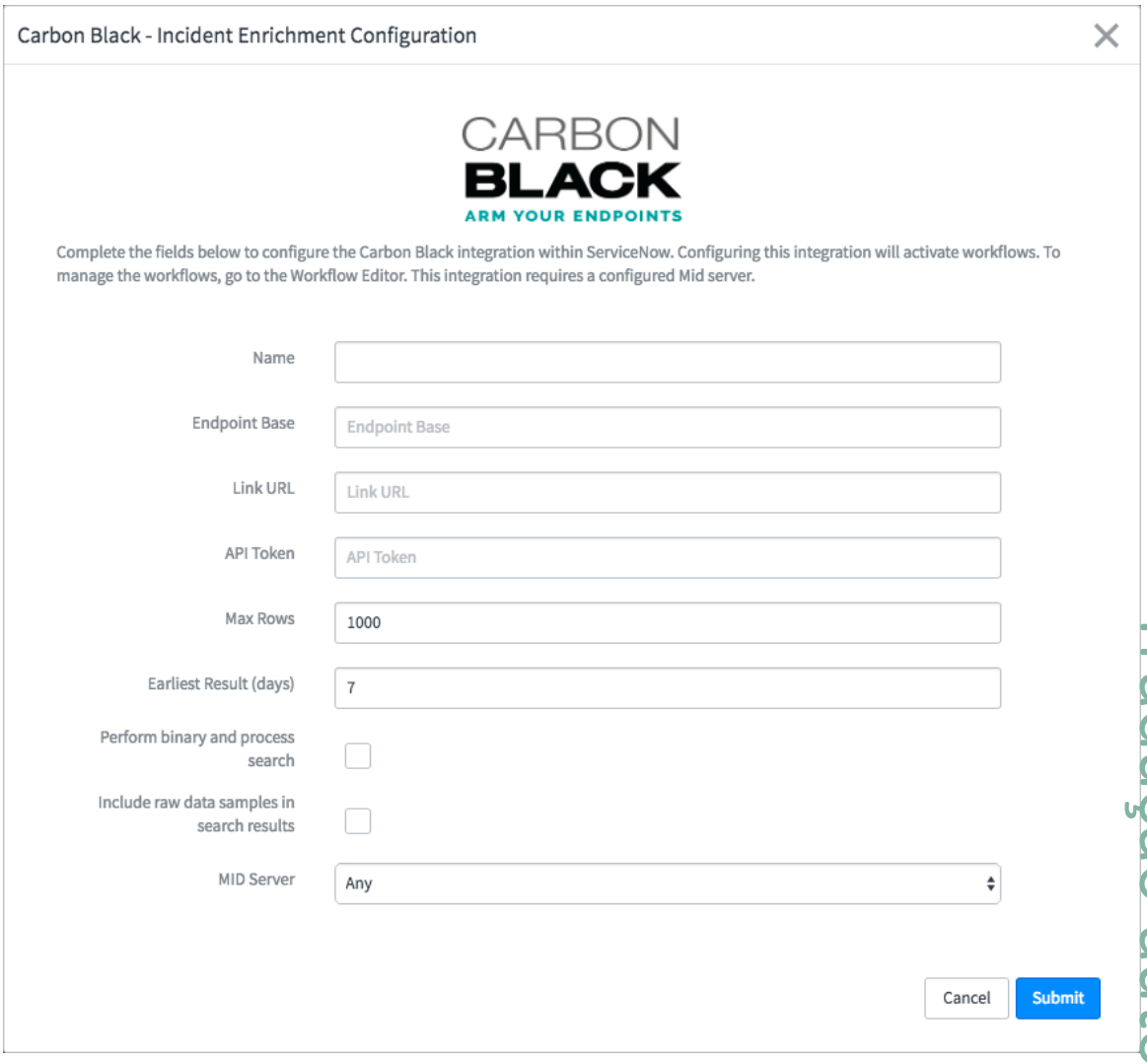
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Carbon Black E obtenha o URL base do endpoint e o token de API em seu perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. Em Carbon Black cartão, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	A base de endpoint que você adquiriu do site Carbon Black.
Token de API	O token de API adquirido no site Carbon Black.
Usar MID Server	Marque esta caixa de seleção se ela ainda não estiver marcada.
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.
Ativar Isolar Host	Marque esta caixa de seleção para permitir que os itens de configuração selecionados sejam isolados do **Itens de configuração** guia lista relacionada em um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Antibot Check Point - Integração do analisador de e-mails

A integração do Check Point Anti-bot - Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do Check Point Anti-bot para criar incidentes de segurança e impulsionar fluxos de trabalho de aprimoramento e resposta.

Configure a integração Check Point Anti-bot - Analisador de e-mail

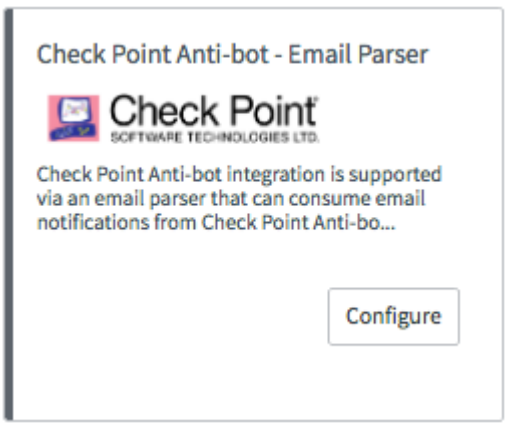
A integração Check Point Anti-bot - Analisador de e-mail usa notificações por e-mail para impulsionar o aprimoramento e fluxos de trabalho de resposta.

Antes de Iniciar
Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa
Um modelo de analisador de e-mail anti-bot do Check Point é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão Check Point Anti-bot - Analisador de e-mail, clique em **Configurar** .
3. Em **Check Point Anti-bot - Configuração do analisador de e-mail** na caixa de diálogo, clique em **Configure o analisador de e-mail** link.
4. Clique em **Anti-bot do Ponto de Verificação** link para editar as configurações no analisador de e-mail do modelo fornecido.
   No mínimo, preencha `O e-mail é de` campo. Para criar um analisador de e-mail, consulte Crie analisadores de e-mail em Operações de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Verifique **Ativo** caixa.
6. Clique em **Atualização** em **Analisador de e-mail** formulário.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração** .

Check Point Next Generation Threat Prevention integração

Este documento descreve as etapas necessárias para integrar os recursos do Check Point Next Generation Threat Prevention (NGTP) com ServiceNow® Resposta a incidentes de segurança(SIR) para que as aplicações funcionem corretamente juntas.

Uma vez instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP, URLs e domínios mal-intencionados usando os recursos de Lista de solicitações de bloqueio com ServiceNow Resposta a incidentes de segurança(SIR) produtos. Esta Lista de solicitações de bloqueio é configurada em gateways de ponto de verificação como um Feed de inteligência personalizada. O recurso Feeds de inteligência personalizada fornece a capacidade de adicionar feeds de inteligência cibernética personalizados ao mecanismo de prevenção de ameaças de última geração. Ele permite buscar feeds de um servidor de terceiros, neste caso ServiceNow Resposta a incidentes de segurança Diretamente para o Gateway de última geração do Check Point a ser imposto por blades antivírus e anti-bot. O analista de resposta a incidentes de segurança cria entradas para a Lista de bloqueios de ponto de verificação a partir de observáveis determinados como mal-intencionados em ServiceNow Incidentes de segurança SIR.

Para a maioria das implementações, uma Lista de solicitações de bloqueio é um arquivo csv hospedado em um servidor web externo. Para esta integração, este servidor web é seu ServiceNow AI Platform Instância, que permite que o mecanismo de prevenção contra ameaças de última geração do Check Point busque a lista de endereços IP, URLs e domínios a serem bloqueados.

Para impor o bloqueio de observáveis no Gateway do Check Point, certifique-se de que a Política de prevenção de ameaças esteja configurada com Blades anti-bot e antivírus ativados. À medida que as entradas da lista de bloqueios são modificadas, o Mecanismo de prevenção de ameaças importa dinamicamente a lista no intervalo configurado e impõe a política sem uma mudança de configuração ou confirmação no firewall. Para esta integração, ServiceNow AI Platform Criou uma tabela que contém entradas da Lista de bloqueios que são recuperadas pelo Gateway de próxima geração do Check Point autorizado nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

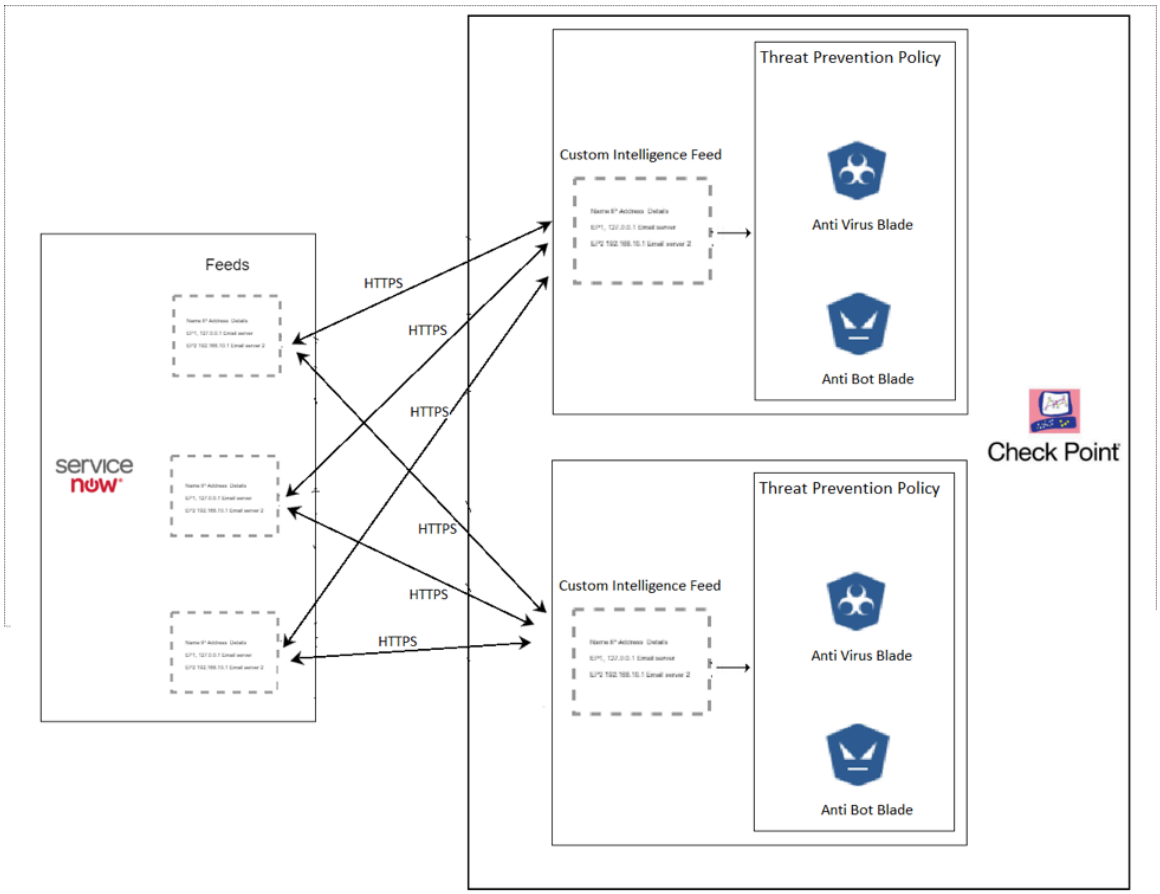
- Flexibilidade para criar várias listas de bloqueio que se aplicam a vários gateways de ponto de verificação.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e permitir sites listados).
- Marcação de ServiceNow AI Platform Incidentes de segurança com entradas da lista de bloqueios por tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração da Lista de bloqueios para manter o tamanho da Lista de bloqueios expirando ou removendo entradas mais antigas automaticamente.
- Pesquisando entradas da lista de bloqueios entre diferentes listas de bloqueios.
- Vincular entradas da lista de bloqueios a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Diagrama da arquitetura de integração

Abaixo está o diagrama de arquitetura de alto nível que descreve os componentes envolvidos e os pontos de integração entre a NOW Platform e os sistemas de Check Point.



Nota: O logotipo da Check Point Systems, a imagem do Anti-Virus Blade e a imagem do Anti Bot Blade são da Check Point Systems ©. Eles são propriedade da Check Point Systems.

Plug-ins

A integração requer que Resposta a incidentes de segurança(com.snc.security_incident) plug-in ser ativado.

Para instalar Resposta a incidentes de segurança plug-ins:

1. Faça login em sua instância com suas credenciais HI.
2. Verifique se você tem a função de administrador (administrador).
3. Navegue até Definição do sistema>plug-ins em sua instância.
4. Selecione e clique em Resposta de incidente de segurança.

Depois que esses plug-ins forem instalados, você poderá carregar o novo plug-in de integração do Check Point da ServiceNow Store e seguir as instruções de configuração a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões do SO do Check Point compatíveis

Esta integração requer o Feed de inteligência personalizada dos blades Check Point e Anti-Bot e Anti-Virus. Estes são compatíveis com R80.20 e superior. Instale o hot fix do recurso Inteligência personalizada conhecido como Check Point R80.10 Jumbo HF Take 121 e superior. Consulte a seção Instalação da documentação do feed de inteligência personalizada do Check Point para obter mais informações sobre a matriz de compatibilidade do produto.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Depois de instalar o hot fix, certifique-se de que os comandos abaixo estejam acessíveis no Gateway do Check Point. SSH para o Gateway e faça login no modo especialista.

```
gw-93440b> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Versões compatíveis da ServiceNow

A versão de lançamento do San Diego ou posterior é compatível.

Referências

Abaixo estão algumas das referências do Check Point que são úteis na configuração dos pré-requisitos.

1. Recurso de feeds de inteligência personalizada - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Para configurar blades anti-bot e antivírus, consulte o Guia do usuário do Check Point. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Para configurar a inspeção HTTPS no Check Point, siga o link abaixo. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Permissões e funções

As seguintes funções da ServiceNow são necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Administrador (admin) para instalação do plug-in da aplicação de integração
- Administrador de incidentes de segurança (sn_si.admin) para criar listas de bloqueios na ServiceNow e aprovar solicitações para adicionar e desativar entradas de lista de bloqueios.
- Analista de segurança (também conhecido aqui como analista de SOC, sn_si.analyst) para criar e manter registros de entrada da lista de bloqueios.

Para obter mais informações sobre como atribuir a função de analista de segurança, em Site de documentação da ServiceNow , Navegue até Operações de segurança>Resposta a incidentes de segurança> Atribuição de analistas de segurança.

Configuração do Check Point NGTP

Antes de poder usar Check Point NGTP Integração, você deve criar uma conta de API, configurar políticas e ativar a integração.

Crie uma conta de API para Check Point NGTP integração

Uma função de conta de API é necessária em seu ServiceNow AI Platform instância desta integração. O nome de usuário e a senha associados a esta conta são criados no ServiceNow AI Platform E inseridos no Check Point, para que o Check Point seja autenticado com ServiceNow AI Platform Ao recuperar entradas da lista de bloqueios.

Antes de Iniciar

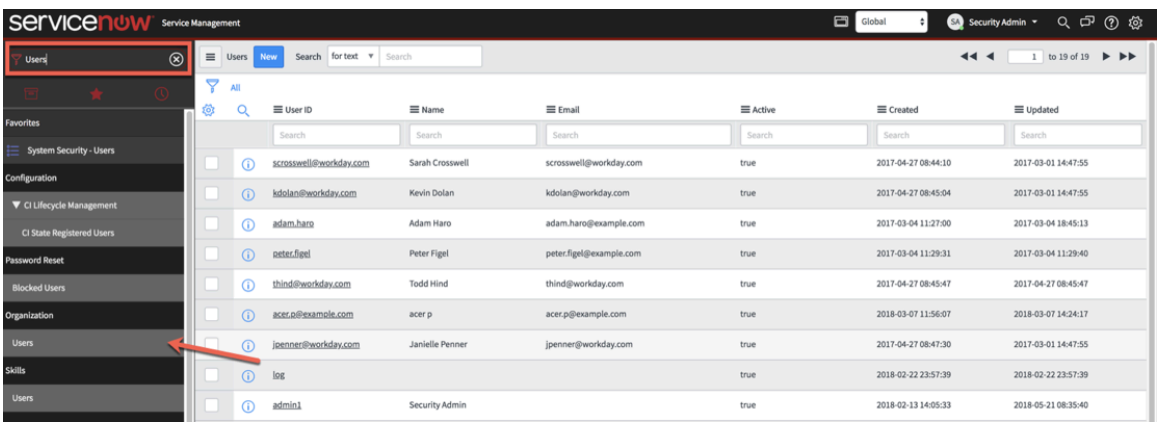
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

. ServiceNow AI Platform o administrador cria uma função de conta de API (sn_sec_checkpoint.api_account_access). Esta conta é usada exclusivamente para inserir credenciais necessárias para autenticação no Check Point, para que o Gateway possa recuperar listas de bloqueios do ServiceNow AI Platform. Esta conta é uma conta de usuário de API separada e exclusiva no ServiceNow AI Platform E atribuído ao administrador do Check Point.

Procedimento

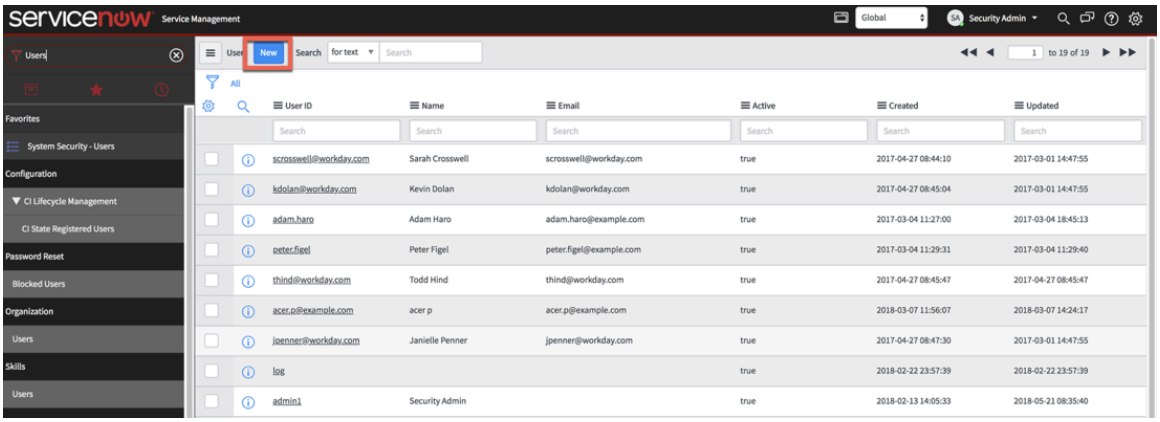
1. Navegar até **Tudo** > **Organização** > **Usuários**.
2. Clique em **Usuários** módulo.



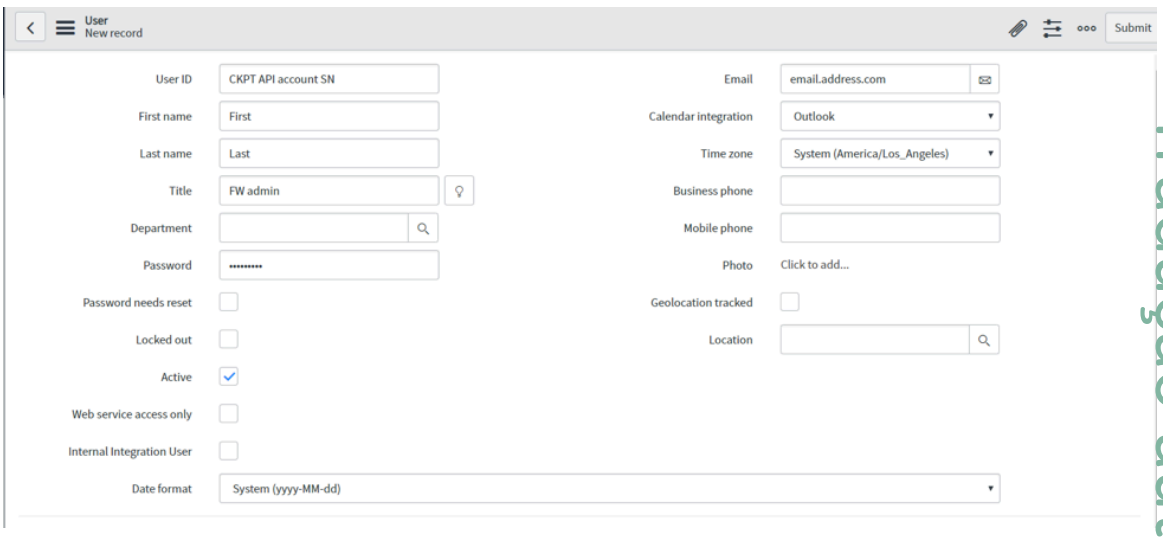
3. Na lista Usuários exibida, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um novo formulário é exibido.



4. Preencha o formulário, conforme necessário.

Nota: Os valores do título do ID do usuário e do endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

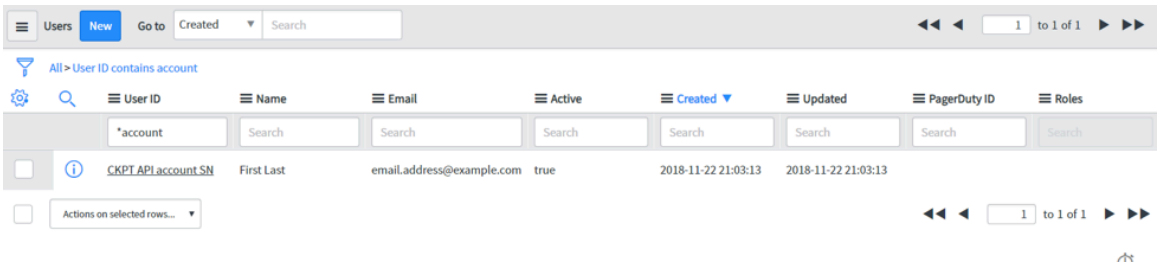
Campo	Descrição
ID do usuário	ID de usuário exclusivo para a função em seu ServiceNow AI Platform instância. Este ID de usuário é inserido em **Nome de usuário** . **Autenticação de cliente** Configuração da lista de bloqueios Gateway do Check Point. Um exemplo é o SN da conta da API CKPT.
Nome	Pessoa que você está atribuindo
Sobrenome	Pessoa que você está atribuindo
Título	Cargo, por exemplo, administrador de FW.
Senha	Senha exclusiva criada para esta função. Esta senha é inserida em **Senha** . **Autenticação de cliente** Configuração da lista de bloqueios no gateway do Check Point.
E-mail	Endereço de e-mail exclusivo

5. Clique em **Enviar**.
Uma vez enviado, você pode atribuir a função.

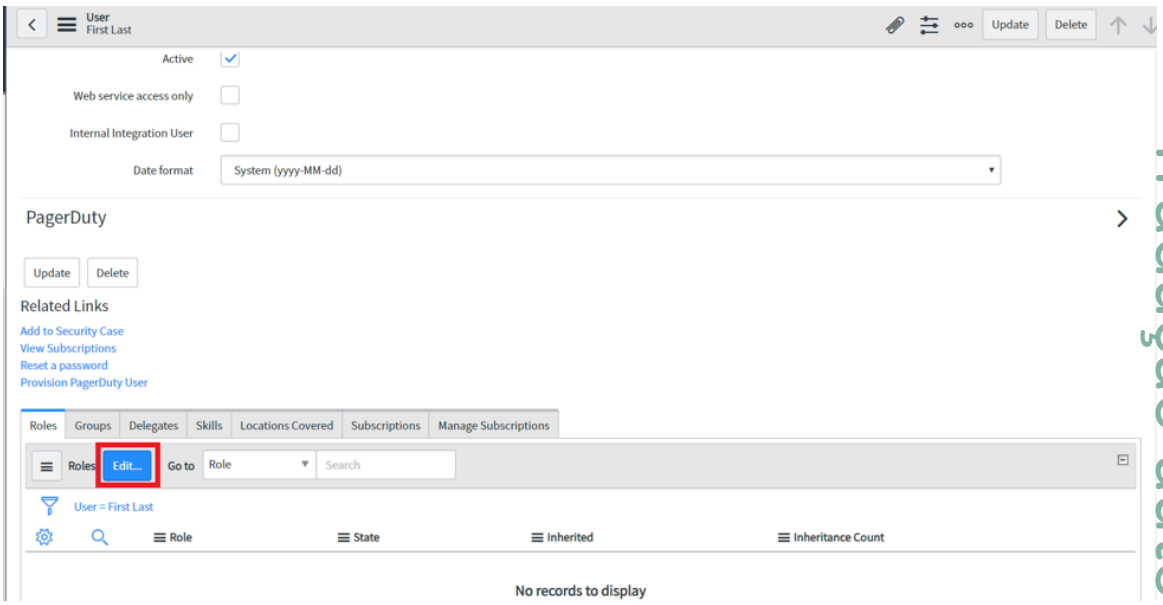
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Na lista Usuários na coluna ID do usuário, clique no nome do ID de usuário inserido, SN da conta CKPTAPI, por exemplo.



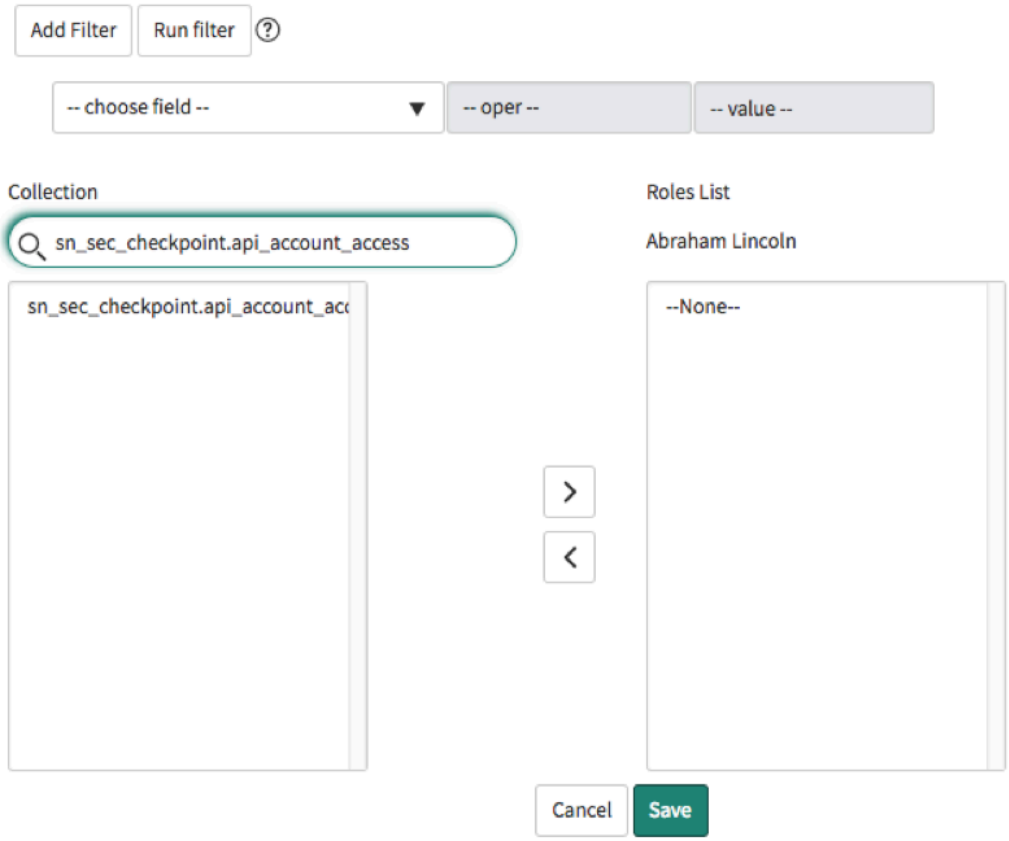
7. No registro Abrir na seção Funções, clique em **Editar** .



8. Em **Editar membros** formulário exibido, insira sn_sec_checkpoint.api_account_access em **Coleção** campo.

Tradução automática

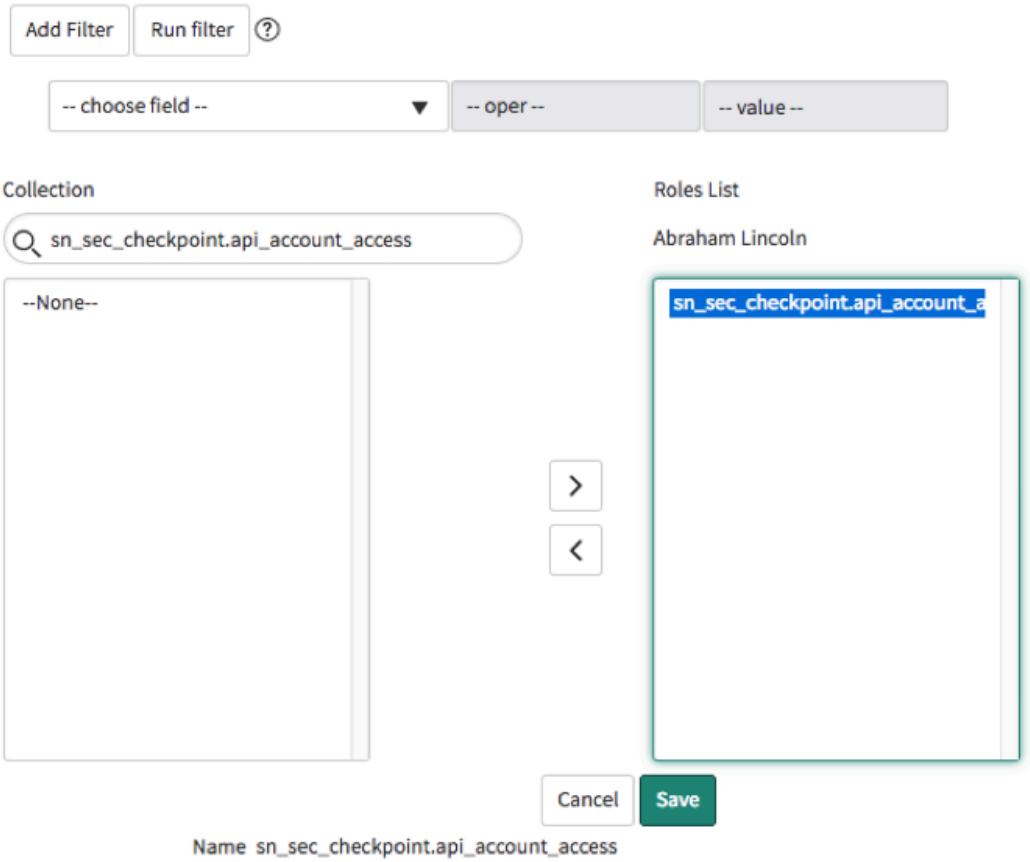
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Em **Coleção** , selecione e mova sn_sec_checkpoint.api_account_access para **Lista de funções** .
10. Clique em **Salvar**.
11. Navegue até **Usuários** e em **Usuário** Na lista, clique no nome do ID que você criou para a função (SN da conta da API CKPT).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





12. O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída.

Configure o. Check Point NGTP integração

Conclua as etapas a seguir para configurar o. Check Point Next Generation Threat Prevention integração. Isso garante que os pré-requisitos para que a integração funcione estejam em vigor.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Verifique se a Política de prevenção de ameaças está configurada com Blades anti-bot e antivírus ativados. Consulte o Guia do usuário do Check Point mencionado na seção Referência para obter informações detalhadas sobre como configurar blades anti-bot e antivírus.

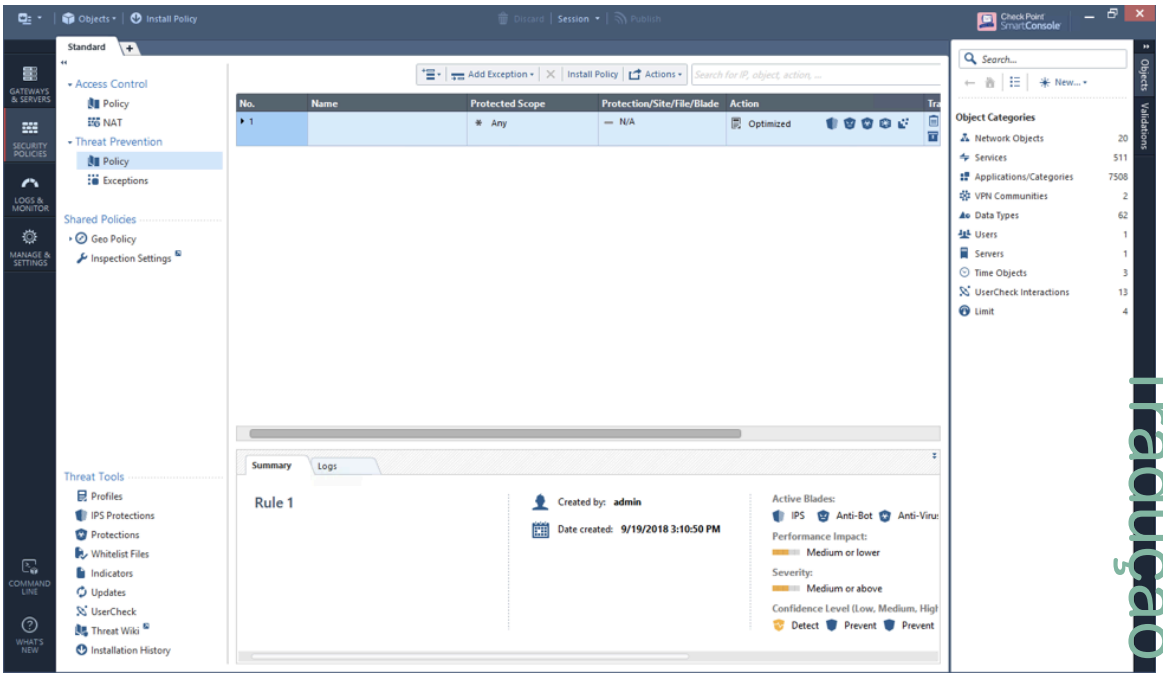
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

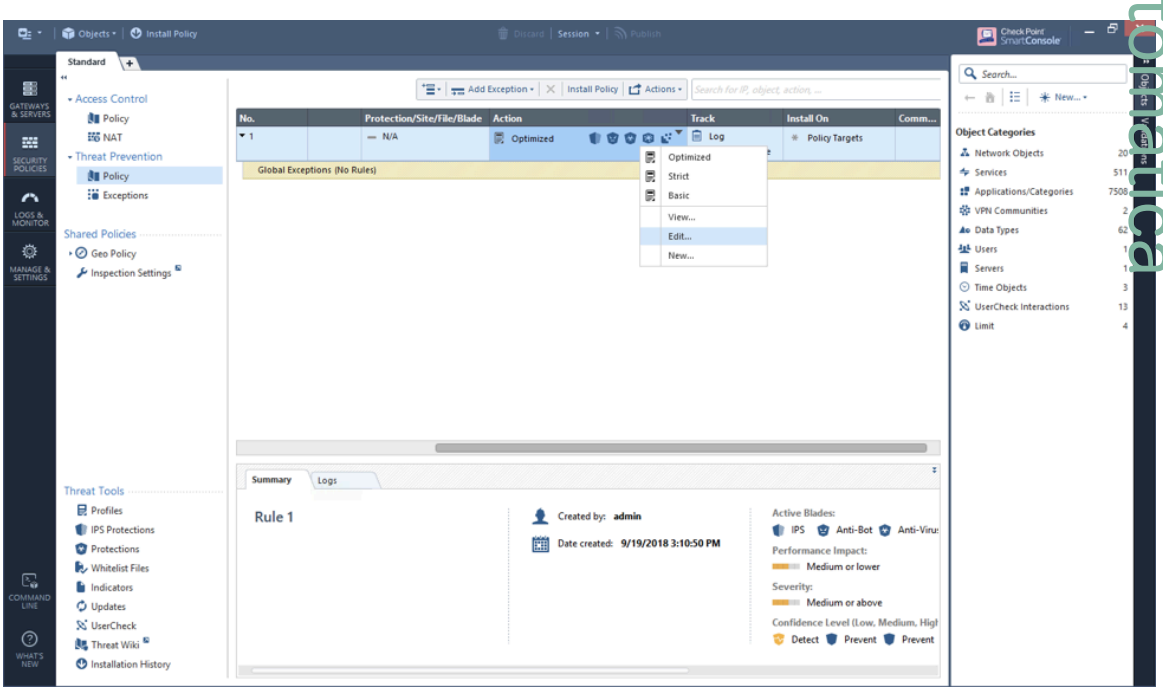
Nota: As imagens neste tópico são privilegiadas e proprietárias e são usadas com permissão da Check Point Software Technologies, Ltd

a. Faça login em **Console inteligente** .

b. Navegar até **Políticas de Segurança** > **Prevenção contra ameaças** > **Política**.



c. Abra a Política de prevenção de ameaças no Modo de edição.



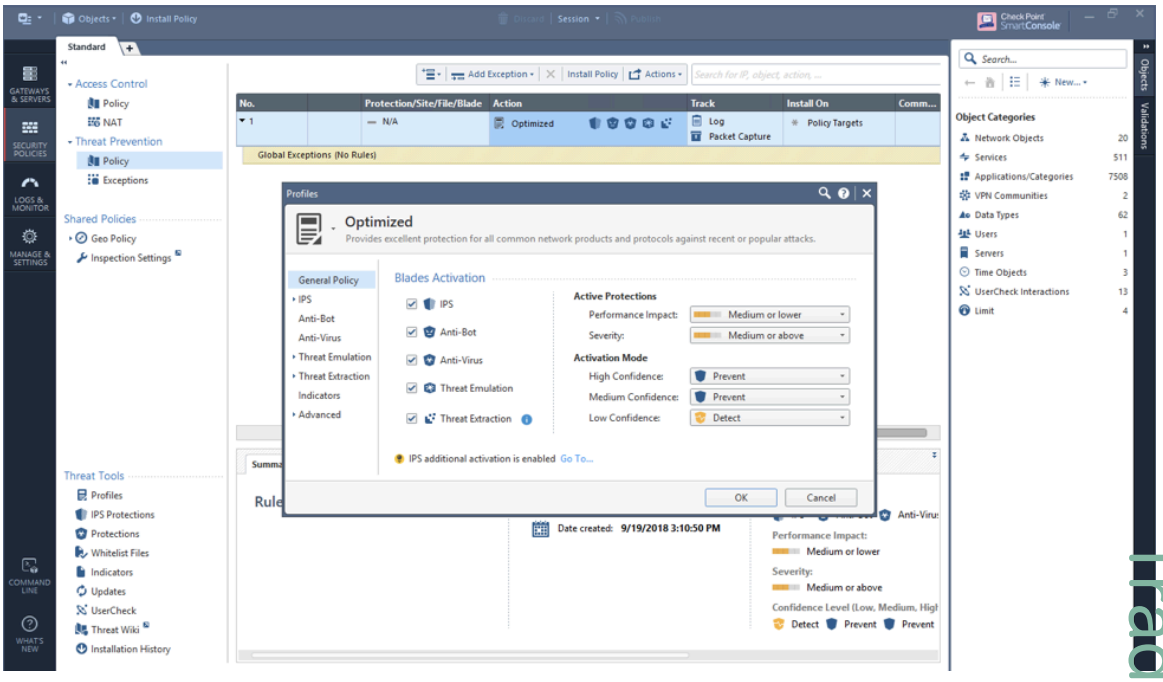
d. Proteções ativas # A gravidade deve ser "Média ou superior"

e. Modo de ativação # A confiança alta deve ser "Impedir"

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Blades Activation à Anti-virus e Anti-Bot devem ser selecionados.



g. Publique as mudanças (se houver) e instale a política.

2. Se ainda não estiverem configurados, os Feeds de Inteligência Personalizada deverão ser adicionados após a ativação dos Blades Anti-Bot e Anti-Vírus.
Consulte a seção Instalação da documentação do recurso Feed de inteligência personalizada do Check Point. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Se ainda não estiver configurado, configure o Gateway do Check Point para rotear todo o tráfego da Internet via proxy HTTP (se estiver configurando a inspeção HTTPS).

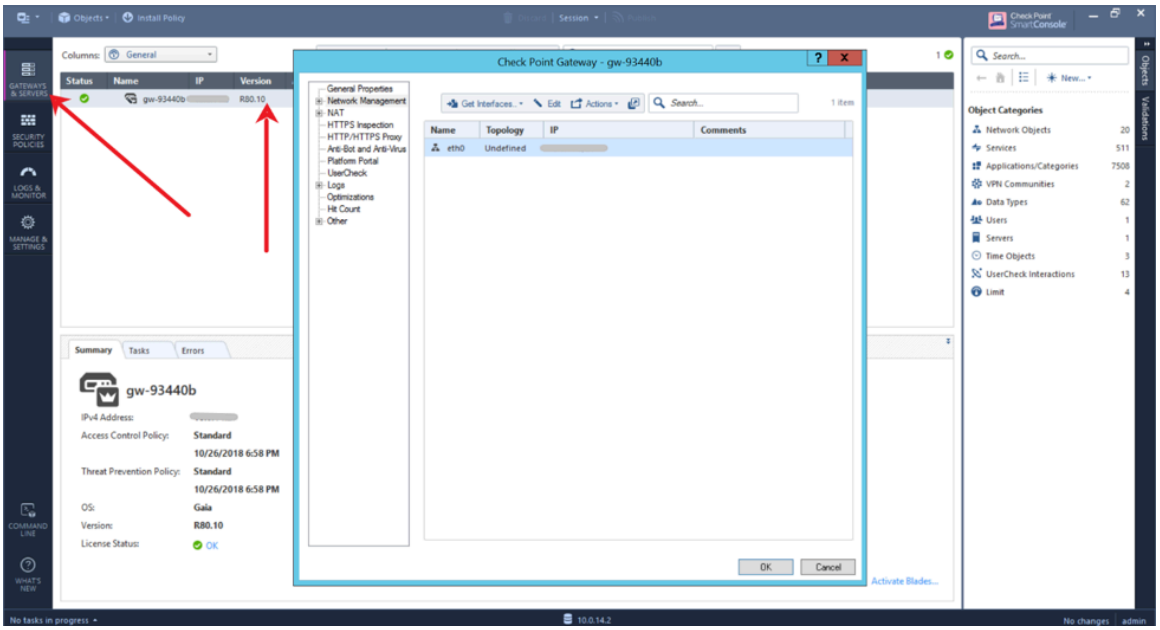
> **Nota:** Para bloqueio de URL no Check Point NGTP, há determinadas configurações que precisam ser asseguradas. O tráfego de internet HTTPS usa o protocolo SSL (Secure Sockets Layer) e é criptografado para fornecer privacidade de dados. No entanto, HTTPS pode ocultar tráfego mal-intencionado que deveria ter sido bloqueado. Para que o Check Point Gateway obtenha visibilidade do tráfego HTTPS, roteie o tráfego via proxy HTTP ou configure a inspeção HTTPS (recomendado). Esta seção detalha as etapas a serem seguidas para configurar o Proxy HTTP no Gateway de Check Point.

a. Faça login em **Console inteligente** .

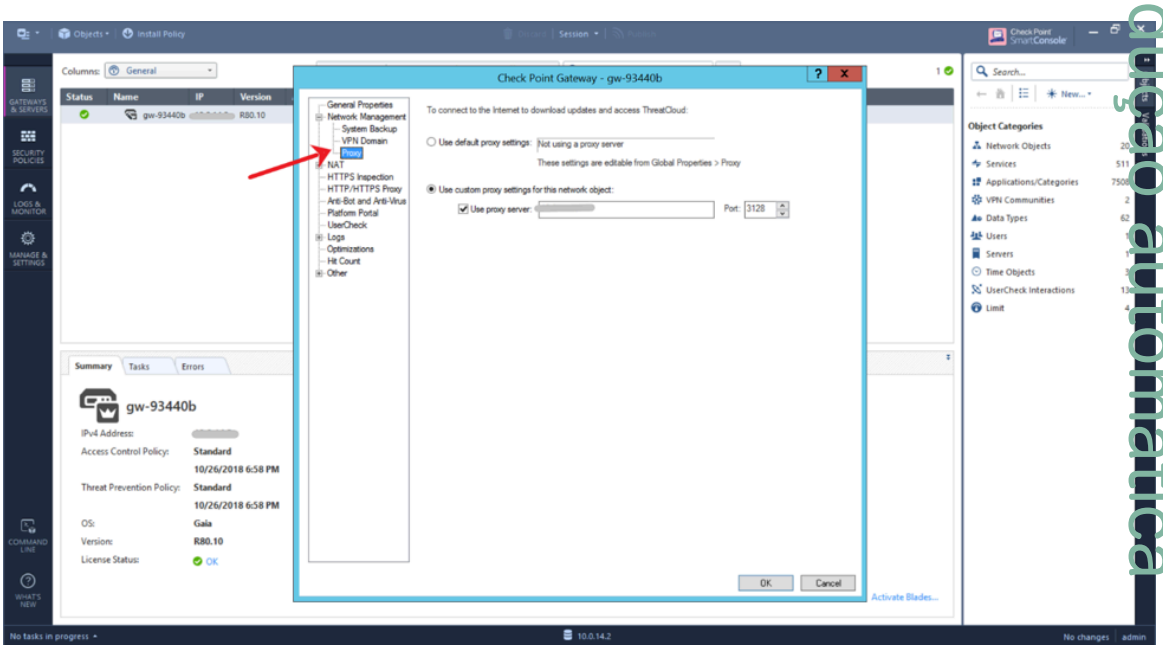
b. Navegue até **Servidores e gateways** e clique duas vezes no servidor aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Navegar até **Gestão de redes** > **Proxy**.



d. Forneça os detalhes do proxy a serem usados para rotear o tráfego HTTP.

e. Certifique-se de que as solicitações HTTP do endpoint do cliente sejam por meio do proxy HTTP.

4. Se ainda não estiver configurado, habilite a inspeção HTTPS (se o proxy HTTP estiver configurado). Quando a maior parte do tráfego é sobre SSL, é recomendável usar HTTPS Inspection Blade. Isso torna o tráfego transparente para o GW. Habilite a inspeção HTTPS no Gateway de Check Point, da seguinte forma.

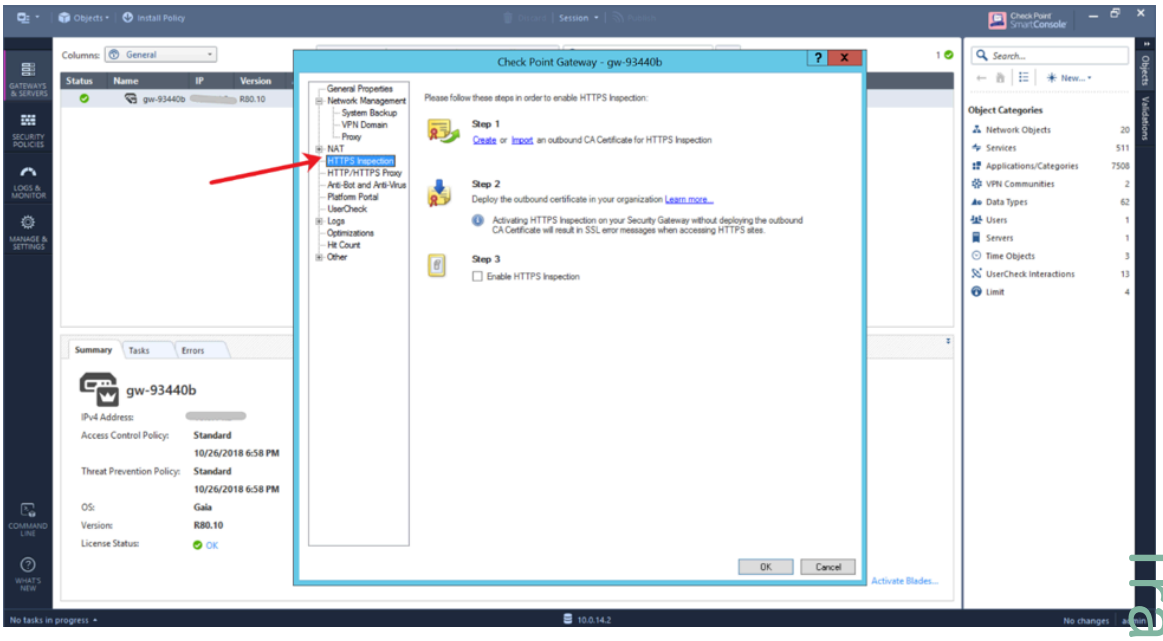
a. Faça login em **Console inteligente** .

b. Navegue até **Servidores e gateways** e clique duas vezes no servidor aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Navegue até **Inspeção HTTPS** .



d. Siga Etapas para configurar a inspeção HTTPS No Guia do usuário do Check Point.

Ative o. Check Point NGTP integração

Se você não instalou o aplicativo, siga as instruções para instalá-lo.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar a aplicação.
2. Navegar até **Aplicações do sistema** > **Aplicações**.
3. Clique em **Downloads** guia.
   Uma lista de aplicações disponíveis para instalação é exibida.
4. Localize Check Point Next Generation Threat Prevention aplicação, selecione-a e clique em **Instalar** .
   Sua aplicação é instalada automaticamente em sua instância.

Trabalhar com listas de bloqueios

. ServiceNow Check Point Next Generation Threat Prevention A integração oferece suporte a listas de bloqueio que aceitam observáveis de IP, URL e domínio.

ServiceNow a lista de bloqueios configurada é um arquivo csv hospedado em um servidor web externo, que para esta integração é ServiceNow AI Platform instância. O Feed de Inteligência personalizada é configurado no Gateway de Check Point, que extrai os endereços IP, URLs e domínios do ServiceNow AI Platform no intervalo pré-configurado.

Esta integração oferece suporte a três tipos de listas de bloqueios:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço IP (isso inclui um endereço IP individual (somente IPv4) para lista de bloqueios e blocos CIDR (intervalos) de endereços para lista de permissões).
- URL
- Domínio

Observáveis compatíveis com Check Point NGTP integração

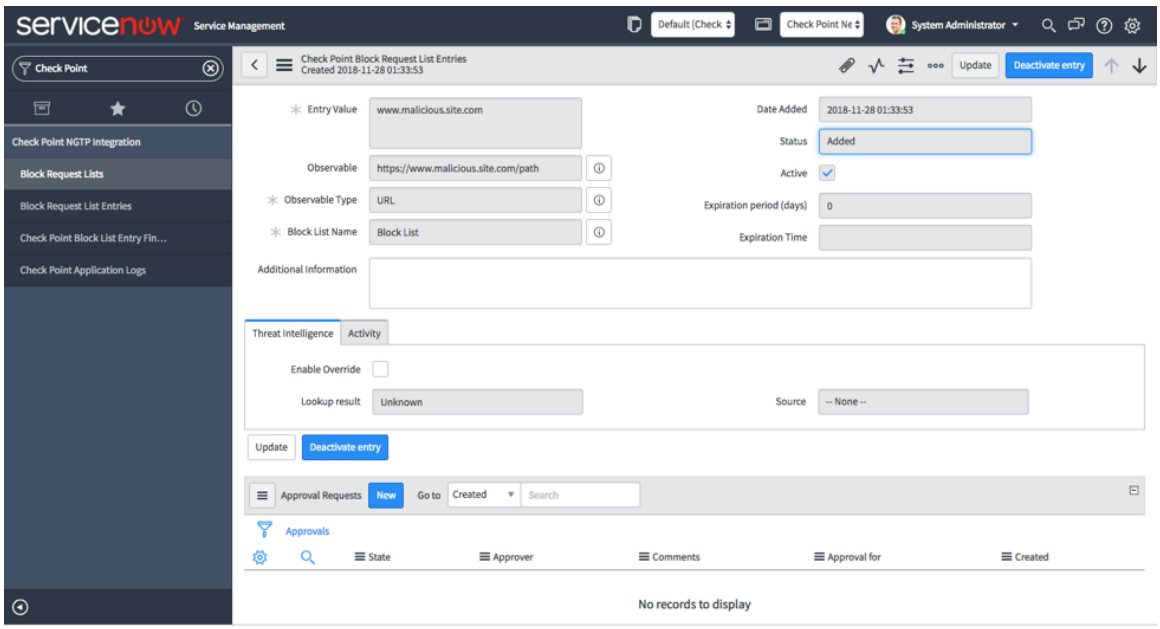
A seção lista descrições dos observáveis compatíveis com esta integração e formatos de exemplo para cada tipo.

Tipo de Observável	Exemplos	Descrição
Domínio	• example.com • mail.example.com	Curingas não são compatíveis.
Endereço IP	95.153.103.54 (IPv4)	Representa um endereço de interface único e distinto. A integração oferece suporte somente aos formatos IPv4 e CIDR (o formato CIDR só é compatível para fins de listagem de permissão). Para fins de lista de permissões, a integração tem suporte para observáveis de endereço IP, incluindo intervalos CIDR (roteamento entre domínios sem classe), por exemplo, 95.153.100.0/22. **Nota:** Uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a uma Lista de bloqueios que você já permitiu listada como parte de um intervalo de CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Descrição - O URL HTTPS é formatado pela aplicação para cortar o caminho do URL e reter somente o nome do domínio. O Check Point NGTP depende da solicitação DE CONEXÃO HTTP para avaliar o tráfego da Web

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

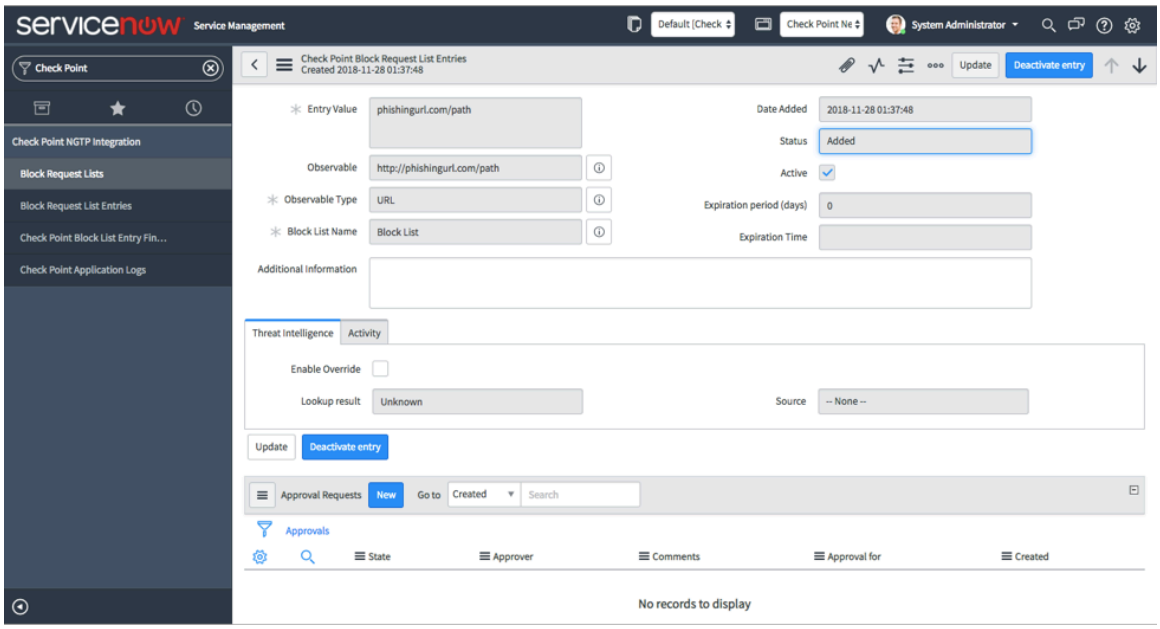
Tipo de Observável	Exemplos	Descrição
		e impor o bloqueio. Para a solicitação DE CONEXÃO HTTPS, o URL inteiro não está visível na solicitação e somente o nome do domínio está visível. Quando um usuário bloqueia qualquer URL HTTPS com um caminho específico (exemplo; https://www.example.com/path), a aplicação corta o caminho automaticamente (www.example.com). A aplicação mantém o relacionamento entre o observável original e o URL formatado. Abaixo está a captura de tela da entrada da lista de bloqueios que mostra o URL formatado e o observável original.



Para URLs HTTP com um caminho específico (por exemplo, http://www.example.com/path), o Check Point bloquearia o URL especificado, já que o URL inteiro está visível na solicitação DO CONNECT.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Crie uma lista de bloqueios para Check Point NGTP integração

Crie uma Lista de bloqueios no seu ServiceNow AI Platform instância. Uma vez aprovado e ativado, você pode criar entradas para essas Listas de bloqueio a partir de observáveis determinados como mal-intencionados em incidentes de Resposta de incidentes de segurança (SIR) da Now Platform e solicitar aprovação para bloqueá-los.

Antes de Iniciar

Função necessária: Administrador de incidentes de segurança (sn_si.admin)

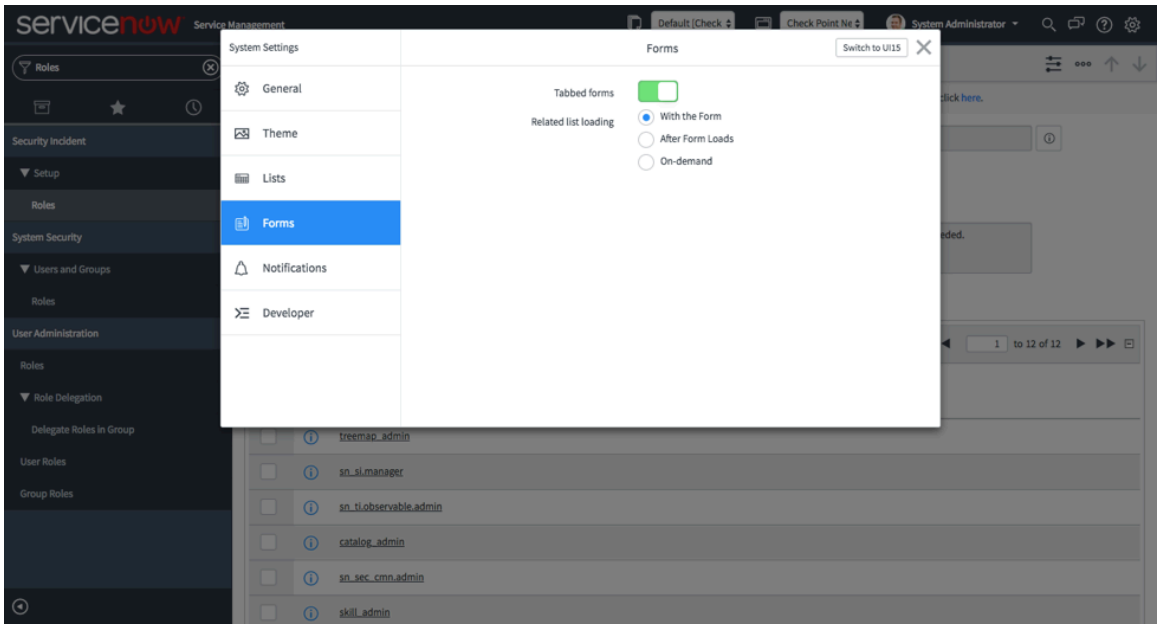
Por Que e Quando Desempenhar Esta Tarefa

Crie a Lista de bloqueios no seu ServiceNow AI Platform Instância para que o Check Point possa importar objetos (endereços IP, URLs, domínios) incluídos na lista. O Feed de Inteligência personalizado é configurado no Gateway de Check Point, que extrai os endereços IP, URLs e domínios da Now Platform em um intervalo pré-configurado. Para garantir o bloqueio dos observáveis, a Política de prevenção de ameaças deve ser configurada com Blades anti-bot e antivírus ativados.

Nota: As figuras neste tópico são mostradas com **Formulários com guias** Limpo em Configurações do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Procedimento

1. Após a conclusão da instalação da aplicação, navegue até **Integrações** > **Configurações de Integração**.
2. Localize **Prevenção contra ameaças de última geração do Check Point** e clique **Configurar** .

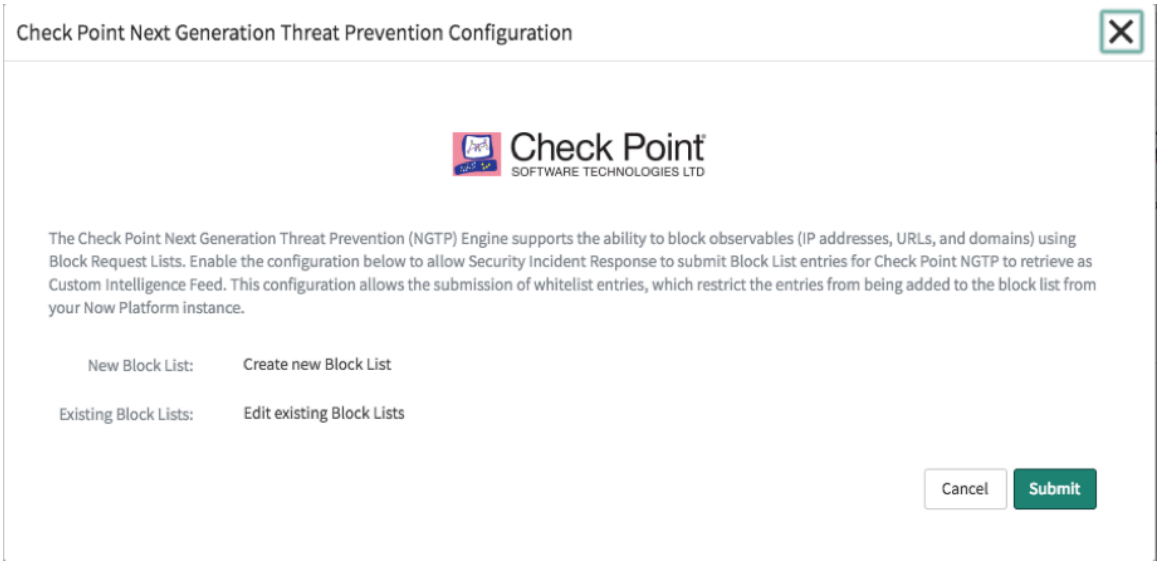


Nota: Conteúdo privilegiado e proprietário usado com permissão da Check Point Software Technologies, Ltd

3. Clique em **Criar nova Lista de bloqueios** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da lista de solicitações de bloqueio do ponto de verificação. Inclua o tipo de observável (URL, IP, domínio) neste campo para que o analista de segurança possa reconhecer facilmente a intenção da Lista de bloqueios pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos da lista de bloqueios estão mapeados. Alguns exemplos de nomes da lista de bloqueios são IP de Malware de Saída ou URL de Phishing de Saída.
Ativo	Esta caixa de seleção é desmarcada por padrão para indicar que a Lista de bloqueios está inativa. Quando inativa, a Lista de bloqueios não pode receber entradas adicionais. Quando a caixa de seleção é marcada (quando a solicitação de mudança é fechada ou a solicitação de mudança não é gerada), a Lista de bloqueios é ativada e disponível para entradas da Lista de bloqueios.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado na Lista de bloqueios. Quando selecionado, o campo "Marcador para observáveis" fica disponível no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido no campo Nome com um prefixo de Ponto de verificação, por exemplo, IP de saída de Malware de Ponto de verificação. Você pode mudar o nome e a cor do marcador. O nome do marcador é exibido no campo "Marcador para observáveis", depois que a Lista de bloqueios é salva. Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o campo "Marcador para observáveis" não está disponível no formulário.
Tipo de Observável	Selecione um tipo de observável que esta Lista de bloqueios aceita na lista: Endereço IP (incluindo CIDR para lista de permissões), URL ou domínio.

Tradução automática

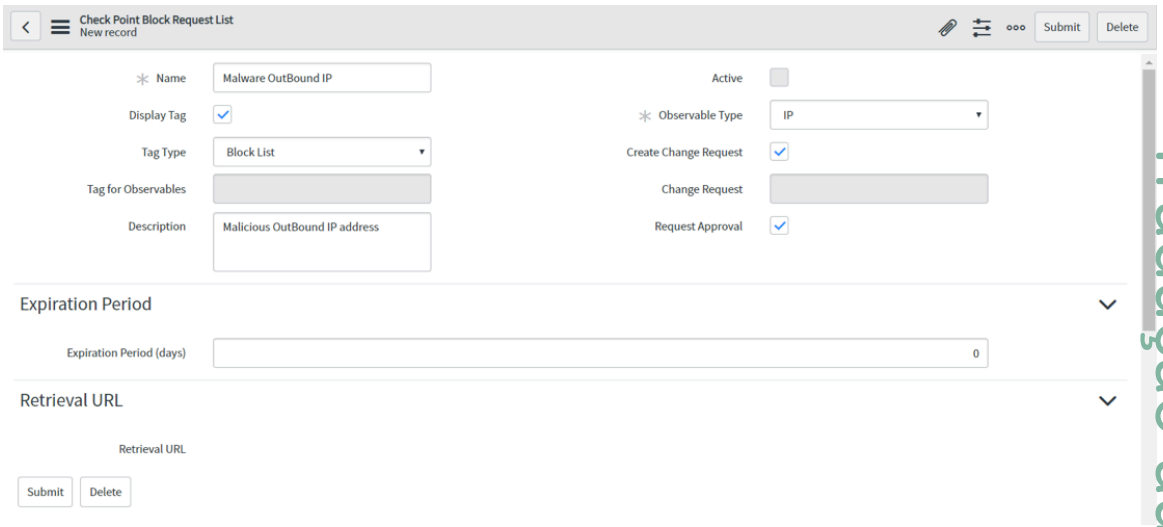
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de marcador	Marcadores que estão disponíveis na lista. Uma lista de bloqueios é uma lista de observáveis que você deseja que o Check Point Next Generation Threat Prevention bloqueie. Uma lista de permissões é uma lista de observáveis que você não deseja bloquear no Check Point Next Generation Threat Prevention. Por padrão, a cor do marcador da lista de bloqueios é preta e a cor do marcador da lista de permissões é cinza. Você pode mudar a cor.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em seu ServiceNow AI Platform Que estão anexadas ao registro da Lista de bloqueios. A solicitação de mudança é usada para configurar o URL de recuperação da lista de bloqueios no gateway do firewall de última geração do Check Point. Esta opção é recomendada se o administrador do firewall também estiver usando o. ServiceNow AI Platform para mudanças de regra ou política de firewall. Se você criar uma solicitação, depois que ela for fechada, a Lista de bloqueios será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente a Lista de bloqueios depois de receber um aviso por e-mail do administrador do firewall de que o Feed de inteligência personalizada foi configurado em todos os gateways de Check Point. Quando a caixa de seleção Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Solicitar Aprovação	Esta caixa de seleção é marcada por padrão para solicitar aprovações para ativar/remover entradas da lista de bloqueios das listas de bloqueios. A aprovação é solicitada dos usuários com a função Administrador de incidentes de segurança (sn_si.admin). A solicitação de aprovação será enviada por e-mail para os aprovadores. Quando a aprovação for aceita, a entrada será ativada nessa Lista de bloqueios. Quando a caixa de seleção não estiver marcada, as entradas dessa Lista de bloqueios não seguirão o fluxo de trabalho de aprovação e serão ativadas diretamente na lista de bloqueios.
Marcador para observável	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que a Lista de bloqueios é salva com um valor padrão do campo Nome. Se a Lista de bloqueios for criada com o nome "URL do malware", o nome do marcador derivado será "Lista de bloqueios - URL do malware"
Solicitação de Mudança	Quando a caixa de seleção Criar solicitação de mudança é marcada, o número da solicitação de mudança é exibido na instância da Now Platform depois que a Lista de bloqueios é salva. Quando a caixa de seleção Criar solicitação de mudança está desmarcada, este campo não é exibido.
Descrição	Lista de bloqueios de ponto de verificação. Geralmente, o nome contém os tipos de sites e observáveis que você espera estar nesta Lista de bloqueios e você pode usar este campo para obter mais detalhes.

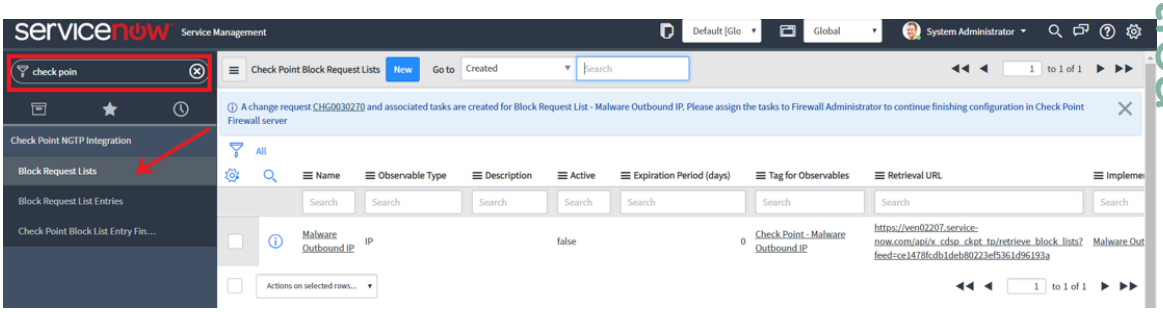
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Período de Expiração (dias)	Período de expiração da Lista de bloqueios. 0 (o padrão) indica que a entrada da Lista de bloqueios nunca expira. Se você mudar este valor, esta entrada ficará ativa para o número de dias que você inserir. Você pode inserir um valor mínimo de 1, que é 24 horas, e não há valor máximo.
URL de recuperação	A URL de recuperação será gerada automaticamente, assim que a Lista de bloqueios for salva. Para configurar esta Lista de bloqueios em gateways de ponto de verificação, você deve usar esta URL. Quando este URL é configurado, o Check Point busca observáveis a serem bloqueados no formato csv.



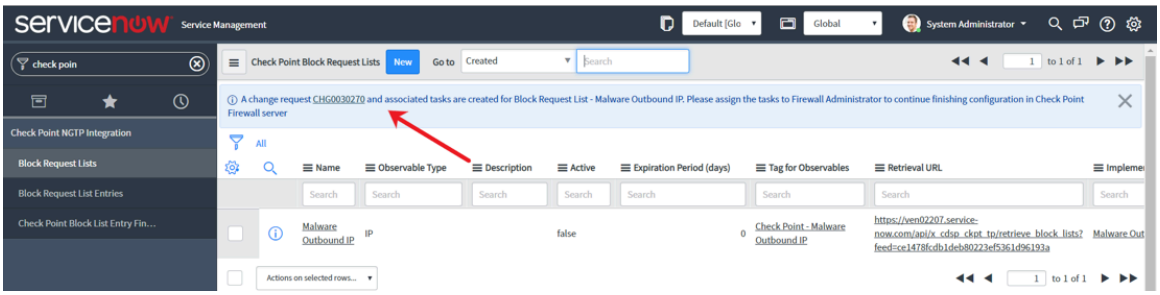
5. Clique em **Enviar**.
6. Se a Lista de solicitações de bloqueio de ponto de verificação não for exibida, navegue até **Integração de NGTP do Ponto de Verificação** > **Listas de solicitações de bloqueio**.



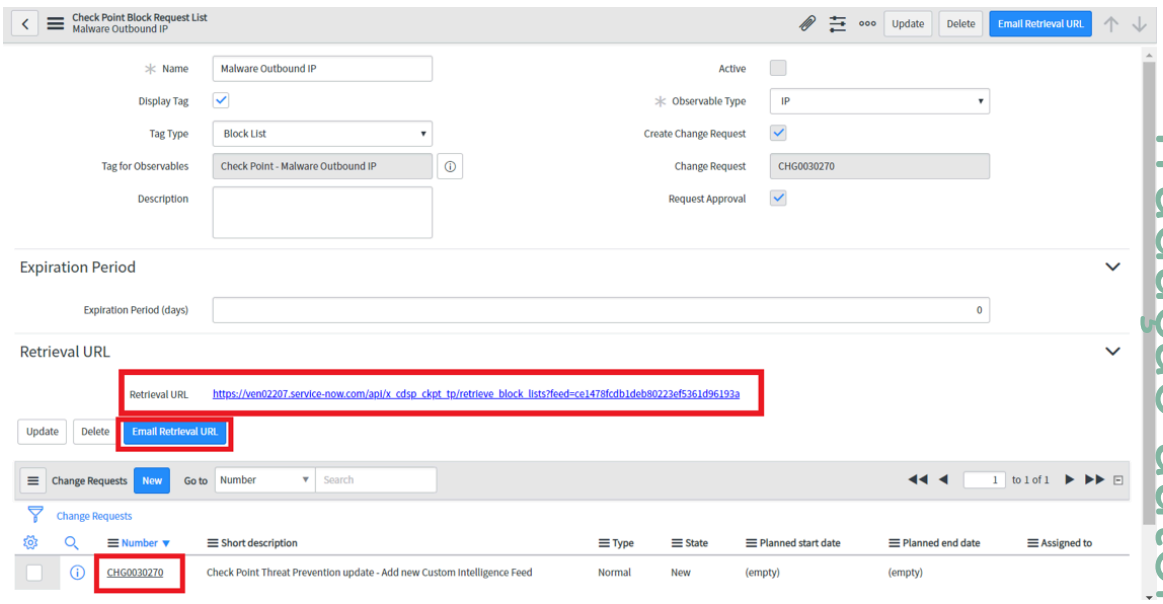
A nova Lista de bloqueios é exibida. O status da Lista de bloqueios ainda é inativo (falso), o que significa que a Lista de bloqueios não está disponível para aceitar entradas. Se Criar solicitação de mudança tiver sido configurado, uma mensagem será exibida indicando que uma solicitação de mudança e tarefas foram criadas em seu ServiceNow AI Platform instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Em **Nome** , clique em um item para abrir o registro.
   O registro da Lista de bloqueios é exibido. Este exemplo mostra uma Lista de bloqueios de IP de saída de malware. Os seguintes campos, opções e links são exibidos no novo registro após o envio e descritos na tabela a seguir.



Campo	Descrição
URL de recuperação de e-mail	E-mail com um aviso informando que o link de bloqueio está disponível para configuração para o administrador do firewall do Check Point.
URL de recuperação	Este URL é usado para configurar o Feed de Inteligência personalizada em gateways de Check Point. **Nota:** Se você tiver suas Configurações do sistema definidas como Formulários com guias, este link será exibido na guia Informações de recuperação da lista de bloqueios na parte inferior do registro.
ServiceNow AI Platform solicitação de mudança	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Excluir	Exclua o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Crie e adicione mais listas de bloqueios conforme necessário.
   As listas de bloqueios são exibidas na página Listas de solicitações de bloqueio do Check Point.

O que Fazer Depois

Ativar a Lista de solicitações de bloqueio manualmente ou com um ServiceNow AI Platform solicitação de mudança.

Ativar uma lista de bloqueios para Check Point NGTP integração

Depois que a Lista de bloqueios tiver sido criada em seu ServiceNow AI Platform E o URL estiver disponível, o administrador do Check Point configura a Lista de bloqueios como Feed de inteligência personalizada em todos os gateways de última geração do Check Point. Para aceitar entradas da Lista de bloqueios, a Lista de bloqueios deve ser configurada no Check Point e ativada no ServiceNow AI Platform.

Antes de Iniciar

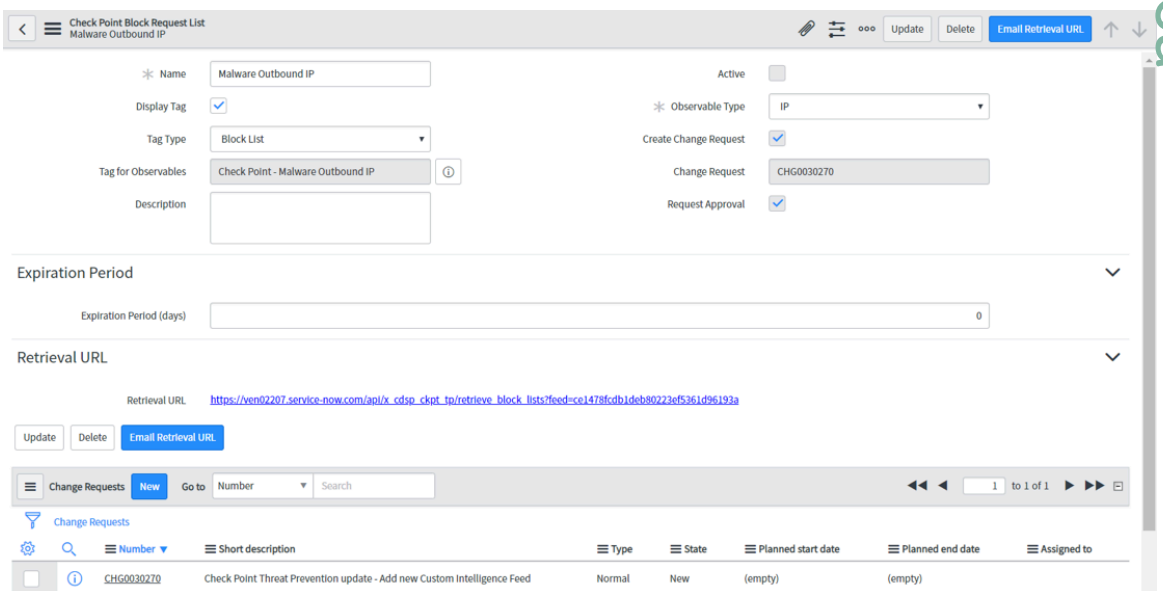
Função necessária: Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Depois que a Lista de bloqueios é configurada, como administrador de incidentes de segurança, você pode ativar a Lista de bloqueios manualmente ou a Lista de bloqueios é ativada automaticamente após a conclusão de um ServiceNow AI Platform Solicitação de mudança. A solicitação de mudança deve ser aprovada e movida do estado inativo para o estado ativo antes de aceitar entradas da Lista de bloqueios.

Procedimento

1. Navegar até **Tudo** > **Integração de NGTP do Ponto de Verificação** > **Listas de solicitações de bloqueio**e selecione **Bloquear listas de solicitações** módulo.
2. Em **Listas de solicitações de bloqueio do ponto de verificação** Que é exibida, selecione sua nova Lista de bloqueios no **Nome** coluna.
3. No registro exibido, observe **URL de recuperação de e-mail** , o link do URL de recuperação da lista de bloqueios ativo e, se configurado, o. ServiceNow AI Platform Solicitação de mudança na seção Solicitações de mudança.
   Observe também que a caixa de seleção Ativo está desmarcada.

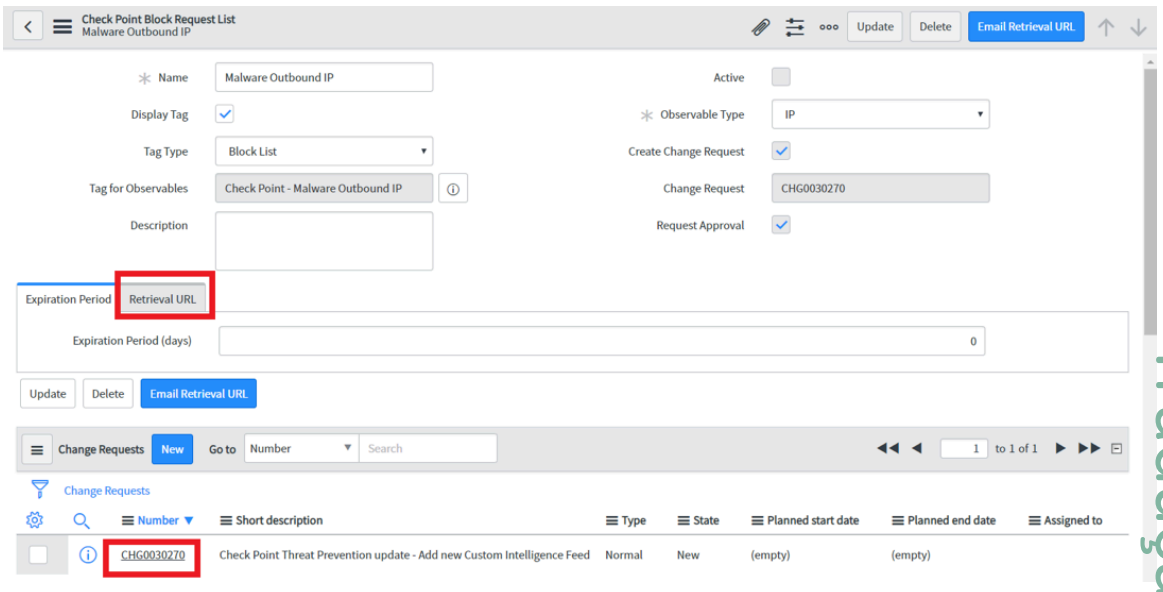


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Com os Formulários com guias limpos nas configurações do sistema, o URL de recuperação da lista de bloqueios aparece na seção URL de recuperação.

4. Clique em **URL de recuperação da lista de bloqueios** Para exibir o URL de recuperação.
   A figura a seguir mostra o URL de recuperação da lista de bloqueios exibido como uma guia com formulários com guias selecionados nas configurações do sistema. O link para a solicitação de mudança (CH0030270) também é exibido.



5. Para concluir a configuração e mover a Lista de bloqueios de inativa para ativa, você deve escolher uma das seguintes opções para notificar o administrador do firewall de que a URL de recuperação está disponível.

Opção	Descrição
Clique em URL de recuperação de e-mail.	URL de recuperação da lista de bloqueios de e-mail diretamente para o administrador do firewall. Esta opção permite que o administrador do firewall conclua a configuração na plataforma Check Point. Escolha esta opção se o administrador do firewall não estiver usando o. ServiceNow AI Platform.
Conclua ServiceNow AI Platform solicitação de mudança e atribua as tarefas de configuração ao administrador do firewall.	Esta opção estará disponível somente se o administrador do firewall do Check Point também estiver usando a Now Platform e o. ServiceNow AI Platform a gestão de mudanças e os processos de aprovação estão configurados. **Nota:** Usuários com a função Administrador de incidentes de segurança (sn_si.admin) podem aprovar o. ServiceNow AI Platform solicitação de mudança. Quando as tarefas de configuração forem concluídas e a solicitação de mudança for fechada, a Lista de bloqueios será ativada automaticamente.

O que Fazer Depois

Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e confirmar que a Lista de bloqueios foi configurada no Check Point, como administrador de incidentes de segurança, a próxima etapa é ativar a Lista de bloqueios. Você ativa a Lista de bloqueios manualmente ou, se configurada, usa o. ServiceNow AI

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Platform Formulário Solicitação de mudança para ativar a Lista de bloqueios. A Lista de bloqueios é ativada automaticamente quando a solicitação de mudança é fechada.

Configure uma lista de bloqueios como um Feed de Inteligência personalizada no Check Point NGTP integração

O administrador do firewall deve configurar o Feed de inteligência personalizada correspondente à Lista de bloqueios criada na NOW Platform.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Esta tarefa precisa ser realizada em cada um dos gateways NGTP do Check Point. O administrador do firewall precisaria do acesso SSH dos servidores do Gateway. Se sua organização tiver ServiceNow AI Platform gestão de mudanças e processos de aprovação, verifique se a capacidade de envio/recebimento de e-mail está habilitada.

O administrador do firewall precisaria do URL de recuperação da Lista de bloqueios e das credenciais do usuário da ServiceNow com função de acesso à conta da API Check Point (sn_sec_checkpoint.api_account_access).

Se o administrador do firewall não estiver usando a NOW Platform, o administrador de incidentes de segurança DA NOW poderá fornecer as informações necessárias por e-mail. Se o administrador do firewall estiver usando a NOW Platform, a solicitação de mudança associada à Lista de bloqueios poderá ser atribuída ao administrador do firewall. Esta solicitação de mudança tem as informações necessárias para configurar o Feed de inteligência personalizada.

Para obter mais informações sobre como configurar o Feed de Inteligência personalizada em gateways de Check Point, consulte: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Procedimento

1. Verifique se a capacidade de envio/recebimento de e-mail está habilitada em seu ServiceNow AI Platform navegando até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**.
2. Em Configuração de e-mail de saída, verifique isso **Envio de e-mail** e. **Recebimento de e-mail** selecionados.
3. Modifique SSH para Gateway de Check Point com o modo especialista.
4. Execute o comando para adicionar o Feed de inteligência personalizado.
   A execução do comando é interativa e solicita o formato e a senha do feed.
   - Quando solicitado o formato do feed, insira "cp_csv"
   - Quando solicitada a senha do usuário da NOW Platform com acesso à API.

   A execução do comando alertará sobre o certificado do servidor (NOW Platform) que não é confiável para a máquina e solicitará a adição do certificado de segurança do servidor ao armazenamento confiável da máquina. Insira **.**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A mensagem "Status: Bem-sucedido" será exibida, confirmando que o Feed foi adicionado com sucesso.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Envie entradas da lista de bloqueios de um incidente de segurança para Check Point NGTP integração

Observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas de lista de bloqueios para diferentes listas de bloqueios. Um processo de aprovação opcional para entradas da lista de bloqueios faz parte do fluxo de trabalho pré-configurado. O gateway importa entradas da lista de bloqueios (endereços IP, URLs, domínios) que estão incluídas nas listas de bloqueios.

Antes de Iniciar

Função necessária:

- Analista de incidentes de segurança (sn_si.analyst) para enviar entradas da lista de bloqueios.
- Administrador de incidentes de segurança (sn_si.admin) para aprovar entradas da lista de bloqueios. Esta autoridade pode ser atribuída conforme exigido pela sua organização.

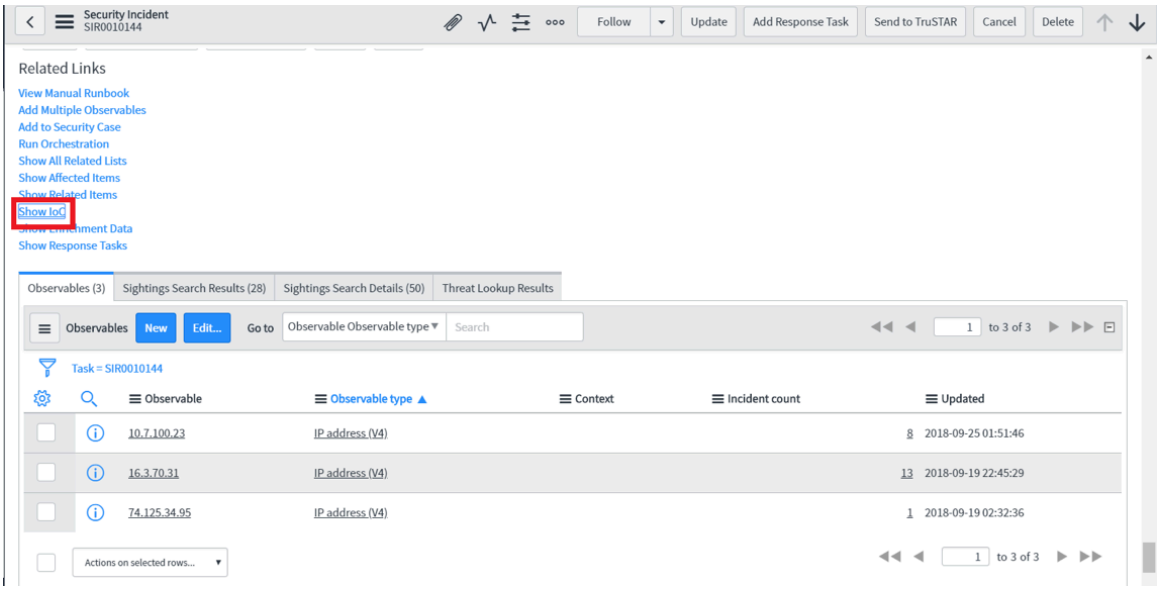
Por Que e Quando Desempenhar Esta Tarefa

Usuários com a função sn_si.analyst enviam entradas de bloqueio solicitando um bloco em observáveis anexados a um registro de incidente de segurança. Uma vez enviada, uma entrada da Lista de bloqueios com status Pendente é gerada e enviada para aprovação. O exemplo a seguir mostra uma solicitação de bloco para um observável de URL.

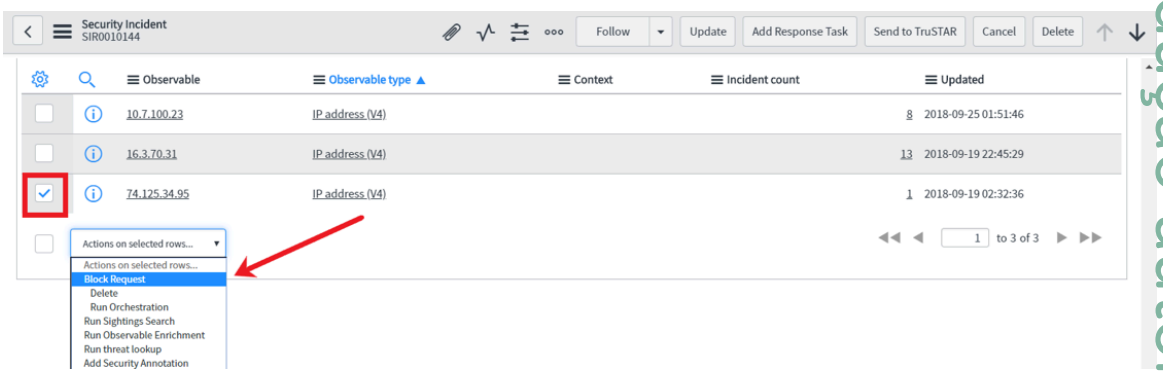
Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique em **Mostrar IOC** link relacionado.

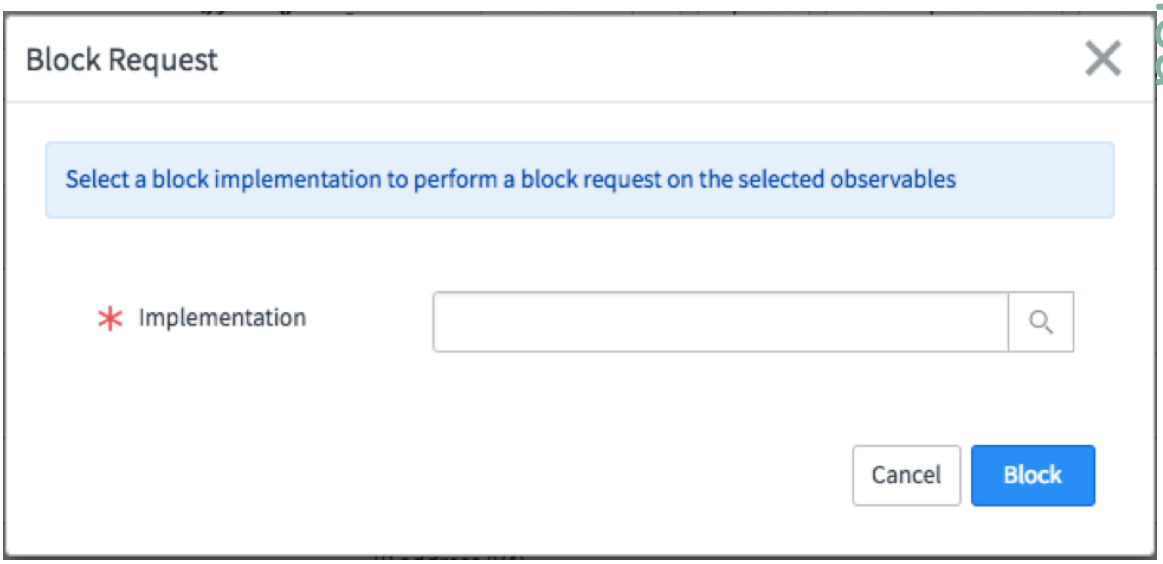
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e, em **Ações nas linhas selecionadas** , selecione **Solicitação de bloqueio** .



4. Na caixa de diálogo exibida, clique no ícone de pesquisa ( )

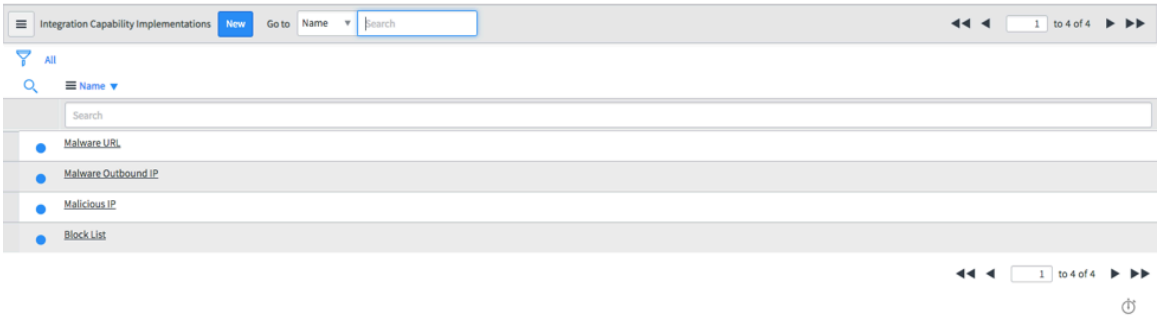


5. Na lista, selecione a Lista de bloqueios à qual você deseja anexar esta entrada.

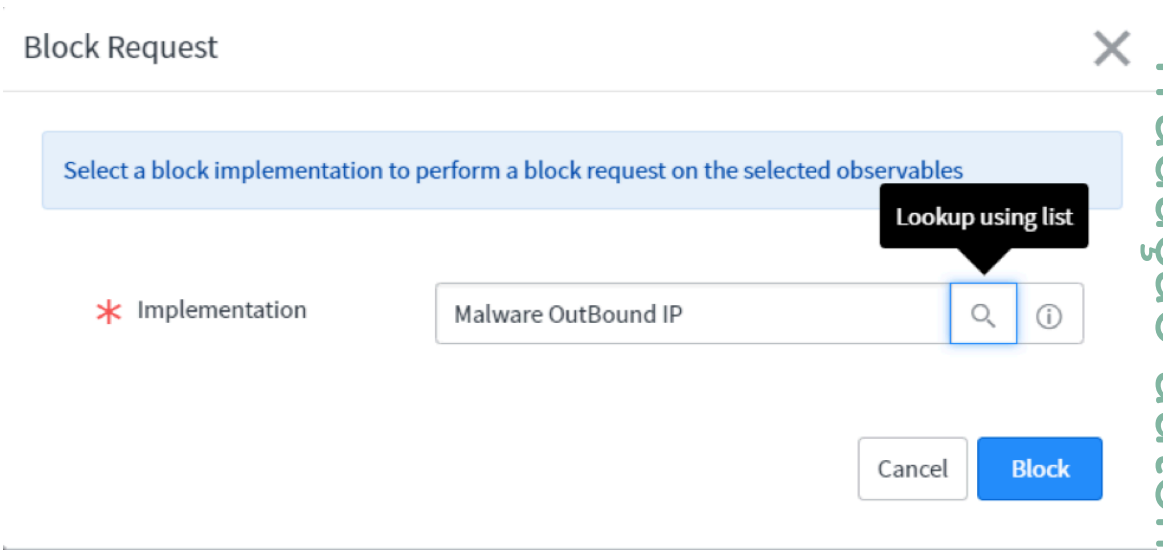
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para este exemplo, o tipo de observável de entrada (IP) deve corresponder ao tipo de observável da lista de bloqueios (IP).

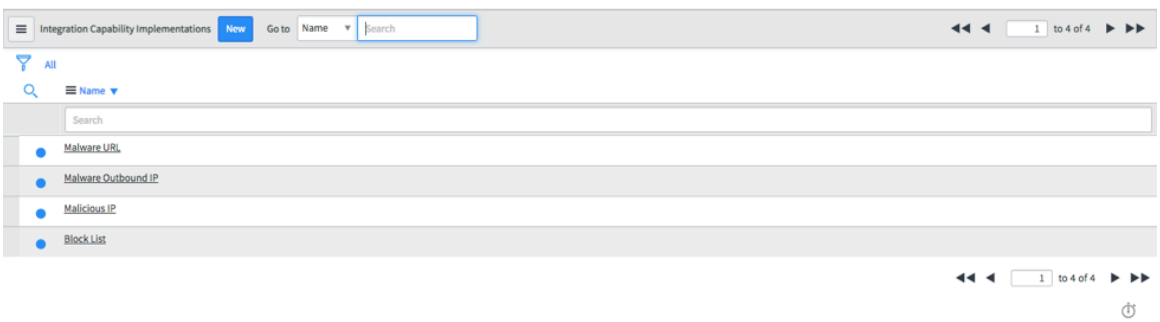


6. Na caixa de diálogo Solicitação de bloqueio com o nome da Lista de bloqueios exibido no campo Implementação, clique em **Bloco** .



7. Na lista exibida, selecione a Lista de bloqueios à qual você deseja anexar esta entrada.

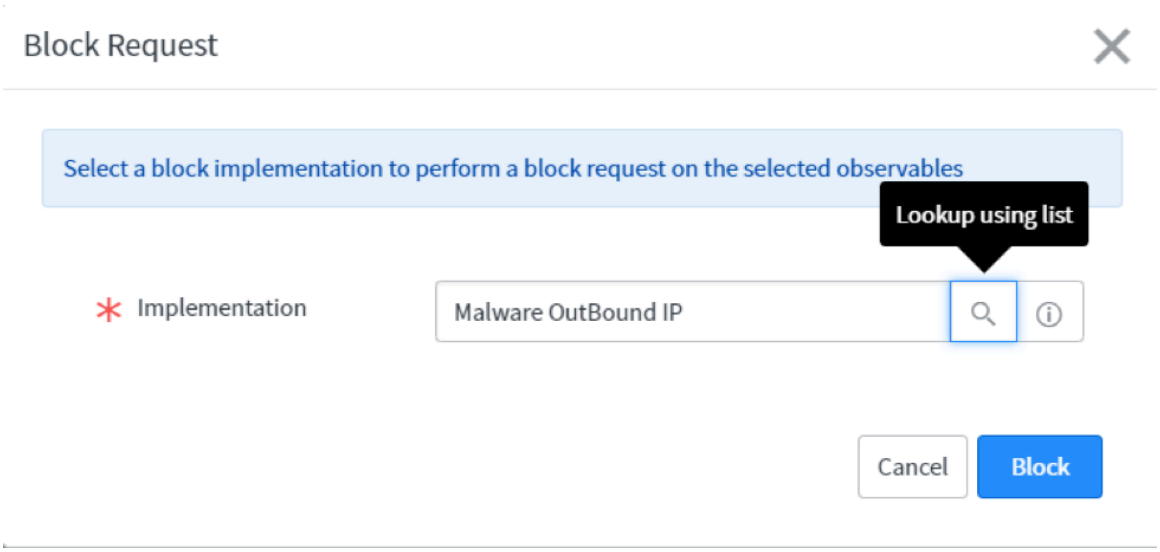
Nota: Para este exemplo, o tipo de observável de entrada (IP) deve corresponder ao tipo de observável da lista de bloqueios (IP).



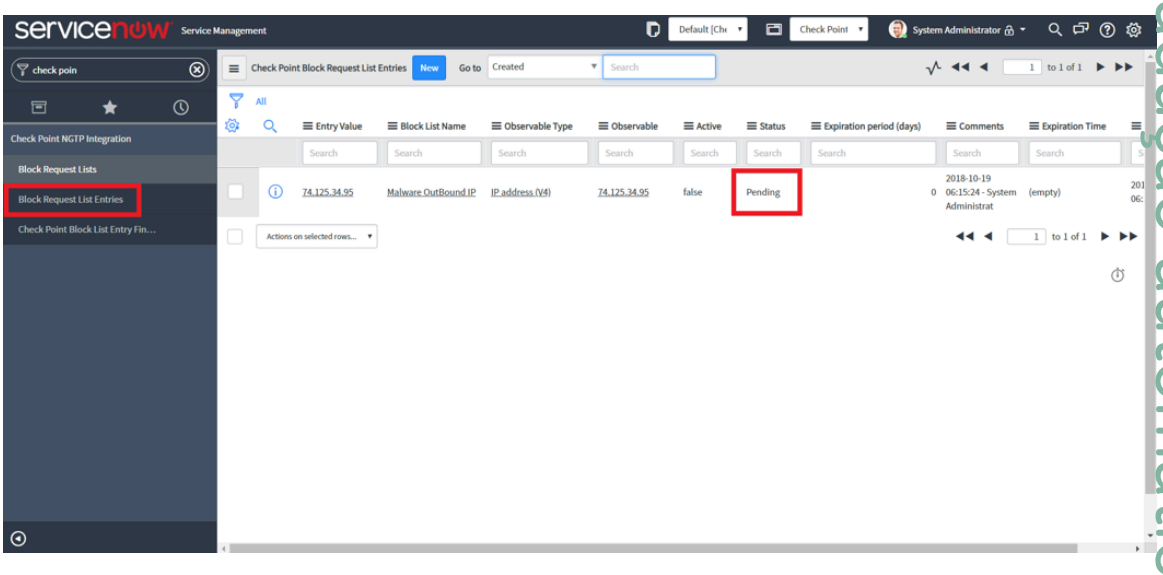
8. Na caixa de diálogo Solicitação de bloqueio com o nome da Lista de bloqueios exibido em **Implementação** clique em **Bloco** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



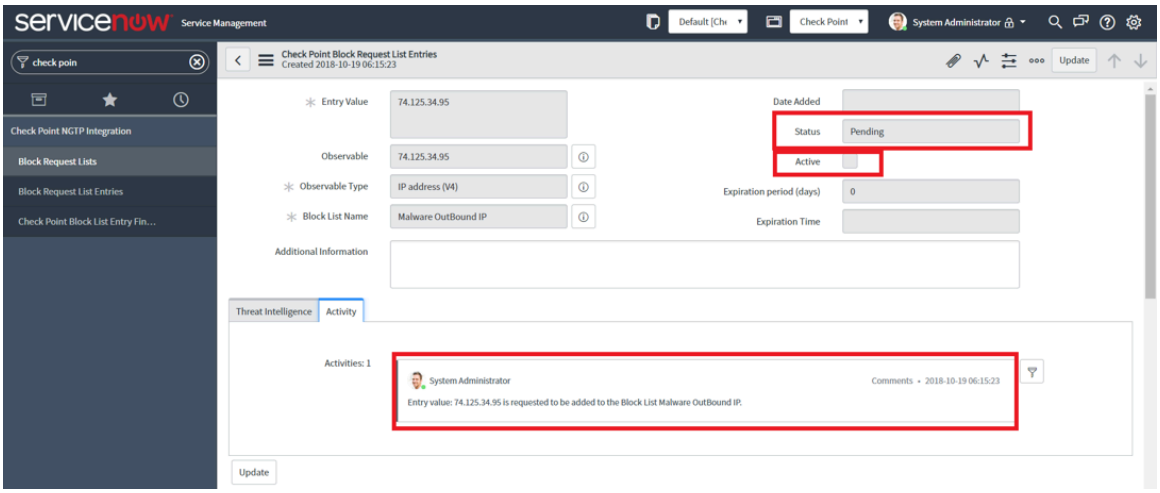
9. Navegar até **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitaçõe**s e clique em **Bloquear entradas da lista de solicitações** .



10. Na lista Entradas da lista de solicitações de bloqueio do Check Point, clique no observável no **Valor de entrada** coluna para abrir o registro.
Para este exemplo, o registro para **74.125.34.95** é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de entrada da lista de bloqueios está pronta para aprovação.

O ícone ao lado do campo observável é um link para ServiceNow AI Platform Tabela observável.

O valor no campo Observável (74.125.34.95) é vinculado à tabela Observável e corresponde ao formato que foi trazido do evento de acionamento de incidentes de Resposta a incidentes de segurança.

Envie entradas da lista de bloqueios diretamente da Tabela de entrada da lista de bloqueios

Para observáveis determinados como mal-intencionados e não associados a um incidente de segurança específico da Now Platform, você envia entradas da Lista de bloqueios da lista de bloqueios.

Antes de Iniciar

Função necessária: Administrador de incidentes de segurança (sn_si.analyst)

Por Que e Quando Desempenhar Esta Tarefa

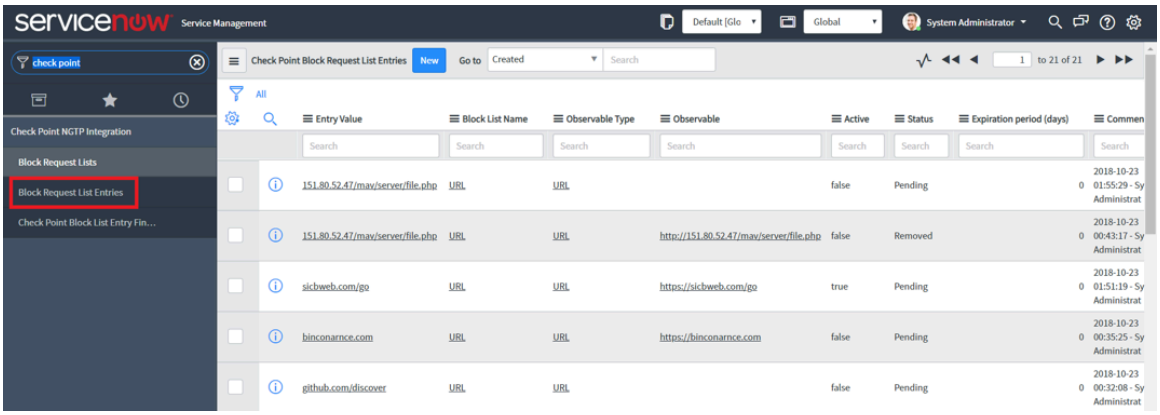
Quando você deseja bloquear um observável que você determinou como mal-intencionado ou permitir que um observável que você determinou não é mal-intencionado e o observável não está associado a um específico ServiceNow AI Platform Registro de incidente de segurança, você envia entradas da lista de bloqueios diretamente da lista de bloqueios. Exemplos desses tipos de entradas da lista de bloqueios podem ser URLs ou domínios para sites específicos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

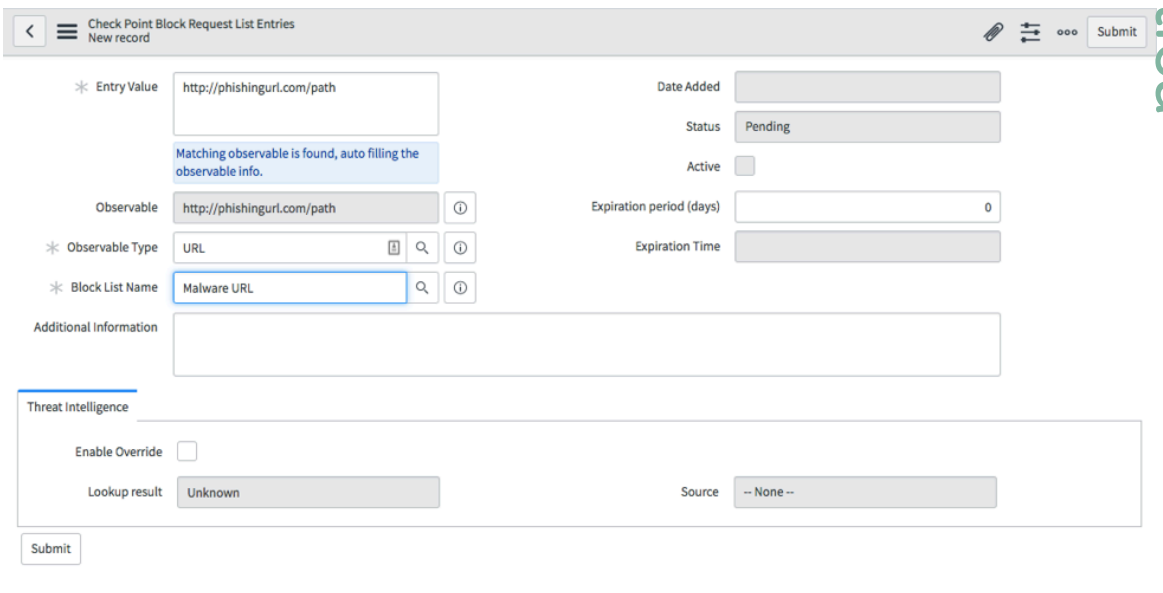
Procedimento

1. Navegar até **Tudo** > **Integração de NGTP do Ponto de Verificação** > **Bloquear entradas de solicitação**.



2. Clique em **Bloquear listas de solicitações** módulo.
3. Na lista Entradas da lista de solicitações de bloqueio do Check Point, clique em **Novo** .
4. Em **Valor de entrada** , insira um valor para o observável.
   Os dois resultados possíveis desta entrada:
   - Os campos restantes no formulário são preenchidos automaticamente.
   - Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione a Lista de bloqueios à qual você deseja anexar esta entrada e clique em Enviar. Selecione a Lista de bloqueios à qual você deseja anexar esta entrada antes de definir o Período de expiração.

   É exibida uma mensagem instruindo você a preencher o formulário. Não foi encontrado um observável correspondente e você deve preencher o formulário. Depois de concluí-lo, selecione a Lista de bloqueios à qual você deseja anexar o observável e clique em Enviar. Um registro observável é criado. A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.

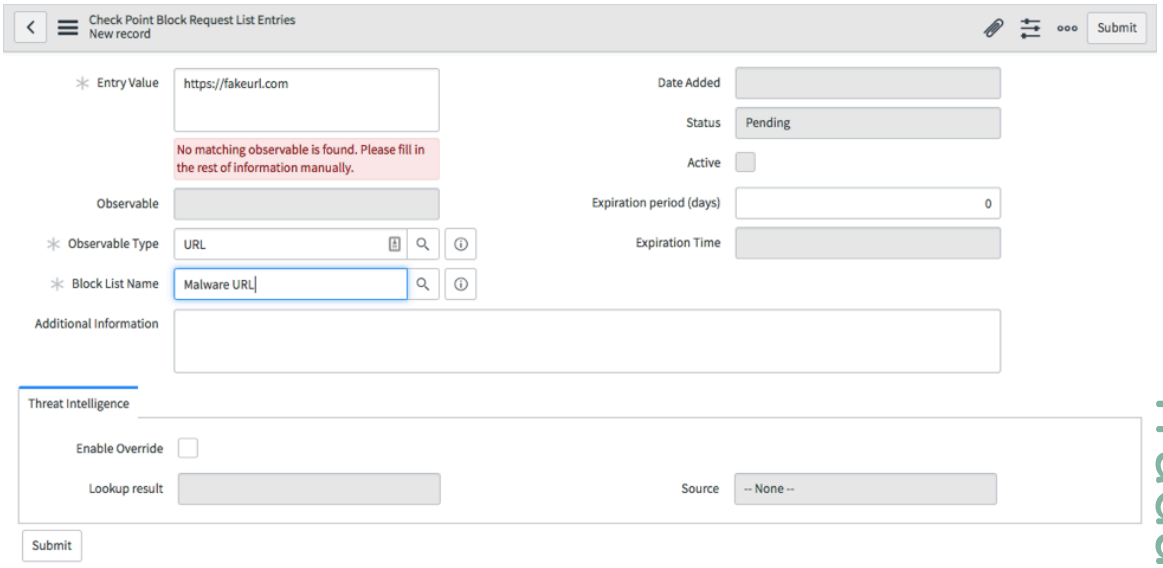


5. Clique no ícone de pesquisa para selecionar a Lista de bloqueios à qual você deseja anexar a entrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
7. Se você tiver a aprovação de e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
   Se uma mensagem for exibida solicitando que você preencha o restante das informações manualmente, preencha os campos.



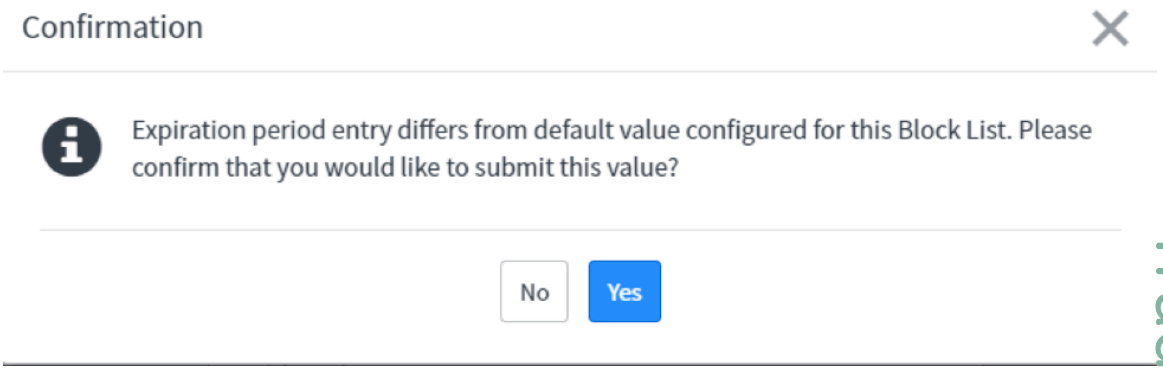
Campo	Descrição
Tipo de observável	Tipo de observável compatível com a caixa de diálogo.
Nome da lista de bloqueios	Lista de bloqueios para a qual você deseja inserir. **Nota:** Selecione a Lista de bloqueios à qual você deseja anexar a entrada antes de definir o Período de expiração.
Habilitar substituição (o padrão é selecionado)	Resultado ou origem da pesquisa. Quando configurado, permite que você insira um Resultado de pesquisa e a origem usada para encontrar os resultados. Normalmente, esses campos são preenchidos quando um registro de incidente de segurança é criado. Nesse caso, não há resultado de pesquisa ou origem e você preenche esses campos manualmente.
Resultado da pesquisa	Selecione **Desconhecido** ou **Mal-intencionado** .
Origem	Origem que executa uma pesquisa de ameaça na entrada da lista de bloqueios, por exemplo, ThreatCrowd etc.
Período de expiração	O período de expiração herdado da Lista de bloqueios por padrão. Você pode substituir este valor, mas somente durante a criação da entrada. 0 indica que a entrada da Lista de bloqueios nunca expira. Se você mudar este valor, esta entrada ficará ativa para o número de dias que você inserir. Você pode inserir um valor mínimo de 1 e não há valor máximo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

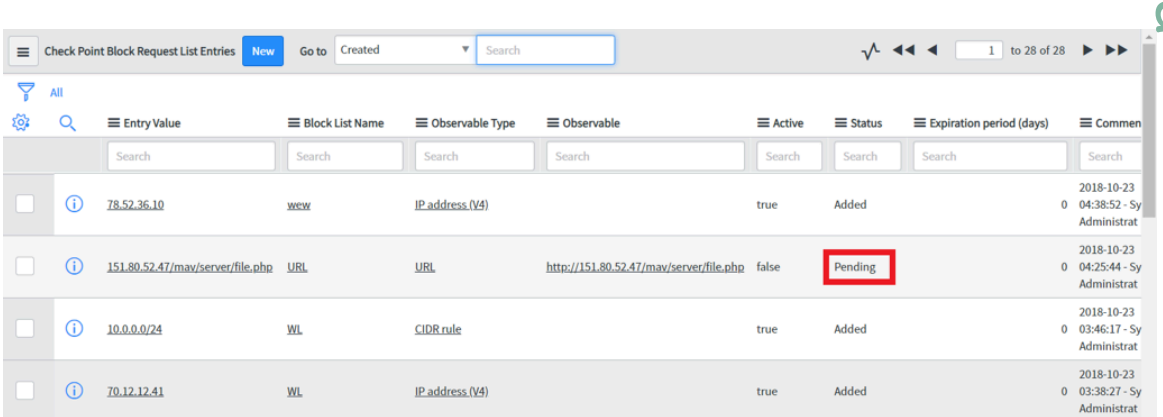
Campo	Descrição
	Por exemplo, se você inserir 30 dias às 2:01 do dia 1 de maio, a entrada da Lista de bloqueios expirará às 2:01 do dia 31 de maio. No entanto, o programador verifica entradas expiradas às 00:00 todos os dias e muda o estado da entrada para "Expirado" em 00:00 de junho de 1.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada da Lista de bloqueios, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente da Lista de bloqueios selecionada.



Opção	Descrição
Sim	Confirma sua substituição de expiração, salva o registro e retorna você para as entradas da Lista de bloqueios do Check Point. Se você tiver a aprovação de e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
Não	Cancela a substituição. Neste ponto, você pode mudar o valor de **Período de expiração** . Depois de alterar o valor, clique em Enviar para retornar à lista de Entradas de bloco de ponto de verificação.

9. Se não for exibido, navegue até **Entradas da lista de solicitações de bloqueio do ponto de verificação** e observe que o status da entrada é **Pendente** .



Agora, a entrada está pronta para aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprovar entradas da lista de bloqueios para Check Point NGTP integração

Um processo de aprovação para entradas da lista de bloqueios faz parte do fluxo de trabalho pré-configurado. As entradas da Lista de bloqueios são aprovadas antes que as entradas sejam ativadas nas Listas de bloqueios. Depois de aprovar a entrada da Lista de bloqueios, o Gateway recupera a entrada e seu observável é bloqueado a partir desse ponto em diante.

Antes de Iniciar

- A aprovação para entradas da lista de bloqueios é atribuída ao Administrador de incidentes de segurança (sn_si.admin) por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização. No exemplo a seguir, ServiceNow AI Platform o administrador tem autoridade de aprovação.

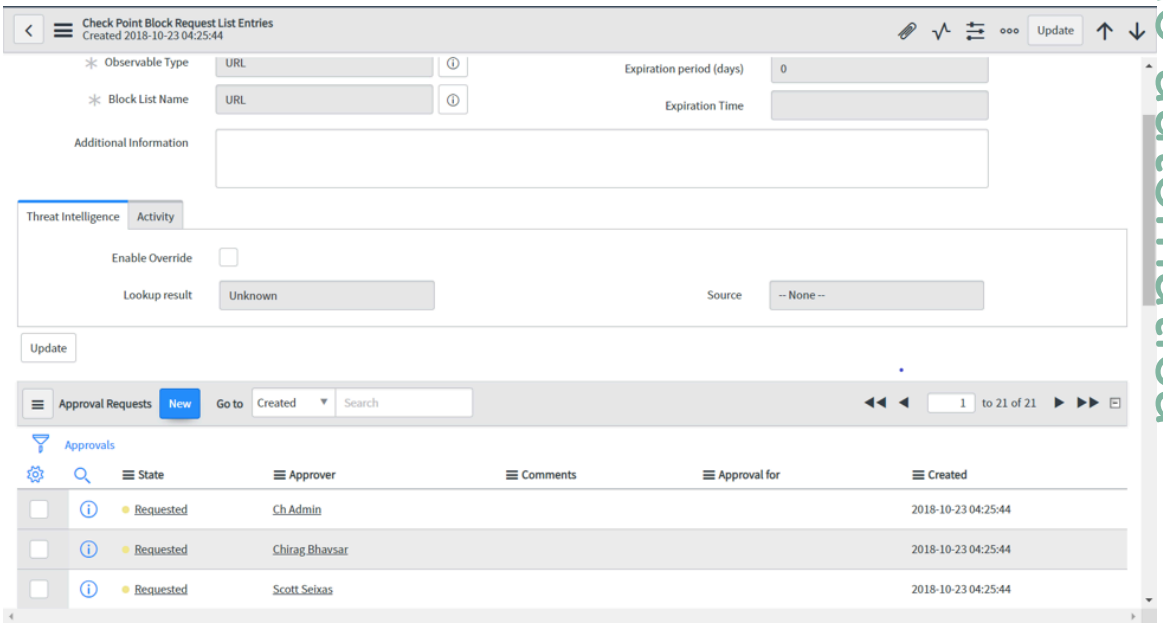
Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada de Lista de bloqueios não é ativada ou desativada na Lista de bloqueios até que seja aprovada.

Procedimento

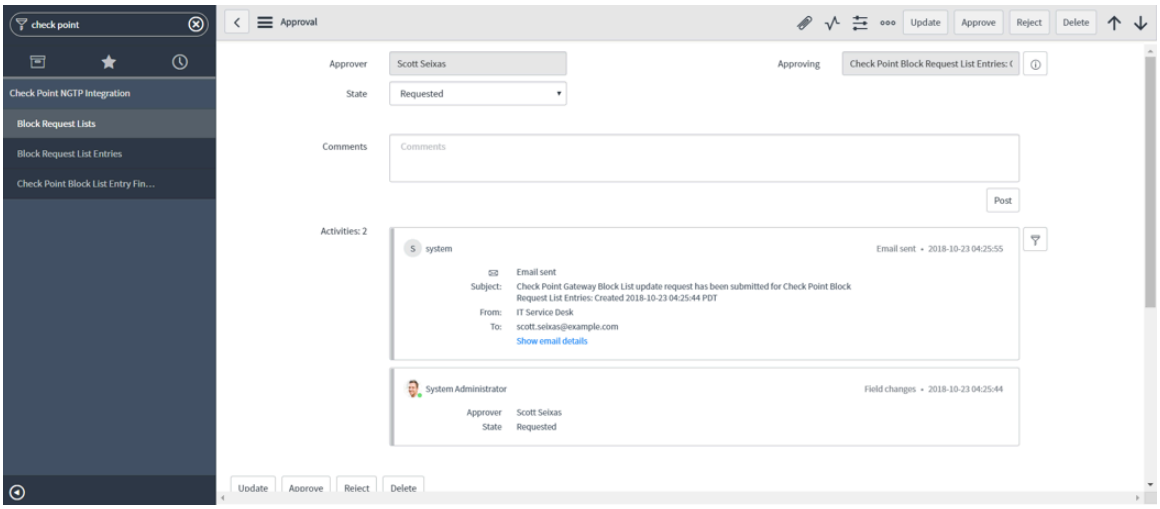
1. Navegar até **Tudo** > **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitações**E abra o registro de Entrada da lista de bloqueios.
2. No registro de Entrada da lista de bloqueios, role até **Solicitações de aprovação** seção.



3. Em Solicitações de aprovação, clique em um item no **Estado** coluna para abri-la.
   O registro de aprovação é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



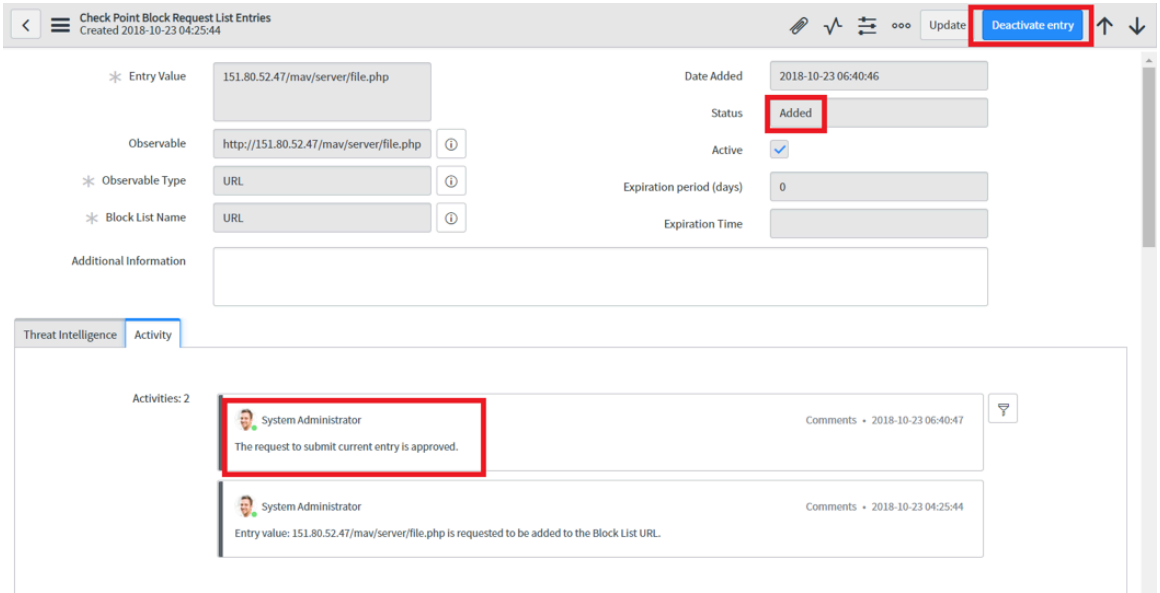
4. Escolha uma opção para aprovar a entrada da Lista de bloqueios.

Opção	Descrição
Aprovar	No registro de entrada, o campo Status muda para Adicionado e a caixa de seleção Ativo é marcada. O botão Desativar é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada da Lista de bloqueios foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para Rejeitado e a caixa de seleção Ativo é desmarcada, indicando que a entrada não está bloqueada no Gateway. As anotações de trabalho mostram que a solicitação da entrada da lista de bloqueios foi rejeitada.

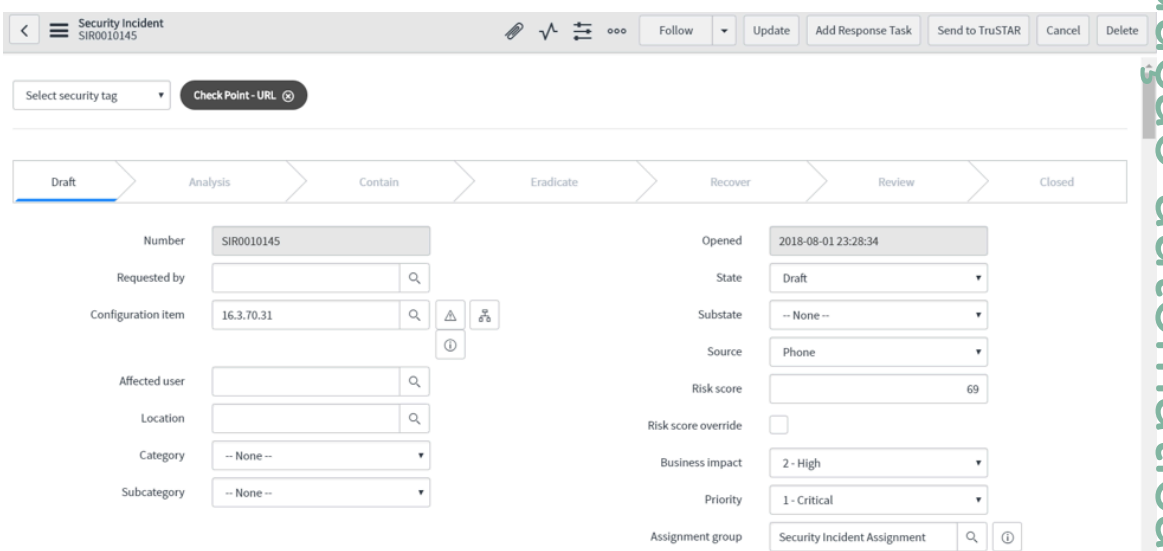
Depois de aprovar a entrada da Lista de bloqueios e ela ser ativada, o firewall de última geração do Check Point recupera a entrada da Lista de bloqueios após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado a partir desse ponto em diante. Na figura a seguir, observe que a caixa de seleção Ativo está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



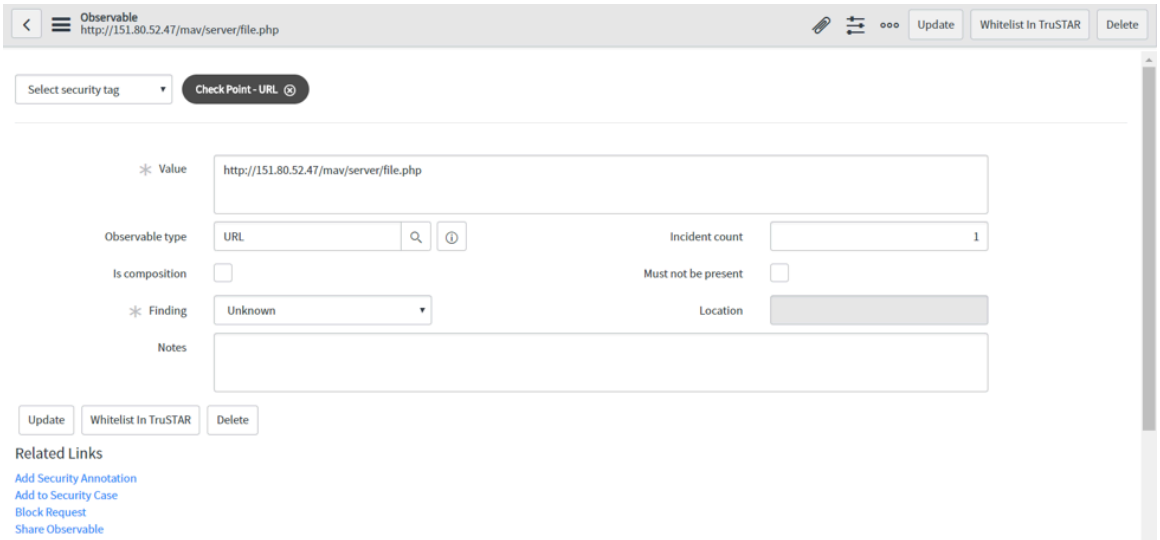
Depois que a entrada da Lista de bloqueios é aprovada e ativada, o registro do incidente de segurança é marcado com um marcador de segurança. O marcador é exibido na parte superior do registro.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O marcador de segurança também é exibido no registro do observável.



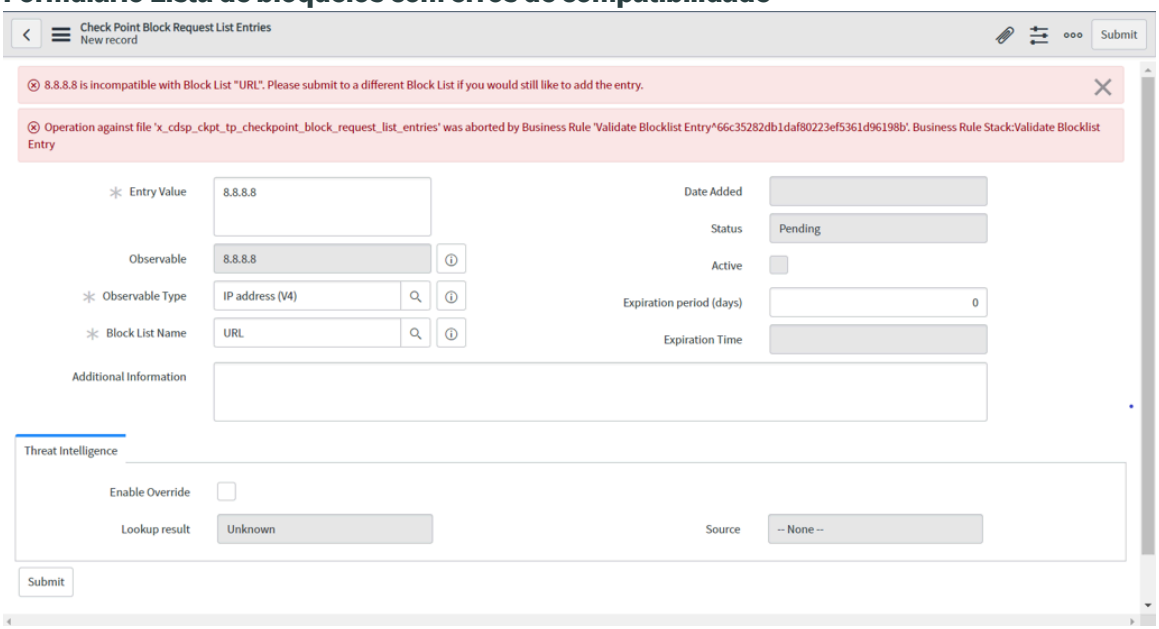
Exceções de entrada da lista de bloqueios para Check Point NGTP integração

Há restrições para adicionar entradas da lista de bloqueios às listas de bloqueios. Se houver conflitos de duplicação, compatibilidade ou CIDR (roteamento entre domínios sem classe) quando você tentar adicionar entradas da lista de bloqueios às listas de bloqueios, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

Exceção de compatibilidade

Cada Lista de bloqueios aceita somente entradas compatíveis com seu tipo de observável. Se você criar uma Lista de bloqueios de domínio e tentar anexar um endereço IP observável a ela, uma mensagem de erro incompatível será exibida. Por exemplo, uma Lista de bloqueios de domínio só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Formulário Lista de bloqueios com erros de compatibilidade

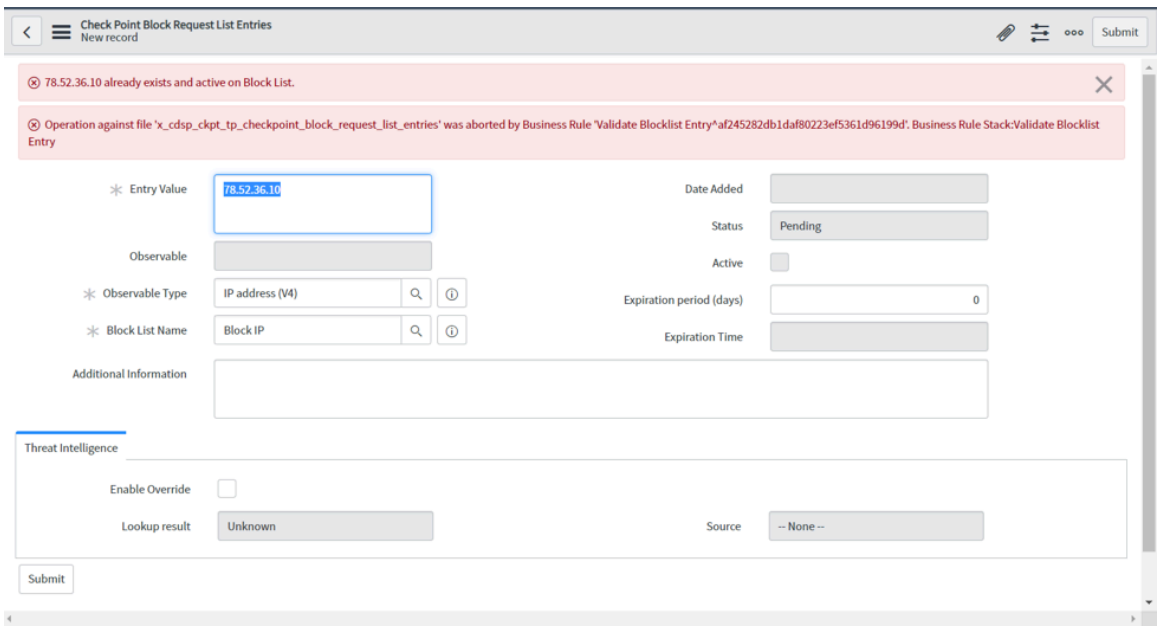


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

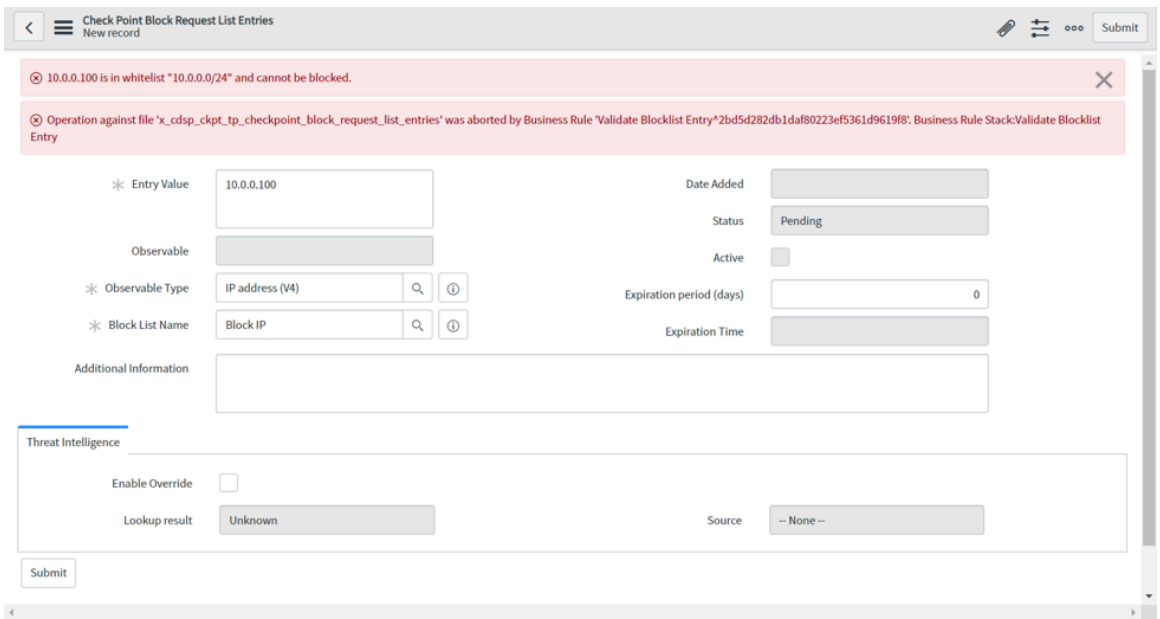
Exceção de duplicação

Um observável não pode ser ativado em várias listas de bloqueio do mesmo tipo de observável. Se um observável de URL já estiver ativado em uma lista de bloqueios de URL e você tentar ativar o mesmo observável em uma lista de bloqueios de URL de phishing, uma mensagem de erro de duplicação será exibida.



Exceção CIDR (roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a uma lista de permissões e este endereço IP fizer parte de um observável de CIDR já em uma lista de bloqueios/lista de permissões, um erro de conflito de CIDR será exibido. Este erro indica que o único endereço IP já está incluído na lista de bloqueios ou na lista de permissões como parte do observável CIDR. Por exemplo, 192.168.24.25 faz parte do bloco CIDR 192.168.0.0/22.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Edite o nome do marcador de segurança do Check Point NGTP integração

Se a caixa de seleção Exibir marcador estiver marcada ao criar o registro Lista de bloqueios, você poderá editar os nomes e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

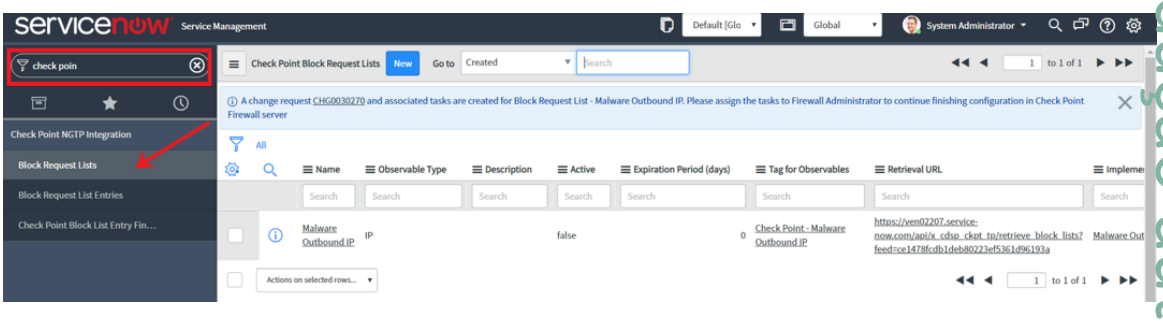
Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

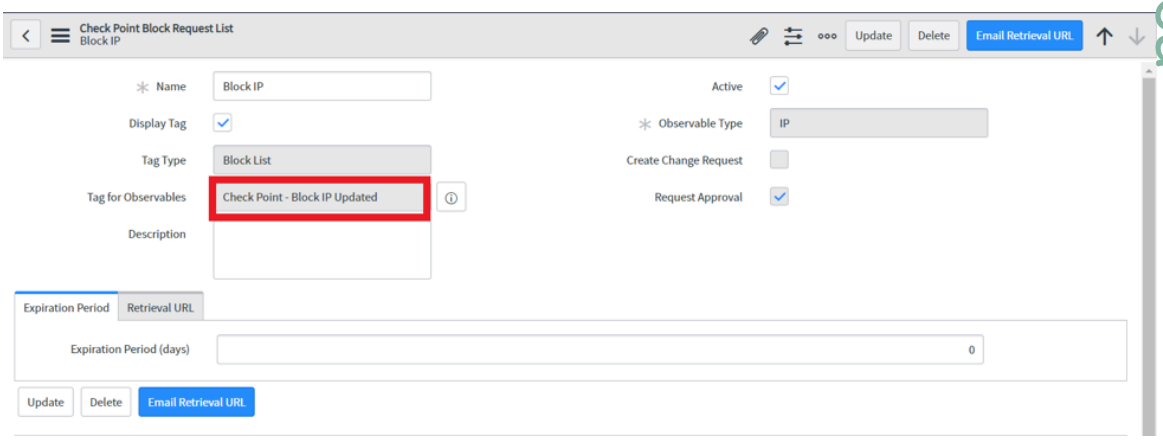
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se ele foi removido de uma Lista de bloqueios. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Procedimento

1. Navegar até **Tudo** > **Integração de NGTP do Ponto de Verificação** > **Configuração da lista de solicitações de bloqueio**.



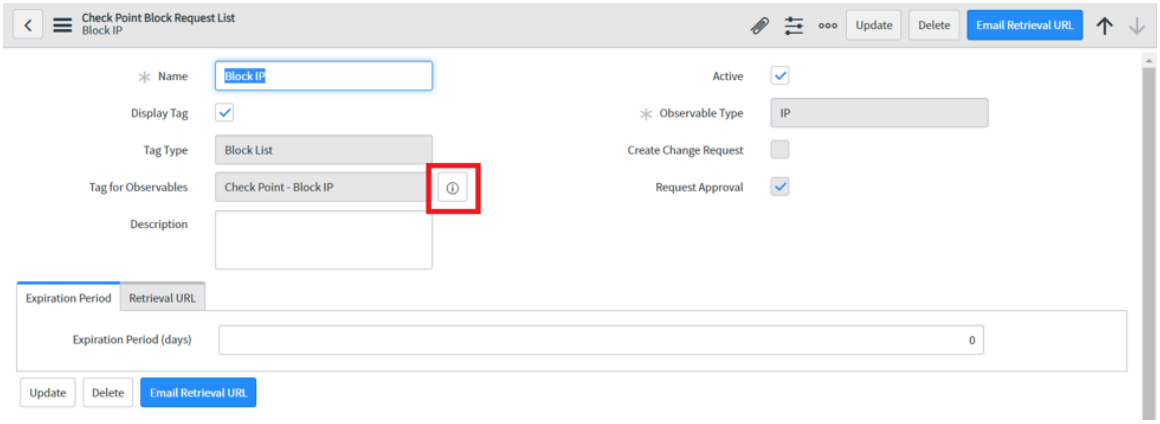
2. Clique em um item no **Nome** coluna para abri-la.
   O registro da Lista de bloqueios é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor inserido no campo Nome da Lista de bloqueios quando você a criou. Por padrão, o nome também inclui um prefixo de Lista de bloqueios, por exemplo, Lista de bloqueios - URLs mal-intencionados de malware.



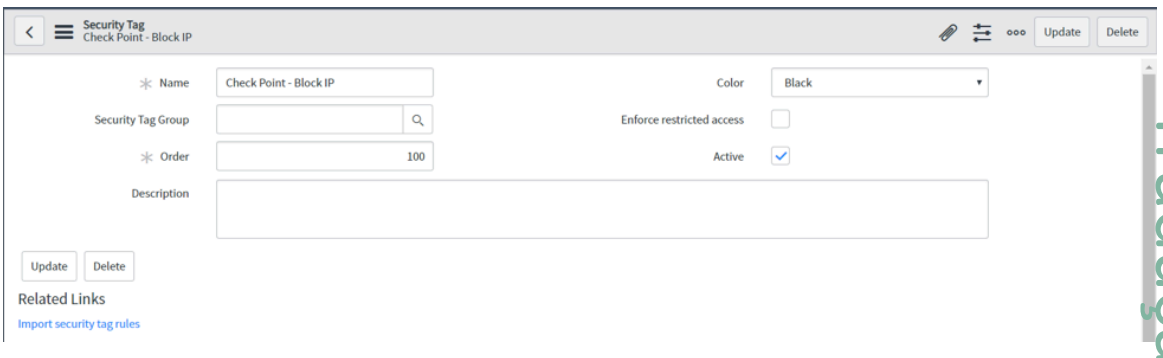
3. Clique no ícone de informações ao lado do marcador para observáveis e em Abrir registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

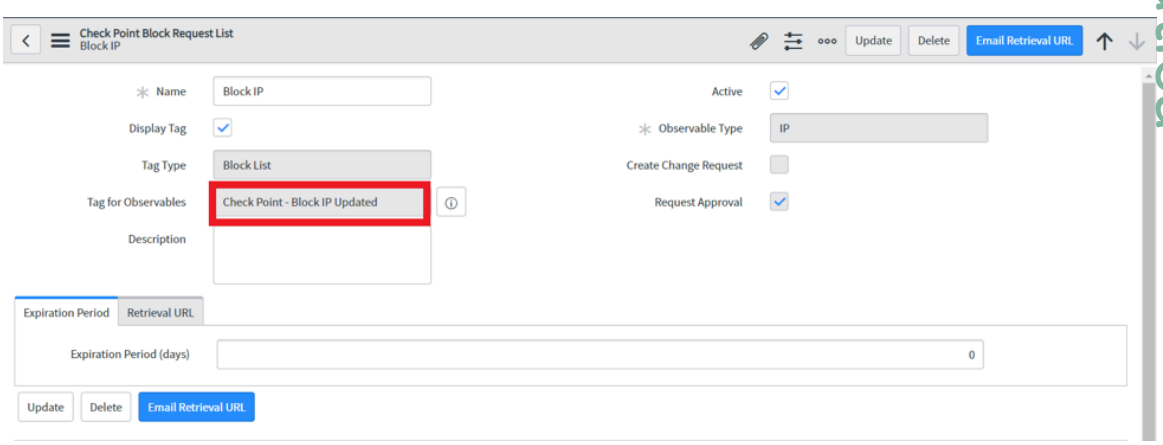


O formulário Marcador de segurança é exibido.



4. Em **Nome** modifique o nome do marcador de segurança.
5. Clique em **Atualizar**.
   O registro da Lista de bloqueios atualizada é exibido com o nome do marcador modificado.

> **Nota:** No exemplo a seguir, Saída foi adicionada ao nome do marcador. Mantenha o prefixo do Check Point no novo nome do marcador para ajudá-lo a identificar se o marcador está associado à integração do firewall de última geração do Check Point.

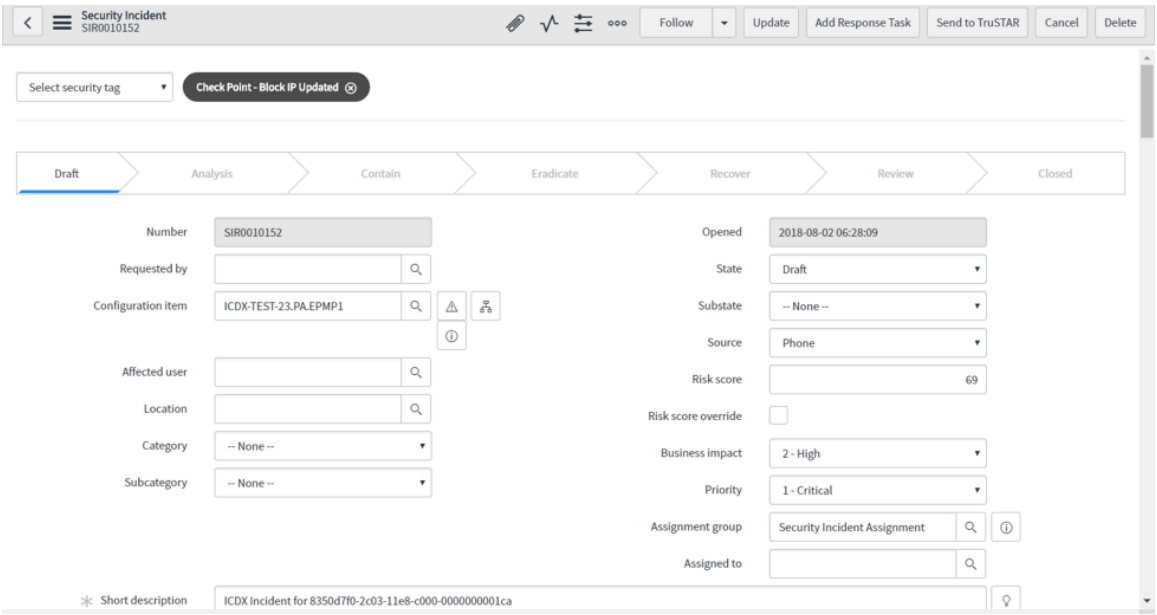


Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, Domínio) no registro de incidente de segurança e no registro do observável sempre que o observável é adicionado à Lista de bloqueios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado



Se um observável já tiver sido adicionado a uma Lista de bloqueios e um marcador de segurança for exibido em um incidente de segurança desse observável, o marcador de segurança da Lista de bloqueios também será exibido automaticamente em todos os registros de incidentes de segurança subsequentes criados. Esta duplicação informa que o observável já está em uma lista de bloqueios. Não é necessário adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro de incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desativado de uma Lista de bloqueios.

Desinstalar o. Check Point NGTP integração

Se você quiser desinstalar Check Point NGTP Integração do seu ServiceNow AI Platform E remover todos os remanescentes da integração, consulte o site de documentação da ServiceNow para obter instruções sobre como desinstalar aplicações.

Função necessária: administrador

Integração do CrowdStrike Falcon Host

. CrowdStrike Falcon Host a integração permite que você envie observáveis em um incidente de segurança para uma lista de observação, tornando-os capazes de gerar alertas adicionais. Esta integração é uma implementação do fluxo de trabalho do CrowdStrike Falcon Host - Publicar na lista de observação.

Explorar	Configurar
Integrações do Resposta a incidentes de segurança	Comece a usar CrowdStrike Falcon Host integração

Usar	Desenvolver
Realizar pesquisas em observáveis	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Host do CrowdStrike Falcon de operações de segurança - Publicar no fluxo da lista de observação

. **CrowdStrike Falcon Host de operações de segurança - Publicar na lista de observação** o flow designer é usado para especificar a lista de observação para gerar alertas ou eventos. Os alertas e eventos são exibidos no sistema CrowdStrike Falcon Host com base em como ele está configurado.

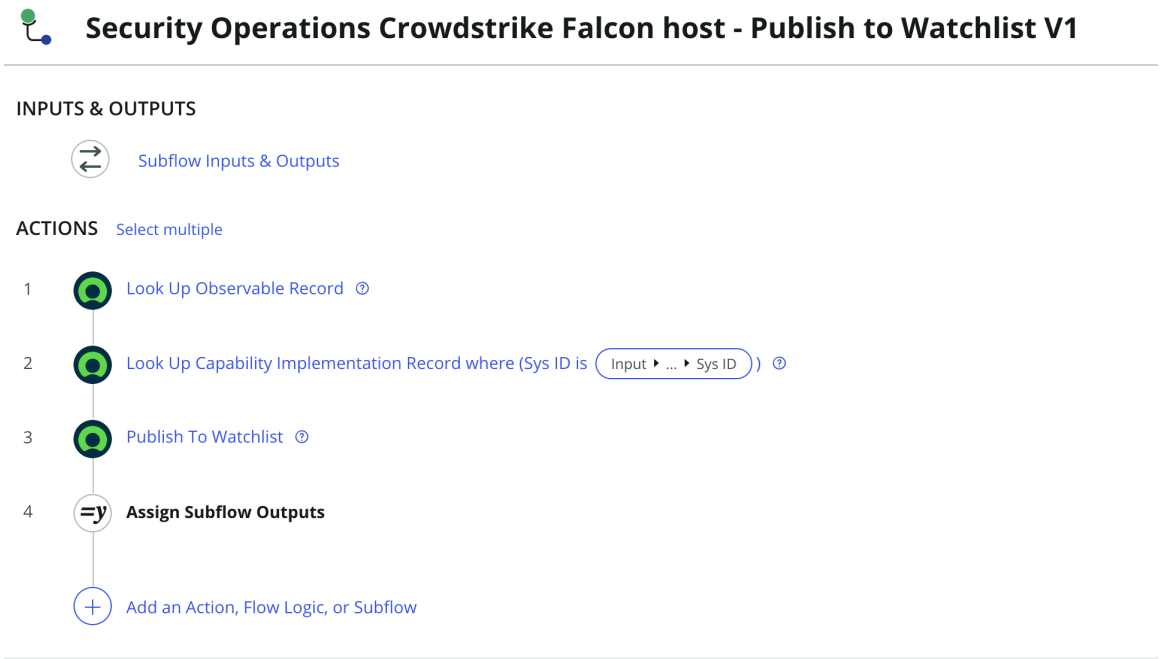
Publicar no fluxo da lista de observação

Este designer de fluxo é acionado pelo Integração de operações de segurança- Publicar na lista de observação Quando você seleciona um ou mais observáveis associados a um incidente de segurança e usa a ação de IU Publicar na lista de observação para enviar os observáveis para uma lista de observação. Os observáveis podem ser usados para gerar alertas adicionais. Para obter

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mais informações, consulte Publique observáveis em uma lista de observação de



terceiros.

Comece a usar CrowdStrike Falcon Host integração

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo CrowdStrike Falcon Host integração. Antes de poder usar CrowdStrike Falcon Host, você deve baixá-lo do ServiceNow Store e, em seguida, adicione um nome de usuário e senha.

Antes de Iniciar

- Se você estiver atualizando CrowdStrike Falcon Host integração de uma versão anterior, em seguida, você deve excluir a configuração existente e definir uma nova configuração. A nova integração oferece suporte à autenticação OAUTH2. Esta atualização requer que você insira **ID do cliente da API** e o. **Segredo do cliente da API** para autenticar e concluir a configuração.
- Em CrowdStrike Falcon Host portal **Escopos de API** habilite o. **Leitura** e. **Gravar** configuração para **IOCs (indicadores de comprometimento)** .

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão Host do CrowdStrike Falcon, clique em **Configurar** .
4. No formulário, preencha os campos para concluir a configuração:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do host do CrowdStrike Falcon

Campo	Descrição
Nome	Nome da integração, por exemplo, demonstração-1 .
ID do cliente da API	O ID do cliente que você obtém na seção de configurações do seu perfil de conta em CrowdStrike Falcon Host portal.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do seu perfil de conta em CrowdStrike Falcon Host portal.

5. Clique em **Enviar**.

Resultado

Depois de configurado, o CrowdStrike Falcon Host a integração pode ser selecionada para publicar observáveis em listas de observação em Resposta a incidentes de segurança.

CrowdStrike Falcon Insight integração

Com CrowdStrike Falcon Insight para Operações de segurança integração, você pode fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando ServiceNow AI Platform Resposta a incidentes de segurança produto.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

. CrowdStrike Falcon Insight para Operações de segurança a integração funciona com ServiceNow AI Platform para que você possa obter informações adicionais sobre o escopo de um incidente. . CrowdStrike Falcon Insight captura todas as atividades de evento de endpoint relevantes, você pode usar ServiceNow AI Platform concentrar-se em investigações e ações de correção.

Conheça esta integração

Identificador do documento	Título do documento
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow
CrowdStrike Falcon Insight para Operações de segurança	Introdução ao CrowdStrike Falcon Insight integração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução ao CrowdStrike Falcon Insight integração

Você pode ativar e configurar o. CrowdStrike Falcon Insight para fazer interface com seu ServiceNow AI Platform instância e. Resposta a incidentes de segurança produto.

Função necessária: administrador

Antes de poder usar CrowdStrike Falcon Insight para Operações de segurança, você deve baixá-lo do ServiceNow Store.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	Estas funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin configura a integração, cria e ativa perfis e atribui a função sn_si.analyst. • A função sn_si.analyst responde a incidentes de segurança, inicia perfis manualmente e pode enviar solicitações para ações como isolar o host e remover o isolamento do host de um grupo aprovado.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você configurar esta integração.	. ServiceNow IntegrationHub Instalador do Enterprise Pack [o plug-in com.glide.hub.integrations.enterprise] é necessário. Este plug-in permite a execução de ações e fluxos do IntegrationHub: . Resposta a incidentes de segurança o plug-in (com.snc.security_incident) é obrigatório. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação uma de cada vez na seguinte ordem para garantir uma instalação tranquila:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	1. Resposta a incidentes de segurança Dependência (com.snc.si_dep) **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança **5.** Inteligência contra ameaças Suporte Comum **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Resposta a incidentes de segurança
Configure um grupo de aprovação.	Um recurso de aprovação opcional está disponível para isolar máquinas host, restaurá-las para a rede e iniciar pesquisas de vistas. Para habilitar esta opção, você precisa de aprovação prévia da função sn_si.admin antes que as máquinas host sejam isoladas e restauradas em sua rede ou quando as pesquisas de vistas forem realizadas. Se você precisar de um nível extra de controle sobre essas ações, habilite **Aprovação necessária** opção ao configurar o perfil. A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação.
Atribua e verifique as funções da plataforma CrowdStrike Falcon.	As seguintes funções são necessárias na Plataforma CrowdStrike Falcon para a configuração de integração: • A função de administrador do Falcon é necessária para exibir, criar ou modificar clientes ou chaves de API. • A função Respondente em tempo real - Administrador é necessária para criar e executar scripts personalizados. • A função Respondente em tempo real - Respondente ativo é necessária para criar e executar scripts personalizados.
Verifique se as funções e permissões de scripts personalizados estão habilitadas na Plataforma CrowdStrike Falcon.	Esta integração usa scripts personalizados do CrowdStrike para alguns dos recursos de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• Verifique se as funções Respondente em tempo real - Administrador e Respondente em tempo real - Respondente ativo estão disponíveis. • Verifique se o **Política padrão (Windows)** A opção está habilitada em Configuração > Políticas de resposta na IU do CrowdStrike Falcon. • Verifique se o **Resposta em tempo real** e. **Scripts personalizados** Em Tempo real, a funcionalidade está habilitada na IU do CrowdStrike Falcon.
Gere clientes e chaves de API na plataforma CrowdStrike Falcon.	Crie os clientes ou chaves da API do CrowdStrike na plataforma CrowdStrike Falcon para usar no ServiceNow AI Platform configuração de integração.

Criar cliente de API do CrowdStrike e gerar chaves

Crie o cliente de API do CrowdStrike e gere o ID e a chave do cliente, que você usa para configurar o. CrowdStrike Falcon Insight integração.

Antes de Iniciar

Função necessária: Administrador do CrowdStrike Falcon

Procedimento

1. Na Plataforma CrowdStrike Falcon, navegue até **Chaves e clientes de API** .
2. Na tabela Clientes de API OAuth2, clique em **Adicionar novo cliente de API** .
3. Insira os seguintes detalhes para definir seu cliente de API:

Campo	Descrição
Nome do cliente	Insira o nome do cliente. Este campo é obrigatório.
Descrição	Insira a descrição do nome do cliente.
Escopos de API	É necessário definir os escopos. **Importante:** Habilite a conta de API e certifique-se de que os seguintes escopos estejam habilitados para a conta de API: ○ Habilitar escopos de leitura e gravação para a API Hosts ○ Habilitar escopo de leitura para API de indicadores

4. Clique em **Adicionar** Para salvar o cliente de API e gerar o ID do cliente e a chave secreta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar CrowdStrike Falcon Insight

Instale e configure o. CrowdStrike Falcon Insight para Operações de segurança aplicação do ServiceNow Store em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: administrador

Nota: Você pode associar uma capacidade a apenas um perfil. Não é possível associar uma capacidade a vários perfis. Ao configurar servidores do CrowdStrike, você não pode reutilizar um recurso do CrowdStrike com vários perfis que compartilham o servidor do CrowdStrike. Seus perfis podem ter a mesma capacidade do CrowdStrike, cada perfil deve usar seu próprio servidor CrowdStrike.

Procedimento

1. Baixe o. CrowdStrike Falcon Insight Para integração de Operações de segurança do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE CrowdStrike Falcon Insight para Operações de segurança bloco de integração e clique em **Configurar** .
4. No formulário, preencha os campos para concluir a configuração:

Configuração do CrowdStrike Falcon Insight

Campo	Descrição
Nome	Nome da integração, por exemplo, `demonstração-1` .
URL da API do CrowdStrike Falcon Insight	URL base que hospeda a API do CrowdStrike. Insira o URL com o protocolo HTTPS. Por exemplo, https://api.crowdstrike.com.
ID de cliente	O ID do cliente que você obtém na seção de configurações do seu perfil de conta no CrowdStrike Falcon Insight portal.
Segredo do cliente	A chave secreta do cliente que você obtém na seção de configurações do seu perfil de conta no CrowdStrike Falcon Insight portal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.

Resultado

Depois que a integração é validada e enviada com sucesso, ela é salva na página Integrações de segurança como um bloco. Você pode exibir CrowdStrike Falcon Insight no navegador de aplicações.

Crie um grupo de aprovação

Crie um grupo de aprovação para CrowdStrike Falcon Insight para Operações de segurança integração que pode aprovar solicitações para isolar máquinas host, restaurá-las para a rede e iniciar pesquisas de vistas.

Antes de Iniciar

Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota: A opção de aprovações no configuração de perfil Aparece somente para os recursos Isolar host e Remover isolamento de host.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.
2. Na lista Grupos, clique em **Novo** .
3. No formulário, preencha os campos.

Formulário do grupo de aprovação

Campo	Descrição
Nome	Nome do grupo que você vê ao enviar uma solicitação de aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	Nome do grupo primário, se associado a um primário.
Tipo	Categorias de grupos.
Fornecedores	função vendor_manager que você atribui aos usuários no processo de gestão de fornecedores da sua organização.
Descrição	Informações adicionais sobre o grupo.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

   Este grupo está disponível para processar solicitações quando você habilita o. **Aprovação necessária** durante a configuração deste perfil.

   Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até **Minhas aprovações** no ServiceNow AI Platform.

O que Fazer Depois
A próxima etapa é a. instalar e configurar . CrowdStrike Falcon Insight Aplicação da ServiceNow Store.

Crie um perfil de capacidade para CrowdStrike Falcon Insight integração

Crie um perfil e selecione CrowdStrike Falcon Insight capacidades que você deseja que o perfil execute.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Considere por que você deseja criar um perfil antes de adicionar CrowdStrike Falcon Insight recursos para ti. A tabela a seguir lista os recursos que você deve adicionar a um perfil quando quiser que o perfil execute determinadas consultas ou ações.

Você pode criar um único perfil que executa consultas para detalhes do sistema, lista usuários conectados, busca serviços em execução, busca processos em execução, busca estatísticas de rede, isola o host e remove o host isolado. Como alternativa, você pode criar vários perfis, cada um com sua própria capacidade única.

Nota: Isolar host, remover isolamento e obter recursos de arquivo não podem ser mesclados com outros recursos ao criar um perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de perfil e capacidades necessárias do CrowdStrike Falcon Insight

Finalidade do perfil	Capacidades do CrowdStrike
Reúna detalhes do host e usuários conectados	• **Obter detalhes do host** • **Obter usuários conectados**
Busque as estatísticas, os processos e os serviços de rede em execução para um host	• **Obter estatísticas de rede** • **Obter processos em execução** • **Obter serviços em execução**
Isolar um host	**Isolar Host**
Remova o isolamento de um host	**Remover isolamento**
Obtenha um arquivo de um endpoint de host	**Obter arquivo**

Procedimento

1. Navegar até **Tudo** > **Integração com CrowdStrike Falcon Insight** > **Perfis de capacidade do CrowdStrike**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

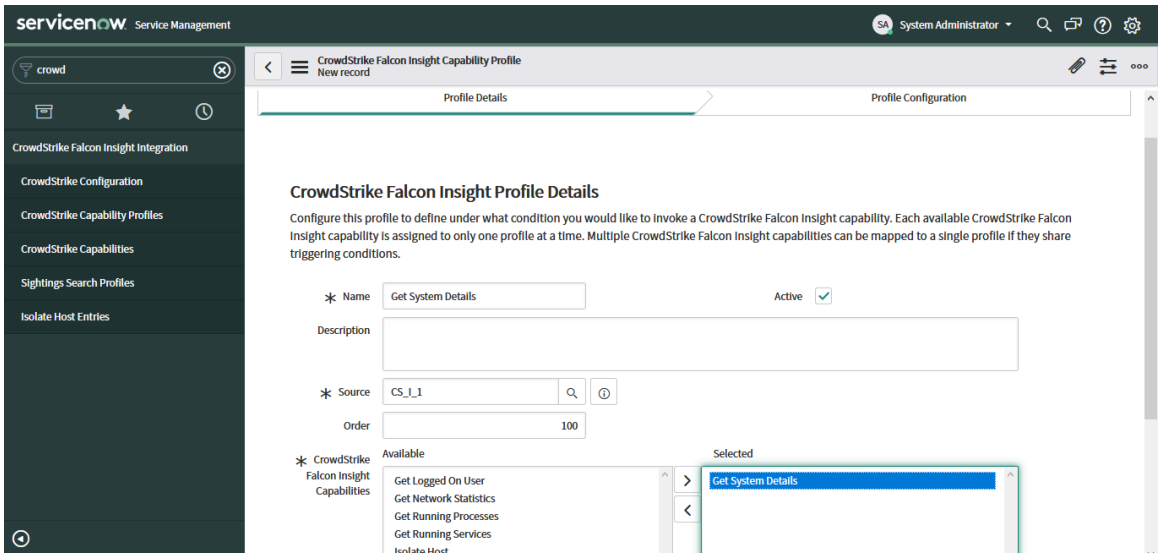
Campo	Descrição
Nome	Nome do novo perfil de capacidade. Este nome ajuda você a identificar o tipo de perfil e também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Indica se o perfil está ativo ou não. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem especificadas na configuração.
Descrição	Descrição exclusiva do perfil de capacidade.
Origem	Nome do servidor. Você só pode exibir servidores configurados anteriormente na lista.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400. Padrão: 100
Capacidades do CrowdStrike Falcon Insight	Capacidades do perfil CrowdStrike Falcon Insight. Selecione os recursos desejados para este perfil em **Disponível** para **Selecionado** coluna.

O exemplo a seguir mostra um formulário completo para um perfil com o recurso Obter detalhes do sistema.



4. Clique em **Avançar**.

O que Fazer Depois

Agora você pode configure seu perfil . Certifique-se de que você tenha revisou os conceitos para configurar perfis e condições do gatilho antes de configurar o perfil.

Configure perfis e incidentes de segurança para CrowdStrike Falcon Insight integração

Defina suas configurações de perfil para que o perfil seja acionado somente sob as condições definidas por você.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente o. CrowdStrike Falcon Insight recursos que você selecionou para o perfil. Você também pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC). Neste campo alternativo, você pode definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Navegue até a página Configuração do perfil somente depois de inserir os detalhes do perfil. Para obter mais informações, consulte Crie um perfil de capacidade para a integração do CrowdStrike Falcon Insight .

Procedimento

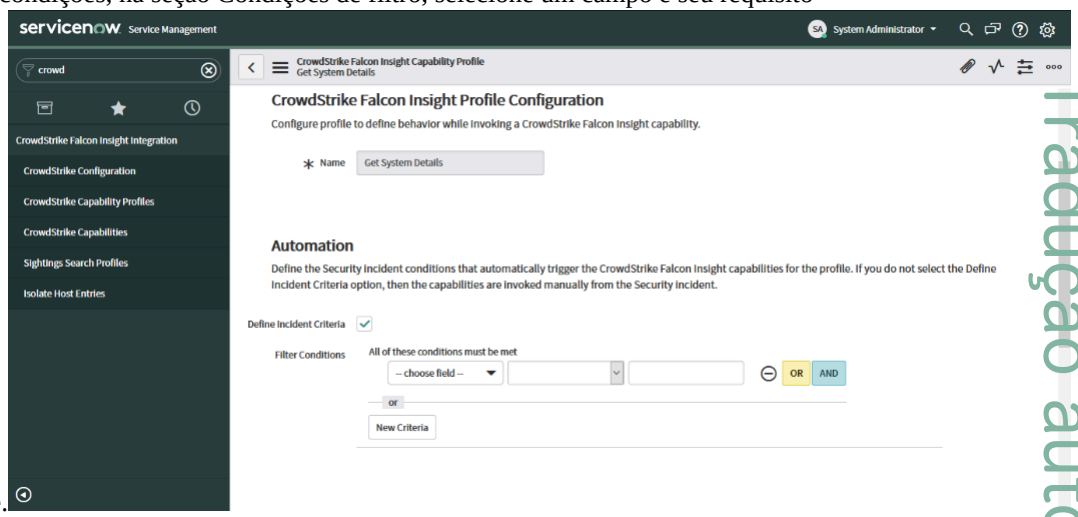
1. Na página Configuração de perfil, revise e configure as seguintes seções:

Definir critérios de incidente (automação)

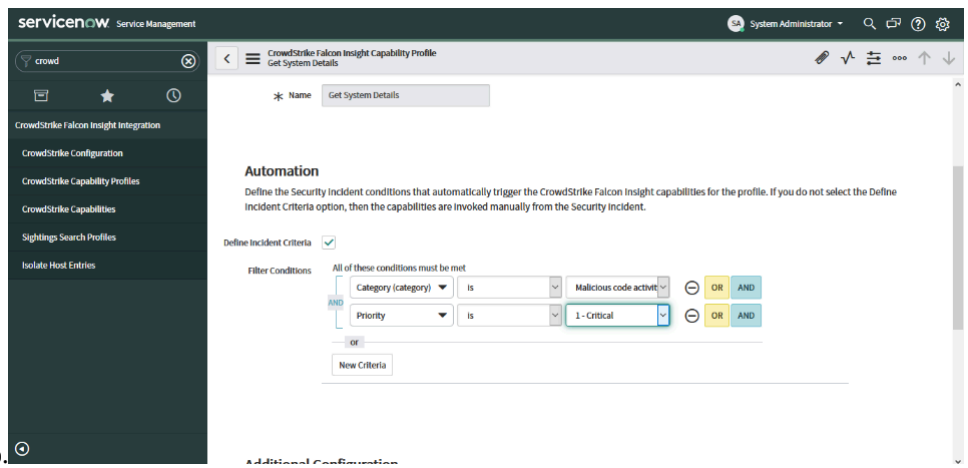
Defina as condições de incidente de segurança que acionam automaticamente o. CrowdStrike Falcon Insight capacidades para o perfil. Se você não selecionar **Definir critérios de incidente** , os recursos são invocados manualmente a partir do incidente de segurança.

a. Selecione **Definir critérios de incidente** opção.

b. Para definir as condições, na seção Condições de filtro, selecione um campo e seu requisito correspondente.



c. Em **Novos critérios** insira os novos critérios e defina **OU** ou **E.**condição.



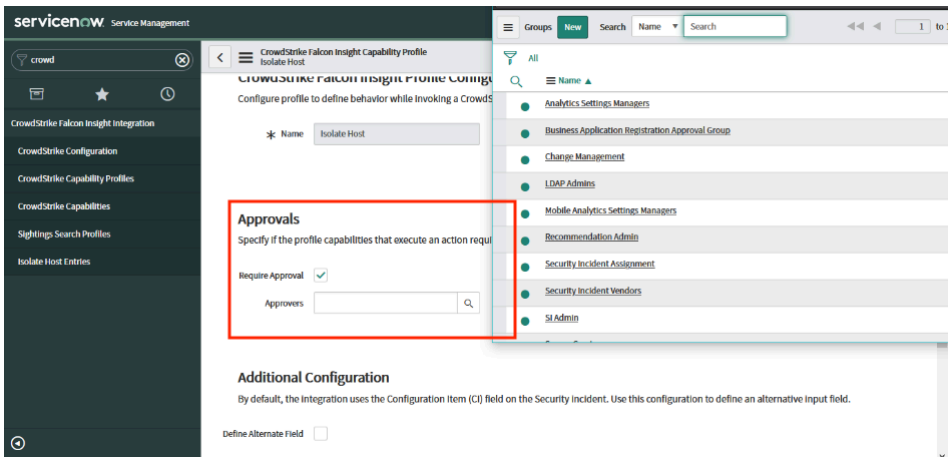
Aprovações

Para fornecer um nível extra de controle quando você estiver usando os recursos do CrowdStrike Falcon Insight, selecione **Aprovação necessária** opção. A opção de aprovações na configuração do perfil aparece somente para os recursos Isolar host e Remover isolamento de host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação. Para obter mais informações, consulte configure um grupo de aprovação .



Configuração adicional

Selecione um campo alternativo no incidente de segurança para exibir todos os dados de IC correspondentes encontrados ao verificar seus ativos. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança.

a. Selecione **Definir campo alternativo** opção.

b. Em **Campo de gatilho de IC alternativo** , selecione um campo de entrada.

Nota: Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração para um perfil .

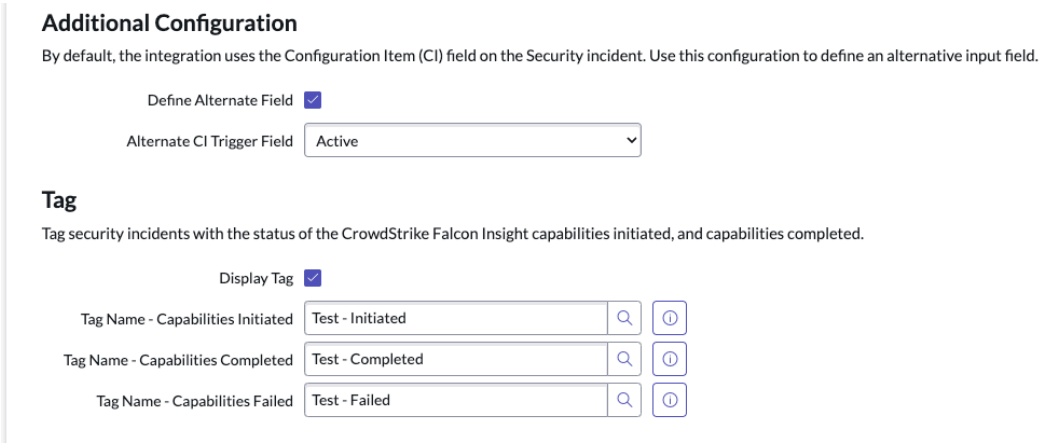
Marcadores

Para marcar incidentes de segurança com CrowdStrike Falcon Insight Marcadores Capacidades- Iniciado, Capacidades-Concluídas e Capacidades-Falha, selecione **Marcadores de exibição** opção. Por padrão, esta opção está desabilitada para todos os perfis.

Nota: Esses marcadores são fornecidos com o sistema de base. Se necessário, você pode criar seus próprios marcadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique em **Concluído**.

Como as condições do gatilho funcionam com um item de configuração para um perfil

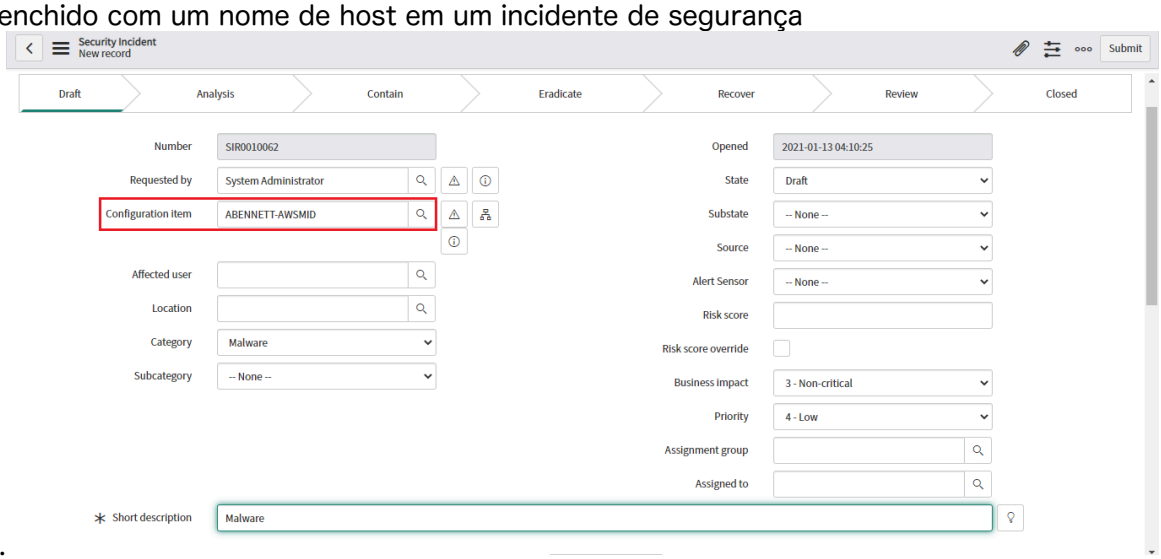
Você pode definir as configurações de perfil para que um perfil seja executado somente quando um conjunto de condições específicas for atendido ou você pode configurar um perfil para pesquisar valores de campo específicos em um incidente de segurança.

Depois de criar um perfil e selecionar CrowdStrike Falcon Insight recursos em que você deseja que o perfil seja executado, você pode definir condições de gatilho para que seu perfil seja executado automaticamente quando os valores de campo padrão corresponderem a. ServiceNow AI Platform incidente de segurança.

Por padrão, a integração usa **Item de configuração** Campo (IC) em um incidente de segurança. Este campo é usado para corresponder seus IDs de ativo com as informações armazenadas em ServiceNow AI Platform banco de dados. Quando um incidente de segurança SIR é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados em busca de um valor correspondente no nome do host ou em um endereço IP.

Quando um valor correspondente é encontrado no banco de dados, esses dados são coletados do CrowdStrike Falcon Insight e é puxado para o seu ServiceNow AI Platform instância em que ele é exibido nas listas relacionadas de um incidente de segurança.

O exemplo a seguir mostra um campo Item de configuração preenchido com um nome de host em um incidente de segurança SIR.



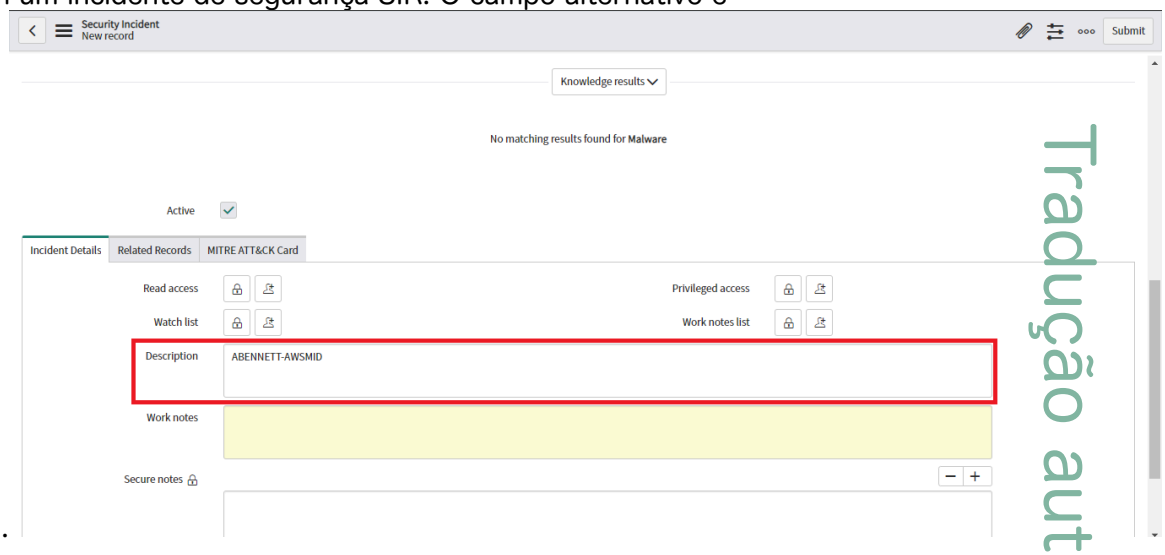
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. **Item de configuração** (IC) não está preenchido com um nome de host ou um endereço IP que corresponda ao banco de dados. Você pode selecionar outro campo no incidente de segurança para exibir todos os dados de IC correspondentes encontrados ao verificar seus ativos.

Ao configurar a configuração do perfil, você pode selecionar uma alternativa **Gatilho de IC** Campo para identificação de endpoint para garantir que os dados de IC do sejam fornecidos CrowdStrike Falcon Insight a pesquisa é preenchida no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Se o campo IC não estiver preenchido no incidente de segurança associado quando o incidente for criado, selecione o campo IC alternativo para garantir que seus perfis sejam acionados.

O exemplo a seguir mostra um campo alternativo preenchido com um nome de host em um incidente de segurança SIR. O campo alternativo é **Descrição**campo.



Verificar CrowdStrike Falcon Insight condições do gatilho de perfil

Teste o perfil e verifique se os filtros de condição do gatilho configurados funcionam conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Ative o perfil baseado nas condições do gatilho configuradas que você especificou para que você possa exibir os resultados da consulta no ServiceNow AI Platform incidentes de segurança.

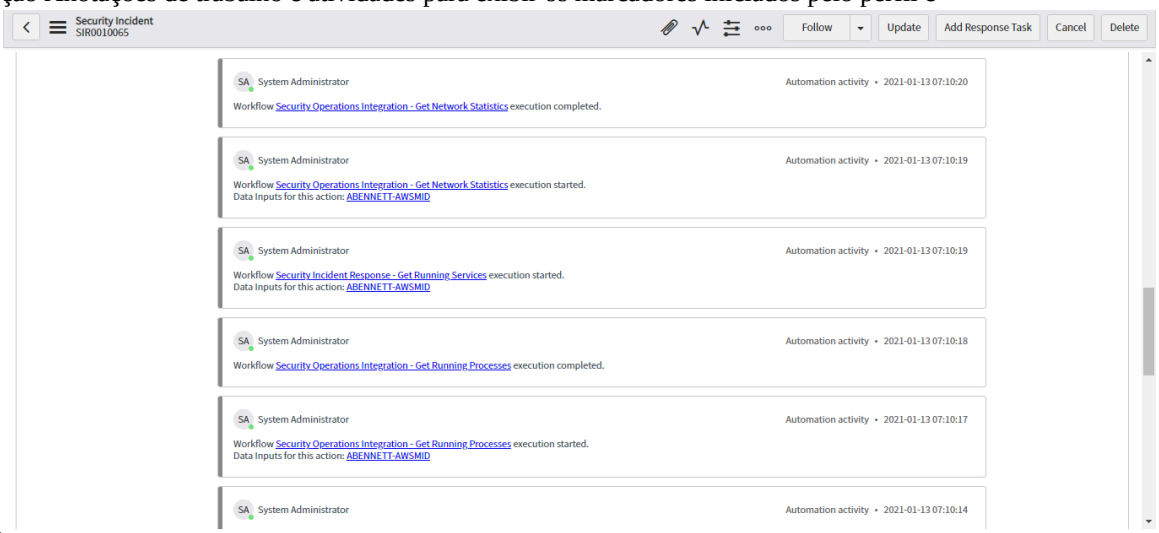
Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione **Novo** para criar um incidente de segurança.
3. Para criar um incidente de segurança, preencha as informações necessárias e clique em **Salvar** .

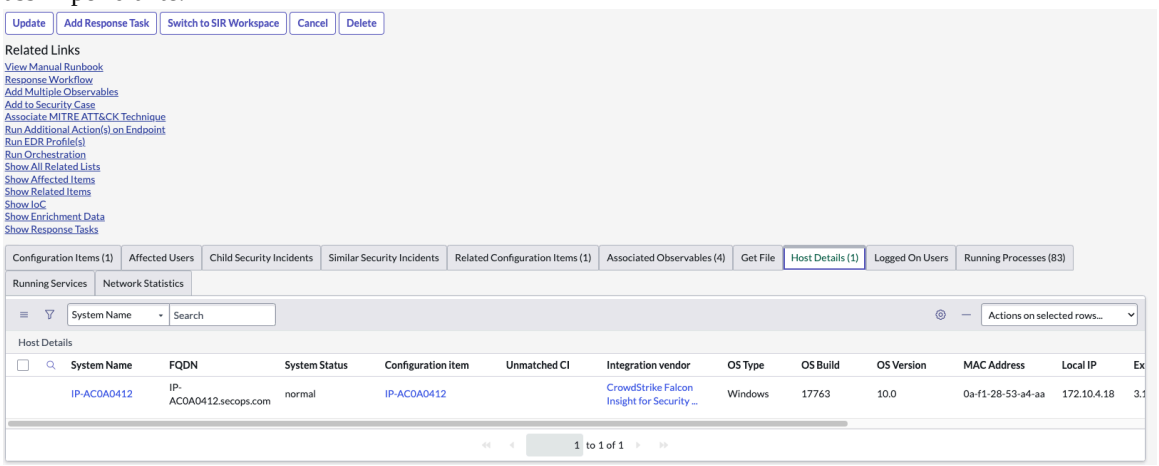
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Revise a seção Anotações de trabalho e atividades para exibir os marcadores iniciados pelo perfil e concluídos.



5. Revise os detalhes em CrowdStrike Falcon Insight Detalhes das listas relacionadas, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, estatísticas de rede e assim por diante.



Gatilho A. CrowdStrike Falcon Insight perfil manualmente a partir de um incidente de segurança

Acione um perfil manualmente depois de revisar um incidente de segurança.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta no ServiceNow AI Platform incidentes de segurança. CrowdStrike Falcon Insight Também permite que você execute capacidades individuais em Itens de configuração (ICs) sem usar um perfil.

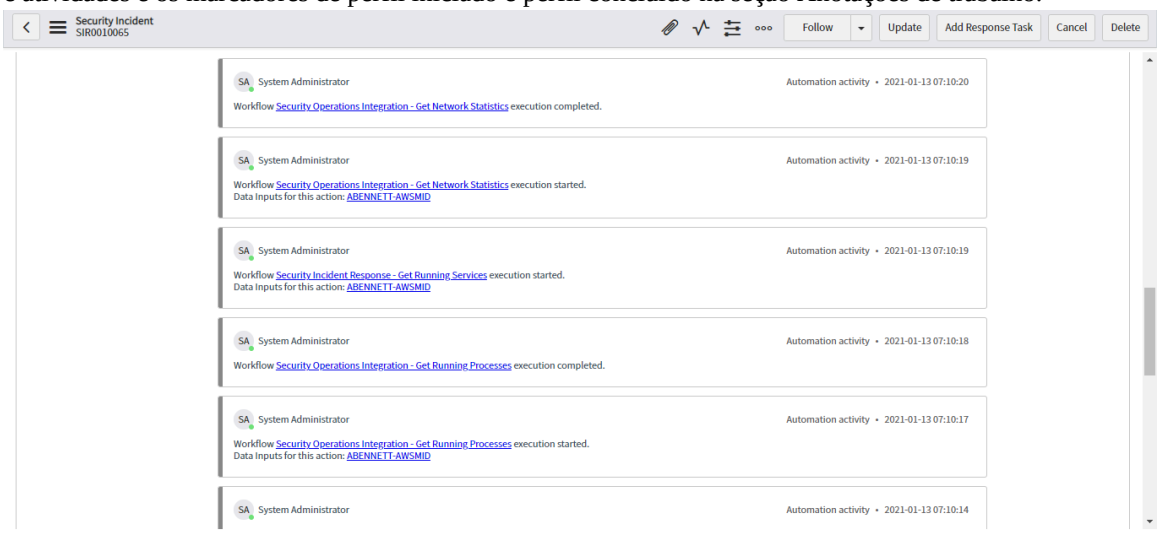
Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com CrowdStrike Falcon Insight informações.
3. Na seção Listas relacionadas, selecione **Executar perfil(s) EDR** .

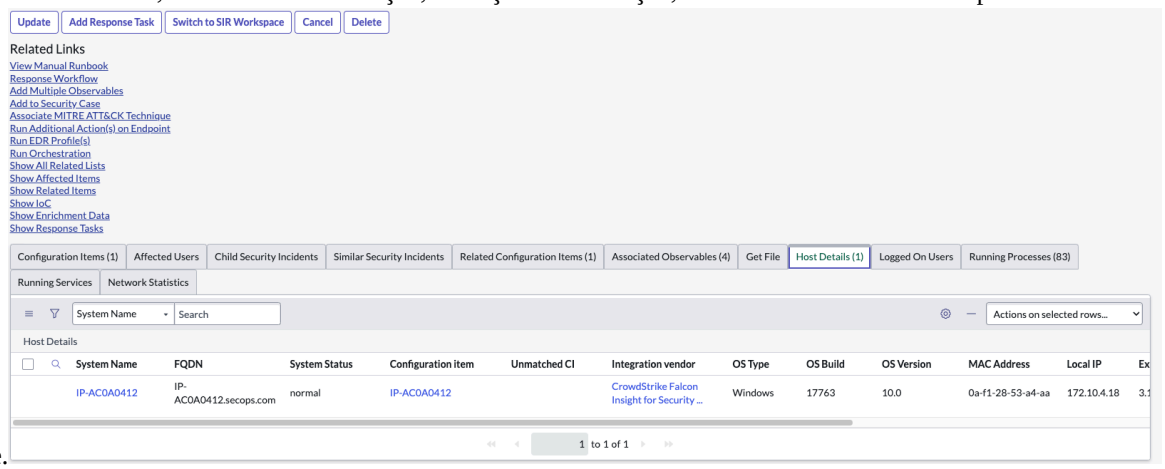
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Procure e selecione um perfil na lista de perfis disponíveis.
5. Selecione **Incluir IC relacionado** Para executar este perfil em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique em **Enviar**.
   O perfil selecionado é acionado manualmente. Você pode revisar a seção Anotações de trabalho e atividades e os marcadores de perfil iniciado e perfil concluído na seção Anotações de trabalho.



7. Os resultados aparecem na forma de listas relacionadas, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, estatísticas de rede e assim por diante.



8. Para executar capacidades individuais em um IC, execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique em **Ações nas linhas selecionadas...** E selecione a capacidade necessária que você deseja executar para o IC selecionado.
   Por exemplo, Isolar host.

   c. PESQUISE a implementação de capacidade necessária para o IC usando a opção de pesquisa e selecione **Isolar host do CrowdStrike Falcon Insight** .

   d. Clique em **Isolar host** Para executá-lo no IC selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie e configure um perfil para a pesquisa de vistas

Use pesquisas de vistas para CrowdStrike Falcon Insight localizar máquinas infectadas na rede da sua organização e lidar com casos de resposta a incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Selecione observáveis individuais ou múltiplos e execute uma pesquisa de vista manual em CrowdStrike Falcon Insight determinar a prevalência de uma ameaça ao longo do tempo.

Procedimento

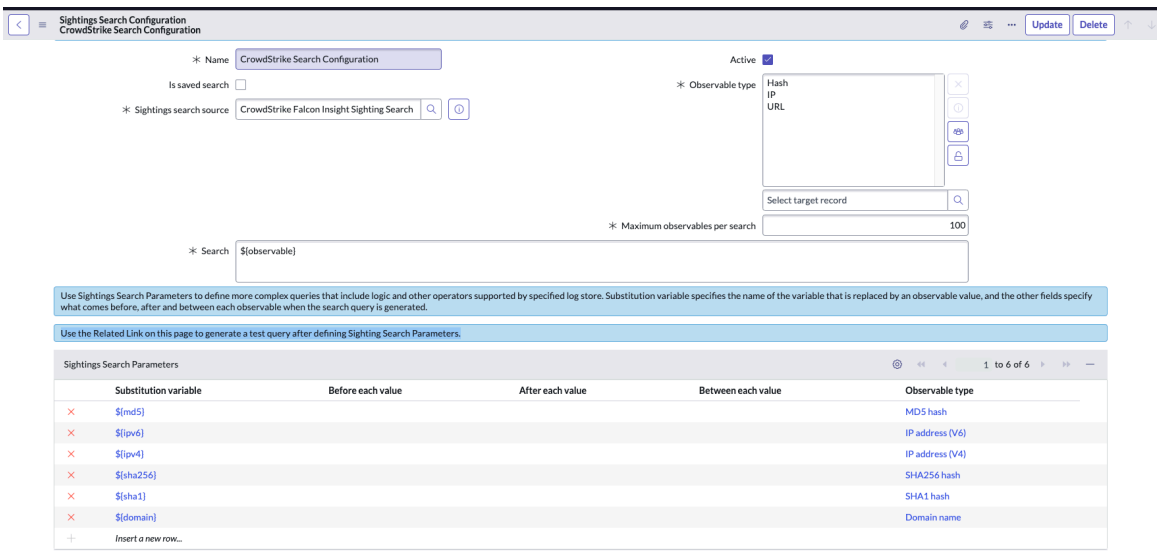
1. Navegar até **Tudo** > **Integração com CrowdStrike Falcon Insight** > **Perfis de pesquisa de detecções**.
2. Clique em **Nova**.
3. Configure este perfil para determinar quais servidores pesquisar um recurso de pesquisa específico do CrowdStrike Falcon Insight.
4. No formulário, preencha os campos:

Campo	Descrição
Nome	Nome do perfil de Pesquisa de vistas.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de vistas. Selecione **Pesquisa de avistamento do CrowdStrike Falcon Insight** como a origem.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de observável	A integração do CrowdStrike Falcon Insight oferece suporte aos seguintes tipos de observáveis: ○ Hash ○ IP ○ URL A pesquisa de vistas é compatível com os seguintes tipos de observáveis: ○ Nome do domínio ○ Endereço IP (V4) ○ Endereço IP (v6) ○ Hash MD5 ○ Hash SHA1 ○ Hash SHA256
Máximo de observáveis por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisar	A cadeia de caracteres de pesquisa padrão é `(observável)` , mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com CrowdStrike Falcon Insight integração.
Parâmetros da Pesquisa de detecções	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de logs especificado Você pode usar os links relacionados na parte inferior da página para gerar uma consulta de teste depois de definir os parâmetros de pesquisa de vistas.



5. Clique em **Enviar**.
   A configuração está concluída e você pode invocar a pesquisa de vistas do ServiceNow AI Platform incidente de segurança.
6. Para verificar a configuração e executar uma pesquisa de vistas, execute as seguintes etapas:

   a. Abra um incidente de segurança, role até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas** .

   b. Se você selecionar um ou mais Itens de configuração (IC) em **Processos em execução** listas relacionadas.

   > **Nota:** Se você executar uma pesquisa de detecção de um IC na lista relacionada Processos em execução, ela será apenas uma pesquisa de detecção de hash de processo.

   c. Clique em **Ações nas linhas selecionadas...** e selecione **Execute a Pesquisa de avistamentos do CrowdStrike** .

   d. PESQUISE o perfil de pesquisa de vistas necessário usando a opção de pesquisa.

   e. Selecione o Perfil de pesquisa de vistas necessário e clique em **Enviar** .

Tradução automática

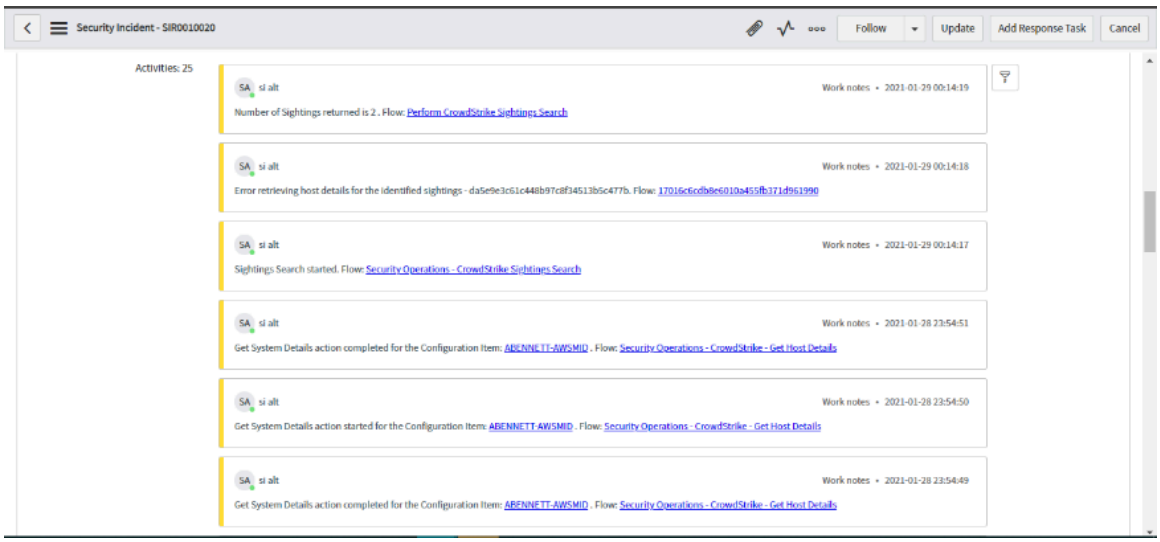
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Se você selecionar um ou mais observáveis no **Observáveis associados** listas relacionadas.

g. Clique em **Ações nas linhas selecionadas...** e selecione **Executar Pesquisa de vistas** .

h. No pop-up Intervalo de tempo, selecione qualquer valor aleatório e clique em **Pesquisa** .

i. Ao concluir a pesquisa, valide os resultados e os detalhes nas anotações de trabalho e nas listas relacionadas.



j. Selecione **Vistas** para exibir os detalhes da vista.

k. Clique em **Visualização** Ícone ao lado do IC para exibir mais informações sobre os detalhes de avistamento do CrowdStrike.

l. Clique em **Detalhes da pesquisa de vistas** para exibir os detalhes da pesquisa de vistas e clique em **Resultados da pesquisa de vistas** guia para resultados da pesquisa.

Configure e acione ações adicionais em CrowdStrike Falcon Insight

. CrowdStrike Falcon Insight a integração oferece suporte à execução de ações adicionais, como expressão regular (regex). . CrowdStrike Falcon Insight a integração fornece 40 ações adicionais com o sistema de base.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Integração com CrowdStrike Falcon Insight** > **Ações adicionais do CrowdStrike**.
2. Clique em **Novo** para criar sua própria ação adicional ou selecionar uma ação existente que vem com o sistema de base.
   Por exemplo, vamos criar uma nova ação adicional.
3. No formulário, preencha os campos.

Tradução automática

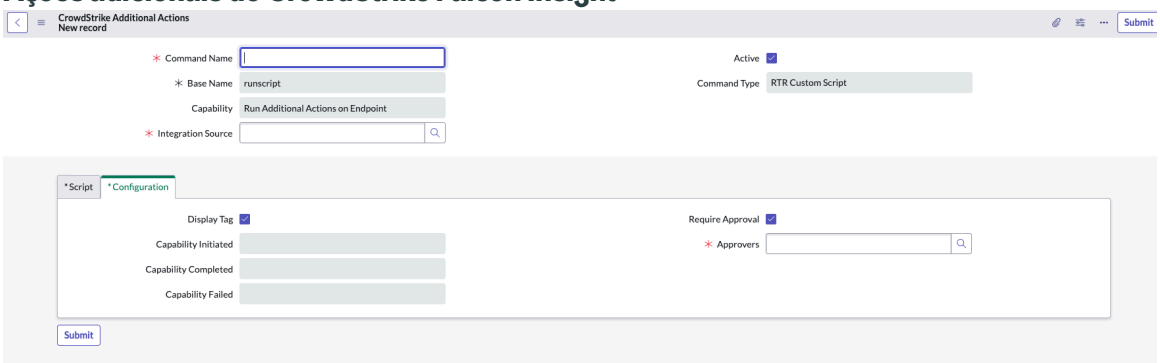
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do Comando	Nome do comando para a ação adicional. Por exemplo, reg set.
Nome base	Nome de base da ação adicional. Este campo é definido por padrão. Por exemplo, reg.
Capacidade	Nome da capacidade da ação adicional. Este campo é definido por padrão. Por exemplo, Executar ações adicionais no endpoint.
Origem da integração	A origem da ação adicional. Por exemplo, Integração do CrowdStrike Falcon Insight.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de Comando	Tipo de comando para a ação adicional. Este campo é definido por padrão. Por exemplo, Script personalizado de RTR.
Script	○ **Tipo de SO** : Opção para selecionar o tipo de SO para o script. Selecione uma das seguintes propriedades: ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ **Nenhum(a)** ○ **Script** : Opção para inserir seu script se você selecionou um dos seguintes sistemas operacionais, exceto a opção Nenhum.
Configuração	○ **Marcador de exibição** : Opção para exibir o marcador da configuração. Você pode selecionar o marcador para os seguintes campos: ▪ Capacidade - Iniciada. Por exemplo, conjunto de registro - Iniciado. ▪ Capacidade - Concluída. Por exemplo, conjunto de registro - Concluído. ▪ Capacidade - Falha. Por exemplo, conjunto de registro - Falha. ○ **Aprovação necessária** Opção para selecionar um aprovador ou grupo que precisa aprovar a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações adicionais do CrowdStrike Falcon Insight



4. Clique em **Enviar**.
5. Você também pode escolher uma das seguintes ações adicionais existentes.
   Há 40 ações adicionais que vêm com o sistema de base, que você pode usar para executar configurações adicionais.

   Nota: Abra a lista Ações adicionais do CrowdStrike e defina a ação adicional necessária como **verdadeiro** caso contrário, a ação adicional não estará disponível no espaço.

Lista de ações adicionais que vem com o sistema de base

CrowdStrike Additional Actions | Command Name | Search | Actions on selected rows... | New

All

Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

Tradução automática

6. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
7. Selecione o incidente de segurança que você deseja revisar com a execução de ações adicionais no endpoint.

   a. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint**.

   b. Procure e selecione a capacidade necessária.
   Por exemplo, clique em **conjunto de registros** capacidade.

   c. Selecione **Incluir IC relacionado** Para executar as ações adicionais em todos os ICs relacionados do endpoint.

   d. Você pode definir **Subchave** Para executar as ações adicionais no endpoint.
   Esta subchave pode ser uma chave HKLM/Software/NEW.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Para iniciar a execução de ações adicionais no endpoint, clique em **Executar ação adicional** .
9. Exiba as atividades de automação da execução e valide-as.
10. Valide o status da ação nas listas relacionadas Ações adicionais no endpoint.

Usando CrowdStrike Falcon Insight Integração no Espaço do analista

Use CrowdStrike Falcon Insight integração para aproveitar o. CrowdStrike Falcon Insight Recursos no Espaço do analista SIR.

Antes de Iniciar

Função necessária: sn_si.admin

Antes de usar CrowdStrike Falcon Insight Integração No espaço Resposta de incidentes de segurança, você deve baixá-lo do ServiceNow Store e configure-o. Para obter mais informações, consulte Introdução ao CrowdStrike Falcon Insight integração.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar CrowdStrike Falcon Insight integração para fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o. Resposta a incidentes de segurança espaço.

. CrowdStrike Falcon Insight a integração permite que os analistas usem o seguinte CrowdStrike Falcon Insight recursos no Resposta a incidentes de segurança Espaço do analista:

- **Obter detalhes do host**
- **Obter usuários conectados**
- **Obter estatísticas de rede**
- **Obter processos em execução**
- **Obter serviços em execução**
- **Isolar Host**
- **Remover isolamento**
- **Obter arquivo**

Procedimento

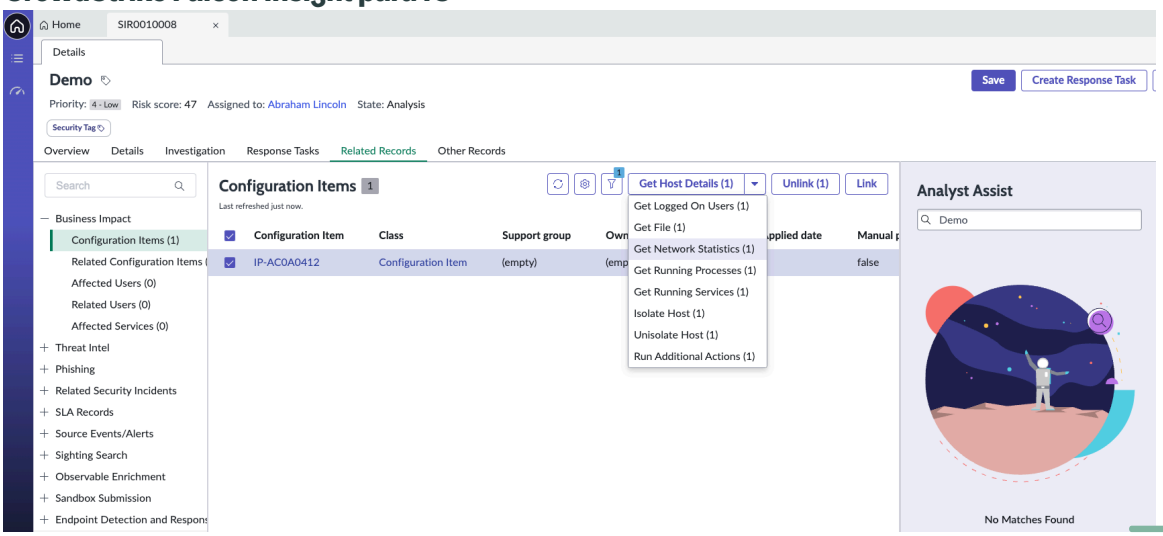
1. No espaço SIR, abra o incidente de segurança necessário e selecione **Registros relacionados** guia.
2. Você pode usar os recursos do CrowdStrike Falcon Insight na lista relacionada Impacto nos negócios para análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione um **Item de configuração** e escolha um recurso na lista suspensa.

CrowdStrike Falcon Insight para IC



b. Selecione **CrowdStrike Falcon Insight** implementação e clique em **Enviar** .
O recurso Obter estatísticas de rede é invocado no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.

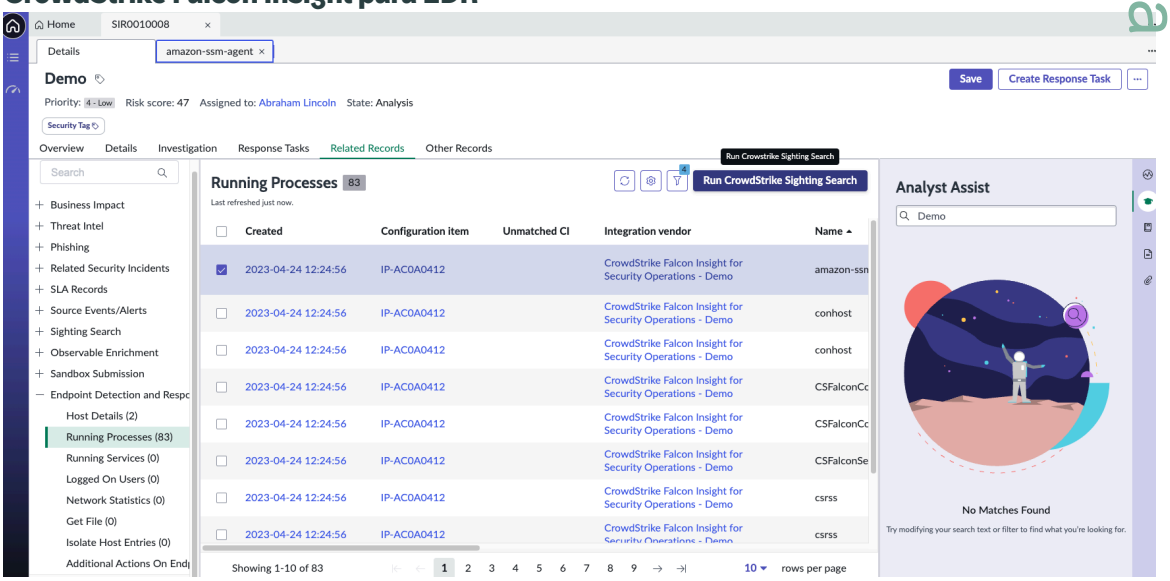
3. Você pode usar os recursos do CrowdStrike Falcon Insight no **Detecção e resposta de endpoint (EDR)** lista relacionada para análise.

a. Na lista relacionada Detecção e resposta de endpoint (EDR), escolha um EDR na lista.

b. Clique em um Processo em execução específico para exibir os detalhes do processo em execução do CrowdStrike Falcon Insight.

c. Para executar uma Pesquisa de avistamento do CrowdStrike Falcon em um processo em execução específico, selecione o processo em execução e clique em **Execute o CrowdStrike Sighting** .

CrowdStrike Falcon Insight para EDR



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

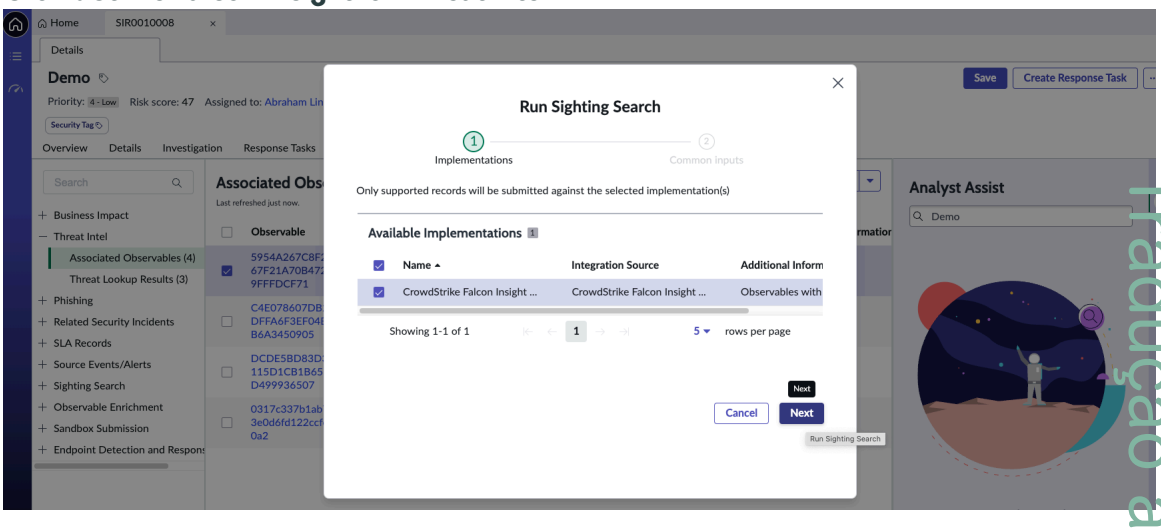
d. Selecione **CrowdStrike Falcon Insight** implementação e clique em **Executar pesquisa** .
Em seguida, uma pesquisa de detecção de hash é executada no processo em execução selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

4. Você pode usar os recursos do CrowdStrike Falcon Insight no **Informações sobre ameaças** para análise.

a. No grupo Intel de ameaças, selecione um **Observável** e escolha um CrowdStrike Falcon Insight capacidade na lista suspensa.

b. Selecione **CrowdStrike Falcon Insight** implementação e clique em **Próximo** .

CrowdStrike Falcon Insight for Threat Intel



c. No pop-up Selecionar data/hora, selecione um valor aleatório e clique em **Enviar** .
Em seguida, uma pesquisa de detecções é executada no observável selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

CrowdStrike Next-Gen SIEM integração

. CrowdStrike Next-Gen SIEM a integração ingere automaticamente dados de detecção que podem indicar possíveis incidentes de segurança e simplifica a criação de incidentes de segurança no ServiceNow® Resposta a incidentes de segurança (SIR), garantindo uma resposta oportuna e eficaz.

Solicitar aplicativos na Store

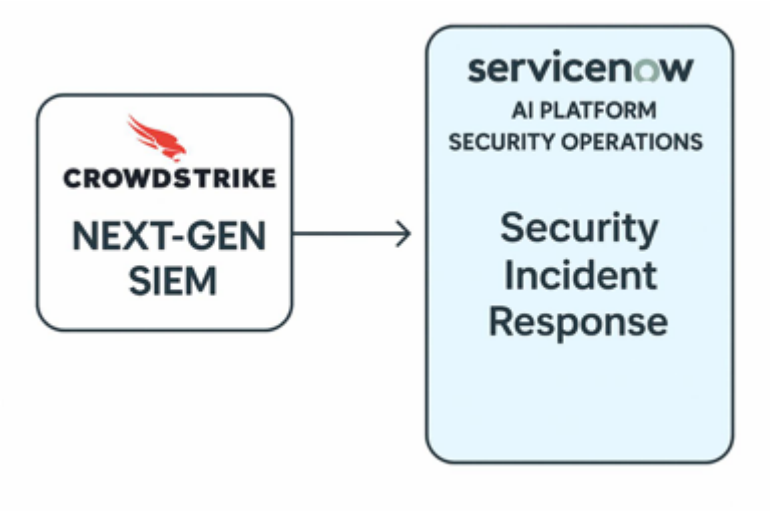
Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral de CrowdStrike Next-Gen SIEM integração

Consulte o gráfico a seguir para saber como CrowdStrike Next-Gen SIEM integra-se ao ServiceNow AI Platform Operações de segurança aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Principais recursos

Use os principais recursos desta integração para executar as seguintes ações:

- Descobrir CrowdStrike Next-Gen SIEM detecções que são candidatas a incidentes de segurança e automatizam a criação desses incidentes de segurança.
- Mapa CrowdStrike Next-Gen SIEM defeito e campos entidade para SIR campos de incidente de segurança.
- Filtro CrowdStrike Next-Gen SIEM defeitos.
- Agregue incidentes a incidentes de segurança em aberto existentes para que você não precise criar incidentes de segurança duplicados.
- Automatizar CrowdStrike Next-Gen SIEM Atualizações de status de detecção para Resposta a incidentes de segurança para que você possa criar e fechar incidentes de segurança.

  Nota: ServiceNow atualiza o status de CrowdStrike Next-Gen SIEM detecções baseadas na criação ou fechamento do incidente de segurança. Esta atualização também inclui comentários de detecções agregadas e novas detecções.

- Programar ingestão de detecção para criar incidentes de segurança periodicamente.
- Sincronizar CrowdStrike Next-Gen SIEM comentários de detecção com SIR Anotações de trabalho.

Comece com CrowdStrike Next-Gen SIEM integração

Ativar e configurar o. CrowdStrike Next-Gen SIEM Plug-in Integration for Security Operation para fazer interface com seu ServiceNow AI Platform instância e. Resposta a incidentes de segurança produto.

Antes de poder usar CrowdStrike Next-Gen SIEM, você deve baixá-lo do ServiceNow Store.

Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração tranquila.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui as funções sn_si.ingestion_profile_admin e sn_si.analyst. • A função sn_si.ingestion_profile_admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria perfis de detecção. ◦ Mapeia o. CrowdStrike Next-Gen SIEM campos de dados de detecção para os campos de incidente de segurança. ◦ Programa a ingestão de detecção contínua. ◦ Habilita atualizações de detecção quando um Resposta a incidentes de segurança a detecção foi criada ou encerrada.
Atribua as funções necessárias do CrowdStrike.	As seguintes funções são necessárias no CrowdStrike para registrar e configurar sua aplicação: • Desenvolvedor de aplicações para registrar a aplicação. • Administrador de locatário para conceder permissões à aplicação chamando o endpoint de consentimento do administrador.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você configurar esta integração.	. Resposta a incidentes de segurança o plug-in (com.snc.security_incident) é obrigatório. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração.
Instalar e configurar	Instale e configure o. CrowdStrike Next-Gen SIEM integração para Operações de segurança aplicação do ServiceNow Store Em sua instância da Plataforma de IA da ServiceNow.

Instalar e configurar

Instale e configure o. CrowdStrike Next-Gen SIEM integração para Operações de segurança aplicação do ServiceNow Store Em sua instância da Plataforma de IA da ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil porque essa função herda as permissões necessárias por padrão.

Procedimento

1. Baixe o. CrowdStrike Next-Gen SIEM integração do ServiceNow Store e instale-o.
   Para obter mais informações, consulte Baixar uma aplicação do ServiceNow Store pela primeira vez.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE CrowdStrike Next-Gen SIEM bloco de integração e selecione **Configurar** .
4. No formulário, preencha os campos.

Formulário de integração do CrowdStrike Next-Gen SIEM

Campo	Descrição
Nome	Nome do CrowdStrike Next-Gen SIEM integração.
ID de cliente	O ID do cliente que você obtém na seção de configurações do seu perfil de conta no portal CrowdStrike.
Segredo do cliente	A chave secreta do cliente que você obtém na seção de configurações do seu perfil de conta no portal CrowdStrike.
Região	Datacenter do qual extrair dados. Especifique a região: US-1, US-2, EU-1, US-GOV-1, US-GOV-2 Por padrão, o campo é definido como US-1

5. Selecione **Enviar**.
   O bloco de integração configurada é exibido.

O que Fazer Depois
Crie um perfil de detecção

Crie um perfil de detecção

Determine CrowdStrike Next-Gen SIEM detecções adequadas para criar incidentes de segurança criando um perfil de detecção em seu ServiceNow AI Platform instância.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil porque a função sn_si.admin herda as permissões necessárias por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > *CrowdStrike Next-Gen SIEM* > **Perfil de detecção**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

CrowdStrike Next-Gen SIEM Formulário Configuração de ingestão de detecção

Campo	Descrição
Nome	Nome do perfil. Este nome também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Opção para tornar o perfil ativo. Quando um perfil está ativo, o ServiceNow AI Platform pesquisa ativamente CrowdStrike Next-Gen SIEM as detecções e as detecções de segurança correspondentes são criadas em Resposta a incidentes de segurança quando as condições de filtragem são correspondidas.
Origem	CrowdStrike locatário que você configurou para ingerir detecções. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de detecção que você planeja ingerir para o perfil.
Ordem	Prioridade na qual os perfis são executados quando dois ou mais perfis compartilham condições de acionamento. Os valores de prioridade geralmente são fornecidos como 100 (o valor padrão), 200, 300 e assim por diante. O perfil com o número mais baixo tem a prioridade mais alta.
Descrição	Descrição opcional do perfil.

4. Selecione **Atualização** .

   O perfil de detecção inicial é criado com informações básicas. Salvar o perfil neste ponto permite que você continue definindo o perfil caso seja interrompido.

5. **Opcional:** Continue com o processo de definição de perfil imediatamente.
   a. Na página Perfis de detecção do CrowdStrike-Nextgen, selecione o perfil que você acabou de criar.
   b. Na barra de andamento, selecione **Regras de correlação** .

O que Fazer Depois

Definir regras de correlação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir regras de correlação

Depois de criar um CrowdStrike Next-Gen SIEM perfil de detecção, selecione regras de correlação para mapear detecções correspondentes a um incidente de segurança. As regras de correlação são atualizadas sempre que um perfil é aberto e novas regras estão disponíveis para seleção. . CrowdStrike Next-Gen SIEM a integração oferece suporte a vários perfis.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil porque a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Se você não estiver continuando na seção anterior do processo de definição de perfil de detecção, acesse o perfil que está definindo.
   a. Navegar até **Tudo** > *`CrowdStrike Next-Gen SIEM`* > **Perfil de detecção**.
   b. Selecione o perfil que você continua a definir.
   c. Selecione **Regras de correlação** na barra de andamento.
2. Limpe **Todas as regras de correlação selecionadas** caixa de seleção.
3. No campo de pesquisa Lista de regras de correlação, insira o nome da regra de correlação criada em CrowdStrike portal.
4. Selecione a regra de correlação.
5. Use a seta para a direita para mover a regra de **Disponível** para **Selecionado** coluna.
6. Conclua esta seção do processo de definição de perfil de detecção selecionando **Continuar** .

O que Fazer Depois

Mapear indivíduo CrowdStrike Next-Gen SIEM campos de detecção para os campos no ServiceNow AI Platform Resposta a incidentes de segurança incidente de segurança. Para obter mais informações, consulte Mapear campos de detecção.

Mapear campos de detecção

Mapeie os campos de detecção do CrowdStrike Next-Gen individuais para os campos no SIR incidente de segurança para que você possa criar detecções com os dados mapeados.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

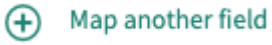
Procedimento

1. Na página de mapeamento, na seção Mapeamento de campo CrowdStrike Next-Gen, selecione um dos métodos de ingestão de amostra.

Métodos de ingestão de amostra

Campo	Descrição
Todos os campos de detecção e eventos padrão	Use este método de ingestão para exibir a lista estática de todas as detecções e campos de evento. Este método contém somente nomes de campo padrão sem valores. Você pode usar essas informações para mapear com SIR campos.
Recupere detecções recentes	Use este método de ingestão para importar os dados de detecções e entidades mais recentes. Se a detecção CrowdStrike Next-Gen contiver vários alertas, o alerta mais antigo que faz parte da detecção será mostrado na seção de mapeamento. Os valores de campo de alerta de segurança mais antigos serão usados durante a ingestão. Você pode ingerir 5 detecções de amostra. Os valores do campo de detecção de amostra são preenchidos quando o perfil ingere as detecções de amostra. Você pode mapear essas detecções para **Campos de destino do incidente SIR** . Os campos e os valores de detecção aparecem como guias individuais.

2. Para adicionar campos aos campos padrão exibidos no incidente de segurança, execute as seguintes ações:

   a. Na seção Campos de destino do incidente SIR, selecione 

Botão Mapear outro campo.
   Mostra uma lista de SIR campos, a partir dos quais você pode selecionar um campo para que um novo campo seja exibido.

   b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

   Nota: Vários observáveis podem ser exibidos no mesmo incidente de segurança. Por exemplo, o. **Observável** o campo pode ser mapeado várias vezes com valores diferentes. Da mesma forma, o **Item de configuração** e. **Campos de anotações de trabalho** suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, verá uma mensagem de erro informando que este campo não oferece suporte a vários valores. Da mesma forma, se um campo em um incidente de segurança tiver uma lista da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista, o campo não será preenchido no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na seção Campos de detecção e evento, arraste e solte o campo para mapeá-lo para o novo campo.

d. Quando você marca a caixa de seleção que corresponde a um campo, todas as mudanças novas ou atualizadas feitas no CrowdStrike atualizarão automaticamente os respectivos dados do incidente SIR com os novos dados do incidente.

Nota: No sistema de base, a propriedade do sistema sn_sec_cs_ngsiem.detection_updates é definida por padrão como falsa para receber as atualizações do CrowdStrike Next- Gen relacionadas a novos alertas vinculados ao SIR.

- Por padrão, os campos Usuários afetados, Itens de configuração e Observáveis são verificados. Sempre que houver novos observáveis ou itens de configuração associados, ou usuários afetados que são adicionados ao incidente, essas informações serão extraídas e preenchidas automaticamente nas respectivas listas relacionadas na Resposta a incidentes de segurança (SIR) durante esse intervalo de pesquisa.
- Para quaisquer outros campos, você deve marcar a caixa de seleção que corresponde a um campo para quaisquer mudanças novas ou atualizadas feitas no registro de detecção do CrowdStrike no CrowdStrike. Isso atualizará automaticamente os respectivos dados do incidente SIR com os novos dados de detecção.

Importante: A due diligence deve ser feita antes de selecionar esta funcionalidade, pois a substituição dos dados existentes pode resultar em dados instáveis para o analista trabalhar e qualquer outra automação definida até mesmo pelos valores de campo do incidente de segurança também pode ser afetada. Portanto, é muito importante fazer a due diligence antes de selecionar qualquer funcionalidade de substituição.

3. Para remover um campo, use Botão Remover item ao lado do campo Expressão de entrada na seção Campos de destino do incidente SIR.

4. Para mapear um valor de campo da seção Campos de detecção e evento para um campo na seção Campos de destino do incidente SIR, use uma das seguintes ações:

a. Arraste o nome do campo de detecção (por exemplo, id) e solte-o ao lado de um nome de campo na coluna Campos de destino do incidente SIR.

Você pode corresponder qualquer valor da seção Campos de detecção e evento a um campo na seção Campos de destino do incidente SIR. Os campos são codificados por cores para que você não ignore ou duplique os campos de detecção no processo de mapeamento. Campos azuis claros indicam que um campo de detecção ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar campos de detecção de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Dessa forma, você pode visualizar quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de incidente importante restante permanece não mapeada.

b. Você pode adicionar uma combinação de texto e campo.
Por exemplo, `O nome da detecção é` . Aqui `O nome da detecção é` pode ser inserido manualmente enquanto `(Detections: Nome` É mapeado na seção Campos de detecção e evento.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Você pode inserir e mapear manualmente diretamente uma detecção de origem ou campos de eventos para um campo de destino.

- Para mapear manualmente um campo de detecção de origem, use oformato "nome do campo". Por exemplo, para mapear uma severidade de campo de detecção, o formato é (Detecções: Severidade) .
- Para adicionar manualmente campos de eventos de origem, use nomes de eventos: campos de eventos formato. Por exemplo, para mapear campos de eventos Descrição de eventos Alerta de segurança, o formato é Eventos: Descrição .

Esta integração classifica determinados subtipos observáveis. Quando você mapeia um campo CrowdStrike Next- Gen com o campo observável SIR, o. ServiceNow AI Platform classifica automaticamente o observável. Se você quiser mapear genericamente o Observable de entrada do CrowdStrike Next- Gen para o tipo de observável em SIR, Em seguida, arraste e solte o campo Detecção e evento no campo Observável. No entanto, se você souber do tipo de observável para o observável de próxima geração do CrowdStrike de entrada em SIR, em seguida, mapeie especificamente para SIR Campo de tipo de observável. Alguns exemplos de tipos de observáveis específicos em SIR Incluir Observable (nome do domínio), Observable (endereço de e-mail), Observable (endereço IP (V4)) e Observable (nome do host).

Se os campos de entrada do CrowdStrike Next- Gen contiverem algum MITRE-ATT&CK e mapeie-as para MITRE-ATT&CK Campo de técnica. Certifique-se de que o campo CrowdStrike Next- Gen de entrada contenha MITRE-ATT&CK ID da técnica ou nome da técnica.

Às vezes, os valores do campo de detecção no CrowdStrike Next- Gen podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos.

5. Para formatar uma tradução de campo para um novo campo de uma detecção CrowdStrike Next- Gen para corresponder a um valor de campo em um Incidente de segurança, selecione **Clique aqui** link no **Campos de destino do incidente SIR** cabeçalho.

6. Para modificar os campos compatíveis com a tradução de campo, selecione  ícone de tradução de campo de formato de script.
Os campos compatíveis com a tradução de campo são **Usuário afetado** , **Item de configuração** e **Prioridade** . Por exemplo, clique em  Ícone ao lado da Categoria. O editor de script CrowdStrike Next- Gen Field Translation é aberto.

7. Insira as mudanças no script e selecione **Atualização** Para salvar as mudanças e retornar à página Mapeamento.
Por exemplo, para Categoria, defina o seguinte no editor de scripts:

```
"<Incoming CrowdStrike Detection Field Value>" : "<Category to assign to the Security Incident>".
```

Este mapeamento garante que um perfil use somente categorias configuradas.

8. Continue seu mapeamento adicionando ou removendo valores de campo.
Você pode usar os mesmos valores de campo no construtor Condições de geração de detecção para definir critérios adicionais que uma detecção de entrada deve atender para criar um incidente de segurança.

9. Para ir para a seção Filtragem e agregação, selecione **Continuar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Defina e defina condições de filtro para que você possa especificar quais detecções devem criar incidentes de segurança. Você pode usar os mesmos valores de campo (definidos na seção Mapeamento) no construtor Condições de geração de detecção (na seção Filtragem e agregação) para definir critérios adicionais que uma detecção de entrada deve atender para criar um incidente de segurança.

Definir critérios de filtro e agregação

Defina e defina condições de filtro para especificar qual entrada CrowdStrike Next-Gen SIEM as detecções devem criar incidentes de segurança. Você também pode definir critérios de campo de detecção adicionais que permitem que uma detecção de entrada seja anexada a um incidente de segurança em aberto em vez de criar um incidente.

Definir condições de filtragem

Defina as condições de filtragem para que os incidentes de segurança sejam criados somente quando as condições de filtragem corresponderem.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda você a isolar incidentes de segurança e limita o número de incidentes de segurança que você cria. Se você definir critérios de filtragem adicionais, somente as detecções necessárias serão ingeridas sem precisar mudar a consulta ou a configuração de detecção acionada.

Procedimento

1. Para definir os critérios que uma detecção de entrada do CrowdStrike Next-Gen deve atender para que um incidente de segurança seja criado, selecione **Filtro com base em condições** .

   As opções no primeiro campo nas Condições de filtro correspondem aos campos exibidos na seção Ingestão de detecção de amostra do CrowdStrike Next-Gen para a detecção que você ingeriu. Esses campos são dinâmicos e mudam dependendo da detecção que você ingerir. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios que você define correspondem aos valores da detecção.

   Use a condição de filtro `detection_id` para os seguintes campos com vários valores:

   - composite_id
   - host_names
   - seconds_to_resolved
   - seconds_to_triaged

   Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar `detection_id` condição de filtro para os campos acima para garantir que os dados sejam filtrados corretamente.

2. Usando as listas e os campos do construtor de condições, defina os filtros para a primeira linha.
3. Para adicionar mais condições, clique em **E.** ou **OU** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **E.** selecionado, todas as condições devem ser correspondidas.
- Se **OU** está selecionado, qualquer condição pode ser correspondida.

4. Para definir uma segunda condição de filtro, clique em **Novos critérios** .

Definir condições de agregação

Defina critérios de agregação de incidentes adicionais que agreguem uma detecção de entrada a um incidente de segurança SIR existente em vez de criar detecções semelhantes e potencialmente duplicadas. Quando você usa critérios de valor de correspondência de campo para cada perfil, essa agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de detecções relacionadas em um único incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Se um novo incidente corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o incidente será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.ingestion_profile_admin trabalhando com incidentes de segurança, você pode exibir todos os incidentes agregados adicionados em uma lista relacionada em um incidente de segurança.

Todos os incidentes agregados em um incidente de segurança são exibidos no CrowdStrike Next-Gen SIEM Lista relacionada de incidentes agregados. Esta lista detalha os carimbos de data/hora associados e os valores de campo agregados. Essas informações ajudam você a entender por que os incidentes são adicionados aos incidentes de segurança existentes.

Procedimento

1. Para definir critérios de campo de incidente adicionais que permitem uma entrada CrowdStrike Next-Gen SIEM detecção a ser anexada a um incidente de segurança em aberto em vez de criar um novo incidente, selecione **Condições de agregação** opção conforme mostrado na figura a seguir.
2. Em **Campos de incidente com valores correspondentes** campo, insira os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform instância. Todos os valores de campo selecionados no campo de entrada de seleção múltipla devem corresponder para que os critérios de agregação sejam atendidos e que este incidente de entrada possa ser anexado a um incidente de segurança existente. Esta seleção implica que é um *E.* Condição em que campos, como Observáveis e Itens de configuração que podem ter vários valores de campo, são mapeados para eles. Se somente um subconjunto dos valores for correspondido, o CrowdStrike Next-Gen SIEM As condições de agregação de incidentes não são atendidas e um novo incidente de segurança é criado.
3. Para adicionar várias condições de correspondência de campo, clique em **Adicionar novos critérios** A agregação ocorrerá se qualquer uma das condições do campo de seleção múltipla que você definir for atendida. Esta seleção implica *OU* condição.
4. Para atualizar a anotação de trabalho de um novo incidente quando ela for adicionada a um incidente de segurança, selecione **Anotação de trabalho em log para o novo incidente** .

   A anotação de trabalho registra em log que um novo incidente foi adicionado e inclui um link para os detalhes do incidente. A anotação de trabalho de log também atualiza mais detalhes que você adiciona ao campo de anotação de trabalho na seção de mapeamento.
5. Para configurar a programação, clique em **Continuar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
Defina uma programação para recuperar os dados do incidente e os incidentes ingeridos que correspondam aos critérios no perfil.

Recuperação de detecção de programação

Configure uma programação para definir como e quando você extrai detecções do CrowdStrike Next-Gen SIEM locatário.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil porque a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Se você não estiver continuando na seção anterior dos critérios de filtragem e agregação, acesse o perfil que está definindo.
   a. Navegar até **Tudo** > *CrowdStrike Next-Gen SIEM* > **Perfil de detecção**.
   b. Selecione o perfil que você continua a definir.
   c. Selecione **Programação** na barra de andamento.
2. No formulário de programação, preencha os campos.

CrowdStrike Next-Gen SIEM Formulário de programação

Campo	Descrição
Ingestão de detecção contínua	Opção para definir a ingestão de detecção contínua que o ServiceNow AI Platform a instância extrai do CrowdStrike Next-Gen SIEM locatário para novas detecções. Os incidentes de segurança serão criados se detecções acionadas forem encontradas e os critérios de filtragem de geração de detecção corresponderem.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos.
Defina o tempo de ingestão da detecção	Opção para adicionar Data e Hora para a ingestão inicial.
Tempo de ingestão da detecção inicial	Data e hora especificadas para a ingestão de detecção.
Recuperação Única	Opção para habilitar a recuperação única de históricos CrowdStrike Next-Gen SIEM e seguida pela reconciliação dos dados. Ao processar os dados, as detecções em andamento e os dados históricos são extraídos. **Nota:** O histórico recuperado CrowdStrike Next-Gen SIEM as detecções passam por verificações de desduplicação para evitar duplicatas no Resposta a incidentes de segurança aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Desde a data	A data desde que as detecções históricas foram ingeridas CrowdStrike Next-Gen SIEM.

3. Conclua esta seção do perfil selecionando **Continuar** .

O que Fazer Depois

Atualizações e fechamentos de detecção automatizados

Atualizações e fechamentos de detecção automatizados

Automatize atualizações e fechamentos de detecção com base no Resposta a incidentes de segurança status do incidente. . CrowdStrike Next-Gen SIEM a integração permite que as detecções criem incidentes de segurança e também atualizem os incidentes depois que eles são criados ou encerrados.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil porque a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Se você não estiver continuando na seção anterior do processo de Programação, acesse o perfil que está definindo.
   a. Navegar até **Tudo** > *CrowdStrike Next-Gen SIEM* > **Perfil de detecção**.
   b. Selecione o perfil que você continua a definir.
   c. Selecione **Opções adicionais** na barra de andamento.
2. No formulário, preencha os campos.

Formulário Automatizando atualizações de detecção

Categoria	Campo	Descrição
Atualizações de criação de incidentes de segurança	Atualize o status de detecção do CrowdStrike Next-Gen após a criação do incidente SIR	Opção para usar a funcionalidade de atualização de detecção automatizada. . CrowdStrike Next-Gen SIEM o status da detecção é atualizado em CrowdStrike Next-Gen SIEM detecção com os comentários após SIR o incidente é criado em ServiceNow AI Platform.
	Atualização do status de detecção inicial	Status de detecção inicial que é atualizado em CrowdStrike Next-Gen SIEM Novo ou Em andamento.
	Comentários iniciais retornados para detecção	Comentários iniciais publicados na detecção no CrowdStrike Next-Gen SIEM ambiente.
Atualizações de fechamento de detecção	Feche a detecção do CrowdStrike Next-Gen após o fechamento do incidente SIR	Opção para usar a funcionalidade de atualização de status de detecção automatizada. CrowdStrike Next-Gen SIEM as detecções são encerradas no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
		CrowdStrike Next-Gen SIEM portal com os comentários fornecidos após SIR o incidente está encerrado em ServiceNow AI Platform.
	Atualização do status de detecção de fechamento	Atualização de status no CrowdStrike Next-Gen SIEM detecção quando o incidente de segurança é encerrado em SIR.
	Comentários de fechamento retornados para detecção	Comentários publicados na detecção no CrowdStrike Next-Gen SIEM detecção quando o incidente de segurança é encerrado em SIR.
Extrair detecções encerradas	Extrair detecções encerradas	Opção para buscar detecções encerradas durante a ingestão contínua e a recuperação única. Encerrado SIR os incidentes não serão atualizados com novos dados de CrowdStrike Next-Gen SIEM
Comentários de detecção e sincronização de anotações de trabalho DO SIR	Atualize a atividade de automação SIR com comentários de detecção do CrowdStrike Next-Gen	Opção para atualizar seu CrowdStrike Next-Gen SIEM comentários em SIR Atividade de automação. O comentário em SIR A atividade de automação aparece com o prefixo *`Comentário do CrowdStrike .`*
	Atualização CrowdStrike Next-Gen SIEM Comentários de detecção com anotações de trabalho SIR	Opção para atualizar seu SIR anotações de trabalho no CrowdStrike Next-Gen SIEM comentários de detecção. O comentário em CrowdStrike Next-Gen SIEM aparece com o prefixo *`Comentário da ServiceNow .`*

3. Selecione **Concluir**.
4. Ative o perfil.
   a. Selecione **Nome** barra de andamento.
   b. Marque a caixa de seleção **Ativo**.
   c. Selecione **Continuar**.

CrowdStrike Falcon X Sandbox para integração de Operações de segurança

Com CrowdStrike Falcon X Sandbox para Operações de segurança, você pode enviar arquivos e URLs como parte do processo de resposta a incidentes de segurança para CrowdStrike Falcon X Sandbox para executar uma análise detalhada de malware e ameaças.

. CrowdStrike Falcon X Sandbox a integração fornece um ambiente virtual isolado sob demanda no qual você pode executar a análise de malware e fornecer resultados para o. ServiceNow incidente de segurança por meio da integração.

Quando você envia seus incidentes de malware, eles são retidos como parte do registro de incidente de segurança. Você pode usar esses registros f Ou resolução adicional de incidentes e automatizar o envio de arquivos e URLs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A integração oferece suporte à automação de playbooks de resposta de phishing e malware que permite que seu Operações de segurança equipe do centro para ser mais produtivo e eficiente na resposta a incidentes de segurança.

Principais benefícios

Com t sua integração , você pode fazer o. seguindo :

- Envio automatizado de arquivos e URLs do usuário - Phishing relatado (URP), mensagens de e-mail, anexos e outros incidentes de segurança.
- Envie ou reenvie manualmente arquivos e URLs analisados anteriormente para análise atualizada.
- Crie várias configurações de envio que se aplicam automaticamente CrowdStrike Falcon X Sandbox parâmetros de envio, como sistema operacional, tipo de verificação e opções de tempo de execução.
- Analisar malware e resultados de ameaças Em um relatório formatado em HTML no SIR incidente. Você pode exibir t Hreat resultados de pesquisa e o histórico do indicador para arquivos e URLs que foram analisados várias vezes.
- Marcador ServiceNow incidentes com o status de processamento de envio, bem como resultados da descoberta de ameaças.

Consulte também

Identificador do documento	Título do documento
CrowdStrike Falcon X Sandbox	CrowdStrike Falcon Sandbox FAQ
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece a usar CrowdStrike Falcon X Sandbox integração

Ativar e configurar o. CrowdStrike Falcon X Sandbox para fazer interface com seu ServiceNow instância e. Resposta a incidentes de segurança produto.

Antes de Iniciar

- Antes de poder usar CrowdStrike Falcon X Sandbox Para integração do Security Operations, você deve baixá-lo do ServiceNow Store .
- Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma tranquilidade CrowdStrike Falcon X Sandbox integração.

Função necessária: admin, sn_si.admin

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• O administrador (admin) instala o. . Integração do Andbox da loja de aplicações da ServiceNow e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O sn_si.admin cria e edita . configuração e. configurações globais e. em seguida atribui a função de analista de incidentes de segurança (sn_si.analyst). • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança , como Enviando arquivos e URLs para . . e analisando os resultados do envio.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você configurar esta integração.	Esta integração é compatível com Paris e. Orlando versões. Certifique-se de que esses plug-ins dependentes estejam instalados . Esses plug-ins habilitar . execução de IntegrationHub ações e fluxos: • ServiceNow Etapa de ação do IntegrationHub - REST (com.glide.hub.action_step.rest) • ServiceNow Tempo de execução do IntegrationHub (com.glide.hub.integration.runtime) **Nota:** Se puder 't encontre um plug-in, talvez você precise solicitá-lo ServiceNow pessoal. Para solicitar um plug-in, siga as etapas em Solicite um plug-in . . Resposta a incidentes de segurança o plug-in (com.snc.security_incident) é obrigatório. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações que são exigido pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança Dependência (com.snc.si_dep) **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança **5.** Inteligência contra ameaças Suporte Comum (necessário para u se os recursos de integração da área restrita) **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Resposta a incidentes de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um produto de Operações de segurança ou aplicação e. Ativar uma aplicação da ServiceNow Store .
Verifique se você está licenciado para a chave de API privada Falcon Sandbox, e. o . CrowdStrike Falcon X Sandbox Chave de API completa.	Esta integração oferece suporte somente à nuvem privada Falcon Sandbox. **Nota:** Esta versão não é compatível com a integração do Falcon X. CrowdStrike Falcon X Sandbox Oferece uma chave de API restrita autoassinada e uma chave de API completa atualizada. Use a chave de API completa para esta integração porque ele permite acesso irrestrito para envios automatizados. Para obter mais informações, consulte Base de conhecimento do CrowdStrike Falcon Sandbox .

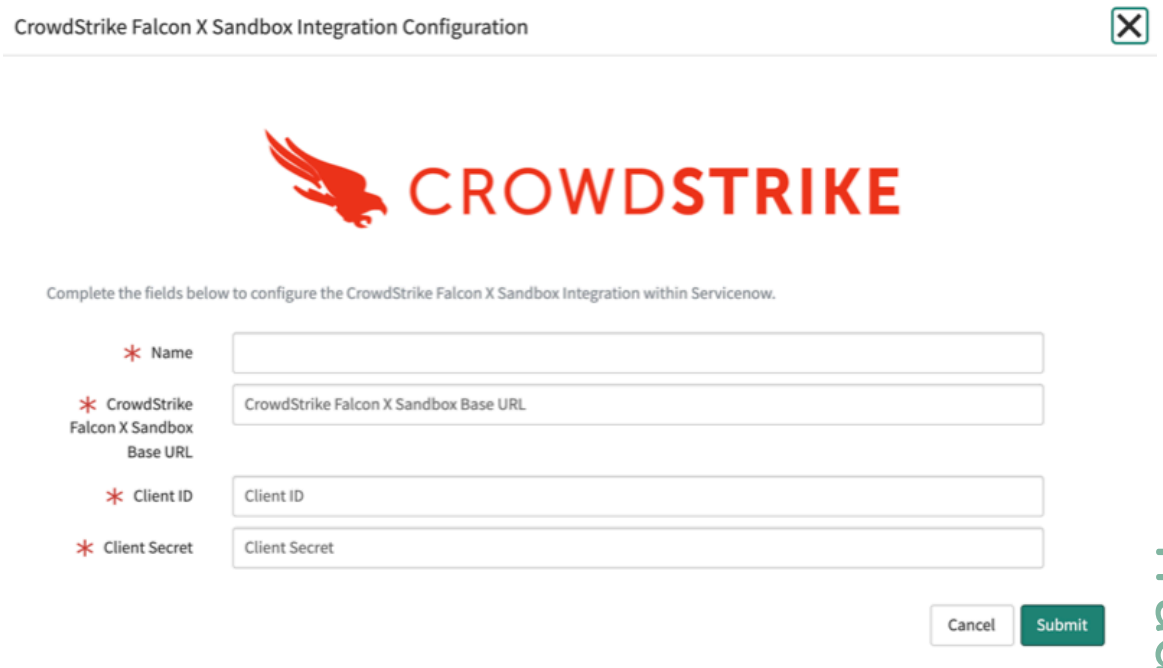
Procedimento

1. Baixe a integração do CrowdStrike Falcon Sandbox for Security Operations na ServiceNow Store .
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de integração** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. PESQUISE CrowdStrike Falcon X Sandbox bloco de integração e clique em **Configurar** .



4. Insira os seguintes detalhes para concluir a configuração:

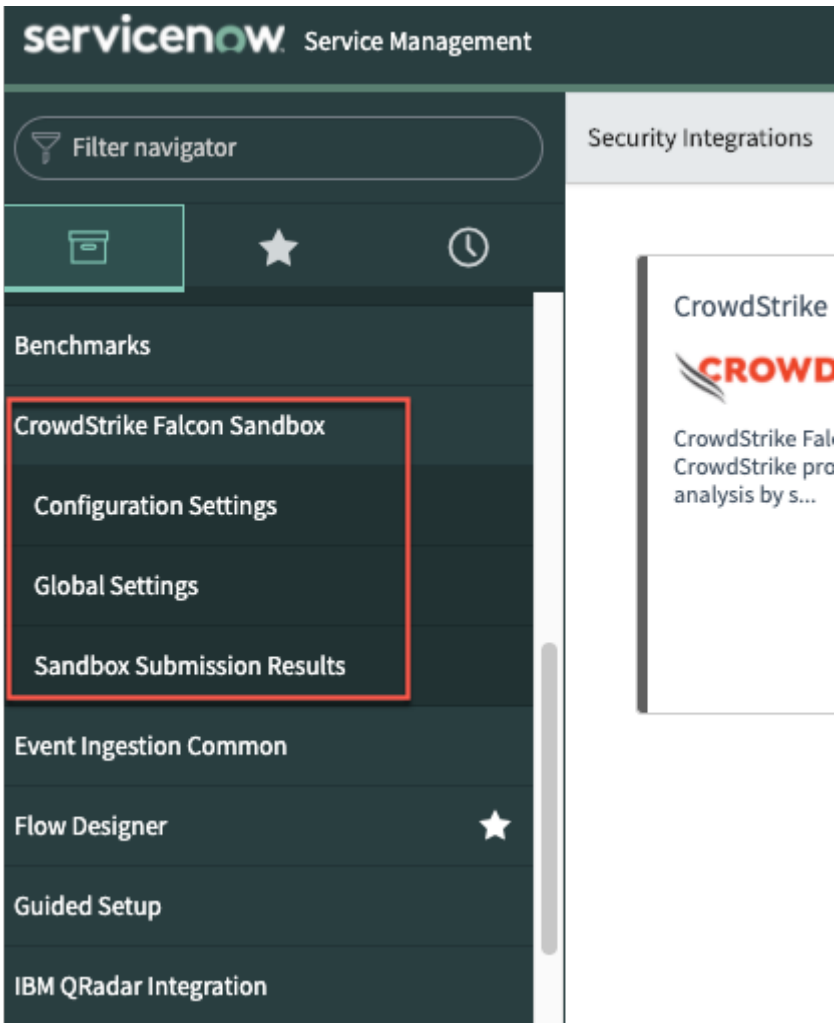
Campo	Descrição
Nome	Nome desta integração, por exemplo, `demonstração-1` . Este é um nome exclusivo para identificar o. . E configuração do andbox, você só pode configurar uma integração por instância da ServiceNow.
URL base da área restrita do CrowdStrike Falcon	. URL base do andbox. Isso URL está disponível após você configura . . e-box.Por exemplo, `https://servicenow .falcon-sandbox.com` É um URL base .
ID de cliente	ID do cliente da API OAuth2. Para obter mais informações, consulte, Chaves e clientes de API .
Segredo do cliente	Chave secreta do cliente da API OAuth2. Para obter mais informações, consulte, Chaves e clientes de API .

5. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a área restrita validado e enviado com sucesso, . É salvo na página Integrações de segurança como um bloco. Agora você pode exibir o módulo Sandbox no aplicação navegador.



O que Fazer Depois

Depois de concluir a integração com sucesso, a próxima etapa é configurar Configurações de envio da área restrita .

Defina as configurações de envio da área restrita

Defina a configuração da área restrita para definir o ambiente de análise e as opções de tempo de execução para os envios de registro de incidente de segurança para a análise de malware.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

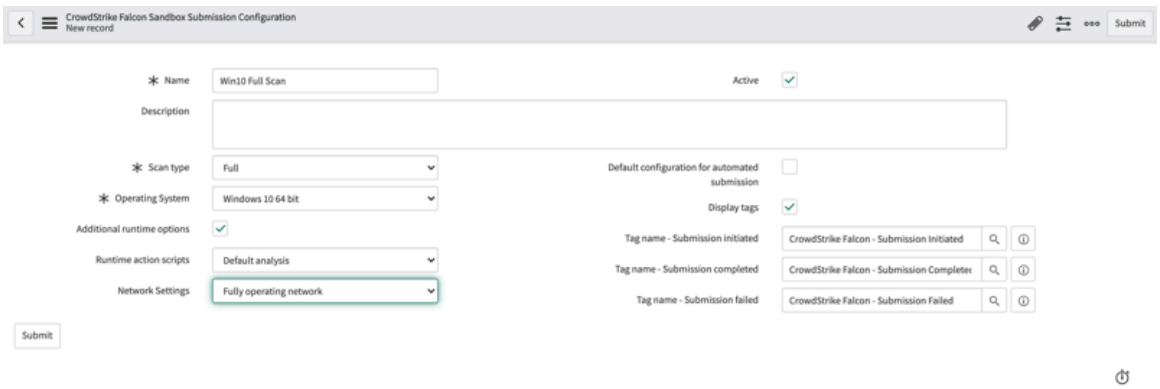
Antes de enviar arquivos ou URLs para CrowdStrike Falcon X Sandbox usando a integração, você deve configurar pelo menos uma configuração de envio. A configuração de envio define o sistema operacional Sandbox, o tipo de verificação, as opções de tempo de execução e outras características de tratamento de incidentes. Você pode criar várias configurações para usar diferentes opções isso disponível em CrowdStrike Falcon X Sandbox ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **CrowdStrike Falcon X Sandbox** > **Definições de configuração**.
2. Clique em **Nova**.



3. Preencha os campos a seguir para criar uma configuração para um Cheio **Tipo de verificação** .

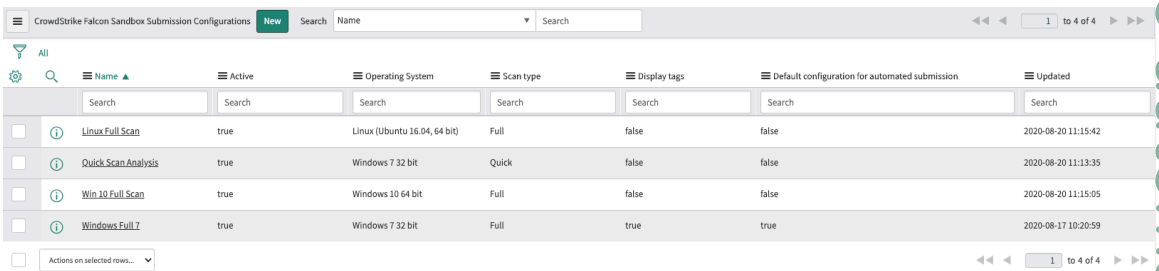
Campo	Descrição
Nome	Nome exclusivo da configuração de envio. Este nome aparece para os analistas quando eles enviam um arquivo. É importante garantir que o nome seja descritivo e facilmente distinguível das outras configurações (exemplo, Verificação completa do Win 10). Se o nome não for exclusivo, um erro será exibido e os nomes de registro de configuração duplicados não serão salvos.
Tipo de verificação	. pode digitar como **Cheio** . . **Rápido** o tipo de verificação fornece uma análise de ameaça limitada.
Sistema operacional	. Ambiente de VM nalysis que s O andbox verifica o arquivo ou a URL no .
Ativo	O opção que você seleciona Ao enviar arquivos ou URLs manualmente.
Configuração padrão para envio automatizado	O opção isso está limpo por padrão. Selecionar esta opção permite que esta configuração esteja disponível para automatizar envios de análise de malware. **Nota:** Você pode ter apenas uma configuração de envio ativa como a configuração padrão para envios automatizados.
Marcadores de exibição	O opção isso está limpo por padrão. Quando você seleciona esta opção, os marcadores são exibidos para fornecer o status de um envio de arquivo ou URL. A análise pode levar vários minutos para ser processada. Os marcadores de exibição são envio iniciado, envio concluído, ou envio com falha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Opções adicionais de tempo de execução	O opção isso está limpo por padrão. Quando você seleciona esta opção, parâmetros de tempo de execução adicionais compatíveis com o Sandbox estão disponíveis.
Scripts de ação de tempo de execução	Opção que permite que você use um . script de ction que simulam . comportamento humano e interação . Com o arquivo ou URL durante a análise. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Consulte CrowdStrike Falcon X Sandbox documentação para obter mais detalhes.
Configurações de rede	Opção que permite selecionar o tipo de configurações de rede usadas ao enviar um URL ou arquivo para a Sandbox.

4. Clique em **Enviar**.
   Depois de enviar a configuração, ela é salva na página Configurações de configuração como um registro. A configuração obrigatório ser **Ativo** a ser usado em . envios do andbox.



O que Fazer Depois

Depois de configurar . e envios de caixa, a próxima etapa é Enviar arquivos ou ULRs manualmente para a Sandbox

.

Enviar arquivos ou URLs manualmente para a Sandbox

Você pode enviar manualmente um arquivo ou URL para uma área restrita quando determinados critérios de incidente, como categoria é phishing, forem atendidos.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

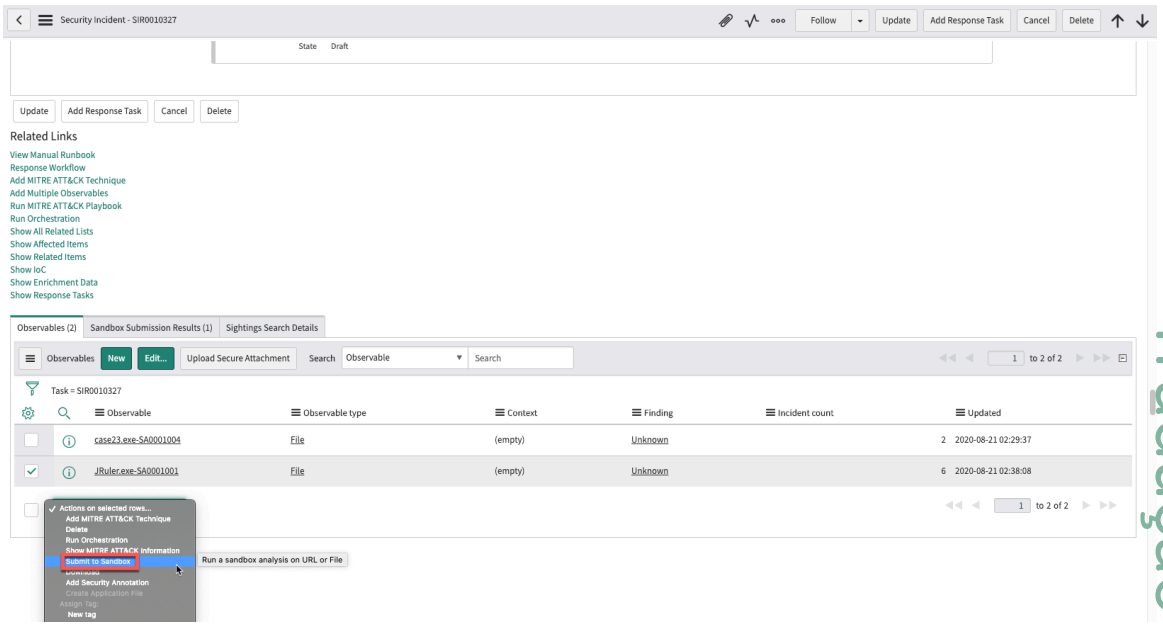
Depois de revisar o incidente de segurança e o arquivo ou URL, você pode selecionar **Enviar para Sandbox** opção para executar uma análise de malware.

Tradução automática

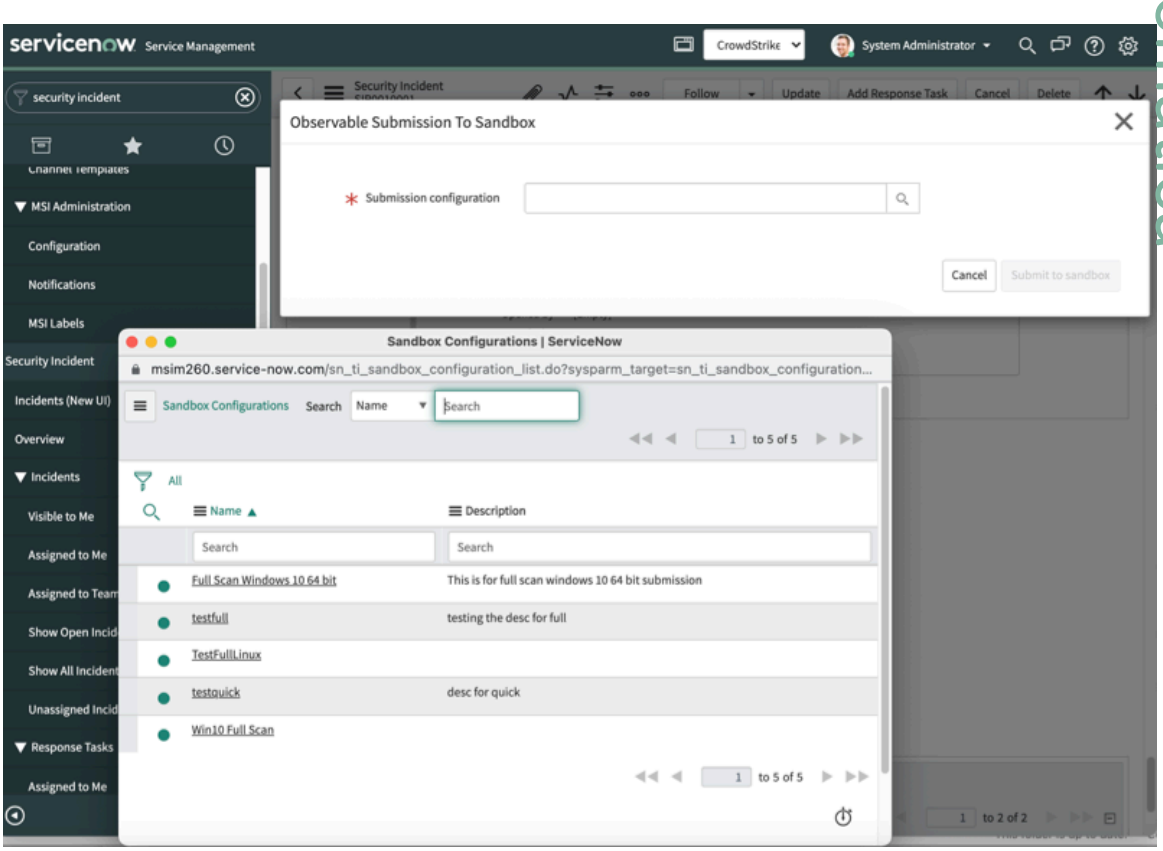
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes** E abra um incidente de segurança para o qual você deseja enviar um registro de tipo observável de arquivo ou URL.
2. Clique em **Mostrar IOC** link relacionado.
3. Em **Observáveis** selecione um registro ou vários registros para os quais você deseja executar análise de malware ou ameaça e clique em **Enviar para Sandbox** .



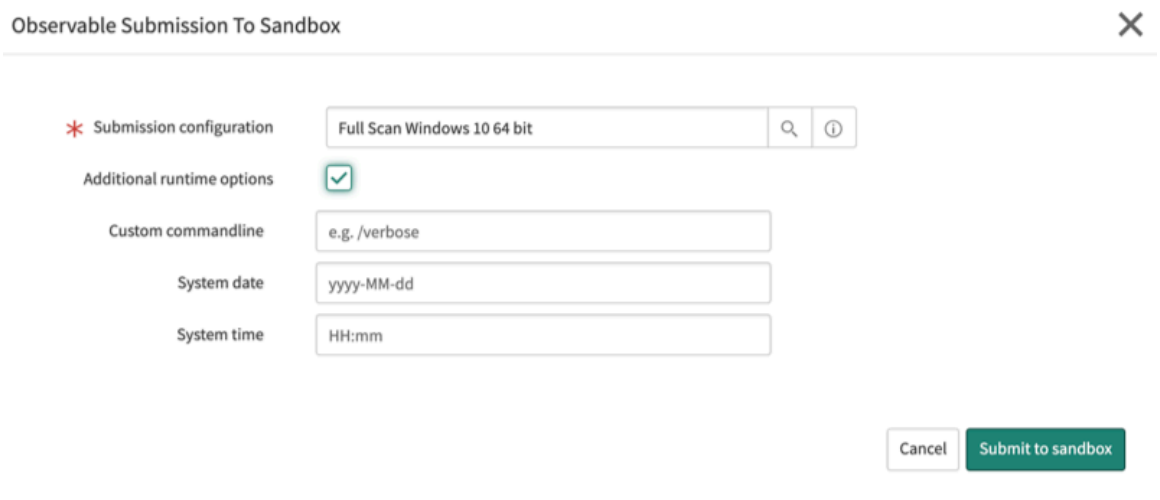
4. Quando o filtro Envio de arquivo for exibido, selecione sua configuração de área restrita preferencial em **Configuração de envio** e clique em **Enviar para Sandbox** .



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Opcional:** Selecione **Opções adicionais de tempo de execução** se você quiser fornecer mais opções personalizadas.



Campo	Descrição
Linha de comando personalizada	Linha de comando da aplicação regular ou uma operação especial.
Data do sistema	Formato aaaa-MM-dd do sistema.
Horário do sistema	Hora do sistema no formato HH:MM.

Depois de iniciar o envio, você pode exibir as anotações de trabalho para ver o status do seu envio. Para obter mais informações sobre o status do envio ou para analisar os resultados, exiba **Resultados de envio da área restrita** .

Nota: No CrowdStrike Falcon X Sandbox, a verificação rápida não é compatível com URLs. Se as anotações de trabalho tiverem muitas informações, você poderá usar a opção Filtro para detalhar as anotações de trabalho necessárias que são relevantes para você.

O que Fazer Depois

Quando você envia os observáveis para a área restrita para análise de malware, exiba os resultados de envio da área restrita para dar as próximas etapas em possíveis ameaças.

Automatizar CrowdStrike Envios da área restrita do Falcon usando o Flow Designer

. CrowdStrike Falcon X Sandbox a integração inclui modelos de fluxo criados usando Flow Designer que funcionam com registros de incidentes de segurança.

Antes de Iniciar

- Verifique se você criou um Configuração de envio da área restrita e habilitaram uma configuração como **Configuração padrão para envio automatizado** . Quando o fluxo é acionado, o envio da área restrita ocorre em sua configuração padrão.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Esses fluxos são projetados principalmente para que você comece quando quiser automatizar os envios de arquivos ou URL como parte do fluxo de trabalho de resposta a incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você ativa um fluxo de amostra, seus anexos de arquivo de phishing são enviados automaticamente se você definir os incidentes de segurança como phishing em seu fluxo de amostra. Como alternativa, você pode enviar todos os arquivos .exe quando este tipo de arquivo estiver anexado a um registro observável.

Você pode modificar esses fluxos de amostra para acionar um envio automatizado em diferentes condições, categorias, condições compostas e assim por diante.

A integração da área restrita consiste em dois fluxos do sistema de base que são desativados por padrão.

- **Enviar arquivo quando a categoria for phishing** : Este fluxo envia um arquivo para a área restrita para análise de malware quando a categoria de incidente de segurança é definida como phishing. Você deve anexar um arquivo ao registro observável no incidente de segurança. Se você estiver usando a funcionalidade de Phishing relatado pelo usuário (URP), qualquer anexo de e-mail será analisado automaticamente e adicionado ao registro de incidente SIR como um registro observável. Nenhuma ação adicional é necessária para automatizar o envio.
- **Enviar quando o tipo de arquivo do observável for exe** : Este fluxo envia um arquivo para a área restrita para análise de malware quando o observável de incidente de segurança é um exe. Semelhante ao fluxo da categoria de phishing, um você deve anexar um arquivo a um registro observável no incidente de segurança. Você pode fazer isso manualmente carregando o arquivo ou automaticamente se um anexo de e-mail de phishing, ou outro mecanismo que esteja criando o incidente, estiver associado aos registros observáveis.

Quando os fluxos são configurados e as condições do incidente atendem aos parâmetros, os envios da área restrita são acionados automaticamente quando você revisa o incidente de segurança. Revise a anotação de trabalho que indica que um envio foi iniciado, um marcador aparece se habilitado na configuração e um registro de resultados de envio pendente.

A integração da área restrita também contém vários subfluxos. Os subfluxos são componentes internos dos recursos gerais de envio de integração. Você pode personalizar e editar os subfluxos para atender aos seus critérios de segurança.

Você pode consultar os subfluxos para solucionar problemas com envios de área restrita. Um registro de execução é criado sempre que você invoca um subfluxo. Este registro indica onde ocorreu um erro específico no fluxo e permite que você corrija o problema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração da Sandbox- Vários fluxos de trabalho

Flows | Subflows | Executions | Help | + New

All > Application Name contains Sandbox

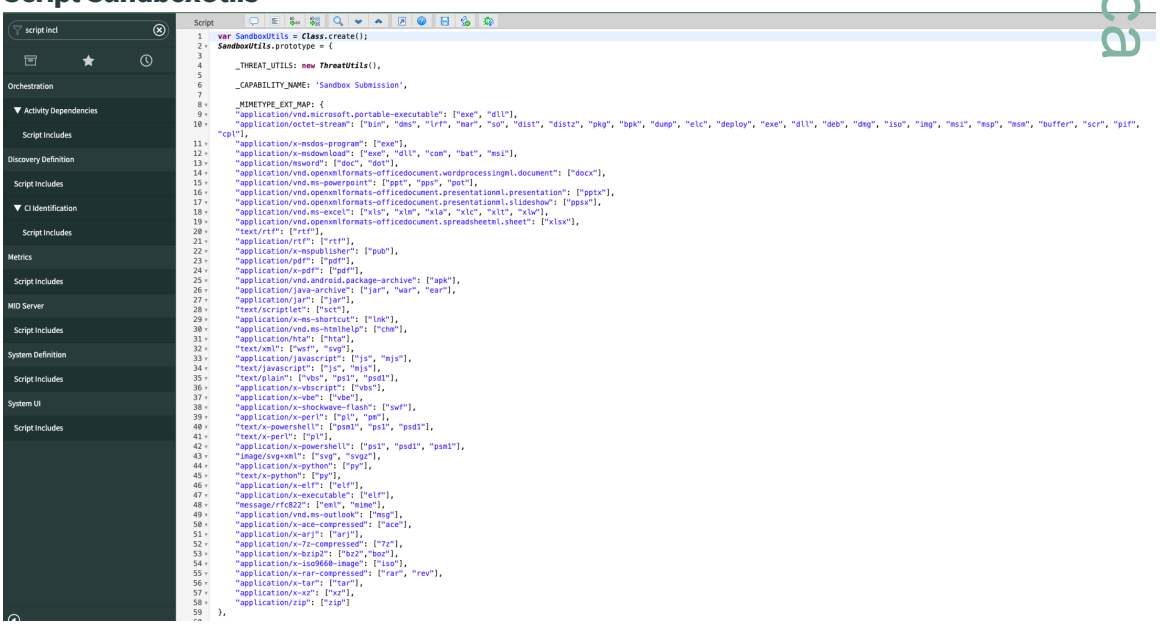
Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

Actions on selected rows... | 1 to 11 of 11

Nota:

- Se você optar por personalizar os fluxos padrão, verifique se o subfluxo Enviar observável para envio automatizado está incluído em seu fluxo para acionar envios automáticos.
- Você pode personalizar e definir suas extensões de arquivo para um exe. Crie uma cópia do fluxo **Enviar quando o tipo de arquivo do observável for exe** e faça mudanças na cópia. O tipo de conteúdo e as extensões de arquivo são mapeados no SandboxUtils script. Para acessar inclusões de script, navegue até **Definições do sistema > Inclusões de script** E pesquise SandboxUtils.

Script SandboxUtils

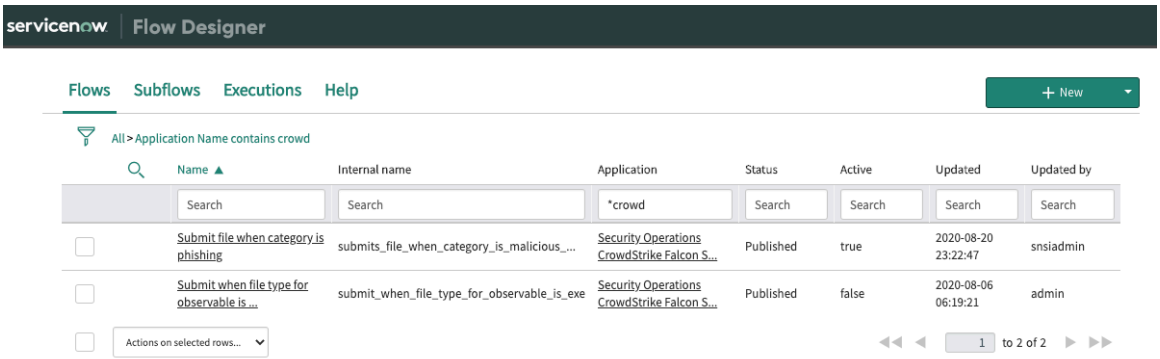


Tradução automática

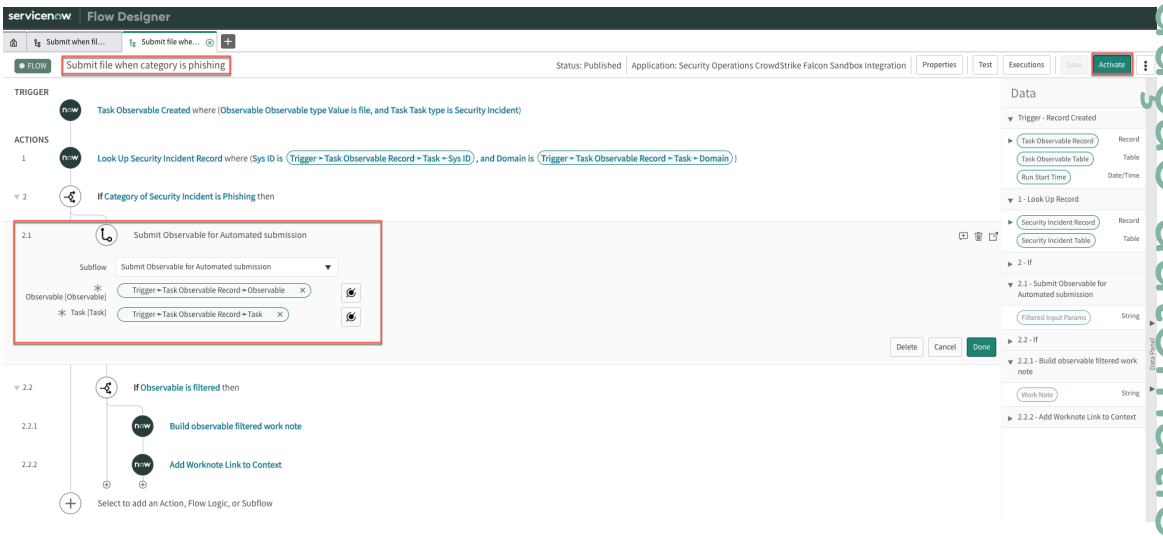
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Flow Designer** > **Designer** > **Fluxos**.
2. Filtre os fluxos pelo **Aplicação** tipo.
   Por exemplo, *crowd filtra os dois CrowdStrike Falcon X Sandbox fluxos.



3. Selecione um fluxo para exibir os detalhes.
   O exemplo abaixo mostra o Enviar arquivo quando a categoria é fluxo de phishing.



4. Clique em **Ativar** e clique em **OK** quando a mensagem de confirmação é exibida.

O que Fazer Depois

Depois de configurar os fluxos de envio automatizados, você pode Exiba os resultados de envio da área restrita para analisar quaisquer ameaças.

Monitore o. resultados do envio na área restrita

Os resultados de todos os envios do Sandbox são mostrados em **Resultados de envio da área restrita** guia para cada incidente de segurança.

Antes de Iniciar

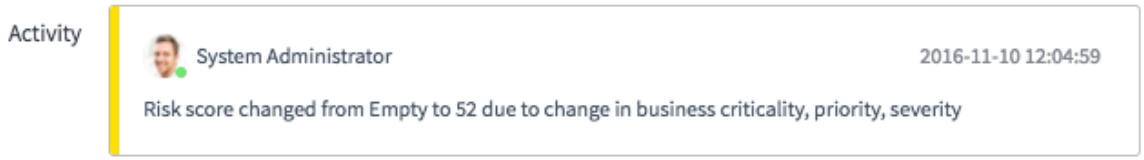
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

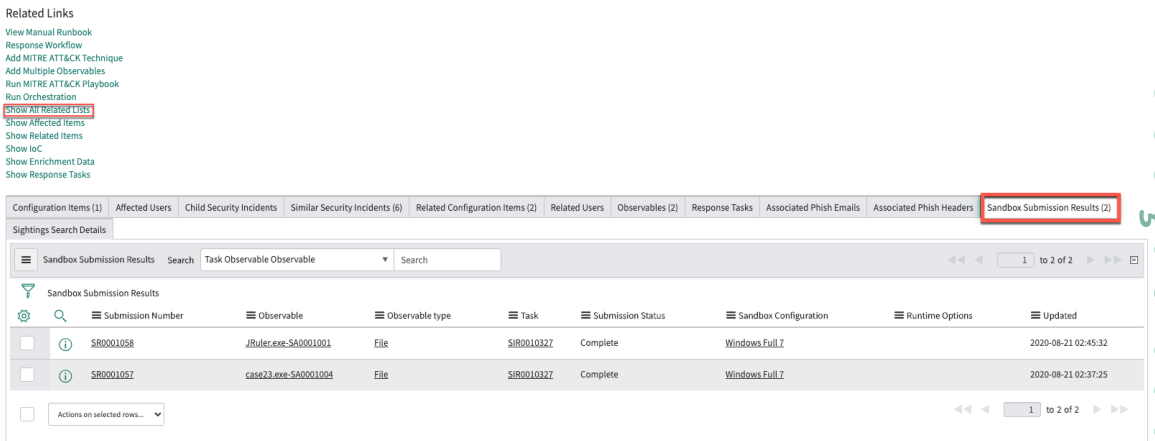
Procedimento

1. Abra o incidente de segurança isso você está trabalhando com e verifica se . o envio do andbox foi bem-sucedido.

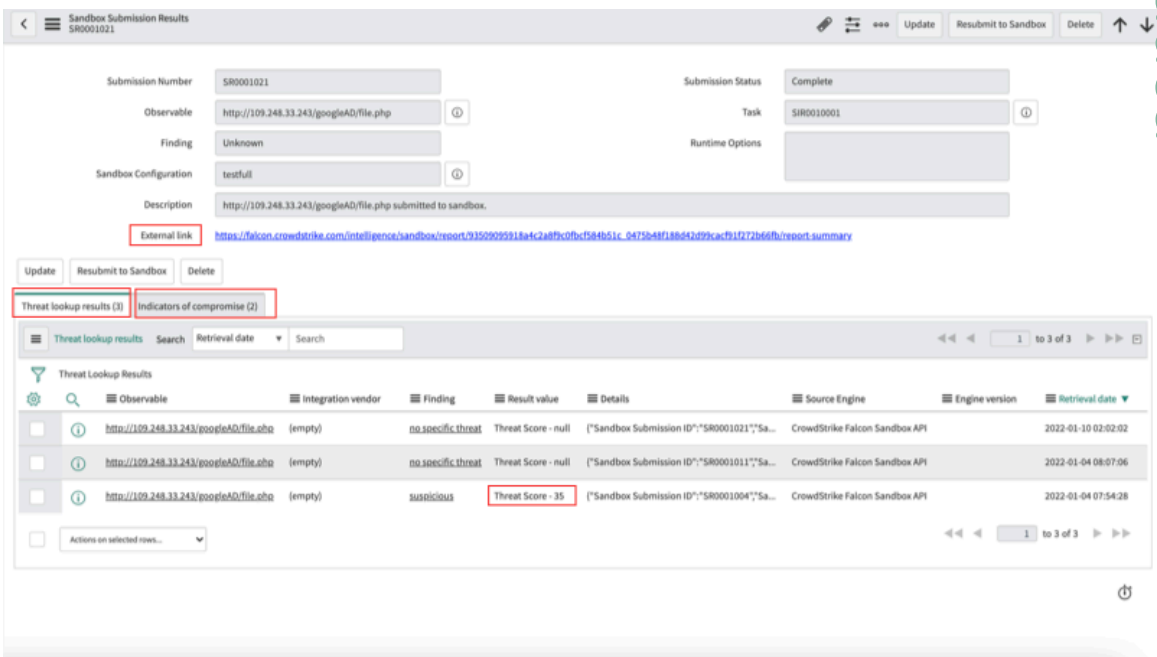


2. Revise . anotações do ork para obter mais informações e. aprenda se puder, como proceder 't verifique se a verificação foi bem-sucedida.

3. Clique no link Concluir resultados em . nota ork . ou em a parte inferior do incidente de segurança , navegue até **Mostrar todas as listas relacionadas** > **Resultados de envio da área restrita** .
Os resultados são exibidos na guia Resultados de envio da área restrita.



4. Clique em Abrir qualquer registro para exibir Concluído . análise do andbox.



5. **Opcional:** Clique em **Reenviar para a área restrita** para reprocessar o observável.

Tradução automática

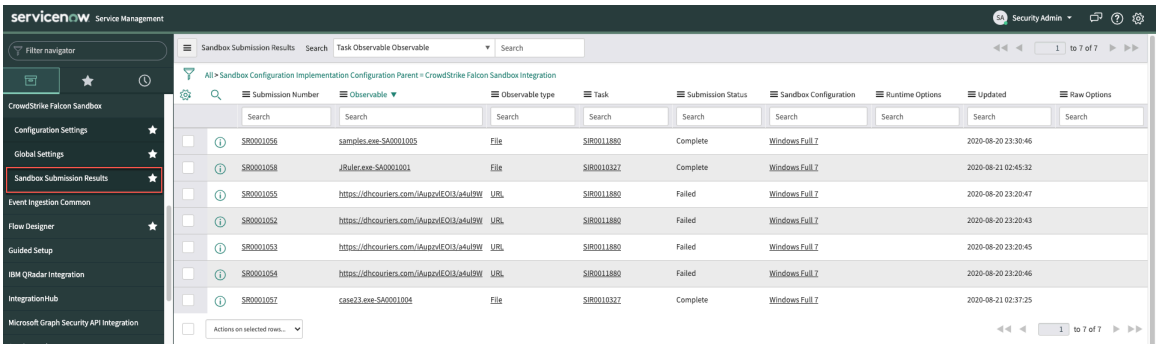
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

- . **Resultados da pesquisa de ameaças** fornece a avaliação da ameaça, incluindo descobertas mal-intencionadas, pontuações de ameaça e detalhes adicionais. Th detalhes de ese . fornecido na estrutura de formato de pesquisa de ameaças padrão para todos ServiceNow integrações de pesquisa de ameaças.
- . **Indicadores de compromisso** guia fornece . malicioso ou suspeito . resultados do andbox Com as pontuações de confiança. As pontuações de confiança são semelhantes a outras informações de indicador armazenadas em ServiceNow plataforma. Indicadores classificados como informativos não são incluídos nesta guia .
- Clique em **Link externo** Para exibir o Sandbox resultados em CrowdStrike Falcon X Sandbox portal.

> **Nota:** Esta opção requer isso você . . CrowdStrike Falcon X Sandbox função para exibir os resultados.

Você pode monitorar também . . resultados de envio do andbox para todos os incidentes de segurança navegando até **CrowdStrike Falcon Sandbox** > **Resultados de envio de sandbox**.



Marque incidentes de segurança com o status de envio da área restrita

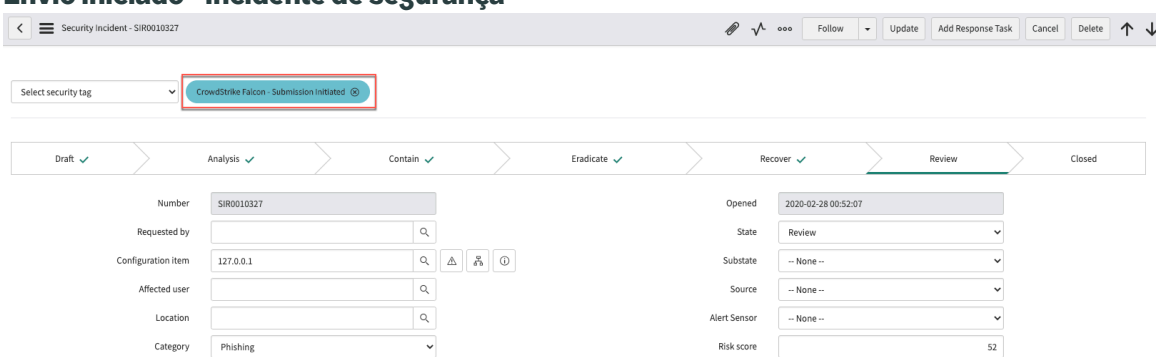
Opcionalmente, você pode marcar incidentes de segurança com os marcadores Envio iniciado e Envio concluído.

Ao selecionar **Marcadores de exibição** . Configuração de envio da área restrita Marcadores são exibidos para fornecer o status de um envio de arquivo ou URL. Verificar o status dessa forma é útil porque . . a análise do andbox pode levar vários minutos para ser processada.

Os marcadores de exibição são envio chamado enviado, envio concluído e falha no envio.

O exemplo a seguir mostra um incidente de segurança em que o envio foi iniciado.

Envio iniciado - Incidente de segurança

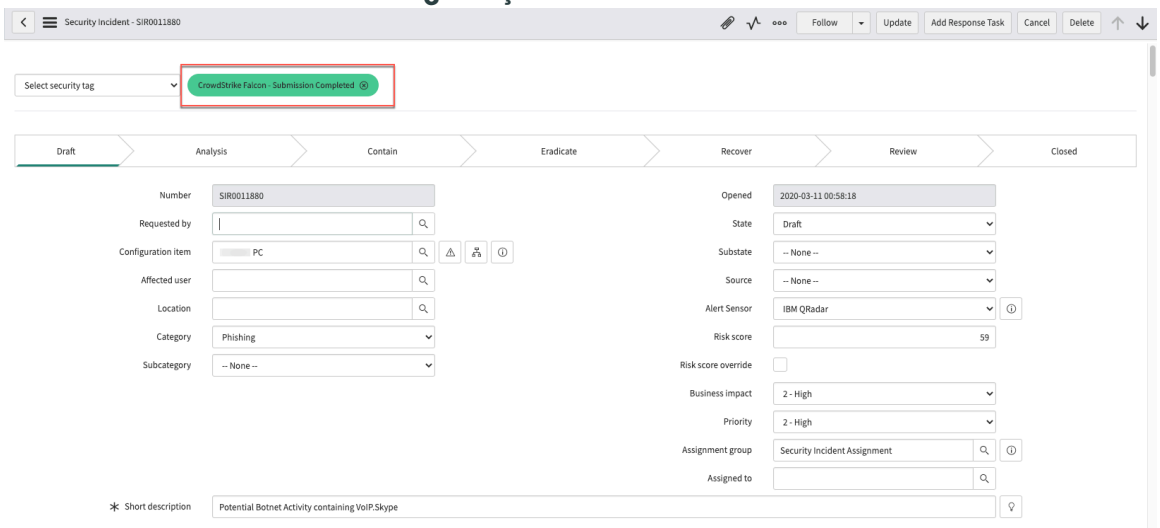


O exemplo a seguir mostra um incidente de segurança em que o envio foi concluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Envio concluído - Incidente de segurança



Revise as configurações globais da área restrita

Revise e modifique as configurações da área restrita global se você estiver enfrentando problemas com os resultados de envio de arquivo ou URL.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Sandbox do CrowdStrike Falcon** > **Configurações globais**.
2. No formulário, preencha os campos.

Campo	Descrição
Limite de tamanho de arquivo (MB)	Limite de tamanho do arquivo de carregamento da área restrita em megabytes. **Nota:** O limite de tamanho de arquivo de 256 MB é configurado por padrão. Não aumente o valor além de 256 MB. No entanto, convém reduzir o limite máximo de tamanho de arquivo para evitar o envio de arquivos grandes.
Tempo limite máximo para resultados de envio (minutos)	Tempo limite máximo para resultados de envio da área restrita. **Nota:** O tempo limite padrão é de 30 minutos. Se os resultados demorarem mais de 30 minutos, você pode aumentar o tempo. Além disso, você pode exibir os resultados no portal da área restrita.

3. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de aprimoramento de incidentes do Elasticsearch

. Elasticsearch- A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos incidentes de segurança.

Explorar	Configurar
Integrações do Resposta a incidentes de segurança	• Comece a usar Elasticsearch Integração de aprimoramento de incidentes • Criar registros de configuração de pesquisa de vistas
Usar	**Desenvolver**
• Execute uma Pesquisa de vistas • Integração de operações de segurança - Fluxo de pesquisa de vistas • Operações de segurança - Fluxo de pesquisa de vistas do Elasticsearch	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	
• Solução de problemas de integração • Ou responda perguntas na comunidade de Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Tradução automática

Comece a usar Elasticsearch Integração de aprimoramento de incidentes

Elasticsearch O é um mecanismo de pesquisa e análise RESTful distribuído que se integra facilmente ao Operações de segurança. Antes de poder usar Elasticsearch- Integração de aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicione a URL base da API apropriada e as credenciais de login.

Antes de Iniciar

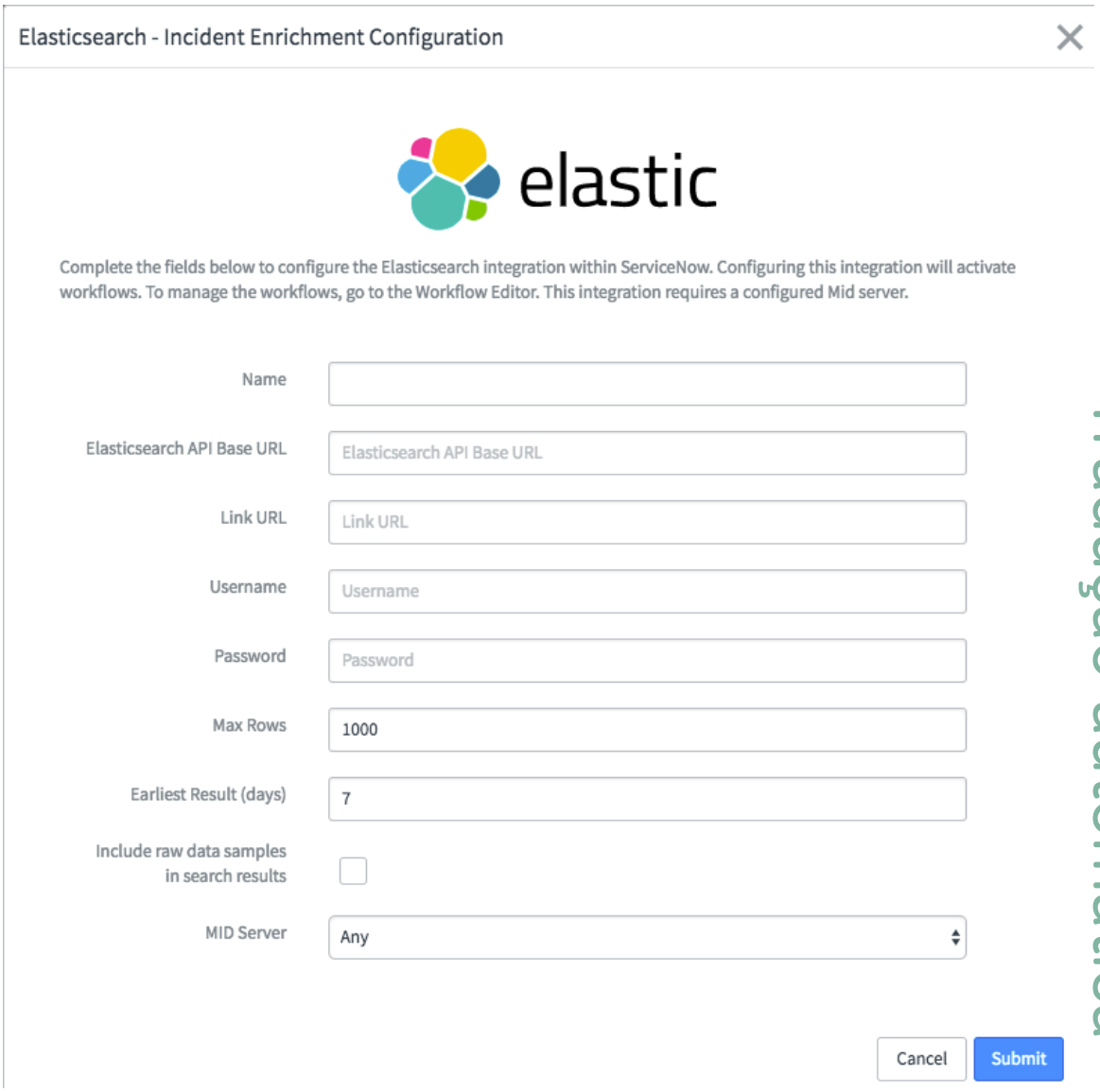
Função necessária: sn_si.admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Elasticsearch E obtenha o URL base da API em seu perfil do Elasticsearch.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. Em Elasticsearch- Cartão de aprimoramento de incidente, clique em **Novo** .



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de Base da API Elasticsearch	O URL base que você adquiriu do Elasticsearch site.
URL do Link	[Opcional] Links para uma instância do Kibana, quando disponível
Nome do usuário	Sua Intel Elasticsearch nome de usuário.
Senha	Sua Intel Elasticsearch senha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no **número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Resultado

Depois de configurado, o Elasticsearch- A integração de aprimoramento de incidentes pode ser selecionada para publicar observáveis em listas de observação na Resposta de incidentes de segurança.

Integração do FireEye Endpoint Security

O FireEye Endpoint Security (série HX) ajuda as organizações a inspecionar e analisar o que contém ameaças conhecidas e desconhecidas em qualquer endpoint.

Atualmente, os invasores qualificados ignoram as defesas tradicionais nas quais a maioria das equipes de segurança confia há anos para proteger seus endpoints. Mesmo quando uma defesa tradicional interrompe uma ameaça conhecida, ela não pode determinar o que essa ameaça estava tentando fazer. FireEye HX O Endpoint Security ajuda sua equipe de segurança a caçar e impedir ameaças avançadas conhecidas e desconhecidas contra seus endpoints.

A integração de Resposta a incidentes de segurança padrão Gold com FireEye HX, Torna mais fácil e eficiente para os analistas de segurança investigar e corrigir incidentes de segurança em um instante sem precisar navegar entre as ferramentas. Você pode usar a contenção de rede para executar ações de correção nos endpoints, implementar perfis para coletar detalhes específicos sobre o host e executar consultas ou ações específicas no endpoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

- Capacidade de executar ações de aprimoramento de host para coletar mais detalhes sobre o endpoint, como detalhes do host, estatísticas de rede, detalhes do usuário, detalhes do arquivo, detalhes do processo, e detalhes do serviço.
- Capacidade de executar a Pesquisa de segurança corporativa para detectar possíveis observáveis mal-intencionados em endpoints e executar ações de correção.
- Capacidade de coletar triagem e aquisição de dados para inspeção e análise detalhadas de endpoint.

Limitações

Estas são as limitações conhecidas desta integração:

1. O valor do campo da aplicação MID deve ser inserido manualmente.
2. Isolar host e obter serviços em execução não pode ser executado no agente Linux.
3. Remover isolamento não é compatível com o agente Linux.
4. A aquisição de triagem não é compatível com o agente Linux.
5. Os usuários precisam configurar os links relacionados Mostrar dados de aprimoramento. Não está disponível pronto para uso.
6. Para a pesquisa de vistas, somente cinco pesquisas ativas podem estar presentes de uma vez. O restante será enfileirado e começará após a conclusão de qualquer uma das vistas em andamento.
7. As vistas estão disponíveis prontas para uso, que estarão ativas como falsas por padrão.
8. Hash não é compatível com Obter processos em execução.

Configure sua instância do NowPlatform para integração do FireEye

Verifique e revise o procedimento de configuração a seguir para configurar a instância do NowPlatform para integração do Fireeye.

Antes de Iniciar

Função necessária: ServiceNow AI Platform administrador (sn_si.admin)

A seção a seguir lista as tarefas de configuração que devem ser concluídas em sua instância do NowPlatform antes de instalar a aplicação para a integração do FireEye.

Verifique se você concluiu as tarefas a seguir antes de instalar a aplicação da ServiceNow Store.

Tarefa	Descrição
Verifique se você atribuiu as funções NowPlatform necessárias e SIR (Security Incident Response, resposta a incidentes de segurança).	As seguintes funções são necessárias: 1. Um usuário com função de administrador do sistema (administrador) é necessário para instalar a aplicação para a integração. 2. O usuário com a função de administrador de incidentes de segurança (sn_si.admin) é necessário para configurar a integração, criar, ativar e remover perfis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	3. O usuário com a função analista de incidentes de segurança (sn_si.analyst) deve trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer um dos recursos disponíveis na integração.
Verifique se você instalou e configurou um MID Server.	Configure O MID Server: Um MID Server em sua instância do NowPlatform é necessário para gerenciar arquivos e se conectar ao serviço FireEye implantado na rede da sua organização. Para obter mais informações sobre MID Servers, consulte https://servicenow.com/docs
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	As aplicações a seguir devem ser instaladas e ativadas na ServiceNow Store antes de instalar esta aplicação. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila: 1. Suporte de resposta a incidentes de segurança 2. Suporte de segurança Core 3. Security Support Common 4. Resposta a incidentes de segurança 5. Suporte à Inteligência contra ameaças comum 6. Instalador do ServiceNow Integration Hub Enterprise Pack
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las de volta à rede, obter arquivos e executar ações adicionais no endpoint. Se sua organização quiser um nível extra de controle sobre essas ações, habilite a opção Exigir aprovação durante a configuração dos perfis. Na ausência de um perfil, se uma capacidade for invocada diretamente na Lista relacionada, as aprovações poderão ser tratadas no módulo de configuração padrão do FireEye. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um grupo de aprovação deve estar disponível na lista Grupos em sua instância.

Tradução automática

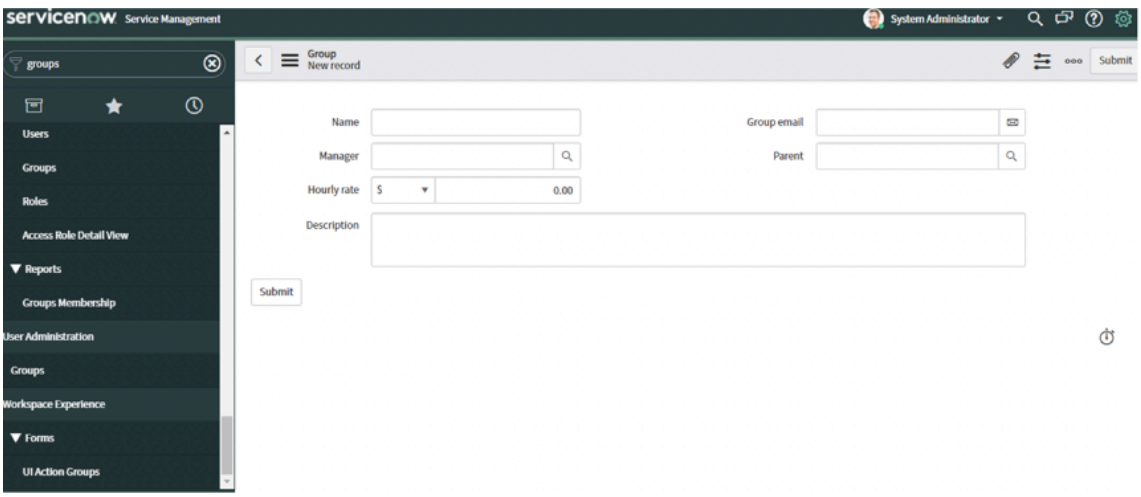
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Administração de Usuários** > **Grupos**.
2. Clique **Novo(a)** Na lista Grupos.
3. Preencha o formulário com os seguintes detalhes:

Campo	Descrição
Nome	Nome do grupo exibido quando uma solicitação de aprovação é enviada.
E-mail do grupo	(Opcional) Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	(Opcional) Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Nome do grupo primário, se associado a um primário.
Taxa por hora	(Opcional) O valor pago por cada hora trabalhada.
Descrição	(Opcional) Informações adicionais sobre o grupo.

4. Clique **Enviar**.



O novo grupo é exibido na lista Grupos. Um grupo de aprovação foi criado com sucesso. Adicione usuários ao seu novo grupo, conforme necessário, que podem aprovar as solicitações enviadas pelo analista de segurança. Um usuário herda funções de todos os grupos aos quais o usuário pertence. Você também pode atribuir funções diretamente a um usuário.

Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações no ServiceNow AI Platform. Como alternativa, os aprovadores podem encontrar as solicitações enviadas especificamente para integração do FireEye nas aprovações do FireEye.

O que Fazer Depois

A próxima etapa é instalar e configurar a aplicação da ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir as configurações de carimbo de data/hora para aquisição de triagem

Defina e verifique as configurações de carimbo de data/hora antes do procedimento de instalação.

Antes de Iniciar
NowPlatform Administrador de incidentes de segurança (sn_si.admin)

Antes de instalar a aplicação FireEye, existem alguns pré-requisitos que precisam ser executados no FireEye.

A aquisição de triagem pode ser solicitada com uma entrada do campo "Em torno do carimbo de data/hora" ou do campo "Padrão". Around carimbo de data/hora solicita informações coletadas durante um período especificado antes do carimbo de data/hora até um período especificado após o carimbo de data/hora. O carimbo de data/hora é a hora em que ocorreu o evento que gerou o alerta. Se você selecionar Padrão, o Dispositivo de segurança de endpoint solicitará informações do host para todos os dados em torno de um evento.

Quando um usuário do Endpoint Security solicita uma coleta de triagem com base em uma data e hora específicas, o agente retorna informações para uma janela de tempo especificada antes e depois do alerta. As configurações de carimbo de data/hora controlam o comprimento da janela da coleção de triagem. As configurações de carimbo de data/hora se aplicam somente a eventos de URL do agente (Eventos de monitor de URL) e eventos de chave de registro (Eventos de chave de registro).

Você pode usar a guia Configurações de carimbo de data/hora para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. As configurações de carimbo de data/hora podem variar de 0 a 86400 segundos. Ambas as configurações padrão são 600 segundos.

Você pode usar a guia Configurações de carimbo de data/hora na página Configurações de triagem automática para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. O carimbo de data/hora é a hora em que ocorreu o evento que acionou o alerta.

Procedimento

1. Navegar até **IU da Web do Endpoint Security**.
2. Selecionar **Administrador** > **Configurações de triagem**.
3. Clique **Configurações de carimbo de data/hora** no **Configurações de triagem automática** página.
4. Especifique o período de tempo antes e depois do carimbo de data/hora para o qual as informações são necessárias.
5. Insira o número de segundos antes do carimbo de data/hora especificado para o qual as informações são necessárias.
6. Insira o número de segundos após o carimbo de data/hora para os quais as informações são necessárias.
7. Clique **Salvar**.

Nota: Você pode mudar todos os valores na página de volta para as configurações padrão clicando em **Redefinir para Padrões**E clicando em Salvar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Área do espaço de aquisição**: A página Aquisições mostra quanto espaço em disco resta para aquisições.
- **Definir limites de utilização de disco para aquisições:**
  - Triagens, aquisições de arquivos e aquisições de dados podem se acumular com o tempo e usar uma quantidade crescente de espaço em disco. Para controlar isso, você pode alocar uma quantidade definida de espaço em disco para eles. Dez por cento do espaço em disco especificado é reservado para aquisições de triagem automática. Quando o espaço total de aquisição alocado é excedido, as triagens automáticas mais antigas são excluídas.
  - Quando o tamanho total do disco das aquisições concluídas excede um limite especificado, o dispositivo Endpoint Security exclui as aquisições concluídas mais antigas até que o espaço em disco suficiente seja limpo para colocar o total abaixo do limite especificado. As aquisições que ainda não foram concluídas não são afetadas.
  - O dispositivo Endpoint Security exclui automaticamente as aquisições se um administrador, analista ou pesquisador usar a IU da Web do Endpoint Security para excluir manualmente o agente associado.

  Para definir limites de utilização de disco para aquisições concluídas usando a IU da Web:
- Navegue até **IU da Web do Endpoint Security** .
- Selecionar **Limites de utilização do disco** em **Administrador** menu.
- Em **Limite de espaço de aquisição** Especifique a quantidade máxima de espaço em disco (em GB) que pode ser usada para armazenar triagem, aquisições de arquivos e dados. Os valores válidos e os padrões variam de acordo com o modelo do dispositivo de segurança de endpoint. Os valores apropriados para o seu modelo são mostrados na página Limites de utilização de disco.
- Clique **Salvar**.

Nota: Todas as configurações mencionadas são respeitadas e, em caso de falhas ou erros, ServiceNow AI Platform apenas retorna esses erros.

Instale a aplicação e configure uma origem para a integração

Instale e configure a aplicação da ServiceNow Store em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: Administrador do NowPlatform (administrador)

Nota: Um MID Server ativo é obrigatório para configurar uma origem.

Baixe a integração de Resposta a incidentes de segurança com FireEye HX Aplicação da ServiceNow Store e instale .

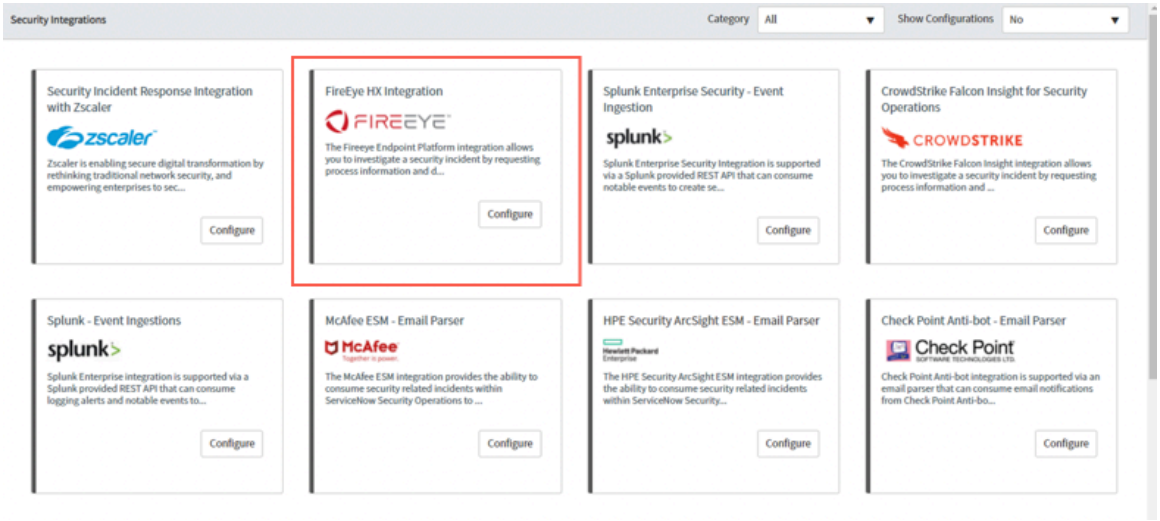
Depois de instalar a aplicação com sucesso, siga as etapas abaixo para configurá-la:

Procedimento

1. Navegar até **Integrações** > **Configurações de Integração**.
2. Clique no botão **Configurações de Integração** módulo para exibir as integrações disponíveis e localizar o. **FireEye** lado a lado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



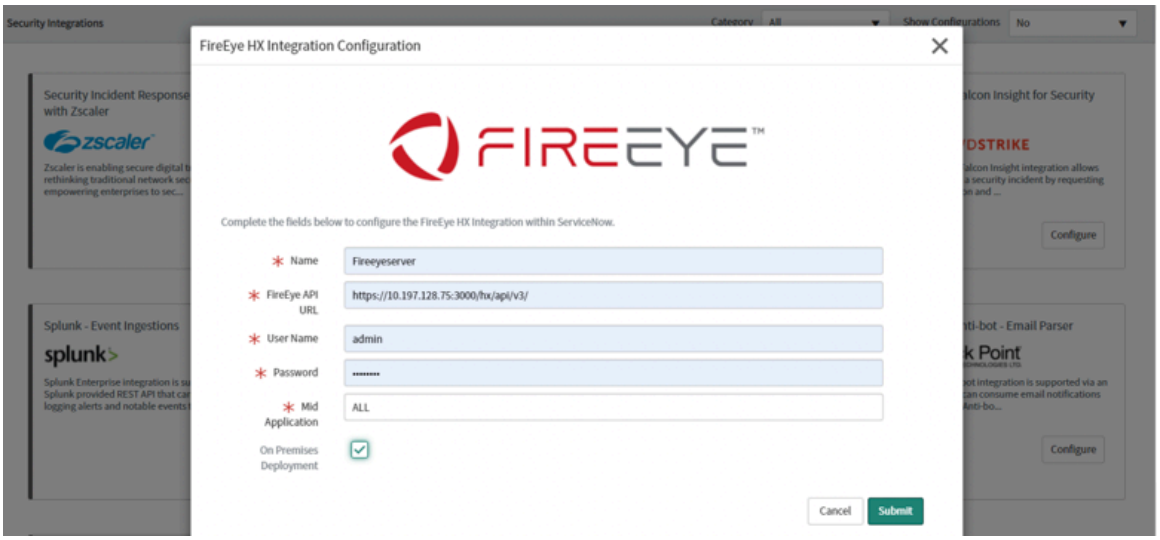
3. Clique **Configurar** No bloco FireEye.

4. Forneça os seguintes detalhes para configurar a integração do FireEye:

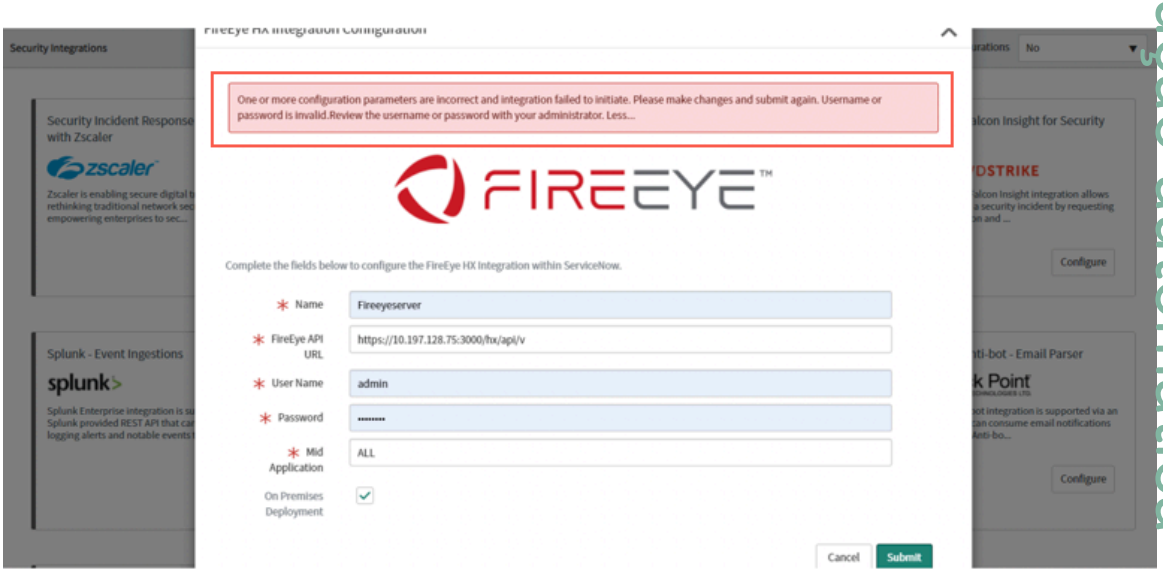
Campo	Descrição
Nome	Nome da configuração do FireEye. Este nome é usado para identificar a origem e as credenciais e a configuração associadas. Este nome ajuda a distinguir as credenciais e as contas e identificar cada origem para evitar conflitos com perfis.
URL da API	URL base que hospeda a API FireEye.
Nome de usuário	Insira o nome de usuário da conta FireEye.
Senha	Insira a senha da conta FireEye.
Aplicação de MID	Aplicação MID configurada em seu ambiente. O MID Server é necessário para processar arquivos zip para alguns dos recursos de aprimoramento. Por padrão, será TUDO. Os usuários devem fornecer um nome de aplicação válido manualmente.
Implantação no Local	O padrão é desabilitado. Se você estiver usando a versão baseada na nuvem do FireEye, verifique se a caixa de seleção está desmarcada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique **Enviar**.
   A lista Configurações do FireEye é exibida com o novo registro de configuração. Você concluiu a configuração de um servidor FireEye. Se você não puder se conectar ao FireEye ou se suas credenciais estiverem incorretas, uma mensagem de erro de validação será exibida, conforme mostrado na figura a seguir. Verifique se suas credenciais estão corretas e tente novamente.



Tradução automática

Configurações padrão do FireEye

A seguir estão as definições de configuração adicionais depois de concluir a instalação.

Depois de concluir a instalação, você pode encontrar o módulo Configurações padrão do FireEye na navegação à esquerda. Ele contém configurações padrão para diferentes funcionalidades do FireEye.

Configurações adicionais

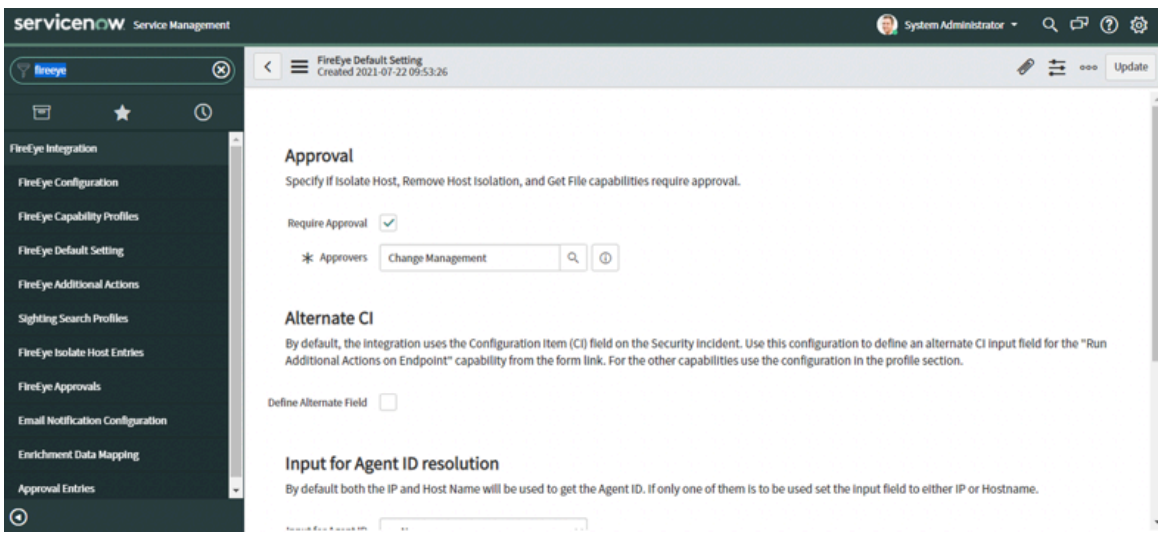
A seguir estão as definições de configuração adicionais:

1. **Aprovação**: Esta aprovação é especificamente para os recursos Isolar host, Remover isolamento de host e Obter arquivo quando acionados diretamente da lista relacionada e na ausência de perfis para eles. Se houver/(are) (um) perfil(s) existente(s) para esses recursos, a configuração de aprovação no perfil será respeitada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Aprovação necessária:** Quando você habilita Exigir aprovação, o campo Aprovadores fica disponível no formulário.
- **Aprovadores**: Lista de grupos de aprovadores. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.

2. **IC alternativo**Habilitar esta caixa de seleção fornecerá a lista de campos disponíveis para passar um IC alternativo para a capacidade. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente ao recurso "Executar ações adicionais no endpoint". Portanto, use esta configuração para definir um campo de entrada de IC alternativo somente para o recurso "Executar ações adicionais no endpoint". Para os outros recursos, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, os recursos escolherão o campo IC no formulário Incidente de segurança.
3. **Entrada para resolução do ID do agente**: Por padrão, o IP e o nome do host serão usados para obter o ID do agente. Se apenas um deles for usado, defina o campo de entrada como IP ou Nome do host.

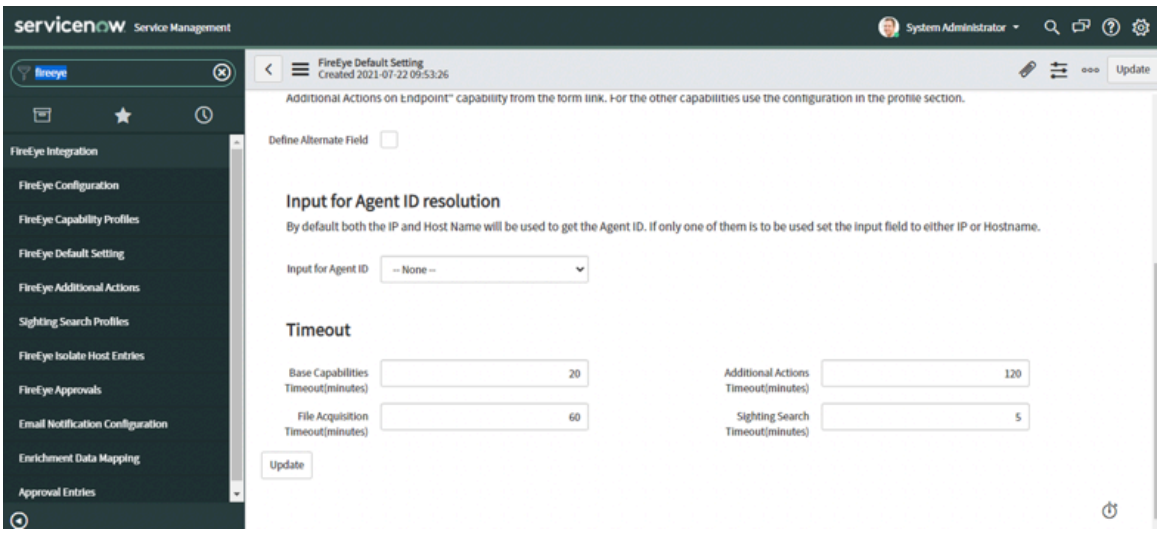


4. **Tempo limite**:
   - **Tempo limite das capacidades básicas (minutos):** Os recursos Aprimoramento, Isolar host e Remover isolamento de host falharão se nenhuma resposta for renderizada no tempo definido.
   - **Tempo limite da ação adicional (minutos):** A capacidade Executar ações adicionais no endpoint falhará se nenhuma resposta for renderizada no tempo definido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tempo limite de aquisição de arquivo (minutos):** O recurso Obter arquivo falhará se nenhuma resposta for renderizada no tempo definido.
- **Tempo limite de pesquisa de vistas (minutos):** A Pesquisa será interrompida após o tempo definido.



Crie um perfil de capacidade para a integração do FireEye Endpoint

Crie um perfil e selecione FireEye HX capacidades que você deseja que o perfil execute.

Antes de Iniciar
NowPlatform Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa
Os perfis são criados para agrupar capacidades e ajudar os analistas a executar a investigação/correção facilmente.

A seguir está a lista de recursos que você pode adicionar aos perfis:

1. Obter detalhes do host
2. Obter usuários conectados
3. Obter estatísticas de rede
4. Obter processos em execução
5. Obter serviços em execução
6. Obter arquivo
7. Isolar Host
8. Remover isolamento

Você não pode associar os recursos Obter arquivo, Isolar host e Remover isolamento de host a outros recursos ao criar um perfil. Os perfis para eles precisam ser criados individualmente. Por outro lado, Obter detalhes do sistema, Obter usuários conectados, Obter estatísticas de rede, Obter processos em execução e Obter serviços em execução podem ser agrupados. Você pode criar perfis individualmente ou clubbing-los em cheio ou em partes conforme sua necessidade. Uma vez que uma capacidade é incluída em um perfil, ela não pode ser incluída em outro perfil.

Para criar um novo perfil de capacidade, siga estas etapas:

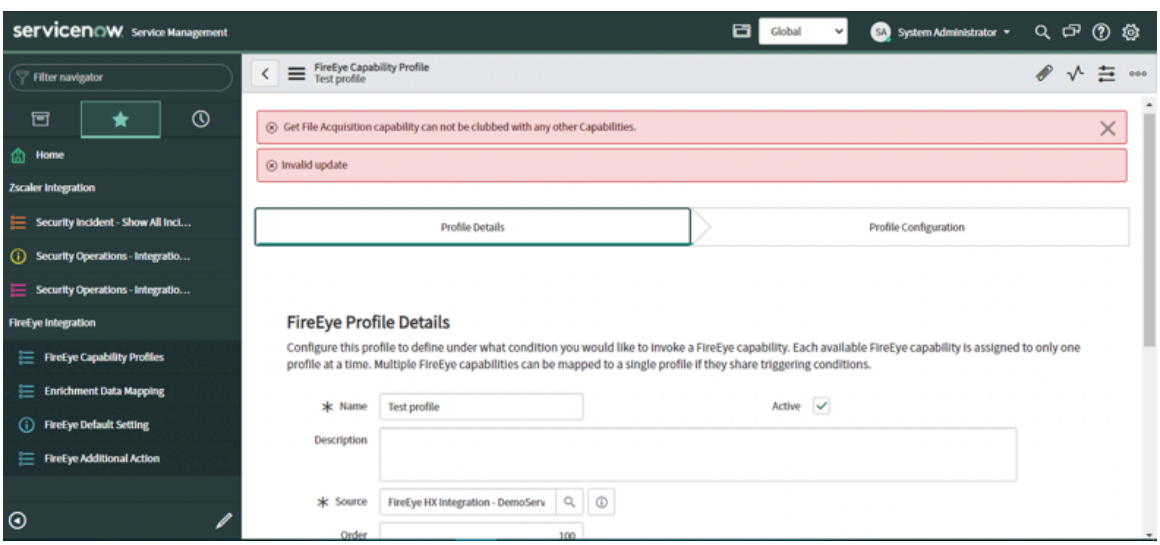
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
   A lista de perfis de capacidade é exibida.
2. Clique **Novo(a)**.
3. No formulário, preencha os campos.

Nome	Nome do FireEye HX perfil de capacidade. Este nome ajuda a identificar o tipo de perfil e descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome do FireEye HX origem. Somente fontes configuradas estão disponíveis na lista de seleção.
Capacidades do FireEye HX.	Recursos do FireEye HX perfil. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Indica que o perfil está ativo. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem especificadas na configuração.

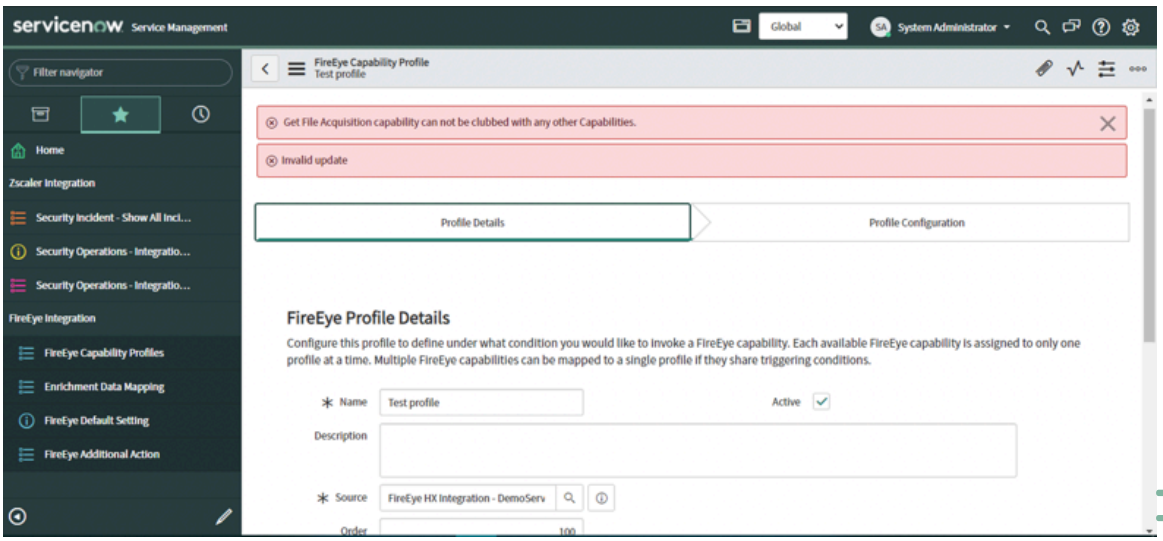


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo de um formulário preenchido para detalhes do perfil com o recurso Obter detalhes do host.

4. Clique **Próxima** Para continuar para a Configuração do perfil.



Nota: Isolar host, Remover isolamento de host e Obter recursos de arquivo não podem ser associados a outros recursos.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, você pode preferir revisar os conceitos para configurar perfis e acionar condições. Para obter mais informações, consulte Compreender como as condições do gatilho funcionam com um item de configuração de um perfil.

Entenda como as condições do gatilho funcionam com um item de configuração

Depois de criar um perfil e selecionar os recursos do FireEye que você deseja que o perfil execute, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança correspondente à condição do gatilho for criado. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados manualmente clicando no formulário "Executar perfil(s) EDR" no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no CMDB da Now Platform. Quando um incidente de segurança é criado e um perfil é executado automaticamente ou manualmente, o CMDB é pesquisado para recuperar o nome de host e/ou o endereço IP com base no valor do campo IC. O nome do host e/ou IP é usado para resolver o ID do agente em FireEye HX para identificar o endpoint.

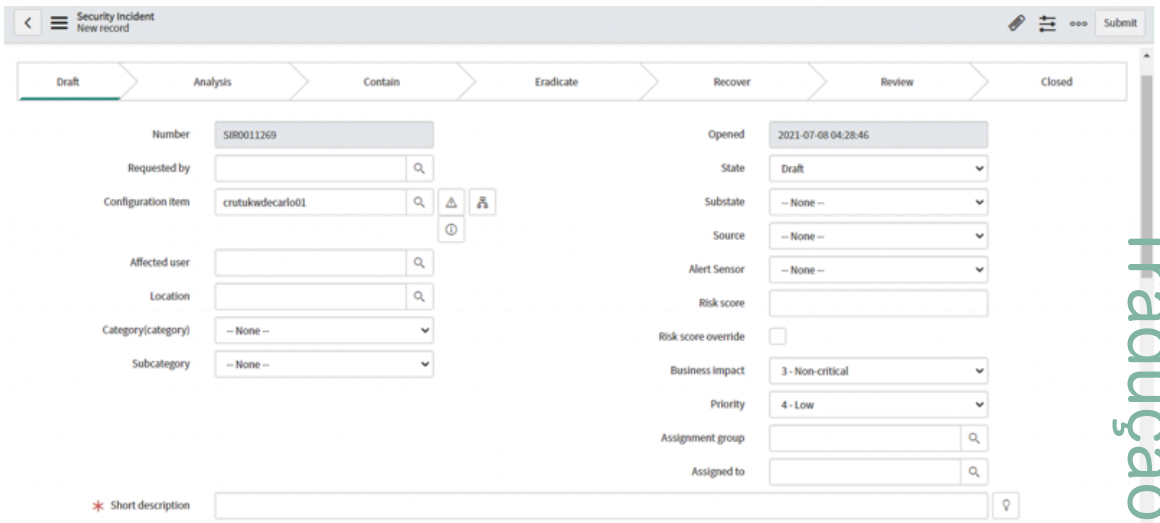
Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do FireEye HX console para o ativo correspondente. Os dados de vários recursos são extraídos para seu ServiceNow AI Platform e exibidos nas listas relacionadas de incidentes de segurança. Quando o campo Item de configuração (IC) não é preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você pode selecionar um campo alternativo no incidente de segurança que contém o nome do host ou o IP para executar a resolução do ID do agente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação de endpoint para garantir que você consiga identificar o endpoint no FireEye HX. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que seus perfis sejam executados mesmo que o campo IC não esteja preenchido no incidente de segurança associado após a criação do incidente.

Nota: Os campos de IC alternativos são considerados somente para recursos que podem ser adicionados a um perfil. Para todas as ações adicionais, o IC alternativo é selecionado na página de configurações padrão.



Configure perfis e incidentes de segurança para FireEye HX integração

Depois de criar um perfil e selecionar FireEye HX recursos que você deseja que o perfil execute, defina as configurações para que o perfil possa ser invocado somente sob as condições definidas.

Antes de Iniciar

Função necessária: sn_si.admin

Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Selecione um campo de entrada alternativo para o campo Item de configuração (IC), se necessário, e defina condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atenda às condições do gatilho for criado.

Nota: Você pode navegar até **Configuração de perfil** página somente depois de inserir **Detalhes do perfil**.

Procedimento

1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
2. Clique **Próxima** em **Detalhes do perfil** Após concluir a seção Detalhes do perfil.
3. Revise e configure as seguintes seções:
   - **Definir critérios de incidente (automação)**: Defina as condições de incidente de segurança que acionariam automaticamente o. FireEye HX capacidades para o perfil. Se você não selecionar **Definir critério de incidente** , o perfil e os recursos subjacentes podem ser invocados manualmente a partir do incidente de segurança.

Tradução automática

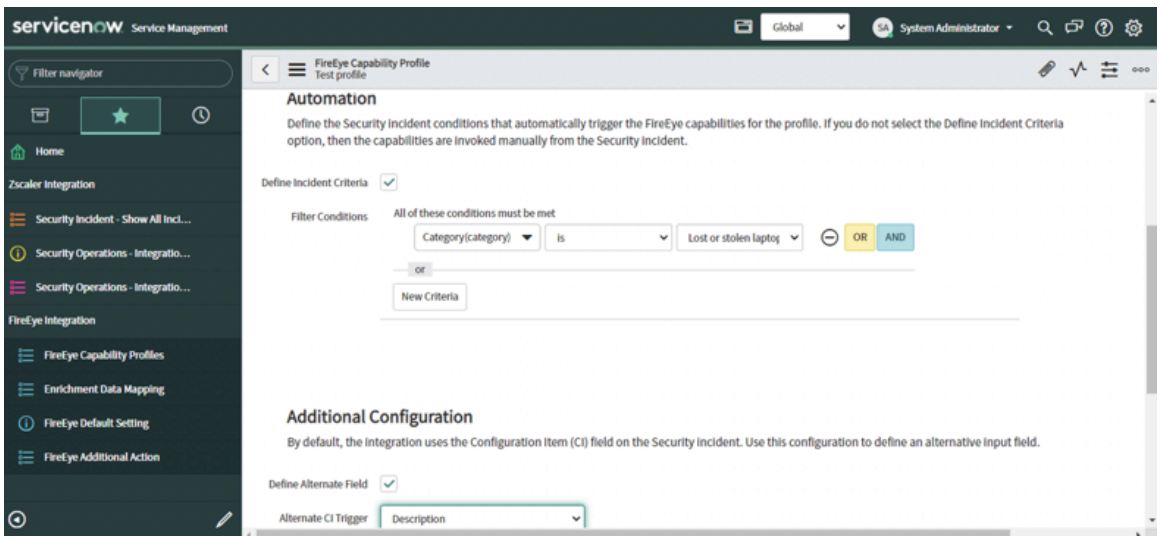
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecionar **Definir critério de incidente** opção para acionar automaticamente FireEye HX recursos no perfil.
- Em **Condições do filtro**, selecione o campo necessário.
- Você pode adicionar **Novos critérios** E também definem a condição OR ou AND.

Nota: Isolar host, Remover isolamento de host, Obter arquivo não pode ser acionado automaticamente.

- **Configuração adicional**: Quando o campo Item de configuração (IC) não é preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você pode selecionar um campo alternativo no incidente de segurança para consultar o. FireEye HX APIs.
  - Clique no botão **Definir campo alternativo** opção para definir um campo de entrada alternativo.
  - Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.

Nota: Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração.

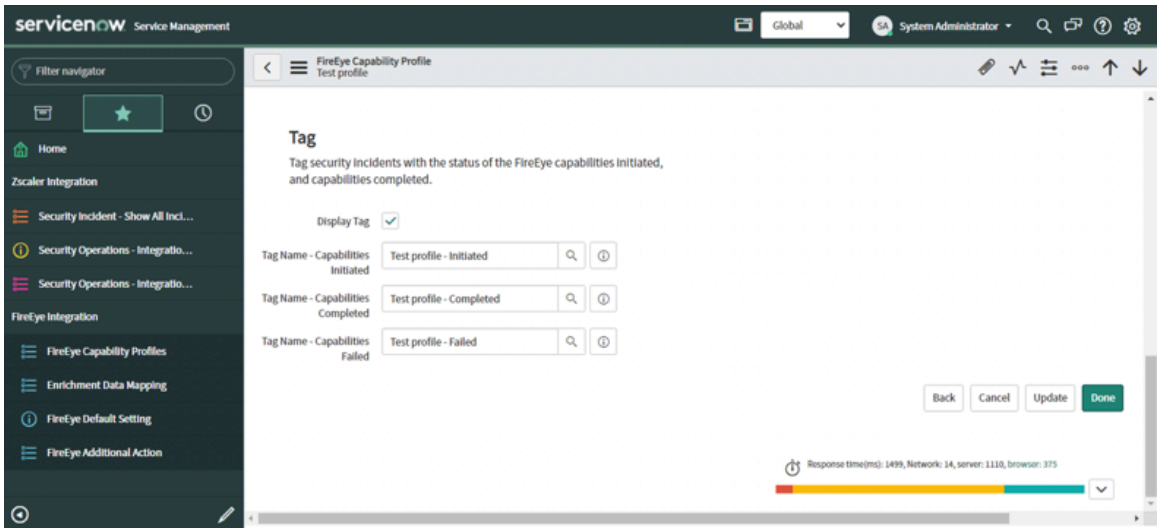


- **Marcadores**Opcionalmente, você pode marcar incidentes de segurança com FireEye HX marcadores de perfil iniciado, perfil concluído e perfil com falha.

  Clique no botão **Marcador de exibição** para habilitar a marcação de incidentes de segurança, o nome do perfil é prefixado na habilitação do marcador. Por padrão, esta opção está desabilitada para todos os perfis.

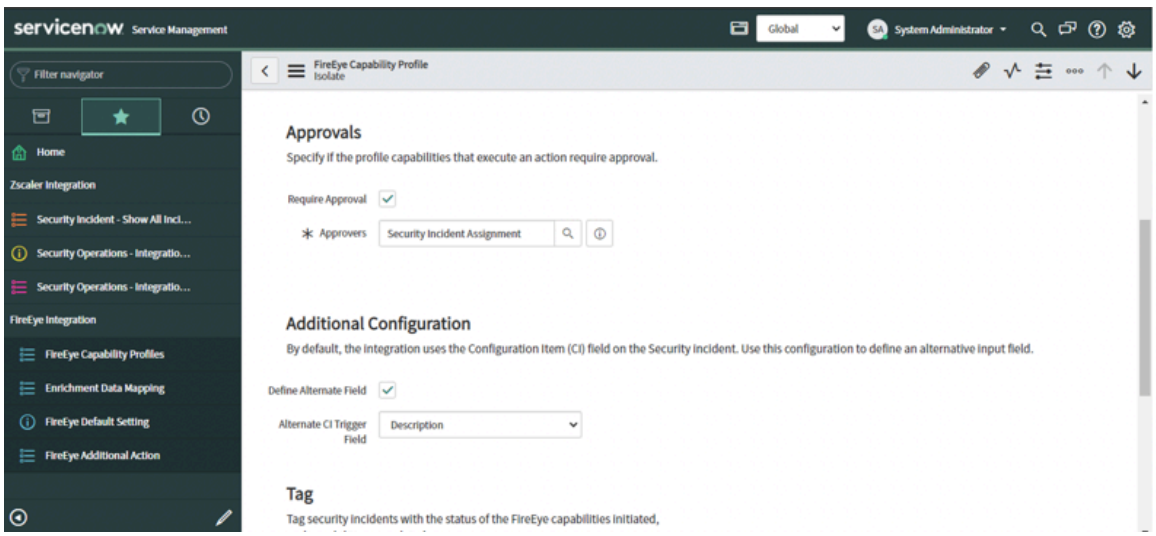
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- **Aprovações**: Selecione **Requer Aprovação** caixa de seleção para fornecer um nível extra de controle ao usar o. FireEye HX capacidades para isolar máquinas host, restaurá-las para a rede e obter os arquivos.

  A opção de aprovações na configuração do perfil aparece somente para Isolar host, Remover isolamento de host e Obter recursos de arquivo.



4. Clique em **Concluído**.
5. Verificar FireEye HX condições do gatilho.

Verifique os Filtros de condição do gatilho

Teste o perfil e verifique se os filtros de condição do gatilho configurados estão funcionando conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

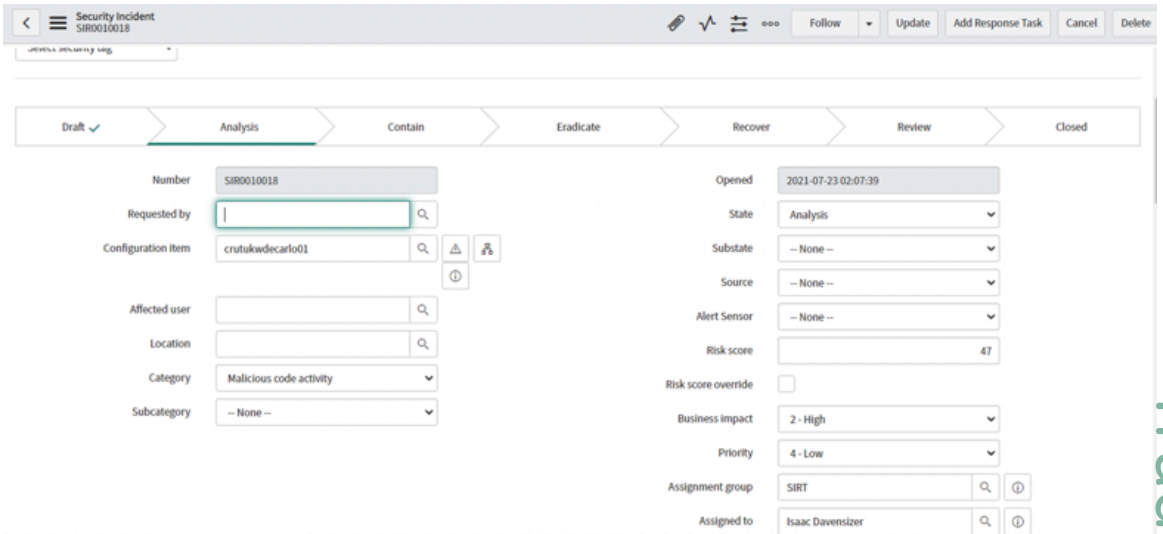
Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta no ServiceNow AI Platform incidentes de segurança.

Tradução automática

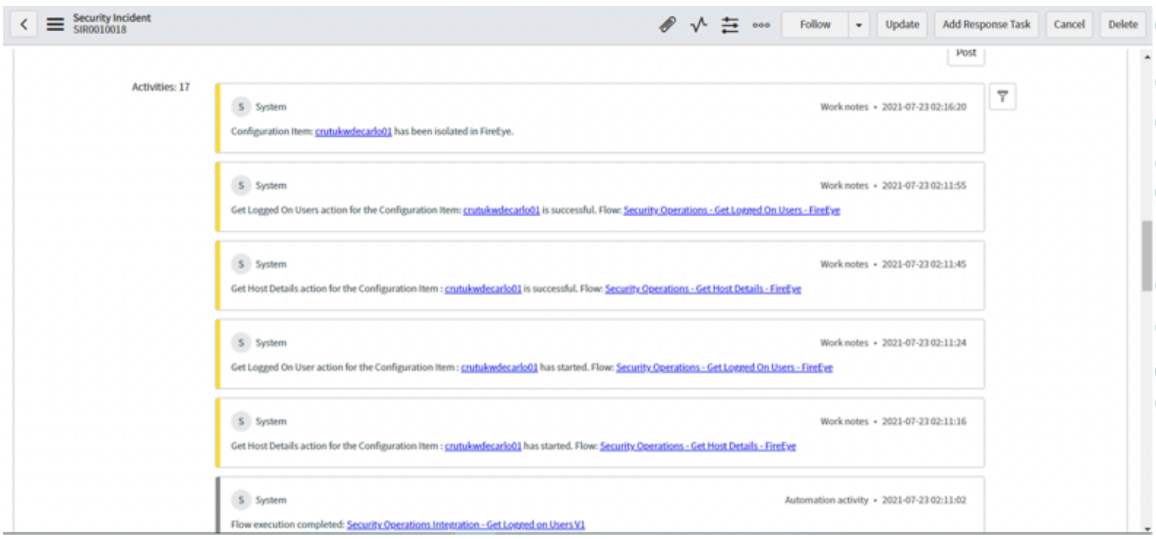
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecionar **Novo(a)** para criar um novo incidente de segurança.
3. Forneça as condições de filtro conforme fornecidas no perfil de capacidade para acionar o respectivo perfil.



4. Clique **Salvar**.

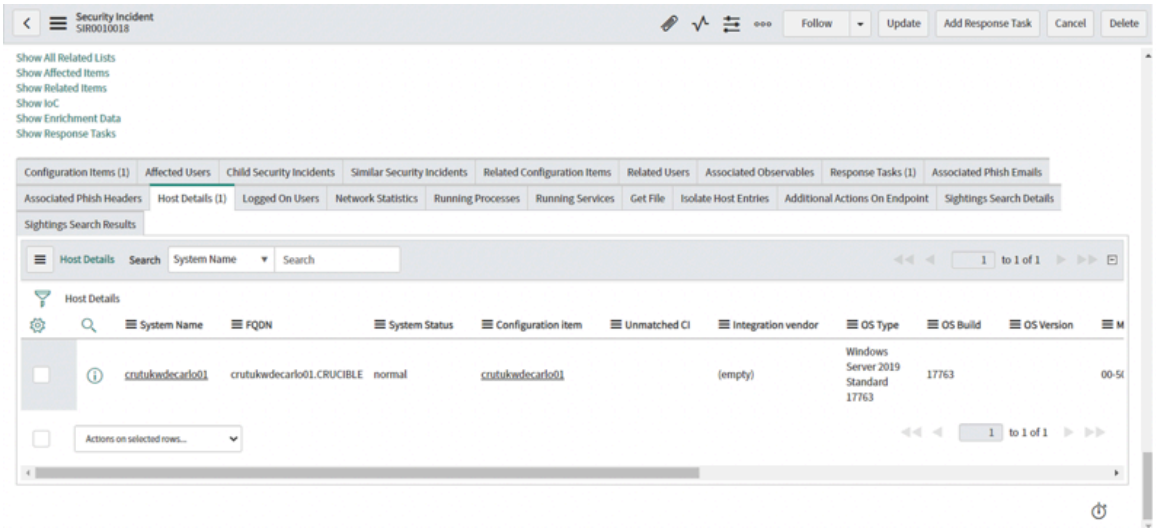


5. Revise a seção Anotações de trabalho e atividades.
6. Exiba os marcadores de perfil iniciado, perfil concluído ou perfil com falha.
7. Clique **Mostrar todas as listas relacionadas**.
8. Clique em qualquer lista relacionada (guia).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, Detalhes do host.



Acionar um perfil de capacidade FireEye a partir de links relacionados

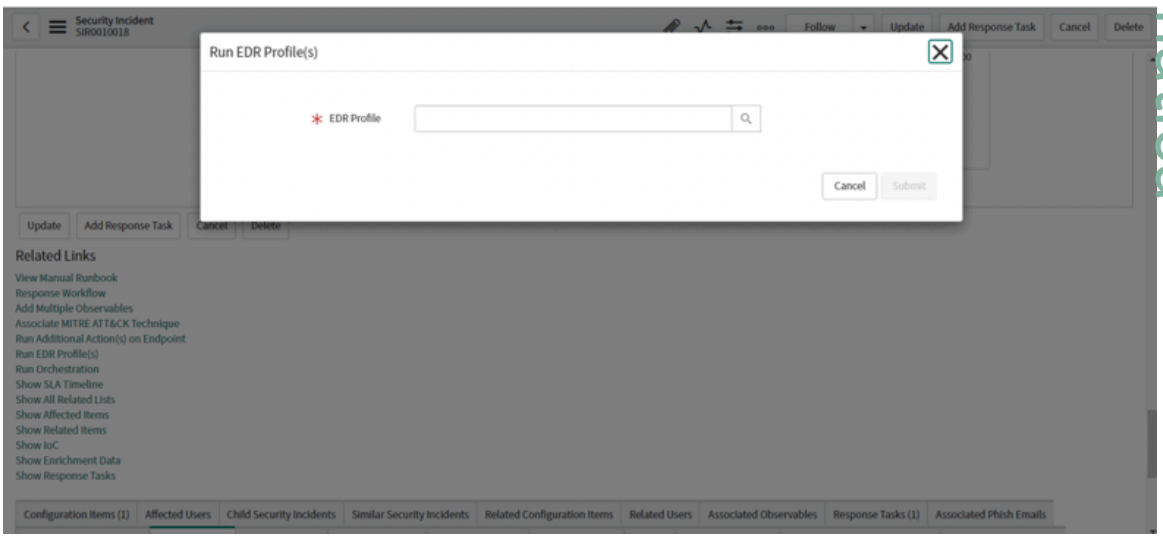
Acionar um perfil de capacidade manualmente depois de revisar um incidente de segurança a partir de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

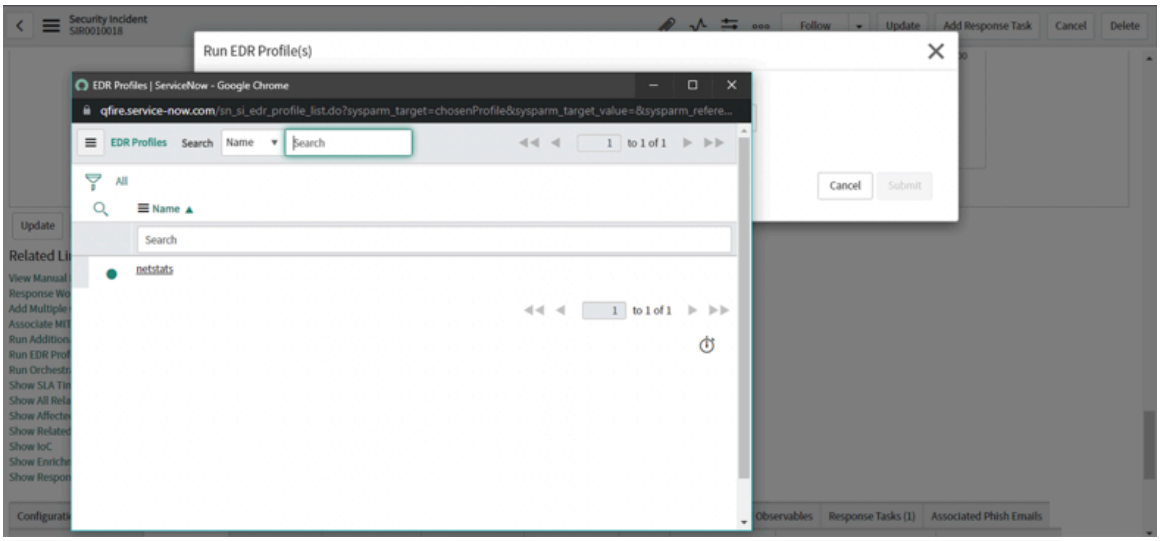
1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar.
3. Clique **Executar perfis de EDR**na seção links relacionados.

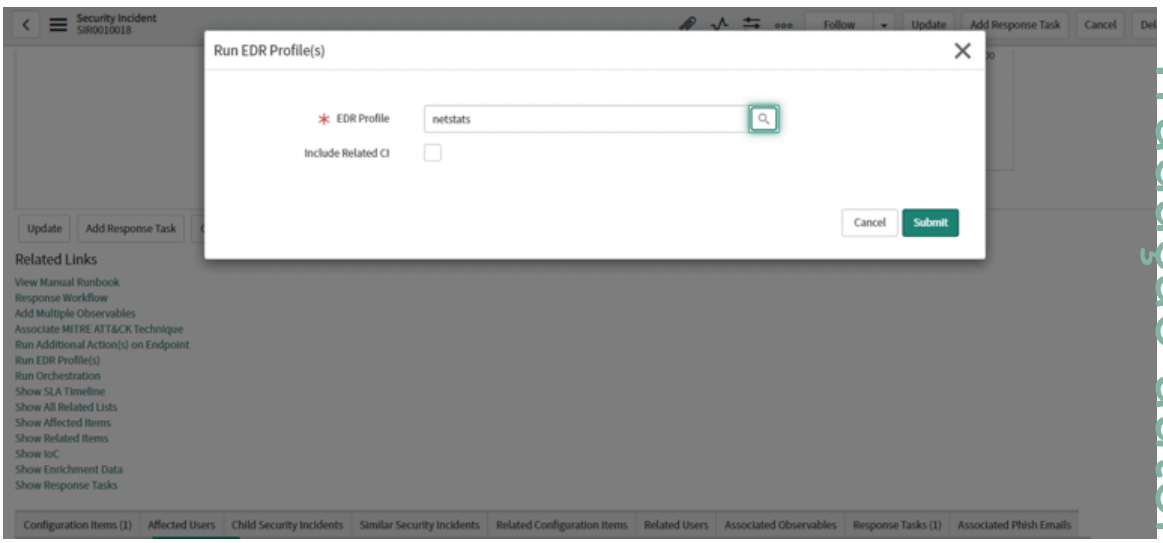


4. Procure e selecione um perfil na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

5. O perfil selecionado é acionado manualmente.
6. Revise a seção Anotações de trabalho e atividades.
7. Exiba os marcadores e verifique as listas relacionadas para os dados.

Nota: Além de executar o perfil para o IC ou o IC alternativo do incidente de segurança, você também pode executar o perfil para valores de IC presentes na lista relacionada Item de configuração marcando Incluir IC relacionado na caixa de diálogo. Também buscará dados para os valores de IC presentes na lista relacionada. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

Acionar um perfil de capacidade FireEye na lista relacionada Item de configuração

Acionar um perfil de capacidade manualmente na lista relacionada do item de configuração.

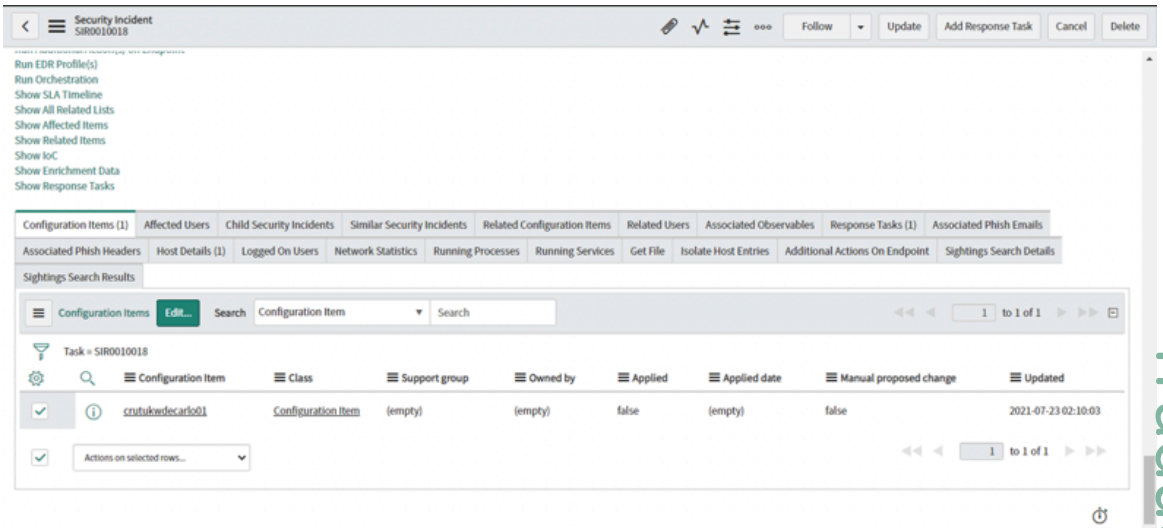
Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

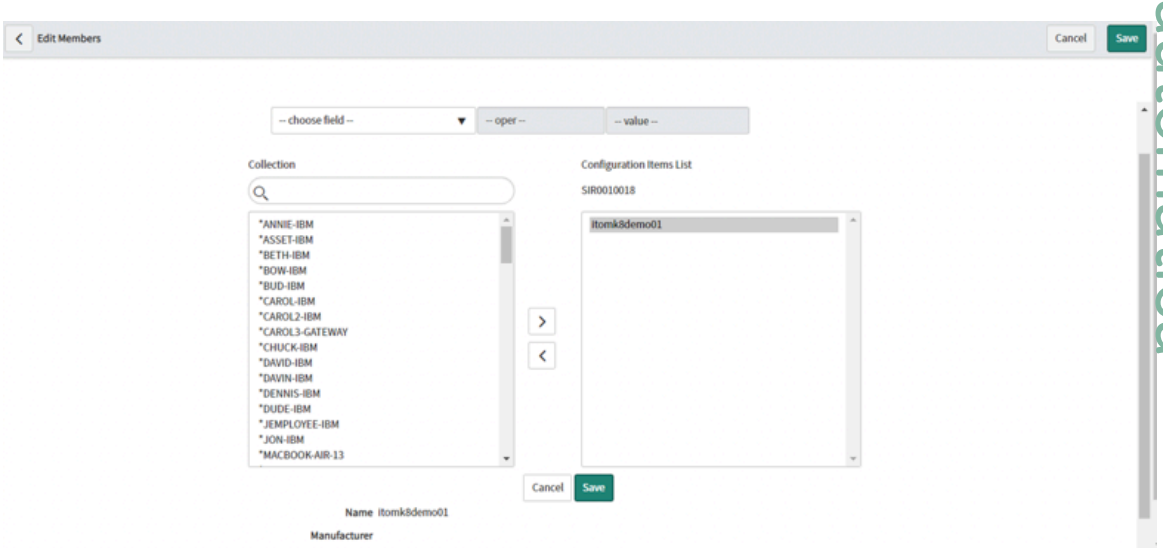
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com FireEye HX informações.
3. Clique **Mostrar todas as listas relacionadas** na seção listas relacionadas.
4. Clique no botão **Item de configuração** lista relacionada.



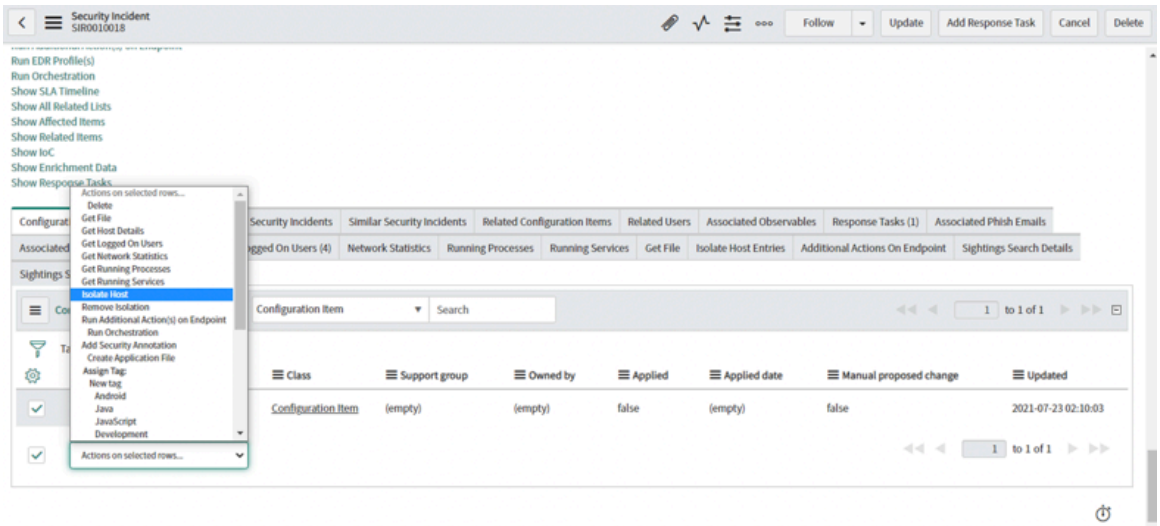
5. Clique **Editar** para adicionar os itens de configuração disponíveis, se os valores ainda não estiverem presentes, clique em **Salvar**.



6. Selecione os itens de configuração adicionados e, em Ações nas linhas selecionadas, selecione uma capacidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. A capacidade selecionada é acionada manualmente.
8. Revise a seção Anotações de trabalho e atividades.
9. Exiba os marcadores e verifique os dados nas listas relacionadas.

FireEye Obter recurso de arquivo

As solicitações de aquisição de arquivo instruem um agente de segurança de endpoint a obter um arquivo do endpoint do host. As aquisições de arquivos são usadas para análise estática ou dinâmica de possíveis compromissos ou verificados, bem como para retenção de evidências durante investigações de ameaças internas. Obter recurso de arquivo deve ser criado como um perfil separado.

Antes de Iniciar

Função necessária: administrador

Acionar Obter perfil de arquivo e criar um FireEye HX perfil de capacidade com **Obter arquivo** capacidade.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar.
3. Clique **Executar perfis de EDR**na seção links relacionados.
4. Procure e selecione Obter perfil de arquivo na lista de perfis disponíveis.
5. Forneça o. **Nome de arquivo** e **Caminho do arquivo**.

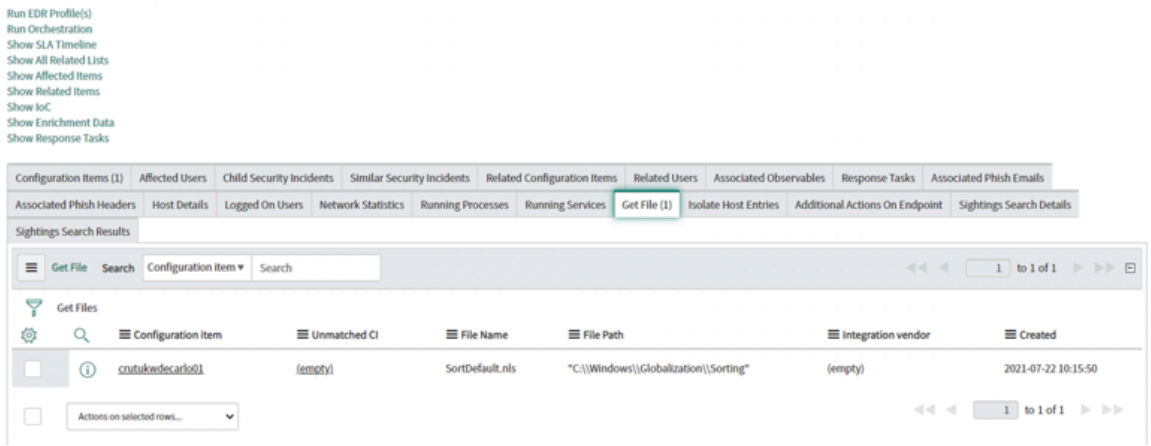
> **Nota:** Insira o nome do arquivo para o qual você deseja adquirir. Especifique um nome de caminho preciso ou outra variável de ambiente do Windows baseada em caminho apropriada. Você deve especificar a letra da unidade ou os nomes do caminho. Endpoints diferentes podem ter mapeamentos de unidade diferentes. Se você especificar explicitamente um nome de pasta, poderá encerrar o caminho com uma barra invertida. No entanto, a barra invertida final não é obrigatória.

6. Clique **Enviar**.
7. Revise a seção Anotações de trabalho e atividades.
8. Exiba os marcadores e verifique os resultados no **Obter arquivo** lista relacionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Obter perfil de arquivo agora é acionado manualmente.



Para revisar uma aquisição de arquivo baixada:

- Abra o arquivo .zip de aquisição de arquivo.
- Insira a senha necessária para abrir o arquivo. A senha pode ser exibida passando o mouse sobre o link de download em FireEye HX Console. Siga as etapas abaixo para exibir a senha:
  - Faça login no console FireEye HX.
  - Navegar até **Aquisições** E filtram por tipo de aquisição - Arquivo.
  - Selecione o registro desejado.

    Nota: Você poderá ver os detalhes do arquivo adquirido na guia à direita.

  - Passe o mouse sobre **Download** link disponível na parte superior para obter a senha.

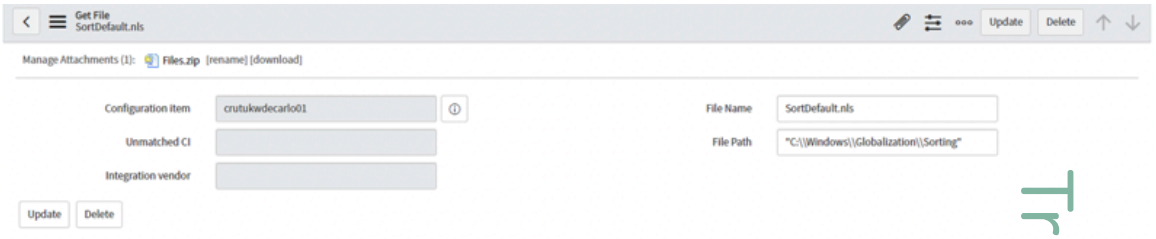
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

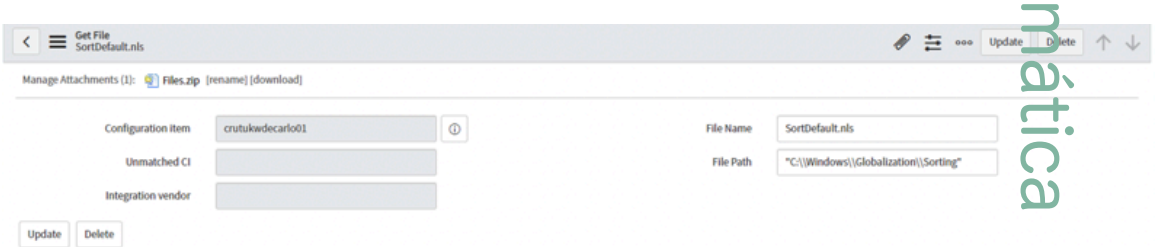
- Abra e revise os arquivos no arquivo .zip usando qualquer editor de texto ou XML.

Nota:

- É recomendável que o arquivo recuperado seja adicionado como observável manualmente, para que possa ser rastreado como uma evidência contra o incidente de segurança. Isso também ajudará a exibir os arquivos no futuro, quando a senha for esquecida ou alterada.
- O tamanho máximo de arquivo compatível com a ação Obter arquivo é de 1024 MB, e esse valor pode ser configurado alterando **com.glide.attachment.max_size**e o tempo limite padrão é de 60 minutos que pode ser configurado no FireEye HX Página Configurações padrão.



- Obter arquivo também pode ser acionado a partir da lista relacionada do item de configuração.



Tradução automática

Ações adicionais do FireEye no endpoint

A integração do FireEye oferece suporte à execução de ações adicionais além das ações padrão ouro.

Essas ações incluem aquisição de triagem e aquisições de dados. Duas aquisições de dados prontas para uso são compatíveis:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Script de detalhes investigativos abrangentes
- Script de detalhes investigativos padrão

Além disso, a aquisição de triagem também é compatível pronta para uso. Todos esses três são criados por padrão junto com a origem. Os clientes também podem criar suas próprias ações, ou seja, aquisições de dados do módulo de ações adicionais do FireEye.[1] O tamanho máximo de arquivo compatível com as ações adicionais do FireEye é 1024, e esse valor pode ser configurado alterando **com.glide.attachment.max_size**E o tempo limite padrão é de 120 minutos que pode ser configurado na página de configuração padrão do FireEye.

Script de detalhes investigativos abrangentes

Permite a coleta de todos os artefatos forenses e investigativos do endpoint, mas é a opção mais proibitivamente cara. Esta configuração é ideal para situações em que haverá apenas uma janela para coletar dados do endpoint em questão, e a capacidade de adquirir mais dados não pode ser garantida posteriormente. Portanto, use esta ação com cuidado.

Script de detalhes investigativos padrão

Habilita as opções mais comuns para coletar artefatos forenses e investigativos de um endpoint. Destinado a ser a ferramenta de resposta primária quando você suspeita de que um endpoint pode estar comprometido e precisa executar uma análise detalhada desse endpoint. O objetivo é encontrar um equilíbrio entre a recolha dos dados mais relevantes e valiosos, evitando as opções dispendiosas que podem ser recolhidas mais tarde, uma vez que uma investigação adicional as prove.

Aquisição de triagem

As coleções de triagem contêm informações do cache de lookback, bem como informações adicionais de auditoria forense, como histórico de download de URL, histórico de download de arquivos, listagens de processos e portas e informações padrão do sistema. Examinar essas informações quando um tráfego de rede anômalo é detectado e você deseja mais visibilidade das ações de endpoint.

Manutenção de scripts de aquisição de dados no FireEye

As solicitações de aquisição de dados (às vezes chamadas de solicitações de resposta em tempo real) permitem que você adquira todos os dados necessários de um único endpoint em execução. Usando a página Scripts de aquisição de dados no FireEye, você pode criar, editar, copiar e excluir os scripts de aquisição de dados usados para solicitações de aquisição de dados.

Acessar a página Scripts de aquisição de dados no FireEye

Para acessar a página Scripts de aquisição de dados:

1. Navegue até Endpoint Security Interface do usuário da web.
2. Selecione Scripts de aquisição de dados no menu Administrador.

Criando um script no FireEye

Para criar um script de aquisição de dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecionar **Scripts de aquisição de dados** > **Administrador** Menu da interface do usuário da web do Endpoint Security.
2. Clique **Criar script**.
3. Insira um nome para o novo script em **Nome do script** campo.
4. Opcionalmente, insira uma descrição do script.
5. Selecione o sistema operacional ao qual o script se aplica. Você só pode selecionar um único sistema operacional na caixa de diálogo Criar script.
6. Clique **Criar** para iniciar a definição do script.
7. Selecione um tipo de dados de aquisição no **Adicione um tipo de aquisição**e clique em **Adicionar**. As opções para o tipo de aquisição solicitado aparecem à direita da lista de scripts.
8. Forneça valores para as opções de tipo de aquisição ou use os valores padrão que já estão selecionados. A IU da Web não avisa você ou remove guias, espaços ou caracteres indesejados (como) em suas especificações.
9. Repita as 2 etapas anteriores para solicitar dados adicionais para o script de aquisição de dados. Alguns tipos de dados de aquisição estão disponíveis apenas uma vez para um script, enquanto outros podem ser especificados mais de uma vez. Depois de adicionar um tipo de aquisição a um script, a lista de tipos de aquisição estará disponível em **Adicione um tipo de aquisição**a caixa suspensa se ajusta adequadamente.
10. Para remover um tipo de dados de aquisição do script, clique no ícone x ( ) na guia aquisição no lado esquerdo da página.

Nota: Esta integração não é compatível com **Permitir edições antes de adquirir** ao criar scripts. Portanto, certifique-se de que a caixa de seleção esteja desmarcada.

Exportando um script do FireEye

Você pode exportar um script de aquisição de dados para um arquivo JSON. Para exportar um script de aquisição de dados:

1. Selecionar **Scripts de aquisição de dados** > **Administrador** Da interface do usuário da web do Endpoint Security.
2. Selecione Scripts de aquisição de dados no menu Administrador.
3. Selecione o script que você deseja exportar no lado esquerdo da página.
4. selecionar **Ações** > **Script de exportação**.
5. Um arquivo JSON é baixado para o seu computador. O nome do arquivo JSON inclui o sistema operacional para que você possa determinar facilmente quais scripts são para qual sistema operacional.

Criação de uma nova ação de aquisição de dados no ServiceNow AI Platform

Para criar uma nova ação, siga estas etapas:

1. Navegar até **Integração do FireEye** > **Ações adicionais do FireEye**. A lista Ações adicionais do FireEye é exibida.
2. Clique **Novo(a)**. O formulário da nova ação é exibido.
3. Preencha o formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Nome da ação FireEye que é executada. Este nome ajuda a identificar o tipo de ação e descrevê-lo.
Aquisição	Uma aquisição obtém os dados para analisar. Este é um campo somente leitura e é padronizado como Aquisição de dados.
Origem	Nome da origem do FireEye. Somente fontes configuradas estão disponíveis na lista de seleção.
Capacidade	Este é um campo somente leitura e é preenchido com a capacidade Executar ação(ões) adicional(is)
Tipo de aquisição	Tipo de ação de aquisição que precisa ser obtida e analisada.
Ativo	Indica que a Ação está ativa.
Requer Aprovação	Quando você habilita a opção Exigir aprovação, o campo Aprovadores fica disponível no formulário. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.
Marcador de exibição	Tipo de sistema operacional, como Windows, Mac, Linux, para adicionar scripts. **Nota:** Atualmente, há suporte para apenas um tipo de SO. Você pode criar uma ação por sistema operacional. Para outros sistemas operacionais, crie novas ações conforme necessário.
Scripts	O script importado do FireEye precisa ser fornecido para o Tipo de SO selecionado. Somente um script pode ser adicionado a cada tipo de SO.

4. Clique **Enviar**.

Acionar aquisições de dados do incidente de segurança

As Ações adicionais criadas podem ser executadas por meio do Link relacionado chamado **Executar ações adicionais no endpoint** no incidente de segurança.

Nota: **Permitir edições antes de adquirir** A funcionalidade FireEye não é compatível com as Ações adicionais no endpoint.

Configure um perfil para pesquisa de vistas com o FireEye Integration

Configure o perfil de pesquisa de vistas usando o procedimento a seguir.

Antes de Iniciar
NowPlatform Administrador de incidentes de segurança (sn_si.admin)

Sempre que uma origem é criada, as configurações de pesquisa de vistas individuais para cinco tipos (Arquivo, IPs(v4), MD5, SHA1 e SHA256) serão criadas e inativas por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você deve ativá-lo antes de usar a Pesquisa de vistas. Cada tipo de observável tem uma consulta de pesquisa diferente para recuperar vistas. Iniciaremos uma pesquisa diferente para cada tipo de observável. A pesquisa de vários observáveis para uma pesquisa de observação não é possível no FireEye, pois ele executaria uma operação AND nos observáveis e o resultado pode ser impreciso.

Nota: Para a pesquisa de vistas, somente cinco pesquisas ativas podem estar presentes de uma vez. O restante será enfileirado e começará após a conclusão de qualquer uma das vistas em andamento.

Se você quiser criar um novo perfil de pesquisa de vistas, siga as etapas abaixo para criar um:

Procedimento

1. Navegar até **Integrações** > **Configuração da Pesquisa de detecções**.
2. Clique **Novo(a)**.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do perfil de capacidade.
Pesquisa salva	Isso executará uma pesquisa salva, ou seja, o campo de Nome deve corresponder ao nome da pesquisa salva.
Origem da pesquisa de detecções	Define a origem configurada para a integração.
Pesquisar	Adicione uma cadeia de caracteres de pesquisa nativa para formar uma consulta.
Ativo	A consulta será executada somente se estiver ativa.
Tipo de observável	Define o tipo de categoria de observável.
Máximo de observáveis por pesquisa	O número de observáveis antes da consulta de pesquisa é dividido em várias consultas. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de vistas	Use os parâmetros de pesquisa de detecções para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado.

4. Clique **Enviar** para concluir a configuração.

Invocar Pesquisa de vistas de um incidente de segurança

Invoque a pesquisa de vistas de um incidente de segurança SIR seguindo o procedimento abaixo.

Antes de Iniciar

Função necessária: ServiceNow AI Platform administrador (sn_si.admin)

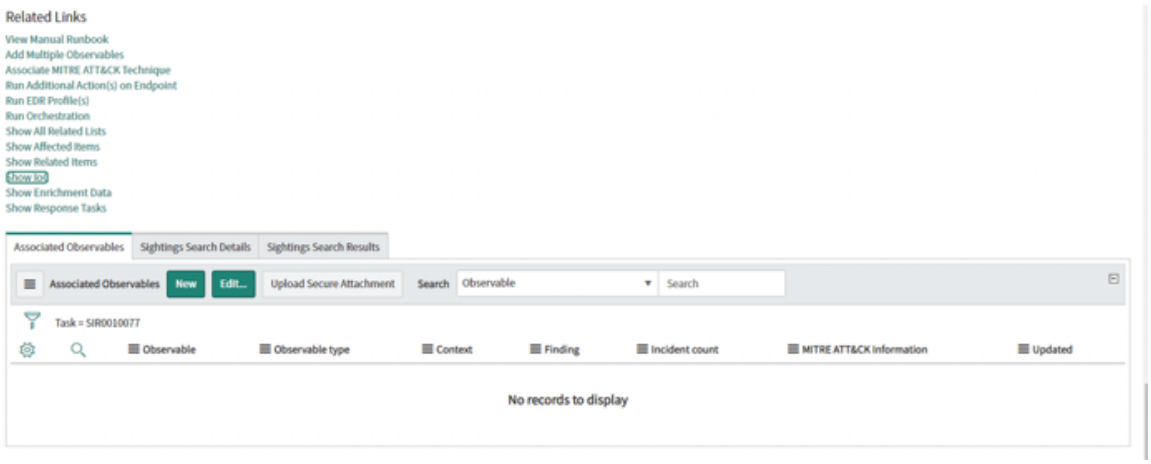
Procedimento

1. Navegue até Incidentes de segurança.
2. Abra qualquer SIR existente ou crie um novo SIR.

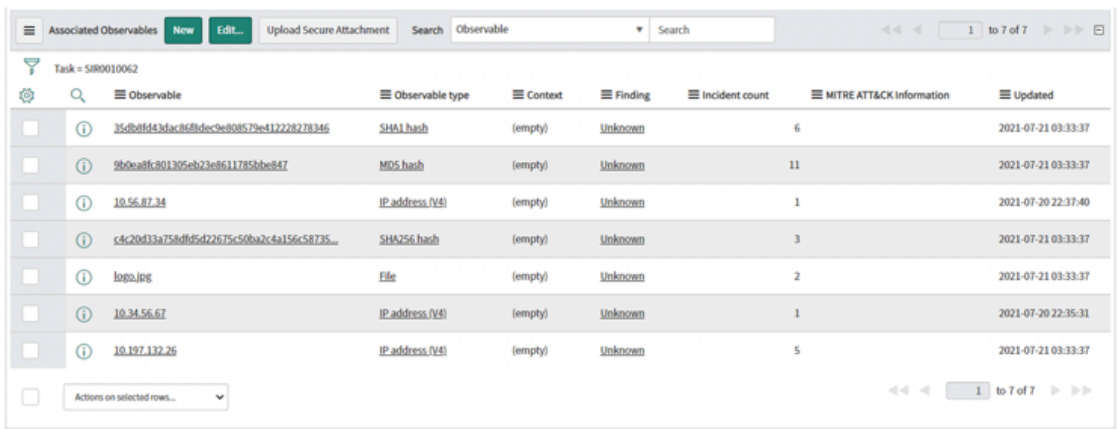
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

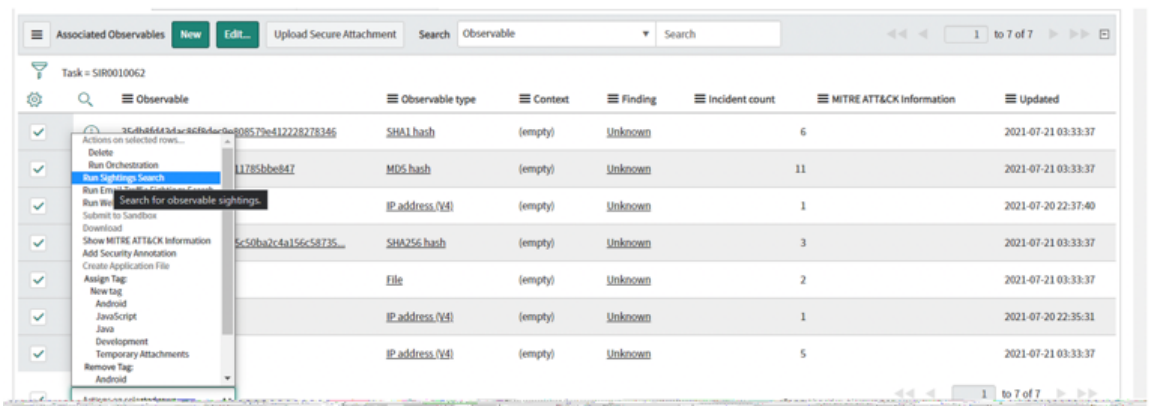
3. Clique em Mostrar IOC em Links relacionados.
4. Clique **Observáveis Associados** listas relacionadas.



5. Adicione observáveis existentes ou crie um novo observável.



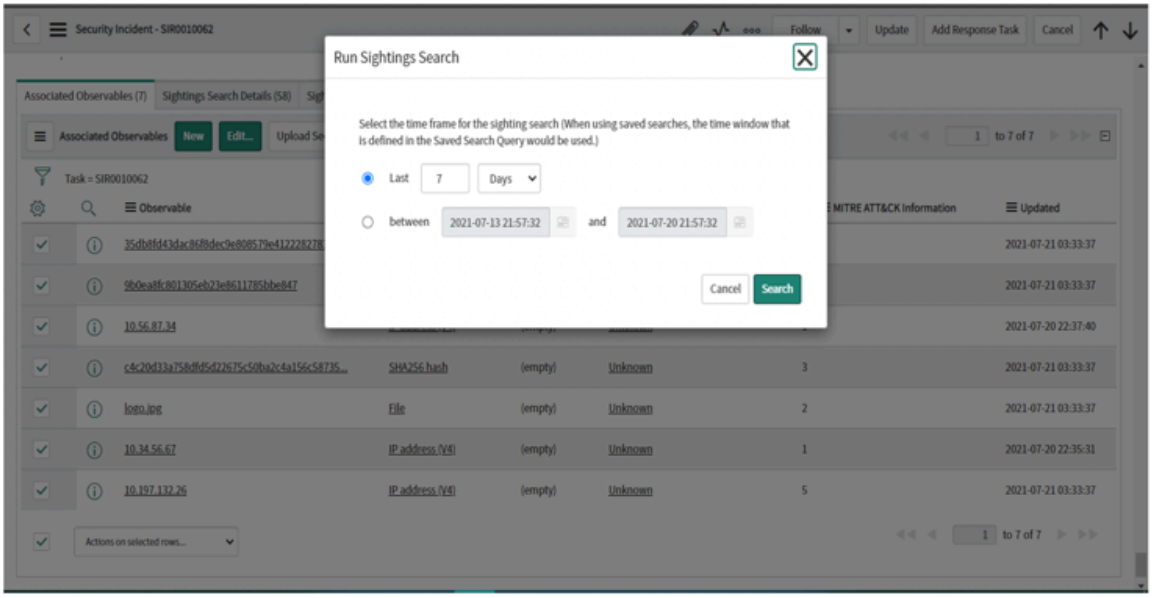
6. Selecione os observáveis e, em Ações nas linhas selecionadas, clique em **Executar Pesquisa de detecções**.



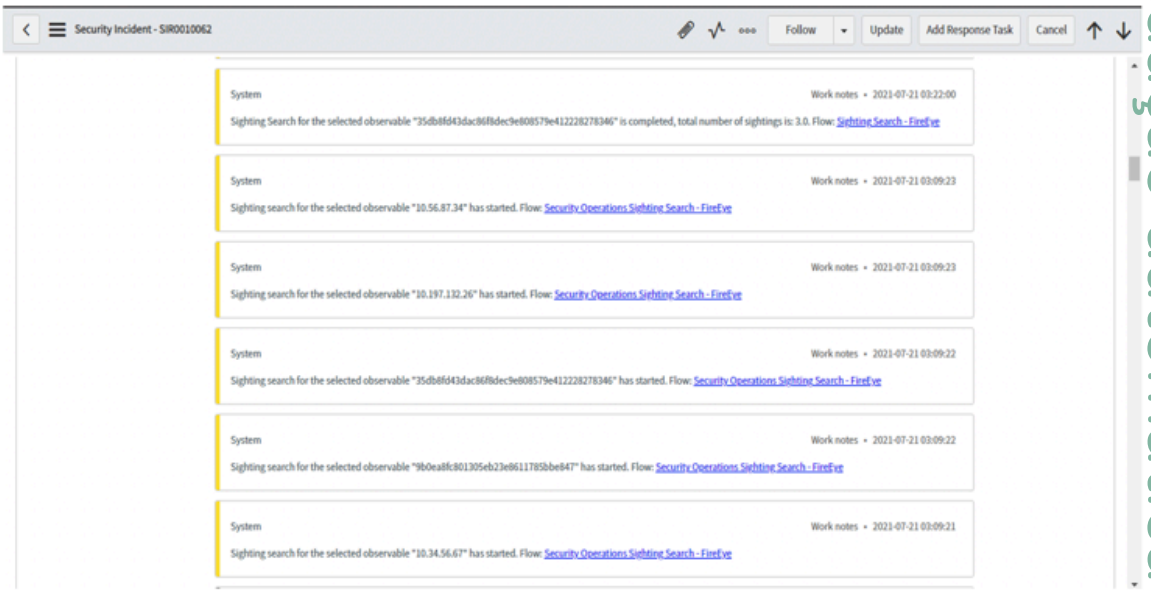
7. Ignore as entradas na próxima caixa de diálogo que solicita dados de tempo.
   Há valores padrão preenchidos. No entanto, a pesquisa é realizada em tempo real e os valores de tempo são ignorados para esta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



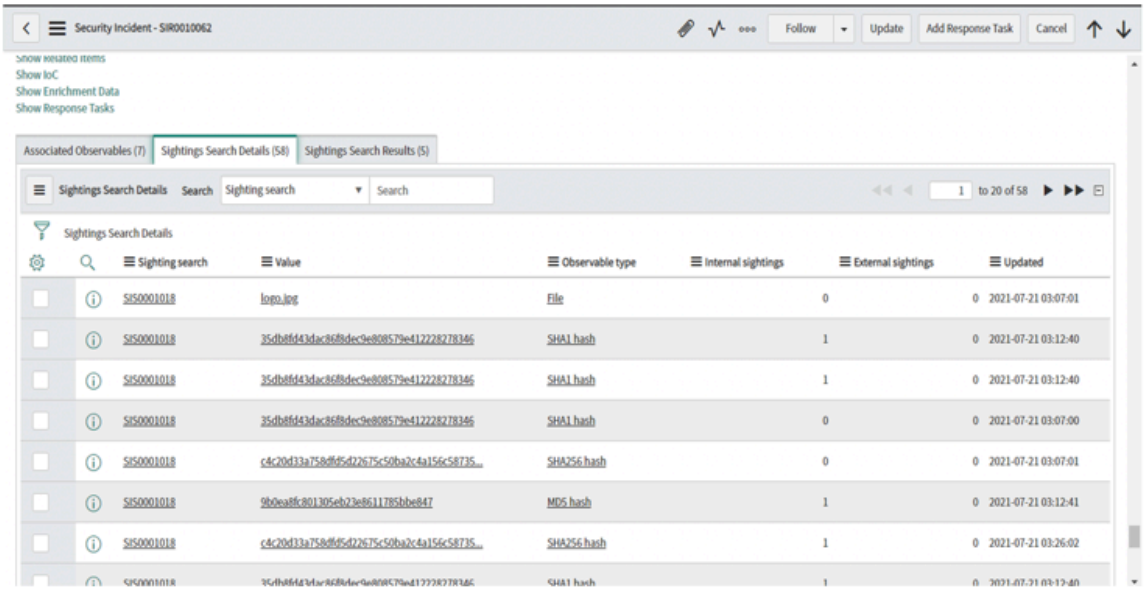
8. Verifique o status das anotações de trabalho.

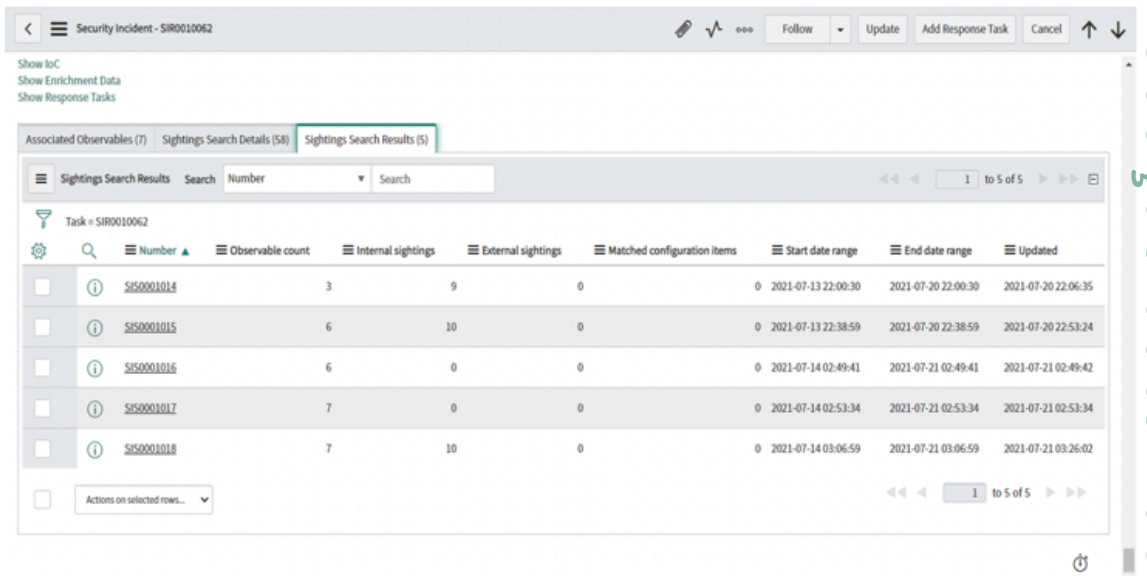


9. Ao concluir a pesquisa, verifique os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes de Pesquisa de detecções** para obter detalhes e. **Resultados da pesquisa de detecções** guia para resultados da pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

Have I been pwned? integração

. Operações de segurança Have I been pwned? a integração permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

- Have I been pwned? configuração de integração
- Ativar

Usar

Realizar pesquisas em observáveis Pesquisa de ameaças - Have I been pwned? fluxo

Desenvolver

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Have I been pwned? configuração de integração

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido à conta on-line ter sido comprometida ou "pungida" em uma violação de dados. Ele se integra facilmente ao Operações de segurança.

Antes de poder usar Have I been pwned? integração, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

. Resposta a incidentes de segurança, Inteligência contra ameaças e Operações de segurança Have I been pwned? plug-ins são necessários para implementar o. Operações de segurança Have I been pwned? integração.

Pesquisa de ameaças - Have I been pwned? fluxo

A Pesquisa de ameaças - Have I been pwned? o fluxo executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, os observáveis são verificados em busca de malware e os resultados são retornados.

Função necessária: sn_si_admin

Este fluxo é acionado pelo Integração de operações de segurança - Recurso de pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis, e o. Have I been pwned? a implementação está selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Eu tenho sido pwwned fluxo



Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Ativar

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Operações de segurança Have I been pwned? integração. Antes de poder usar Have I been pwned?, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser instalado e ativado antes que você possa usar Operações de segurança Have I been pwned? Integração.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.
Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereços do navegador.
   Por exemplo: `https://<3rdparty>/` .

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e clique em **Segurança** guia.

   d. Clique em **Exibir certificado** e clique em **Detalhe** guia.

   e. Clique em **Exportação** Para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Deve começar com `------ INICIAR CERTIFICADO------` e termine com `------ CERTIFICADO FINAL-------` .

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e. crie um novo registro para a integração.
4. Em **Certificado PEM** cole o certificado baixado e copiado para a área de transferência anteriormente.
5. Adicione o certificado ao registro do Provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até **Certificados X.509** lista relacionada e clique em **Editar** .
   d. Mova o certificado recém-criado para **Selecionado** coluna.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Nota: Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituição de um certificado SAML prestes a expirar .

HPE Security ArcSight ESM - Integração do analisador de e-mail

A integração do HPE Security ArcSight ESM - Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configure a integração do HPE Security ArcSight ESM - Analisador de e-mail

HPE Security ArcSight ESM - A integração do analisador de e-mail usa notificações por e-mail do ESM para impulsionar fluxos de trabalho de aprimoramento e resposta.

Antes de Iniciar

Função necessária: sn_si_admin

Tradução automática

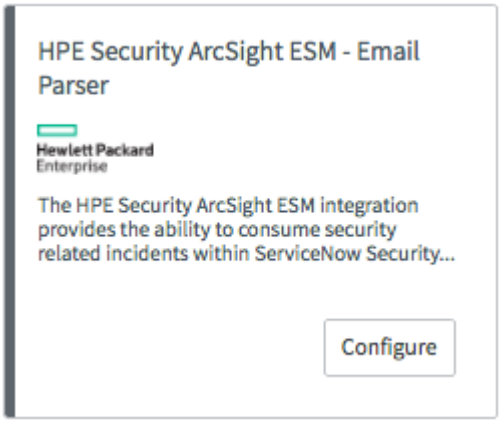
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Um modelo HPE Security ArcSight ESM - Analisador de e-mail é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão HPE Security ArcSight ESM - Analisador de e-mail, clique em **Configurar** .
3. Em **HPE Security ArcSight ESM - Configuração do analisador de e-mail** na caixa de diálogo, clique em **Configure o analisador de e-mail** link.
4. Clique em **ArcSight ESM** link para editar as configurações no analisador de e-mail do modelo fornecido. No mínimo, preencha O e-mail é de campo. Para criar seu próprio analisador de e-mail, consulte Crie analisadores de e-mail em Operações de segurança.
5. Verifique **Ativo** caixa.
6. Clique em **Atualização** em **Analisador de e-mail** formulário.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração** .

HPE ArcSight Logger Integração de aprimoramento de incidentes

. HPE ArcSight Logger- A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos incidentes de segurança.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

- Comece a usar HPE ArcSight Logger
- Criar registros de configuração de pesquisa de vistas

Usar

- Execute uma Pesquisa de vistas
- Integração de operações de segurança - Fluxo de pesquisa de vistas

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Operações de segurança - Fluxo de pesquisa de vistas do Arcsight Logger
- Exibir detalhes da pesquisa de vistas
- Exibir resultados da pesquisa de vistas
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Comece a usar HPE ArcSight Logger

HPE ArcSight Logger transmite dados em tempo real e categoriza-os em logs específicos e se integra facilmente ao Operações de segurança. Antes de poder usar HPE ArcSight Logger- Integração de aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicionar URL de API e credenciais de login.

Antes de Iniciar

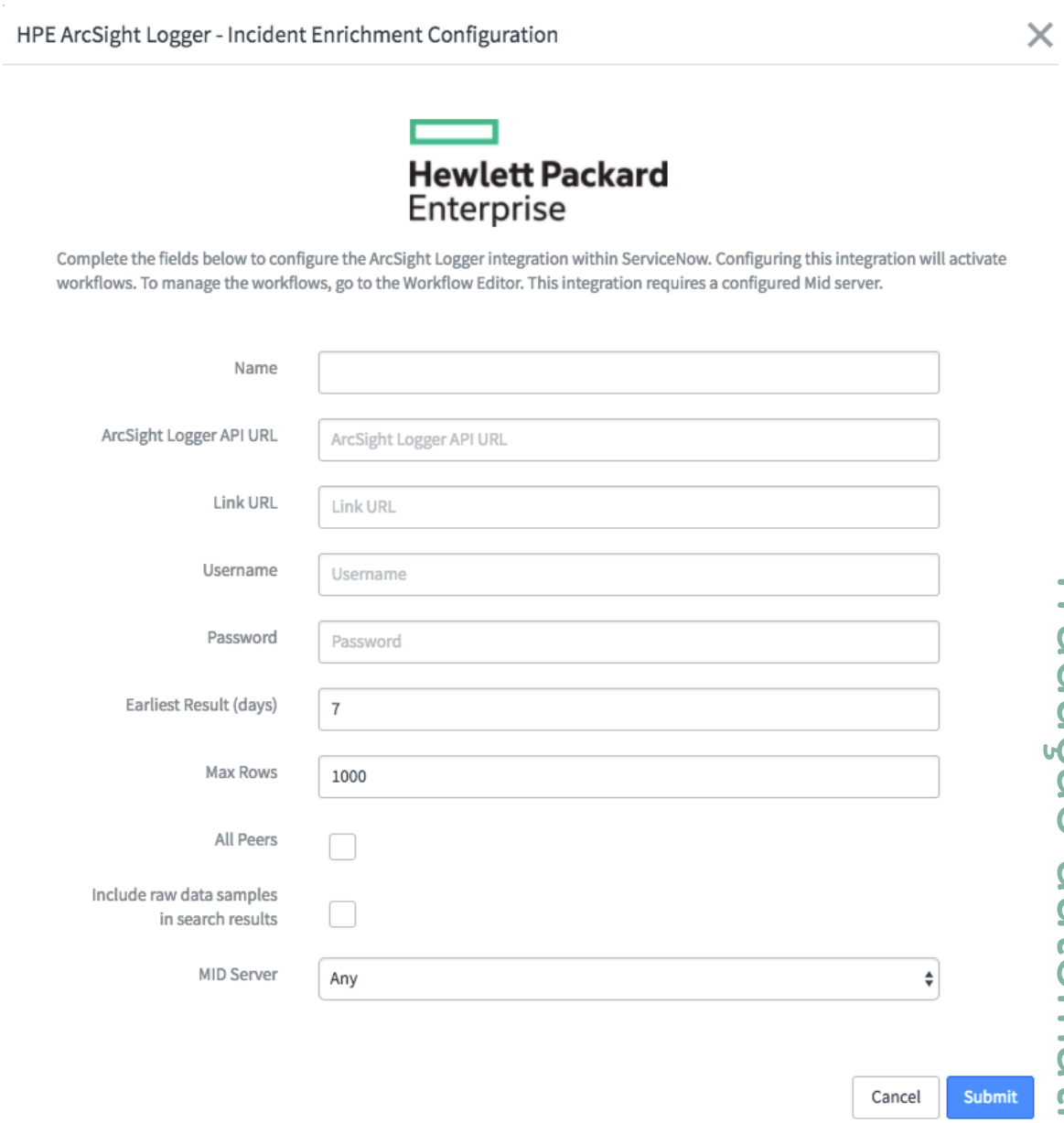
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. Em HPE ArcSight Logger- Cartão de aprimoramento de incidente, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

4. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de base da API do ArcSight Logger	O URL base que você adquiriu no site do HPE Security ArcSight Logger.
URL do Link	[Opcional] O URL do link vinculado a uma instância do HPE Security ArcSight Logger, quando disponível.
Nome do usuário	Sua Intel HPE ArcSight Logger nome de usuário.
Senha	Sua Intel HPE ArcSight Logger senha.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Todos os Pares	O padrão é desmarcado e pesquisa somente o agente de log local ao qual você está conectado. Quando marcado, ele pesquisa todos os loggers que estão conectados uns aos outros.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no **número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Análise híbrida integração

. Análise híbrida A aplicação faz parte de uma comunidade on-line aberta na qual os usuários analisam arquivos e URLs em busca de ameaças. Você compartilha resultados e utiliza pesquisas da comunidade para obter respostas a incidentes mais eficazes. Quando integrado ao ServiceNow AI Platform Operações de segurança, a inteligência contra ameaças compartilhada fornece informações adicionais sobre a gravidade de observáveis específicos.

. Análise híbrida a integração executa pesquisas de ameaças nos seguintes observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

O fluxo verifica se há novos observáveis conforme eles chegam em incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração de API, os observáveis serão avaliados. Observáveis determinados como mal-intencionados são marcados.

Instalar e configurar

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para Análise híbrida a aplicação se integra corretamente com ServiceNow AI Platform Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador (admin) instala o app e atribui a função Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao Operações de segurança e atribui a função sn_si.analyst.
Obtenha uma chave de API.	Visite Análise híbrida Site para obter informações sobre chaves de API e para criar uma conta: Site de análise híbrida . A configuração requer que você insira as chaves de API.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Para a versão Madrid e versões posteriores da família, o plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações. A seguir Operações de segurança as aplicações devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila: **1.** Framework de integração de segurança **2.** Security Support Common **3.** Orquestração do suporte de segurança **4.** Resposta a incidentes de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Execute as etapas a seguir para atualizar as propriedades do sistema e instalar e configurar a integração.

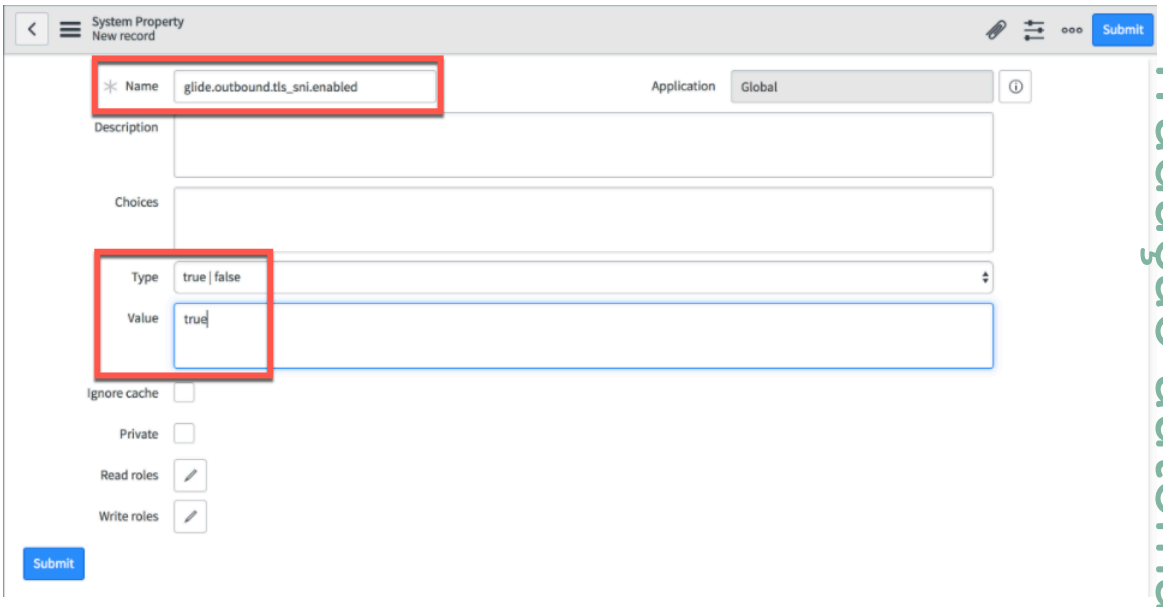
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No filtro de navegação, insira `sys_properties.list` e pressione **Insira** .
   . **Propriedades do sistema** a lista é exibida.
2. Clique em **Nova**.
   Um novo registro é exibido.
3. Preencha os campos ou selecione os valores listados na tabela a seguir e clique em **Enviar** .

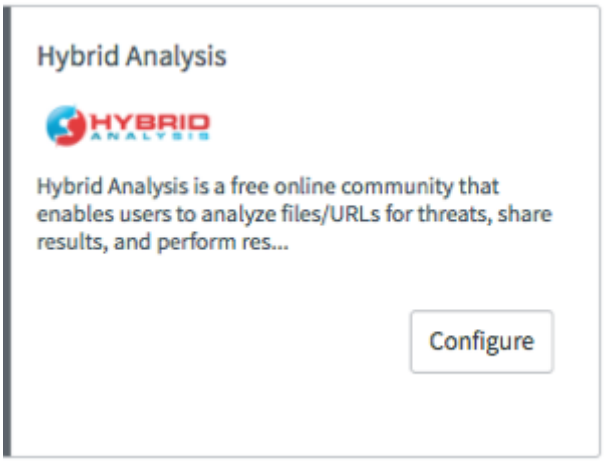
Nome do campo	Valor
Nome	glide.outbound.tls_sni.enabled
Tipo	Selecione **verdadeiro I falso**
valor	verdadeiro



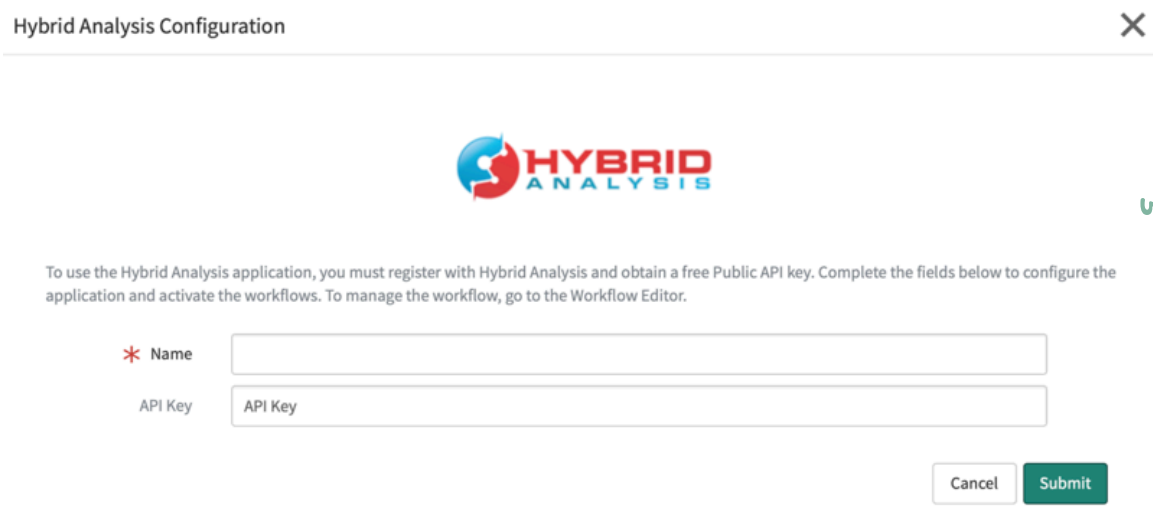
4. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
5. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize Análise híbrida lado a lado.
6. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Em **Configuração de análise híbrida** , insira a chave de API que você obteve do Análise híbrida site e clique **Enviar** .



8. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, o Análise híbrida A chave de API pode ser inválida.

Verifique os resultados esperados

Observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Localize os resultados da pesquisa no incidente de segurança para verificar se a pesquisa de ameaças foi executada com sucesso. Exiba também dados brutos e execute pesquisas de ameaças em observáveis secundários.

Antes de Iniciar

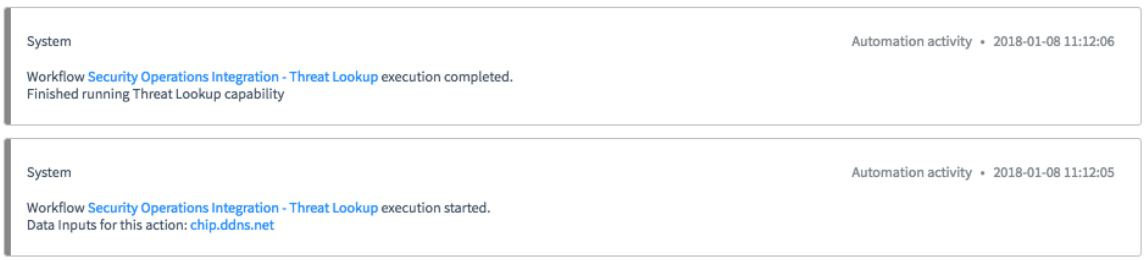
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

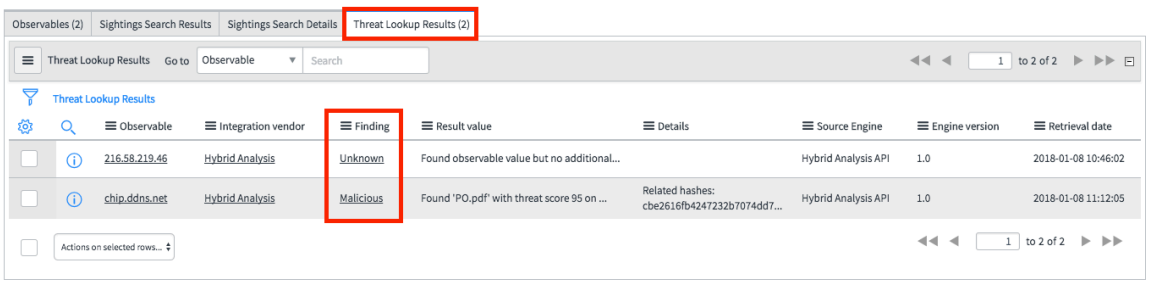


   Depois que a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações sobre como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

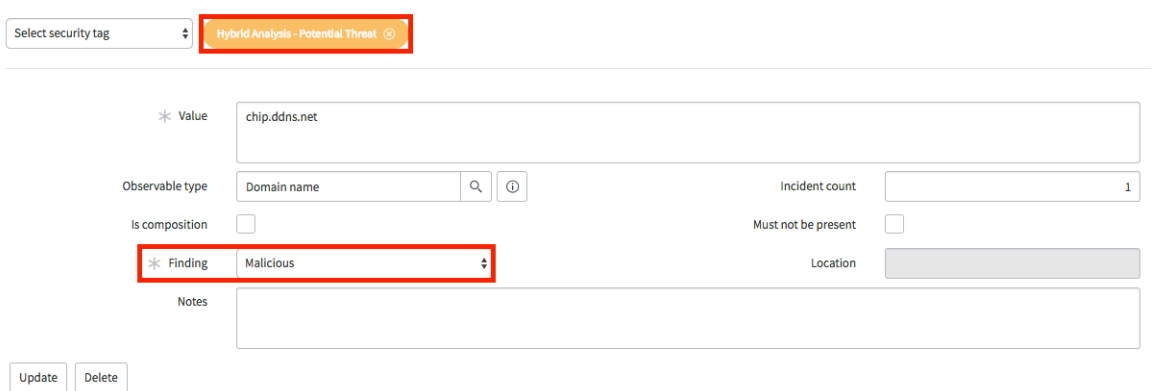
3. Navegue até a parte inferior do registro de incidente de segurança e clique em **Mostrar todas as listas relacionadas** link relacionado para exibir resultados.

   Nota: As figuras nas etapas a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema. No canto superior direito da moldura da faixa, clique no ícone de engrenagem Configurações. Em **Configurações do sistema** caixa de diálogo exibida, clique em **Formulários** e verifique isso **Formulários com guias** e. **Com o formulário** selecionados.



   . **Resultados da pesquisa de ameaças** exibe os resultados da pesquisa na parte inferior do registro do incidente de segurança. Observe **Descoberta** a coluna é exibida Desconhecido para registros não determinados como mal-intencionados. Para resultados correspondentes a mal-intencionados, o. **Descoberta** a coluna é exibida Mal-intencionado .

4. Em **Observável** , clique em um observável para abrir o registro.



Tradução automática

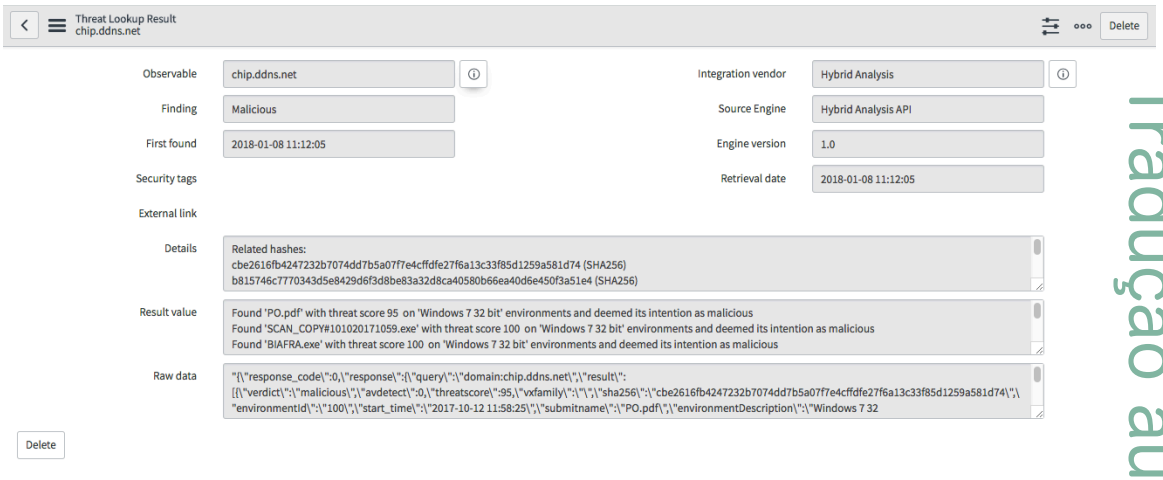
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para pesquisas correspondentes a mal-intencionadas, o. **Descoberta** o campo é exibido Mal-intencionado e o observável é marcado com Inteligência contra ameaças origem que descobriu que era mal-intencionado, neste caso, o. Análise híbrida integração.

5. **Opcional:** Siga as etapas para exibir dados brutos, exibir uma lista de observáveis secundários e executar uma pesquisa de ameaças em observáveis secundários selecionados.

   a. Navegue de volta para o incidente de segurança e no **Resultados da pesquisa de ameaças** clique no ícone azul de informações ao lado de um observável.

   b. Na janela exibida, clique em **Registro em aberto** para exibir os dados.
   De todos os observáveis visíveis nos dados brutos exibidos na pesquisa, o. Análise híbrida a integração também cria observáveis secundários ou relacionados.



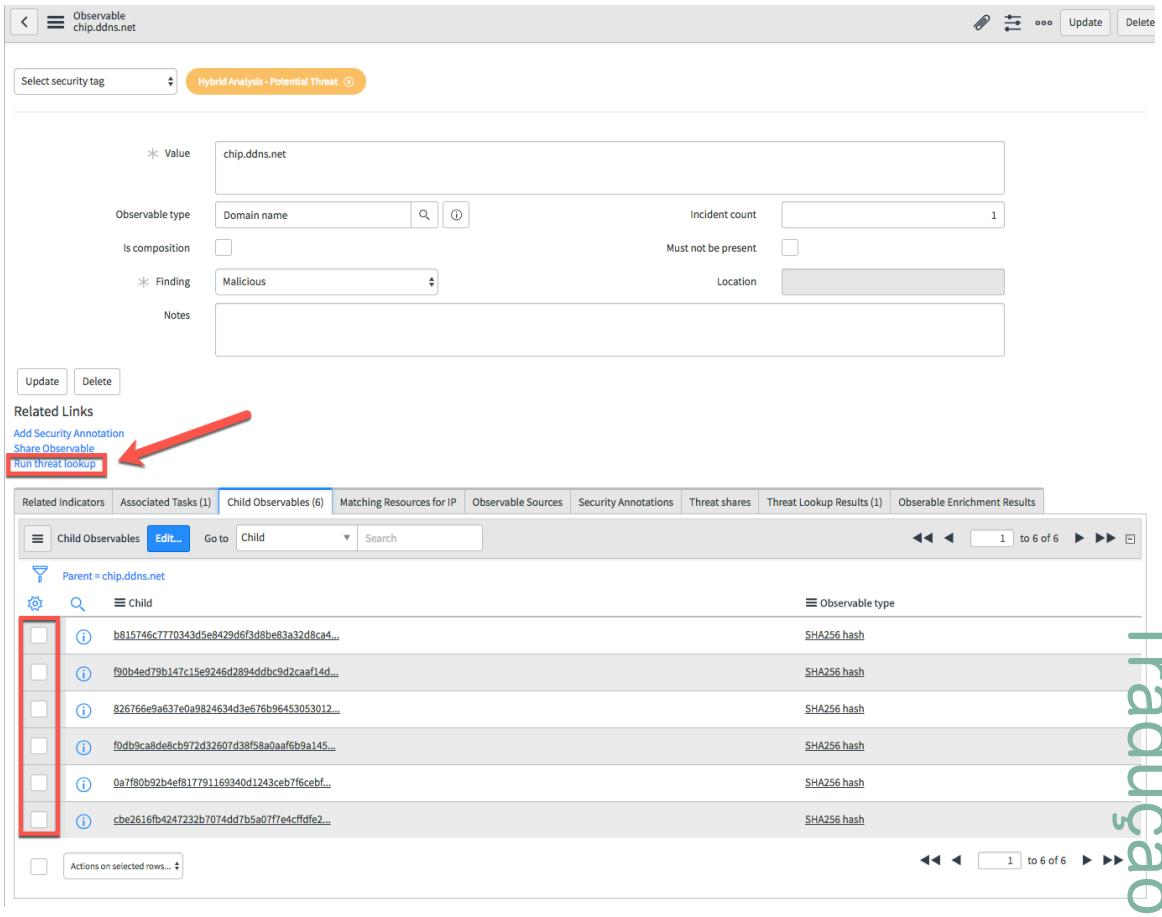
   O link criado pela API, os dados brutos e outras informações são exibidos.

   c. Navegue de volta para o incidente de segurança e clique em **Mostrar IOC** link relacionado.
   Os observáveis secundários são exibidos no **Observáveis secundários** no incidente de segurança, porque a pesquisa encontrou uma conexão existente entre esses observáveis relacionados e o observável enviado inicialmente.

   d. Clique no campo ao lado de um observável no **Secundário** coluna para selecioná-la, seguida por **Executar pesquisa de ameaças** link relacionado para executar uma pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na caixa de diálogo exibida, verifique se Análise híbrida a integração é selecionada e clique em **Enviar** .

f. Nas anotações de trabalho, verifique se a pesquisa foi executada com sucesso e no **Resultados da pesquisa de ameaças** no incidente de segurança, localize os resultados da pesquisa para os observáveis secundários.

Trouble?

Se você não vir resultados em **Resultados da pesquisa de ameaças** verifique se o observável é um tipo compatível com pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Análise híbrida

Você pode anexar observáveis manualmente quando quiser executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

Antes de Iniciar

Verifique se o observável é de um tipo compatível com a integração. A integração executa pesquisas nos seguintes tipos de observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

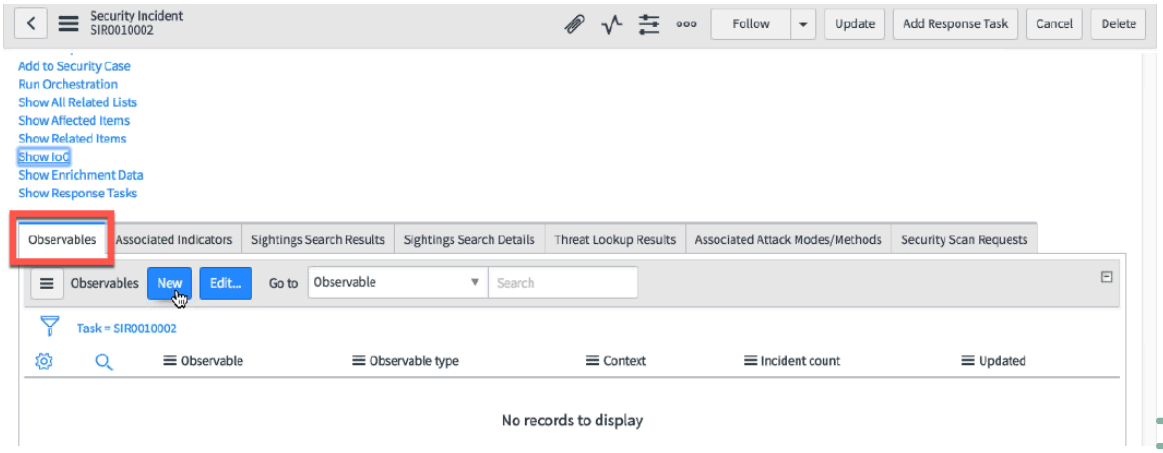
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

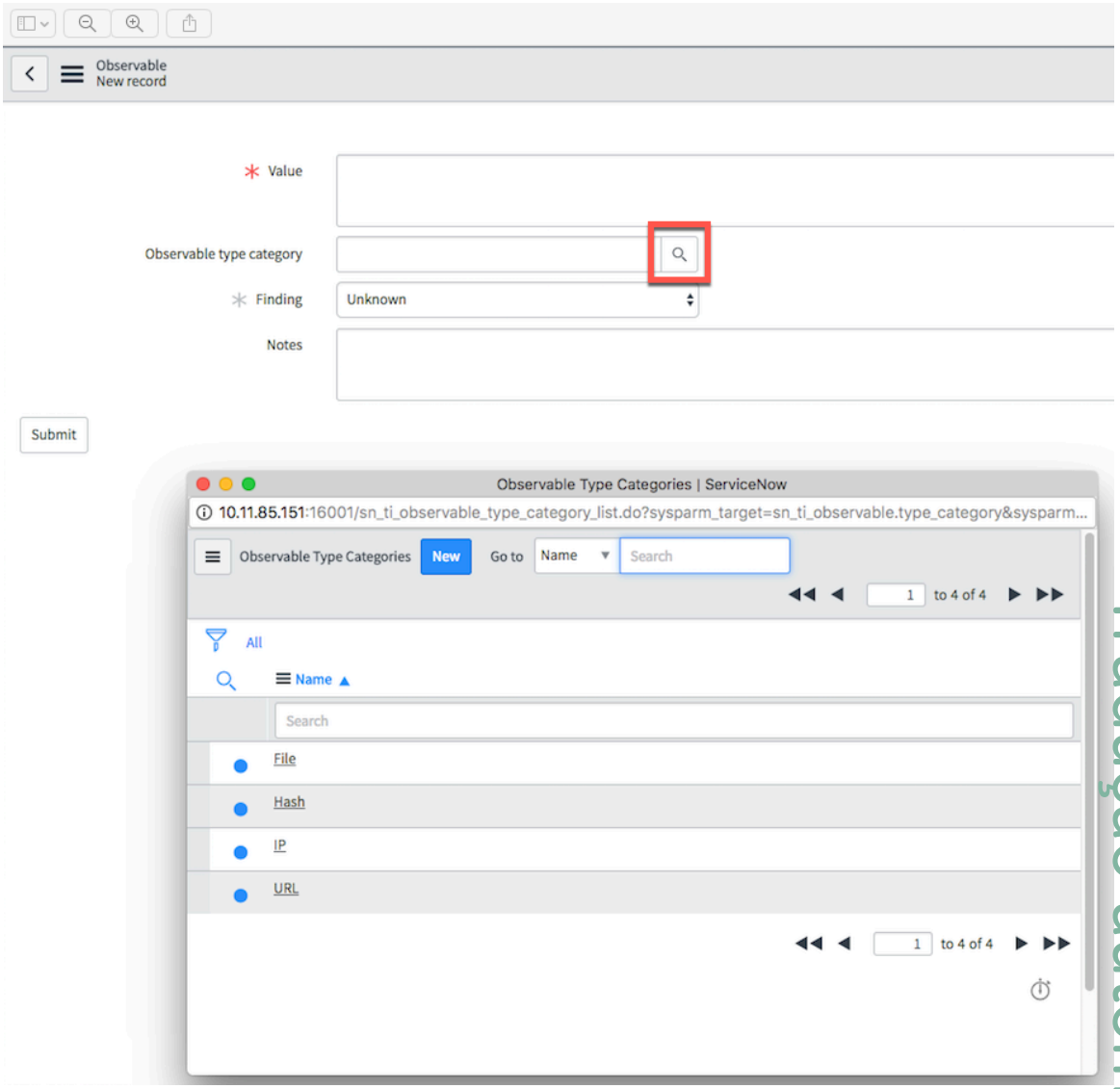
1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. Em Incidente de segurança aberto, clique em **Mostrar IOC** link em **Links relacionados** .



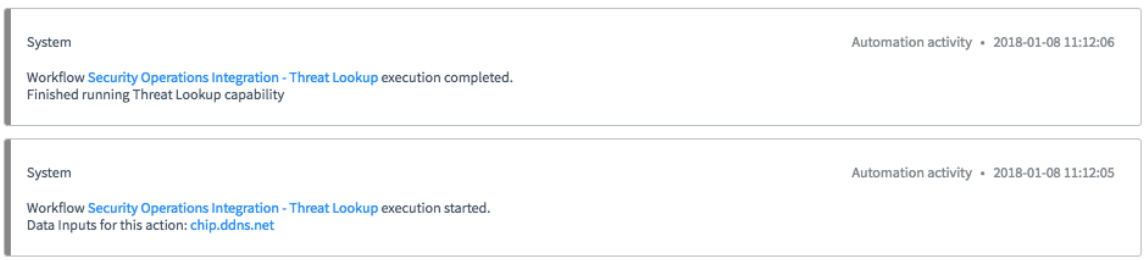
3. Em **Observáveis** clique em **Novo** .
   O formulário Observável é exibido.
4. Em **Valor** Insira um observável (hash de arquivo, endereços IP ou URL).
5. Clique no ícone de pesquisa e no **Categorias de tipo de observável** , clique no tipo de observável desejado na lista para preencher o campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



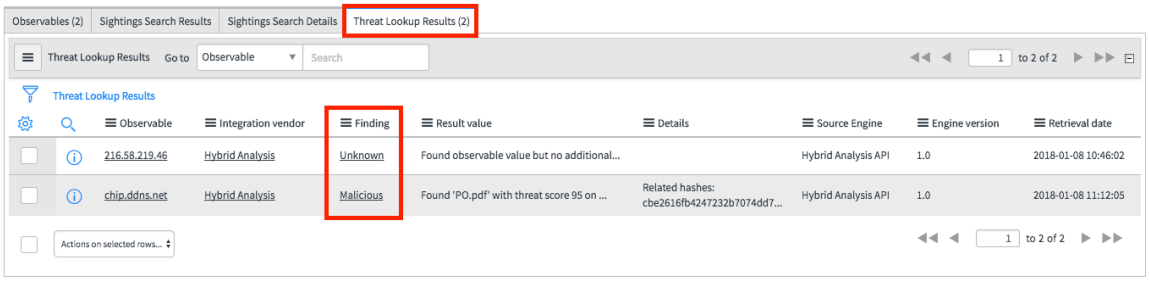
6. Clique em **Enviar**.
   O fluxo é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção Anotações de trabalho no registro de incidente de segurança.
7. Navegue até o incidente de segurança e revise as anotações de trabalho.



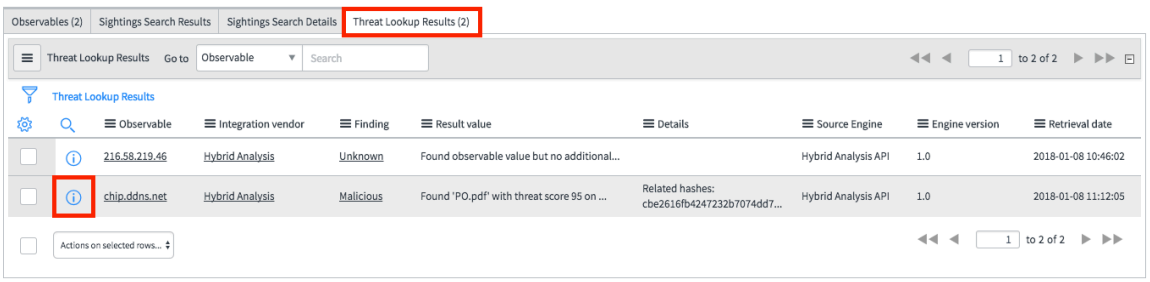
8. Na parte inferior do registro, clique em **Mostrar todas as listas relacionadas** link relacionado.
9. Clique em **Resultados da pesquisa de ameaças** para exibir os resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Em **Observável** , clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.



11. Na caixa de diálogo exibida, clique em **Registro em aberto** para exibir os dados brutos e mais detalhes. Como alternativa, você também pode anexar um observável existente ao registro de incidente de segurança.
12. **Opcional:** Com **Observáveis** selecionada, clique em **Editar** .
13. **Opcional:** Em **Editar membros** mover um observável existente do formulário exibido **Coleção** . **Lista de observáveis** e clique em **Salvar** .
    Você retornará ao incidente de segurança.
14. Na coluna extrema esquerda, selecione os observáveis nos quais você deseja executar a pesquisa e em **Ações nas linhas selecionadas...** lista de seleção, selecione **Executar pesquisa de ameaças** .
    Uma mensagem é exibida na parte superior do registro informando que a solicitação está sendo processada. Verifique se a pesquisa foi executada com sucesso.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

IBM QRadar Offense Ingestion Integração

. IBM QRadar Offense Ingestion a integração permite que você busque automaticamente IBM QRadar e converta-os em incidentes de segurança e habilite ações de resposta automatizadas.

Esta integração oferece suporte ao seguinte:

- Descoberta de IBM QRadar infrações candidatas a incidentes de segurança.
- Buscando eventos ou fluxos recentes associados a uma infração.
- Rastreie as principais atualizações de infrações periodicamente.
- Mapeamento de campos de infração, evento e fluxo para campos de incidente de segurança.
- Exibição preliminar dos campos mapeados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configure ingestões programadas de infrações para criar incidentes de segurança periodicamente.
- Encerre as infrações quando os incidentes de segurança forem encerrados.

Instale e configure o. ServiceNow aplicação para IBM QRadar integração de ingestão de ofensa

Antes de executar a integração no seu ServiceNow AI Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se você não instalou o. IBM QRadar aplicação do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize IBM QRadar lado a lado.
3. Para configurar a aplicação, clique em **Novo** .
4. Como alternativa, se for um **Configurar** é exibido em um bloco, clique nele para editar uma configuração existente.
5. Em **Configuração de ingestões de ofensa** que é exibida, preencha os campos.

Campo	Descrição
Nome	Nome do IBM QRadar console ou IBM QRadar instância usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis.
URL de base da API IBM QRadar	URL do host para seu IBM QRadar instância. **Nota:** Você precisa inserir somente o URL e o número da porta aqui. Por exemplo, https://ibm-qradar.com:8443. Se o número da porta for 443, ele não precisará ser inserido explicitamente.
URL do painel IBM QRadar	O URL do IBM QRadar ou o console. Este URL é usado para criar automaticamente os hiperlinks para infrações no IBM QRadar painel. Insira somente a URL do host, por exemplo, https://qradar.com. Não inclua .jsp no URL, por exemplo, https://qradar.com/console/qradar/jsp/QRadar.jsp é um formato inválido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

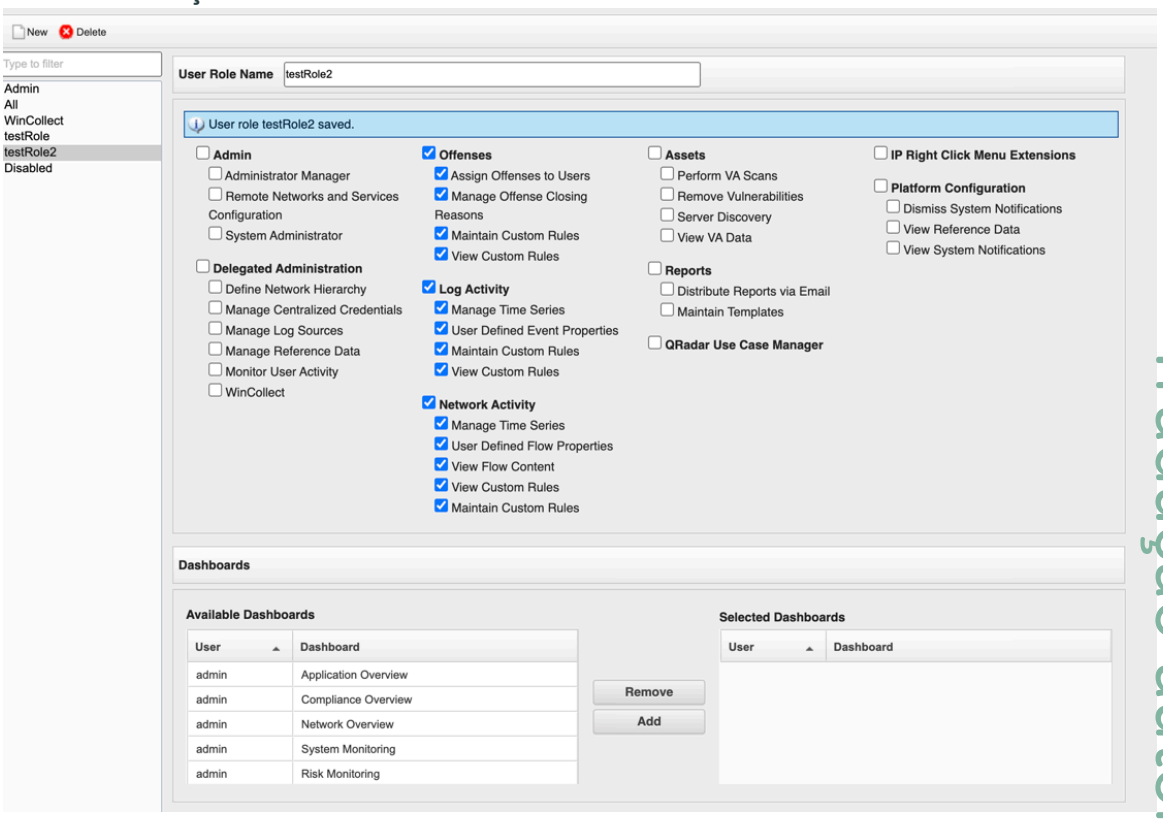
Campo	Descrição
	Nota: Se o URL do painel não estiver disponível, insira IBM QRadar URL base da API aqui.
IBM QRadar Versão da API	As versões 10 e superior são compatíveis.
IBM QRadar Token de serviço autorizado de API (no local)	. IBM QRadar o token de serviço autorizado é usado para autenticação. O token de serviço autorizado deve ter as seguintes funções mínimas de usuário: **Infrações** , **Atividade de log** e **Atividade de rede** junto com um perfil de segurança do usuário que não tem restrições. Para gerar o token de serviço autorizado, siga estas etapas: ◦ Em IBM QRadar console, navegue até **Administrador** e clique **Serviços Autorizados** . ◦ Se existir um token de serviço autorizado válido, verifique a data de expiração e use este token. Se um token de serviço autorizado não estiver disponível, siga estas etapas: ◦ Em IBM QRadar, navegue até **Administrador** e clique **Serviço autorizado** . ◦ Clique em **Adicionar serviço autorizado** e criam um token com a função do usuário e o perfil de segurança. Especifique uma data de vencimento para um longo período de validade.
IBM QRadar Token de serviço autorizado de API (para QRoC)	Se você estiver usando o IBM QRadar on Cloud (QRoC), use a aplicação de autoatendimento para gerar o token de serviço autorizado com a função de usuário administrador e o perfil de segurança de administrador para autenticação.
Implantação no Local	O padrão é desabilitado. Se esta opção estiver habilitada, você deverá especificar um Nome de aplicação MID. Se você estiver usando IBM QRadar Na nuvem (QRoC), verifique se a caixa de seleção está desmarcada.
Nome da aplicação do MID	Especifique uma aplicação DO MID Server que esteja configurada em seu ambiente. Se você não tiver uma aplicação do MID Server configurada, deverá criar uma nova aplicação DO MID Server para esta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

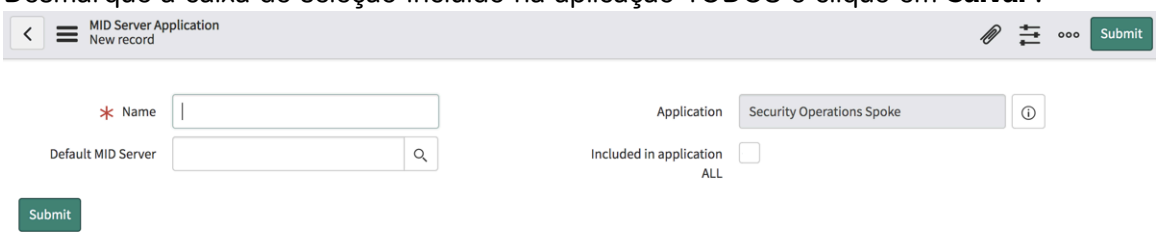
Campo	Descrição
	Nota: A aplicação MID Server pode ser configurada somente por usuários com função de administrador do sistema.

Mínimo de funções de usuário



Para criar uma nova aplicação DO MID Server, siga estas etapas:

- Navegar até **MID Server** > **Aplicações** e clique em **Novo** .
- Insira um nome para a aplicação DO MID Server e selecione um MID Server a ser usado como padrão.
- Desmarque a caixa de seleção Incluído na aplicação TODOS e clique em **Salvar** .

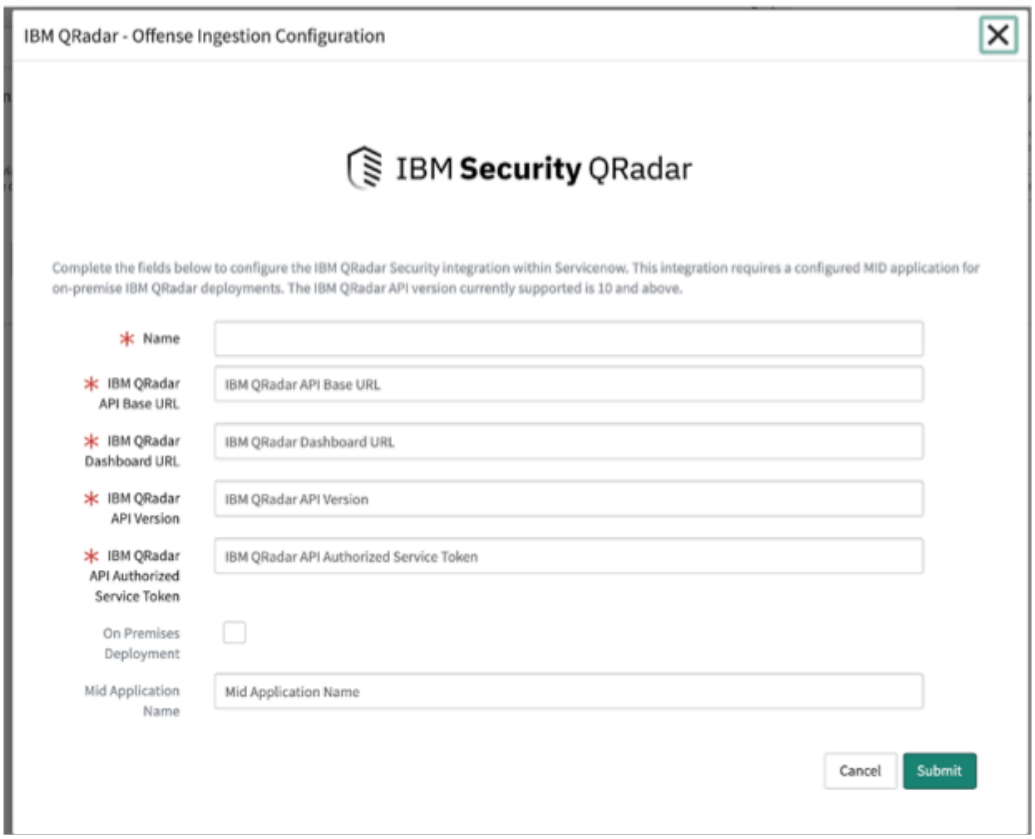


- Clique em **Editar**. Em **Editar membros** , selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar** . Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.

6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A origem que você configura no **Configuração de ingestão de ofensa do IBM QRadar** o formulário pode ser reutilizado para vários ServiceNow AI Platform perfis, desde que cada perfil ingere infrações.

7. Clique em **Enviar**.
   Cada um deles é validado e enviado com sucesso IBM QRadar A configuração do servidor é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim** .

Nota: Se você encontrar alguns problemas com IBM QRadar recurso de segmentação de domínio, contato IBM QRadar Suporte ao cliente para obter assistência.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar o perfil.

Configure seu ServiceNow AI Platform® instância do IBM QRadar integração de ingestão de ofensa

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform® E Resposta a incidentes de segurança (SIR).	As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform® instância. • Um usuário com ServiceNow AI Platform® a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no ServiceNow AI Platform®: ◦ Cria e edita perfis de infração. ◦ E mapeia IBM QRadar campos de dados de infração para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração. ◦ Ingestão de infrações contínua. ◦ Habilita atualizações de infração quando um incidente SIR é criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no Site de documentação do produto ServiceNow .
Verifique se você está usando as seguintes versões: • IBM QRadar versão 7.3.2 ou posterior. • IBM QRadar API versão 10 ou posterior. Versões anteriores não são compatíveis.	Se você tiver acesso ao IBM QRadar, você tem acesso à API necessária para esta integração. Não há outra configuração especial necessária para a API.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação DO MID Server configurada. Um MID Server em seu ServiceNow AI Platform® a instância é necessária para se conectar ao IBM QRadar se o IBM QRadar o servidor está implantado em sua rede corporativa. Consulte Site de documentação do produto da ServiceNow Para obter informações sobre MID Servers.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Se você estiver usando IBM QRadar Um MID Server não é necessário.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Ingestão de evento e alerta para operações de segurança: Esta aplicação requer: ○ Tempo de execução do IntegrationHub da ServiceNow com.glide.hub.integration.runtime ○ Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in de ingestão de evento e alerta. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

O que Fazer Depois

Você configurou com sucesso seu ServiceNow AI Platform® instância da integração. A próxima etapa é instalar o. IBM QRadar aplicação do ServiceNow Store para a integração.

Crie um perfil para IBM QRadar integração de ingestão de ofensa

Como um usuário com a função sn_si.admin, você cria um perfil de ofensa em seu ServiceNow AI Platform e determinar quais infrações criam incidentes de segurança. Antes ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança são criados a partir de infrações, os valores de campo de infrações são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

De uma perspectiva de integração usando APIs disponíveis, IBM QRadar as infrações são ingeridas automaticamente no Operações de segurança do seu ServiceNow AI Platform instância dependendo do tipo de perfil definido. Os fluxos de trabalho de integração ingerem diferentes tipos de infrações, como tentativas de acesso não autorizado e malware, por exemplo. Essas infrações são ingeridas com base nos perfis que você configura no Operações de segurança ambiente da sua instância. Inicialmente, todas as infrações são ingeridas para um tipo de infração configurado em um perfil. As infrações ingeridas podem ser filtradas ainda mais para especificar quais infrações criam incidentes de segurança. Por exemplo,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

você pode preferir filtros que criem incidentes de segurança somente para infrações identificadas como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de infrações ingeridas, os valores de campos individuais nas infrações são mapeados para os campos correspondentes em um layout de incidente de segurança para uma visualização.

Nomes dos perfis de ofensa em seu ServiceNow AI Platform a instância deve ser exclusiva. Você pode criar várias configurações para várias origens e também pode criar vários perfis para uma única origem.

Crie perfis para ingestão IBM QRadar infrações

Você pode configurar um perfil para ingerir infrações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para uma infração em seu ServiceNow AI Platform instância, navegue até **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

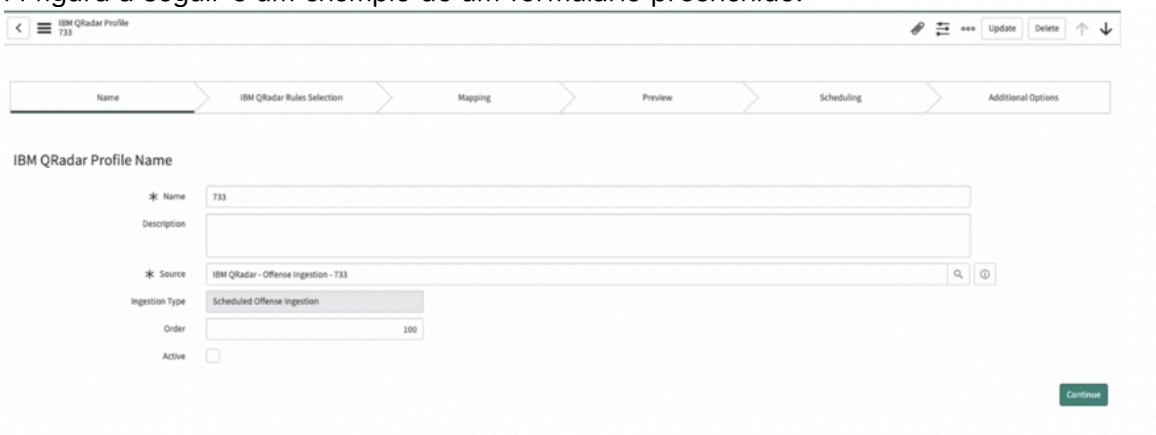
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e os nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.
Ativo	A caixa de seleção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo e a ingestão não ocorrerá. **Nota:** Você deve concluir todas as seções no perfil antes de ativá-lo.
Origem	. IBM QRadar servidor que você configurou para ingerir infrações. Se você tiver vários IBM QRadar servidores configurados, selecione o servidor apropriado para os tipos de ofensa que serão ingeridos para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. O fluxo de trabalho no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é selecionar as infrações para ingestão.

Selecione IBM QRadar regras

Com base em IBM QRadar Origem, selecione um ou mais IBM QRadar regras para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba o disponível IBM QRadar regras em seu ServiceNow AI Platform para que você saiba o ativo IBM QRadar regras para as quais você deseja ingerir e criar incidentes de segurança.

Em IBM QRadar, Você pode identificar regras por origem como regras do sistema, substituição e usuário. Por padrão, a origem de uma regra está vinculada a uma regra do sistema. Quando você modifica uma regra do sistema em IBM QRadar Sua origem é definida como Substituir.

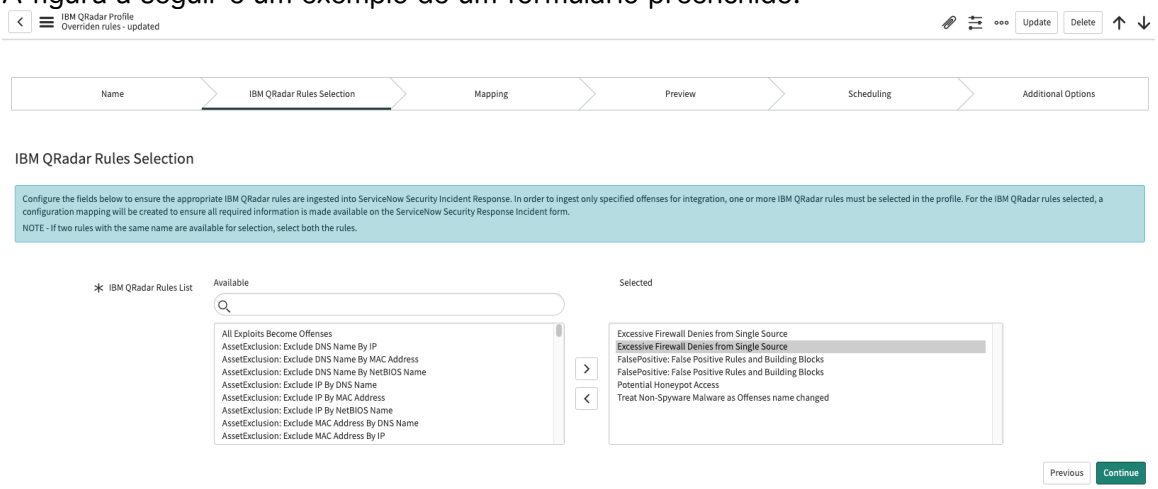
Clique na lista em IBM QRadar Campo Lista de regras. Uma lista de ativos IBM QRadar regras que estão presentes no IBM QRadar O console é exibido. Selecione uma ou mais regras na lista e mova-as para **Selecionado** coluna. Infrações acionadas por um ou mais dos IBM QRadar as regras selecionadas são ingeridas neste perfil.

Regras com o mesmo nome : Em ServiceNow AI Platform uma lista de regras ativas ou habilitadas é exibida. Se você modificar uma regra do sistema ativa ou habilitada em IBM QRadar Uma nova regra de substituição é criada. Duas regras são exibidas com o mesmo nome no ServiceNow AI Platform. Quando esse cenário ocorrer, selecione as regras para ingerir e criar incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo de um formulário preenchido:



Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

Mapeamento de campos de infração para IBM QRadar integração

Depois de selecionar as regras, a próxima etapa é mapear campos de infração, evento ou fluxo para os campos no formulário de incidente de segurança.

Visão geral

Para a etapa de mapeamento, você deve primeiro ingerir exemplos de infrações para um ou mais selecionados IBM QRadar regras. Em seguida, você deve garantir que todos os dados do campo de infração relevantes sejam mapeados para o local apropriado em SIR formulário de incidente e visualize o. SIR incidente na seção de visualização.

O mapeamento dos campos de infração de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: Consulte Ingestão da amostra IBM QRadar infrações.
- Mapeando os campos de infração para o incidente de segurança: Consulte Mapeamento IBM QRadar campos de infração para campos de resposta a incidentes de segurança.

Ingestão da amostra IBM QRadar infrações

Você pode ingerir exemplos de infrações para um ou mais selecionados IBM QRadar regras.

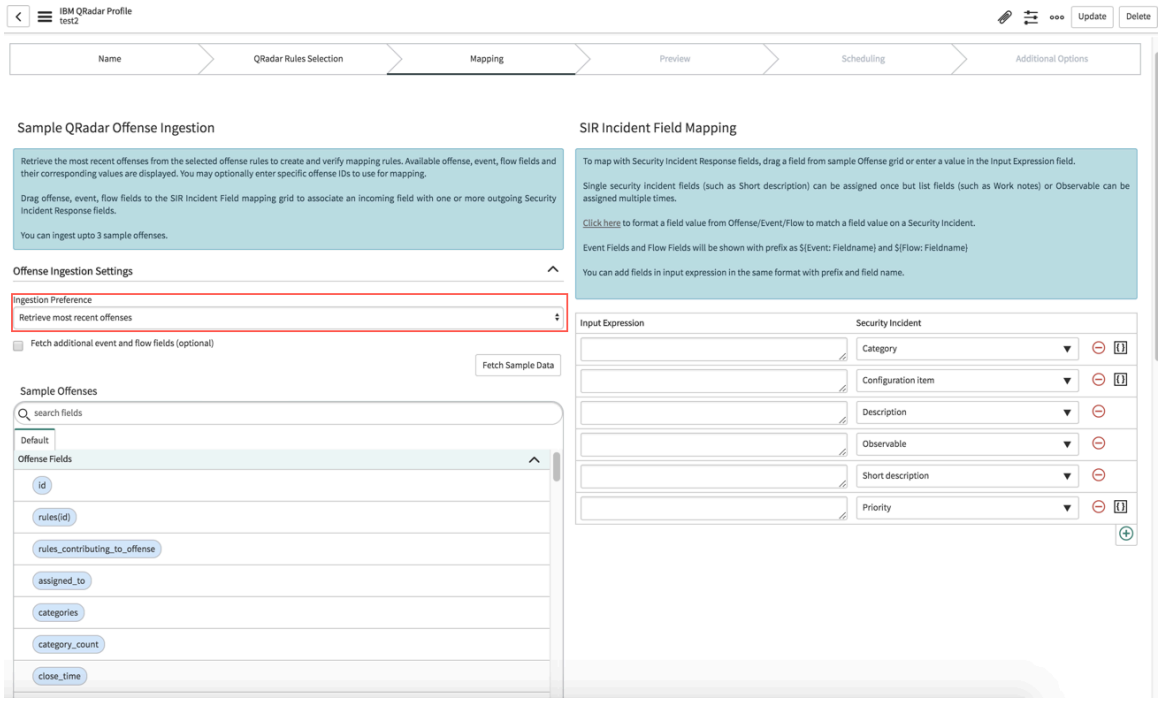
Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair as três infrações de amostra mais recentes ou fornecer os IDs de infração exclusivos para as infrações específicas que você deseja usar para sua experiência de mapeamento.
   Em **Preferência de ingestão** lista de seleção, selecione uma das seguintes opções:
   - Recuperar infrações mais recentes: As três infrações mais recentes das regras selecionadas são recuperadas.
   - Selecionar infrações com base no ID de infrações: Especifique o ID de infração para as infrações a serem recuperadas. Você pode especificar um máximo de 3 ids de ofensa separados por vírgulas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Buscar dados de amostra** para extrair os dados de infração de amostra mais recentes do IBM QRadar console para as regras de infração selecionadas.

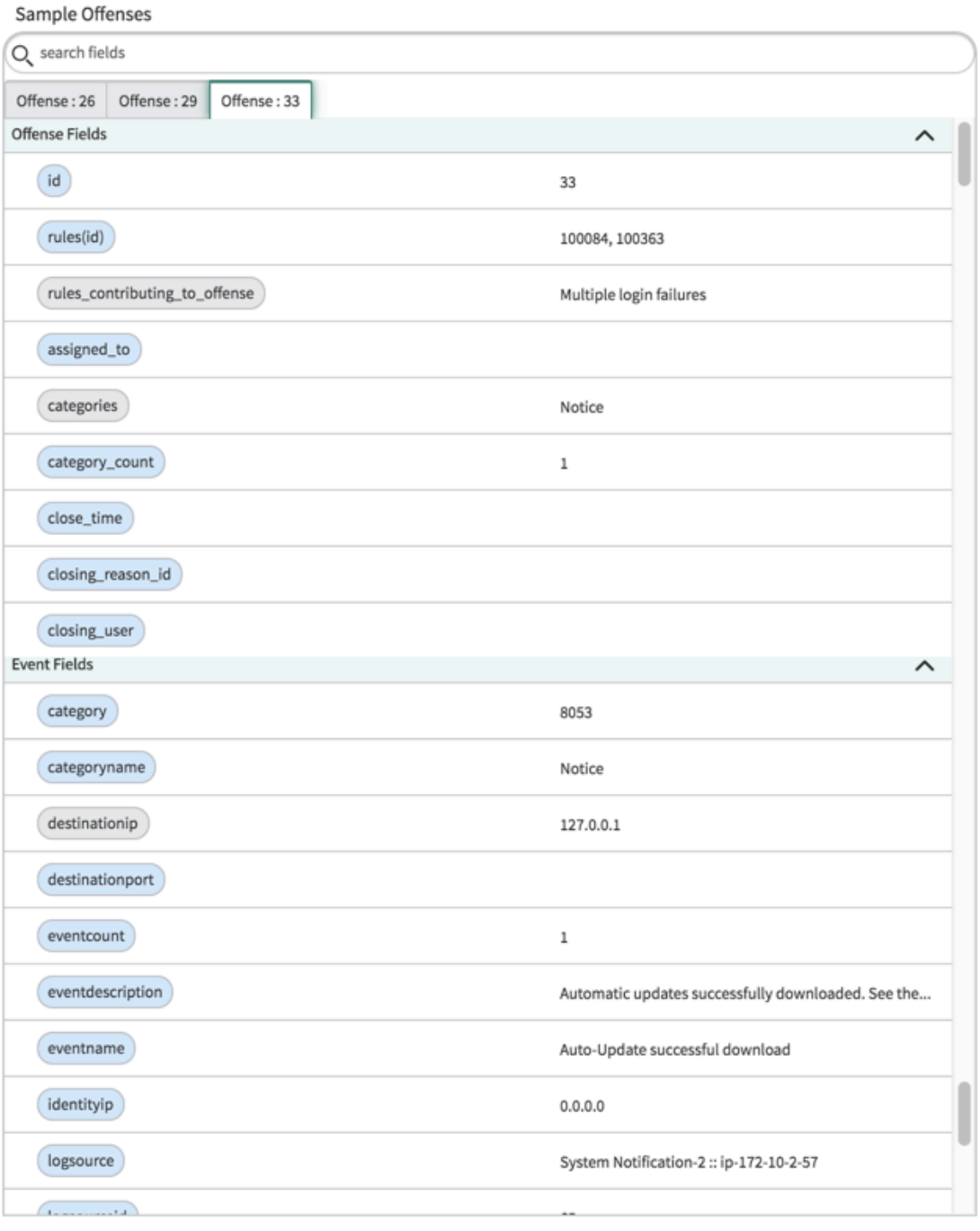
   Os campos de infração e os resultados de valores são exibidos como guias individuais. Uma infração pode ser acionada por três tipos de regras:

   - Evento: Nesta regra, os logs de evento são verificados e, se os critérios especificados forem atendidos, uma infração será criada.
   - Fluxo: Os dados e o tráfego da rede são verificados e, se determinadas condições forem atendidas, uma infração será criada.
   - Comum: Nesse caso, você pode especificar condições para eventos ou fluxos e uma ou ambas as condições forem atendidas, uma infração será criada.

   A extração de exemplos de infrações pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Dependendo da regra ou regras que acionaram a infração, junto com os campos de infração, os campos de evento ou fluxo são preenchidos conforme mostrado na figura abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Nota: Os campos de evento ou fluxo exibidos pertencem ao primeiro evento ou campo de fluxo que acionou a infração com base no evento ou regra de fluxo correspondente.

4. Os seguintes campos de infração personalizados criados para esta integração.
   Campos de infrações padrão, além desses campos personalizados, estão disponíveis para mapeamento.
   - contributing_to_ofense: IBM QRadar Regras que contribuíram para a infração com base no ID da regra.
   - Usuários: Nomes de usuário da infração
   - Remote_destination_ip: Os IPs de destino remoto da infração.

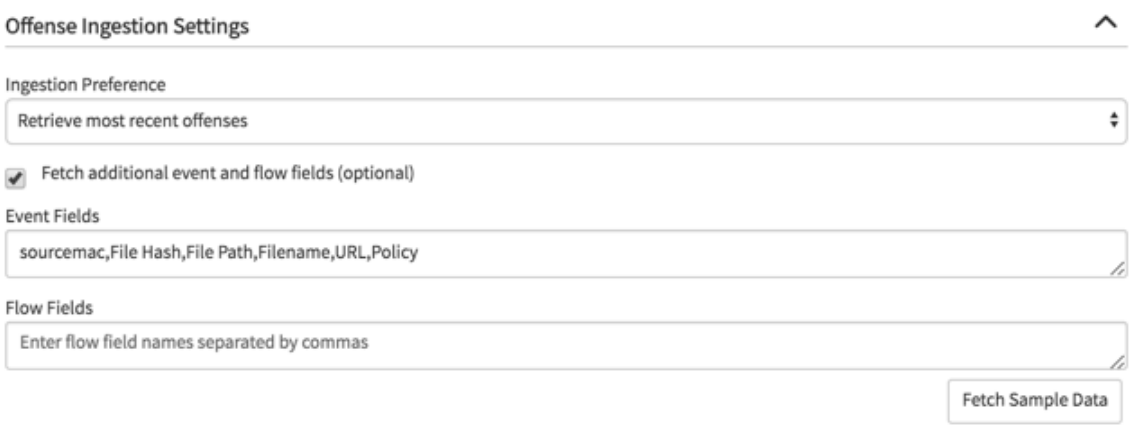
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com base nos IDs de destino local da infração, os seguintes campos de endereço de destino local personalizados estão disponíveis:

- local_destination_address (domain_id)
- local_destination_address (event_flow_count)
- local_destination_address (first_event_flow_seen)
- local_destination_address (id)
- local_destination_address (last_event_flow_seen)
- local_destination_address (local_destination_address_ids)
- local_destination_address (magnitude)
- local_destination_address (rede)
- local_destination_address (ofense_ids)
- local_destination_address (local_destination_ip)

- Os seguintes endereços de origem estão disponíveis com base nos IDs de origem da infração:
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (id)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (magnitude)
  - source_addresses (rede)
  - source_addresses (ofense_ids)
  - source_addresses (source_ip)

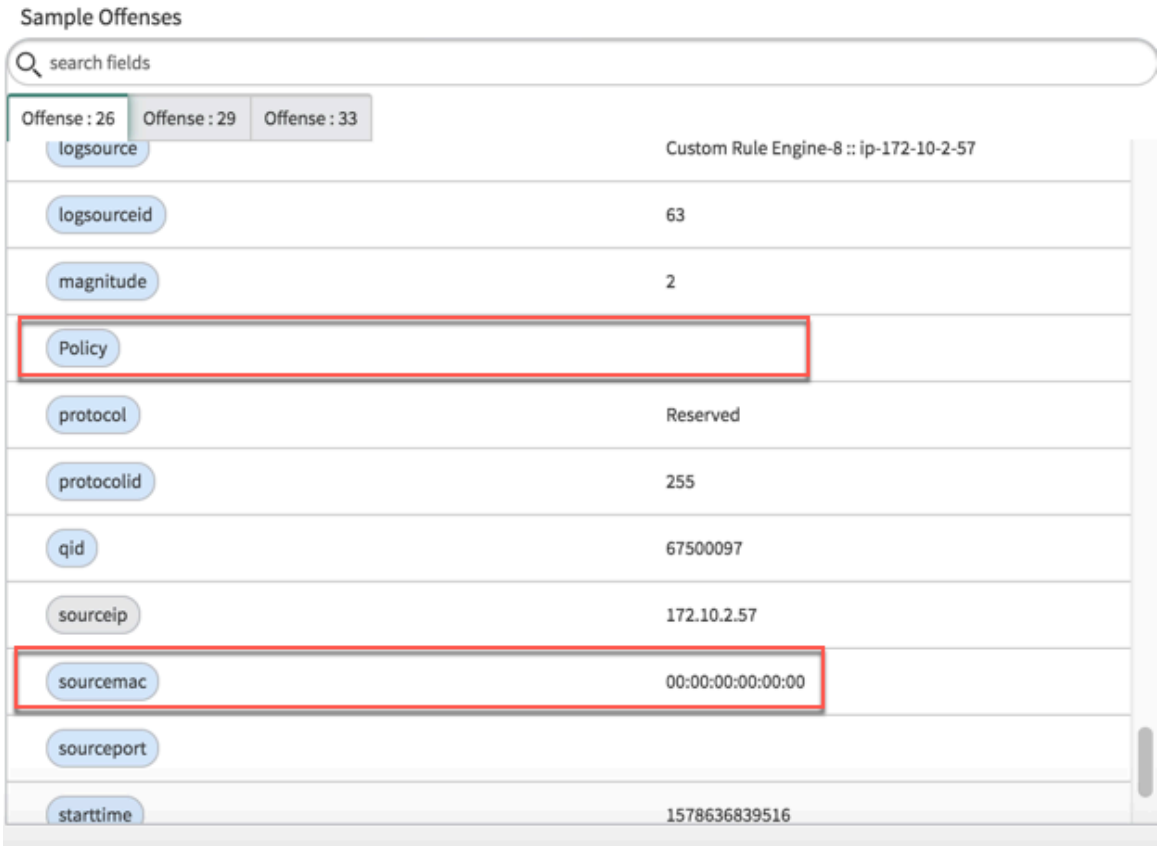
Selecione **Buscar campos adicionais de evento e fluxo (opcional)** caixa de seleção. Você pode buscar dados de fluxo e evento de amostra de qualquer evento personalizado ativo válido e campos de fluxo. Especifique os campos personalizados separados por vírgulas, conforme mostrado abaixo:



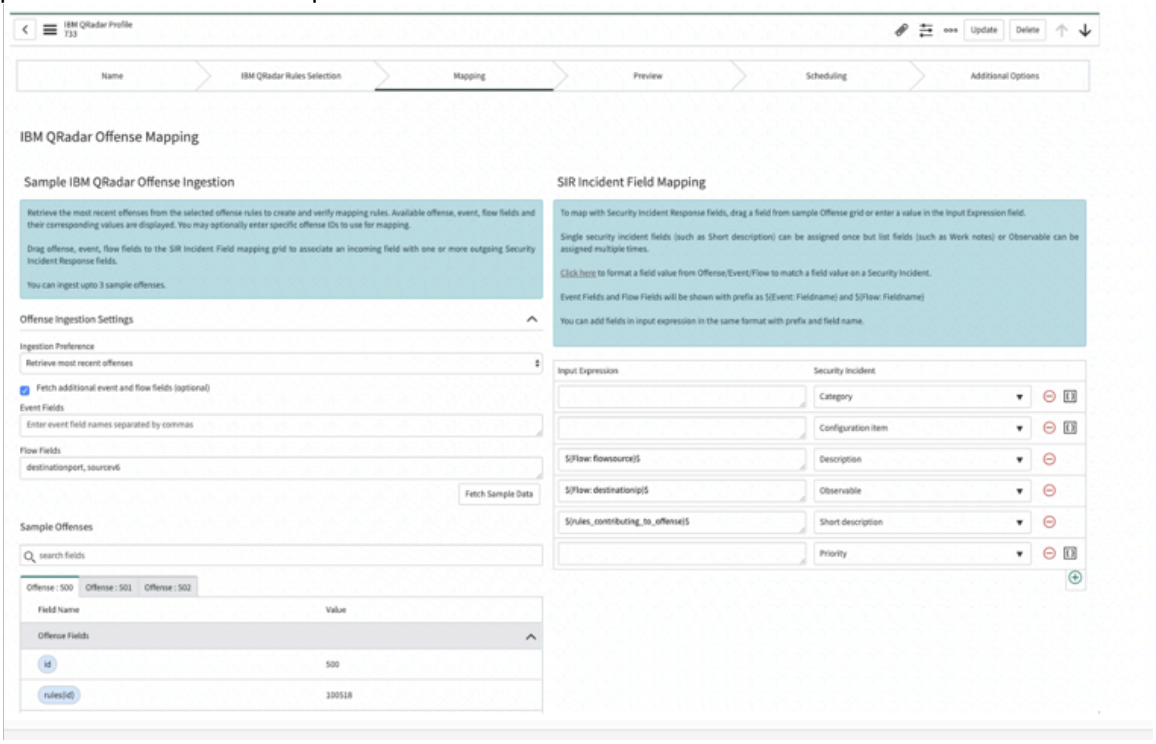
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique em **Buscar dados de amostra** . Os campos de evento ou fluxo especificados junto com seus valores (se disponíveis) são anexados à seção Evento ou Fluxo, conforme mostrado abaixo:



Depois de buscar os dados de amostra, os valores correspondentes desses campos são preenchidos no lado esquerdo do formulário.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de infração para o incidente de segurança.

Mapeamento IBM QRadar campos de infração para campos de resposta a incidentes de segurança

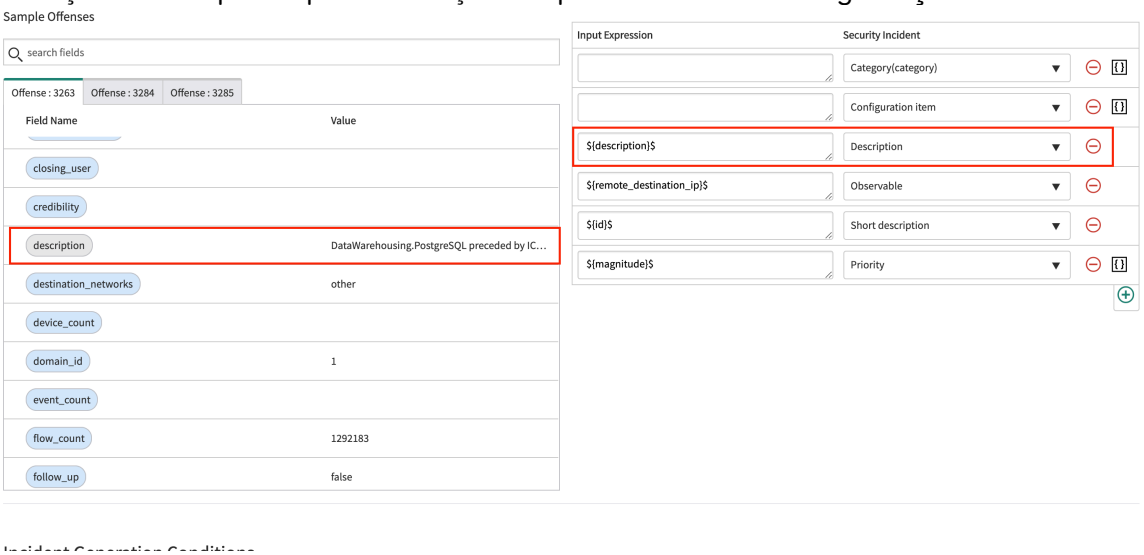
Mapeie campos de infração individual, evento e fluxo para campos em um ServiceNow AI Platform SIR incidente de segurança.

Mapeamento do campo de infração

Como um usuário com a função sn_si.admin, use os campos da seção Exemplos de infrações à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR. Edite a configuração de mapeamento arrastando campos de ofensa, evento ou fluxo do lado esquerdo e soltando-os no ServiceNow SIR seção de mapeamento de incidentes à direita. O mapeamento à direita associa o campo de infração de entrada a um campo de incidente de segurança de saída.

1. Depois de obter os dados de amostra, a próxima etapa é mapear os campos de infração, evento ou fluxo para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, descrição E solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

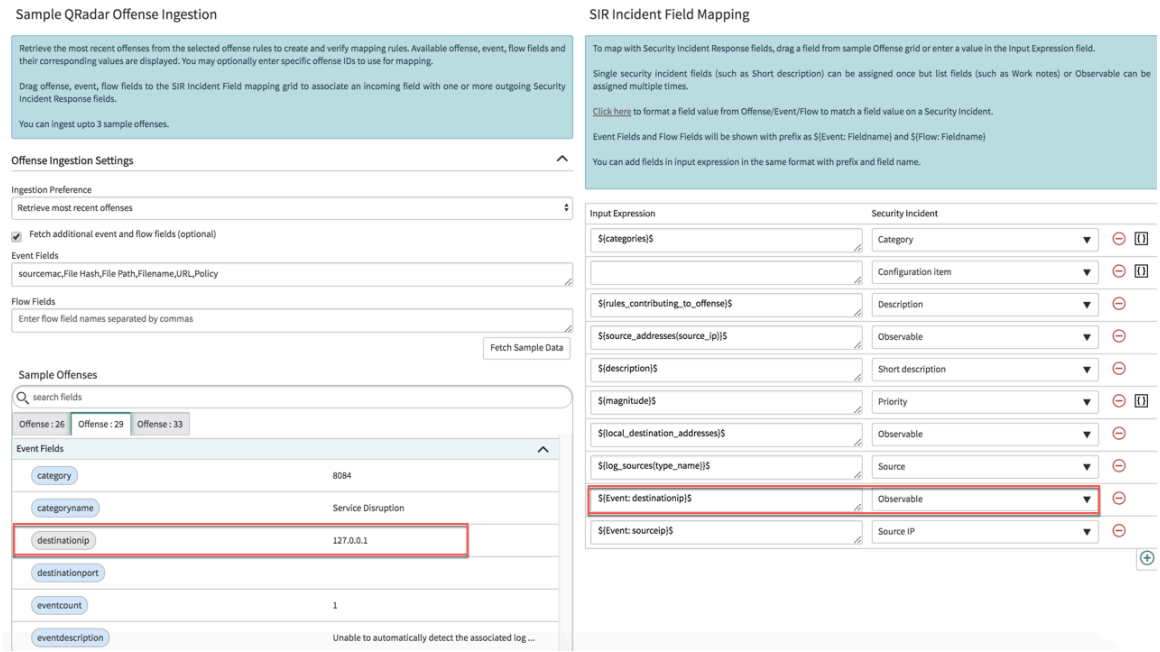
   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, descrição está mapeado para Descrição campo no incidente de segurança.



Nota: Se você inserir o nome do campo de fluxo ou evento manualmente na seção Expressão de entrada, deverá adicionar um prefixo como `Event:eventfield` ou `(Flow:flowfield)` antes do nome do campo que está sendo mapeado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



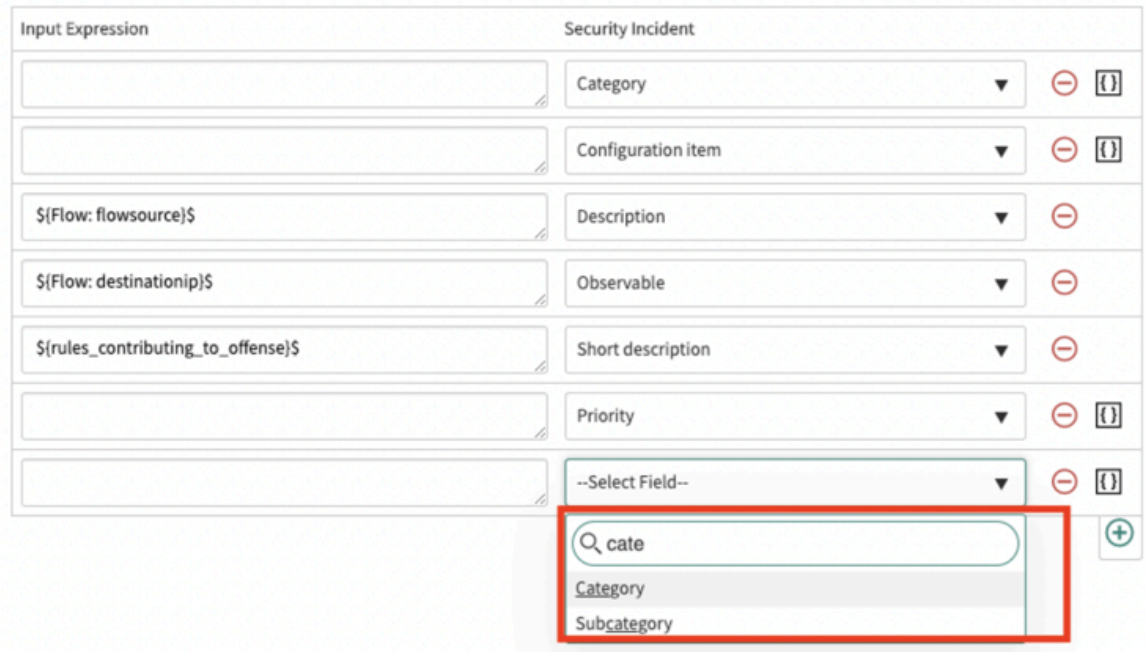
Para ajudar você a garantir que nenhum campo de infração, evento ou fluxo seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de ofensa ajuda a acompanhar os valores de ofensa que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de infração importante restante permanece não mapeada.

Campos azuis claros à esquerda indicam que um campo de infração ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de infração, evento ou fluxo de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Esta codificação por cores ajuda você a rastrear o mapeamento.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário, na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de adição. Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida do novo campo, alguns campos são sombreados. Na figura a seguir, Categoria tem um fundo cinza, porque foi mapeada no incidente de segurança. Semelhante à codificação por cores dos campos de ofensa no lado esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente DE SIR já mapeados.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, selecione o campo Ofensão e arraste-o e solte-o em um campo de incidente de segurança apropriado à direita.

4. Remova campos usando o ícone - ao lado do nome do campo na seção de mapeamento de campo de incidente SIR.

5. Continue o mapeamento adicionando ou removendo valores de campo ao mapeamento.

Campos de infração com vários valores

- Campos de incidente de segurança, como **Categoria** e. **Usuário** Os campos (por exemplo, usuário afetado, Atribuído a) disponíveis com o produto de base não são compatíveis com vários valores.
- A seguir IBM QRadar os campos oferecem suporte a vários valores:
  - *categorias*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_ofense*
  - *usuários*

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

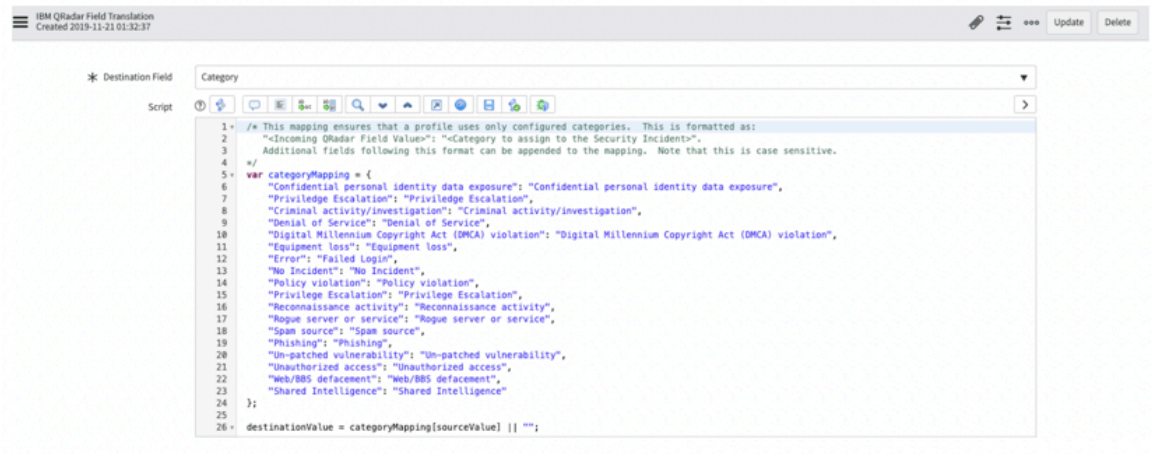
Se você precisar mapear os campos acima para qualquer Resposta a incidentes de segurança Campos além dos campos de IC e do tipo observável, você deve criar novos Resposta a incidentes de segurança campos do tipo **Lista** e usá-los para mapeamento.

Nota: Por padrão, somente não referência **Lista** campos de tipo são compatíveis.

Tradução de campo de formato

Em determinados casos, os valores do campo de infração em IBM QRadar Não pode ser traduzido diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria Alerta de malware e infecção por vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser traduzidos em uma Atividade de código mal-intencionado comum no campo Categoria no incidente de segurança SIR usando a funcionalidade Tradução de campo de formatação.

Para usar o editor de scripts, clique em {}. O editor de script é exibido.



Insira as mudanças no script e clique em **Atualização** Para salvar as mudanças e retornar à página Mapeamento.

Condições de geração de incidentes

Quando a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais infrações devem criar incidentes de segurança versus quais infrações devem ser filtradas, por exemplo, infrações de baixa prioridade. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que uma infração de entrada deve atender para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até **Condições de geração de incidentes** no formulário e selecione **Filtro com base em condições** marque a caixa para habilitar a opção.

   O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos na seção Amostra de ingestão de infração do QRadar para as infrações que você ingeriu. Esses campos são dinâmicos e mudam dependendo das infrações que você ingerir. Os critérios inseridos diferenciam maiúsculas

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de minúsculas e devem corresponder exatamente aos valores de IBM QRadar infração. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao IBM QRadar console e revise suas infrações em busca das palavras-chave.

Nota: `.categorias` , `destination_networks` , `source_address_ids` , `local_destination_address_ids` , `remote_destination_ips` , `rules_contributing_to_ofense` e `usuários` os campos de ofensa podem ter vários valores (pois os valores são armazenados em matrizes). Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar `contém` condição de filtro para esses campos para garantir que os dados sejam filtrados corretamente.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
   - Se **E.** selecionado, todas as condições devem ser correspondidas.
   - Se **OU** está selecionado, qualquer condição pode ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

   A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



   Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando as duas condições de filtragem inseridas forem correspondidas.

   Este tipo de filtragem de condição de geração de incidentes ajuda a restringir as infrações e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a regra ou os filtros subjacentes em IBM QRadar. Se critérios de filtragem adicionais forem definidos, somente as infrações que corresponderem a todos os critérios serão mapeadas para incidentes.

   Nota: Se qualquer um dos nomes de campo de ofensa tiver caracteres especiais, como aspas ("), hifens ("), sublinhados (-) ou ampersands ("), esses caracteres podem precisar ser substituídos para fins de filtragem, mas um sufixo numérico será anexado para diferenciar campos com nomes de ofensa duplicados. Por exemplo, se o campo Primeira infração for `alerts.alert` e o segundo campo de ofensa é `alertas em alertas` esses campos não podem ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de infração e o campo é renomeado para `alertas em alerta (1)` Quando exibido na lista Condições de filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios de agregação de infrações para lidar com infrações semelhantes e evitar incidentes duplicados

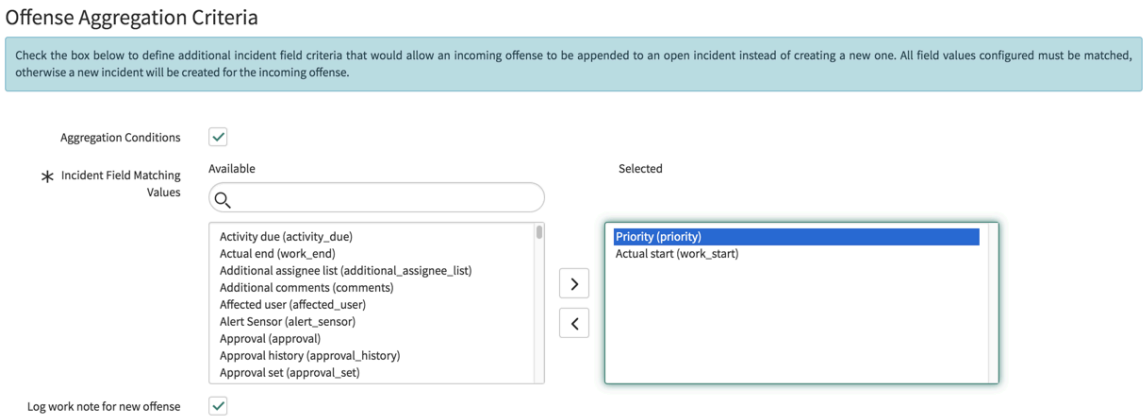
Defina critérios de agregação de infração adicionais que agreguem uma infração de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, esse recurso de agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de infração relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

1. Role até a seção Critérios de agregação de ofensa no formulário e selecione **Condições de agregação** marque a caixa para habilitar esta opção.

   As colunas Valores de correspondência do campo do incidente são exibidas. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform E mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de ofensa mapeados para eles. Todos os valores devem corresponder. Se somente um subconjunto dos valores for correspondido, as condições de agregação de infração não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para obter o mapeamento de campos de vários valores.



   Se uma nova infração corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, a nova infração será adicionada automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todas as infrações agregadas adicionadas em uma lista relacionada em um incidente de segurança. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam você a entender por que essas infrações estão sendo agregadas aos incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique em **Mostrar todas as listas relacionadas** link.

3. (Opcional) Para registrar em log uma anotação de trabalho para uma nova infração que foi adicionada recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra em log que uma nova infração foi adicionada junto com um link para os detalhes da infração e quaisquer outros detalhes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

Valores mapeados com sucesso de um IBM QRadar violação aos campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexou infrações a incidentes de segurança existentes quando os valores do campo de infração correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um SIR incidente de segurança

Visualizar incidente de segurança

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de infração que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

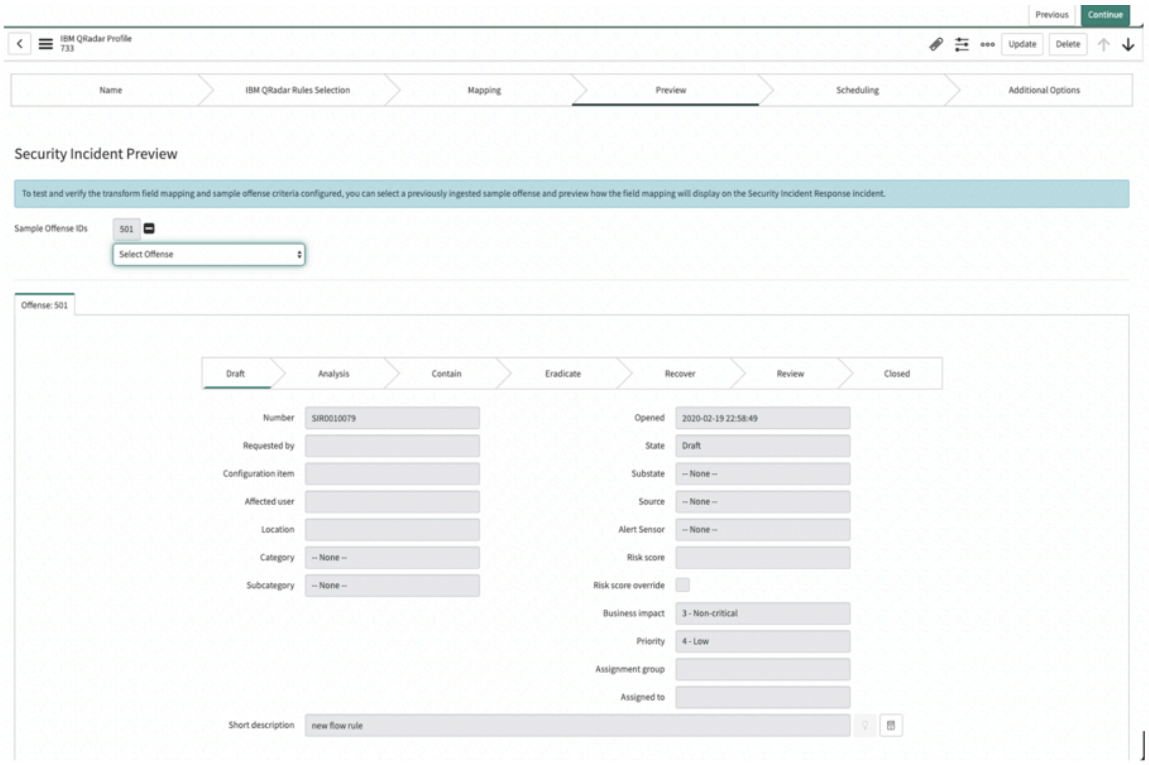
Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. Visualizações de SIR os incidentes de segurança não são salvos como incidentes reais no Resposta a incidentes de segurança produto.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
2. Na lista de seleção IDs de infração de amostra, selecione um item.
   O incidente de segurança é exibido. Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de infração no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será definir a programação.

Definir programação

Você pode definir a programação para a ingestão de infração. Durante esta etapa, você pode verificar as configurações padrão para a recuperação da infração ou modificar a programação conforme necessário. Esta etapa também permite recuperar infrações históricas usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode escolher se deseja ingerir infrações históricas durante a etapa de Programação. Você também escolhe com que frequência pesquisará novas infrações futuras e infrações atualizadas que correspondam à configuração do perfil.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho do IBM QRadar a integração de ingestão de ofensa pode ser afetada pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no IBM QRadar servidor contra o desejo de ser notificado o mais rápido possível quando uma infração é criada ou atualizada. Um valor

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo infrações novas e atualizadas

Quando a programação de pesquisa é definida, o trabalho agendado extrai infrações novas e atualizadas que foram extraídas anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso fornece a flexibilidade para criar incidentes com base em critérios que podem não estar presentes quando uma infração é criada pela primeira vez, mas se torna disponível após a ocorrência de uma atualização, por exemplo, durante a fase de investigação. Quando um incidente é criado para uma infração específica, suas atualizações subsequentes são ignoradas, pois espera-se que a infração agora esteja sendo tratada como ativa ServiceNow incidente de segurança. No entanto, todas as outras infrações que foram ingeridas anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídas e verificadas em relação aos critérios de geração de incidentes até se tornarem parte de um incidente ativo.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando as infrações são extraídas do IBM QRadar console.

Opção	Descrição
Campo Ingestão de infração contínua selecionado	Ataque contínuo Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do IBM QRadar servidor para infrações novas e atualizadas a cada cinco minutos. Os incidentes de segurança serão criados se infrações forem encontradas e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar o desejo de sobrecarga de pesquisa de ingestão de obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, esse valor pode ser modificado para um minuto, se necessário.
○ Ingestão de infração contínua selecionada ○ Defina o tempo de ingestão da infração inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas: ○ Selecione os campos Ingestão de infração em andamento e defina Tempo de ingestão de infração inicial. ○ Especifique a hora no campo Tempo de ingestão de infração inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida no campo Incremento de pesquisa (minutos).

Tradução automática

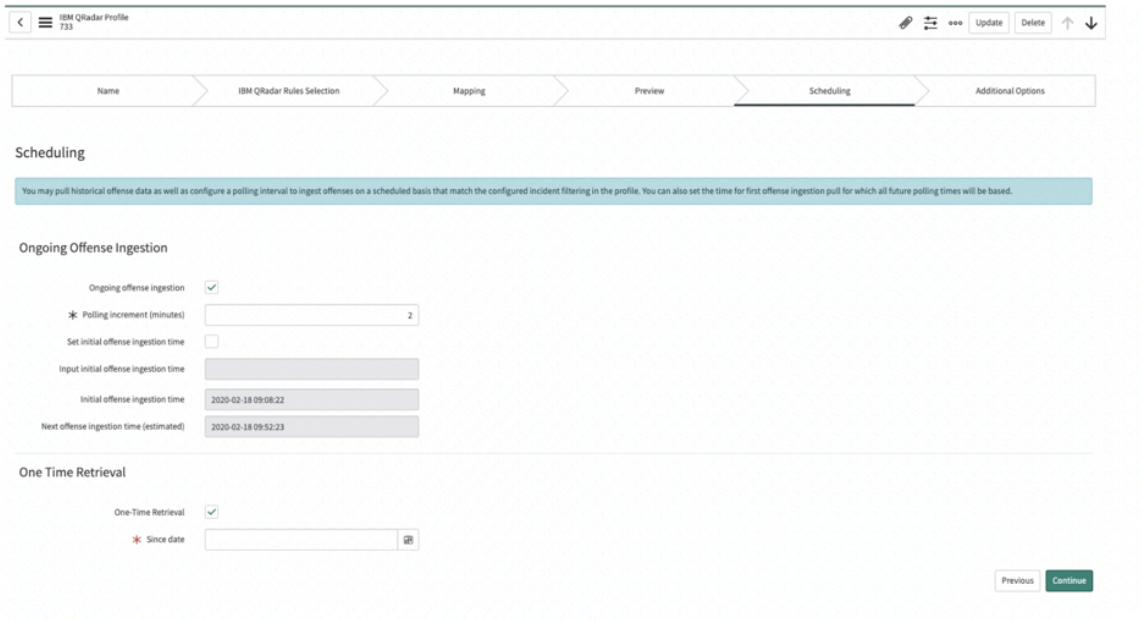
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Como exemplo para programar um tempo de ingestão de infração inicial, se você tiver um diário IBM QRadar Verificação de segurança que é executada uma vez por dia às 4 hora local, você pode configurar o perfil de infração correspondente em seu ServiceNow AI Platform Instância a ser executada às 4:05 hora local para capturar a falha de segurança imediatamente e criar um incidente de segurança. Insira `<date> 04 05 00` No campo Ingestão de infração inicial. No campo Incremento de pesquisa (minutos), insira `<date> 1440` (24 horas) para programar a próxima ingestão de infração por 24 horas a partir da ingestão inicial de infração. A hora de ingestão da infração inicial e a hora de ingestão da próxima infração são exibidas nos campos. A ingestão inicial ocorrerá às 4:05 horas. As ingestões subsequentes serão baseadas no intervalo de pesquisa. Como o incremento de Pesquisa é de 24 horas, a próxima ingestão ocorrerá no dia seguinte às 4:05 horas.
Campo Recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única consuma infrações históricas. Quando esta configuração é definida, um perfil é usado uma vez para recuperar infrações de eventos históricos baseados em um intervalo de datas. À direita do campo Desde data, clique no ícone de calendário. No calendário exibido, selecione a data em que você deseja começar a extrair infrações. A partir do valor de data Desde, as infrações são recuperadas até a data atual. Observe que você pode extrair até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de infrações históricas de IBM QRadar por motivos de arquivamento, mas sim uma quantidade mínima de infrações em voo que estão sendo ativamente trabalhadas no momento da ativação do perfil. Depois que as infrações forem extraídas, esta configuração não recuperará mais infrações para este per-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	fil a partir da data atual. Esta configuração preenche o incidente de segurança com todas as infrações encontradas para o intervalo inserido.



3. Clique em **Continuar** Para navegar até a página Opções adicionais.

Automatize atualizações de infração e fechamento com base no status do incidente SIR

. IBM QRadar A integração tem uma interface bidirecional que permite que ambas as infrações criem incidentes de segurança, bem como a capacidade de atualizar as infrações depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como número do incidente de segurança, grupo de atribuição, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais** .
2. Siga as instruções abaixo para concluir a configuração para atualizar infrações quando o incidente de segurança for criado.

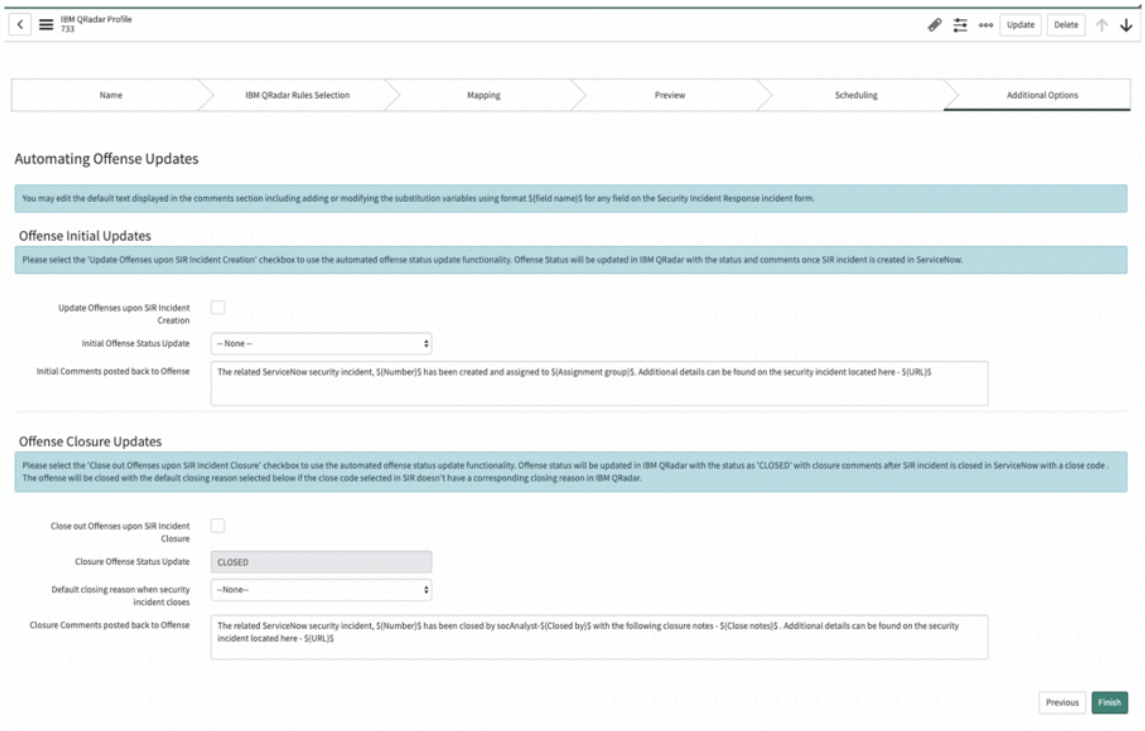
Opção ou Campo	Descrição
Atualizar infrações após a criação do incidente SIR	Selecione esta opção se quiser atualizar o status da infração e adicionar comentários adicionais quando um incidente de segurança for criado a partir da infração. Isso pode ocorrer tanto para as infrações de gatilho iniciais que criam o incidente de segurança, quanto para as infrações agregadas.
Atualização do status da infração inicial	Você pode selecionar:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou Campo	Descrição
	○ Aberto: O status da infração é definido como **Aberto** e um comentário é adicionado indicando que um incidente de segurança foi criado para a infração. ○ Oculto: O status da infração é definido como **Oculto** e esta ofensa está oculta no IBM QRadar painel.
Comentários iniciais retornados para a ofensa	Com base na fase selecionada, os comentários iniciais conforme definido em IBM QRadar o console é exibido aqui.
Encerrar infrações após o fechamento do incidente SIR	Selecione esta opção se quiser usar a opção Encerramento automatizado de infração. Quando o incidente de segurança é encerrado em ServiceNow com um código de fechamento relevante, o status da infração é atualizado em IBM QRadar. **Encerrado** com comentários de fechamento. **Nota:** O código de fechamento especificado para o incidente de segurança deve corresponder ao motivo de fechamento especificado em IBM QRadar painel. A infração é encerrada em IBM QRadar somente se um motivo de fechamento correspondente for encontrado. Se um motivo correspondente não for encontrado, a infração será encerrada com um código de fechamento padrão.
Comentários de fechamento retornados para Ofenção	Os comentários de fechamento conforme definido em IBM QRadar os painéis são exibidos aqui.
Motivo de fechamento padrão quando o incidente de segurança é encerrado	O motivo padrão a ser usado quando um incidente de segurança é encerrado, quando um incidente de segurança é encerrado, um código de fechamento (ou o motivo do fechamento) é especificado no registro de incidente de segurança, se o código de fechamento não corresponder ao motivo de fechamento especificado em IBM QRadar e você tentar fechar o incidente de segurança, uma mensagem de erro será exibida. Nesses casos, o motivo de fechamento padrão especificado aqui é usado quando o incidente de segurança é encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Concluir** para concluir a configuração e mover o perfil para **Aguardando** estado.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair infrações do IBM QRadar console baseado em sua programação.

Definições de configuração

Use esta opção para modificar IBM QRadar propriedades do sistema padrão da integração de ingestão.

Para modificar as propriedades do sistema, faça login como um usuário com *sn_si.admin* e navegue até **Integração do IBM QRadar** > **IBM QRadar Integration Settings**.

IBM QRadar Integration Settings

Nome da Propriedade	Descrição
Imponha um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_qradar.max_si_per_day	Especifica o número máximo de incidentes de segurança que podem ser criados em 24 horas. • Tipo: inteiro • Valor padrão: 1000
Impor um limite no número de infrações que podem ser agregadas a um único incidente. sn_sec_qradar.max_aggregation_per_si	O limite de agregação de infração para um incidente de segurança. Por exemplo, se houver 102 infrações, as primeiras 100 infrações serão agregadas a. incidente de segurança_1 e os restantes 2 a. incidente de segurança_2 .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IBM QRadar Integration Settings

Nome da Propriedade	Descrição
	• Tipo: inteiro • Valor padrão: 100
Esta propriedade define o período de tempo do AQL para buscar eventos/fluxos recentes para uma infração específica. sn_sec_qradar.on_demand_recent_days_limit	Especifica o número de dias para buscar eventos ou fluxos recentes para uma infração específica. • Tipo: inteiro • Valor padrão: 7
Esta propriedade limita o número de eventos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_event_limit	Especifica o número de eventos que são recuperados para uma infração. Os eventos mais recentes são recuperados primeiro com base no carimbo de data/hora do evento. • Tipo: inteiro • Valor padrão: 100
Esta propriedade limita o número de fluxos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_flow_limit	Especifica o número de fluxos que são recuperados para uma infração. Os fluxos mais recentes são recuperados primeiro com base no carimbo de data/hora do fluxo. • Tipo: inteiro • Valor padrão: 100
Esta propriedade define o valor de tempo limite (segundos) para o AQL que busca fluxos/eventos recentes para uma infração específica. sn_sec_qradar.on_demand_timeout	• Tipo: inteiro • Valor padrão: 300
Tempo limite de IDs de pesquisa (segundos) para registros na fila para pesquisa de AQLs de uma infração. sn_sec_qradar.sid_ttl	Tempo limite do AQL para uma infração na fila antes de criar um incidente de segurança. Por exemplo, se houver 90 infrações, as primeiras 50 infrações serão processadas para dados de AQL no primeiro lote e as 40 infrações restantes no lote subsequente no mesmo intervalo de pesquisa. • Tipo: inteiro • Valor padrão: 300
Limite para controlar o número de pesquisas que podem ser executadas em IBM QRadar em um horário acionado pela integração programada	Especifica o número de infrações que você busca em um único lote em um intervalo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IBM QRadar Integration Settings

Nome da Propriedade	Descrição
job.sn_sec_qradar.records_threshold_in_que_for_aql	• Tipo: inteiro • Valor padrão: 50
Este é o número de dias para limpeza de tabelas de integração. sn_sec_qradar.queue_item_expire	Estas são as tabelas de integração: • sn_sec_qradar_events - Eventos do IBM QRadar • sn_sec_qradar_flows - Fluxos do IBM QRadar • sn_sec_qradar_ofense_updates - Atualizações de ofensa do IBM QRadar • sn_sec_qradar_ofense_to_task - IBM QRadar Ofense para tarefa • Tipo: inteiro • Valor padrão: 30
Limite de ofensa por execuções de trabalho programadas por perfil na recuperação única ou na ingestão contínua. sn_sec_qradar.max_ofense_limit_per_run	Especifica o número de infrações que você busca em ServiceNow AI Platform em uma única recuperação. • Tipo: inteiro • Valor padrão: 1000
Defina esta propriedade para ativar o recurso Atualizações de ofensa. sn_sec_qradar.get_ofense_updates	**Nota:** Habilitar esta configuração pode causar um atraso na criação de um incidente de segurança. • Tipo: Verdadeiro| falso • Valor padrão: falso

Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Opcional: Copie um IBM QRadar perfil

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis para economizar tempo.

Antes de Iniciar
Função necessária: sn_si.admin

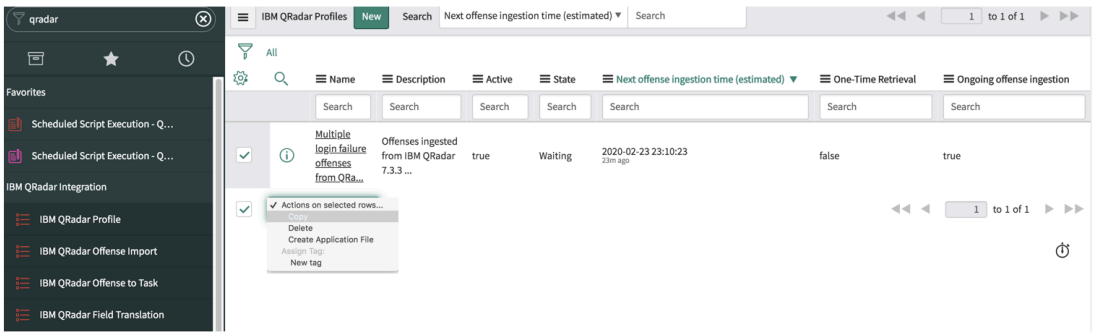
Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

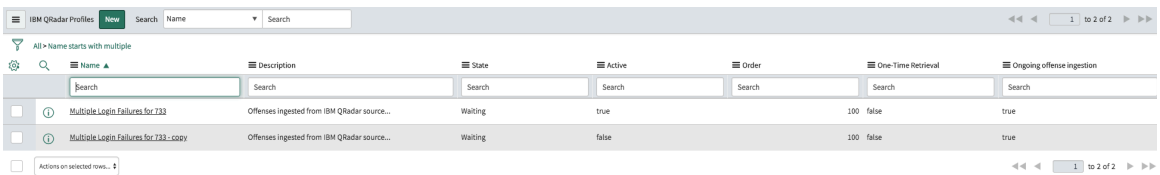
Procedimento

1. Navegar até **Tudo** > **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Na lista Perfis do IBM QRadar exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Cópia** .



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia . Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

Nota: Se você selecionar uma origem diferente para o perfil, deverá selecionar novas regras (Selecione IBM QRadar regras) para o perfil. Mas se você usar a mesma origem e selecionar novas regras, os exemplos de infrações serão limpos.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que **Ativo** o status da coluna é definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Domain Separation e. IBM QRadar Ingestão de ofensa

Domain Separation é compatível com IBM QRadar ingestão de ofensa. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

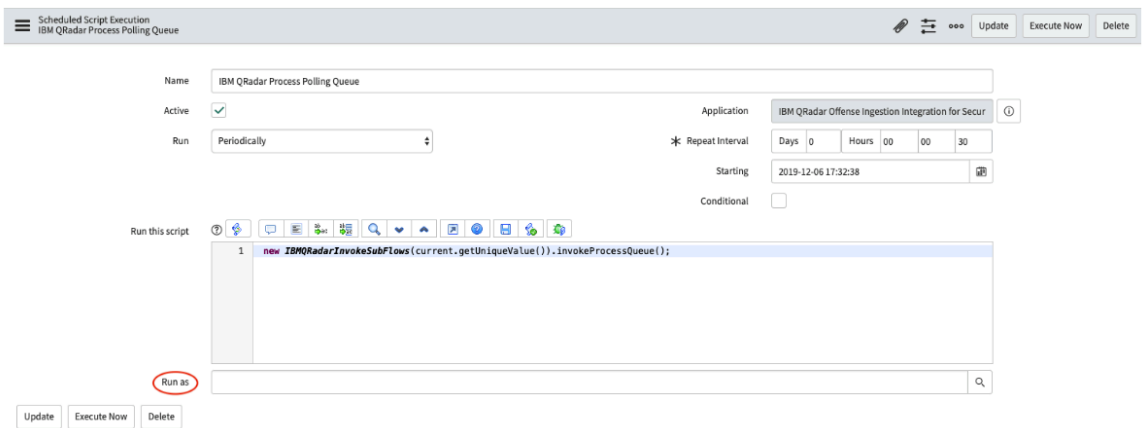
Como o Domain Separation funciona no IBM QRadar Ingestão de ofensa

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com `sn_si.admin` função no respectivo domínio.

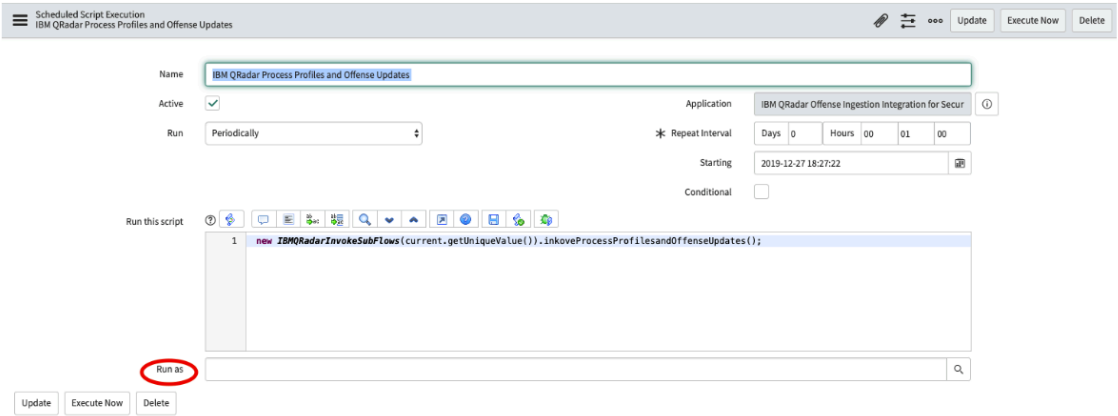
> **Nota:** Ao criar o perfil, use o seletor de domínio para selecionar o domínio específico. Não crie o usuário no domínio primário e altere posteriormente o domínio do perfil. Você deve ter um usuário específico para cada domínio do seu perfil com `sn_si.admin` função. Use este usuário para criar ou modificar configurações no perfil.

- Desabilitar trabalhos agendados existentes.
- Replique o. IBM QRadar Fila de pesquisa do processo, o. IBM QRadar Perfis de processo e os trabalhos agendados Atualizações de infração para cada domínio.
- Mude **Executar como** do usuário do sistema para o usuário com `sn_si.admin` no respectivo domínio e execute o trabalho agendado.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tópicos relacionados

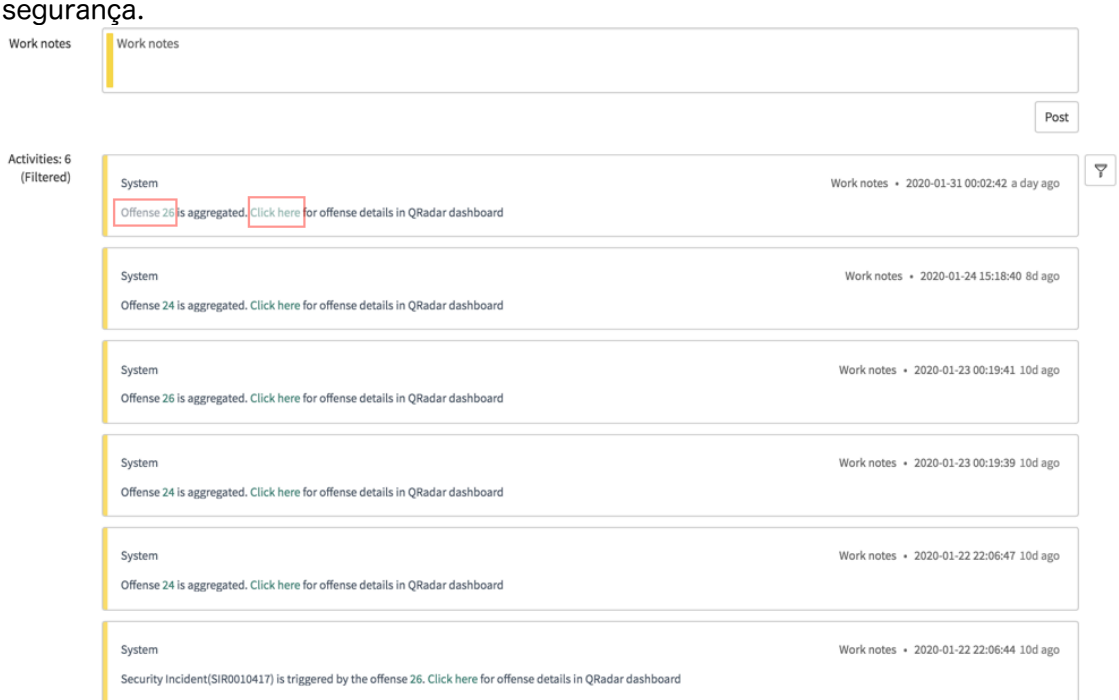
Domain Separation para provedores de serviço

Formulário de resposta a incidentes de segurança após ingestão de infração

Depois de um IBM QRadar a infração foi ingerida, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada com detalhes da infração que acionou o incidente de segurança.

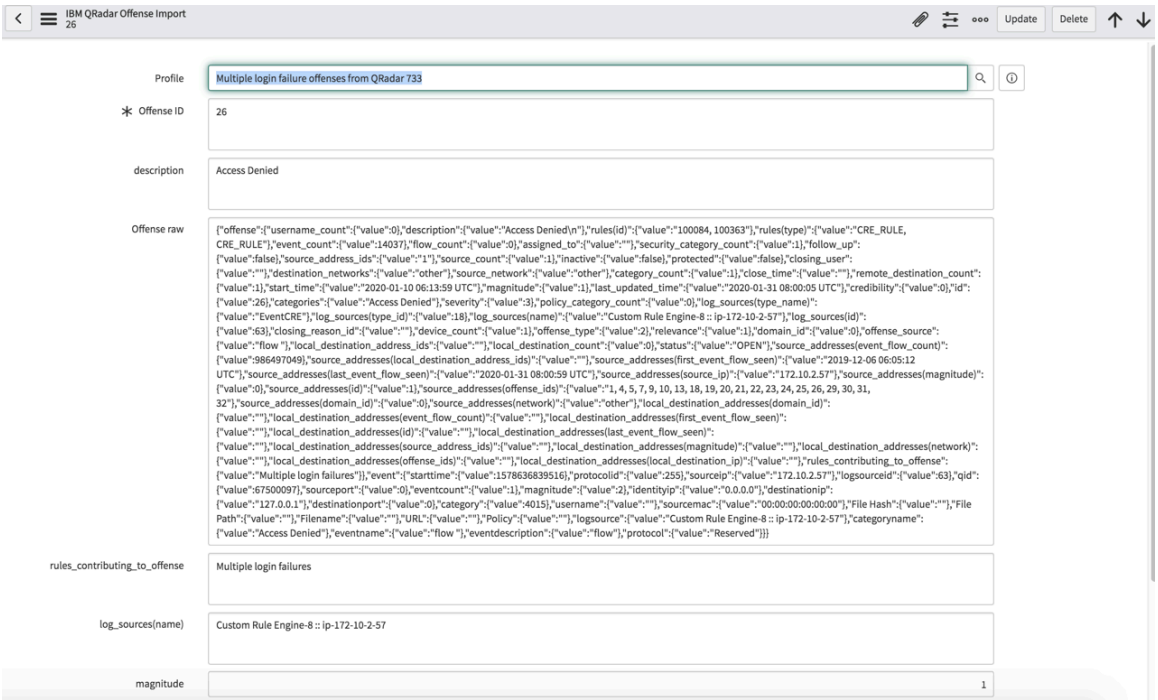


Clique no link de infração para navegar até o registro de incidente de segurança interno. . **Clique aqui** o hiperlink leva você para IBM QRadar painel onde você pode exibir os detalhes da infração.

Se você tiver selecionado **Registrar anotação de trabalho para nova infração** Opção nos Critérios de agregação de ofensa conforme descrito em Mapeamento IBM QRadar campos de infração para campos de resposta a incidentes de segurança uma anotação de trabalho é publicada quando a infração é agregada.

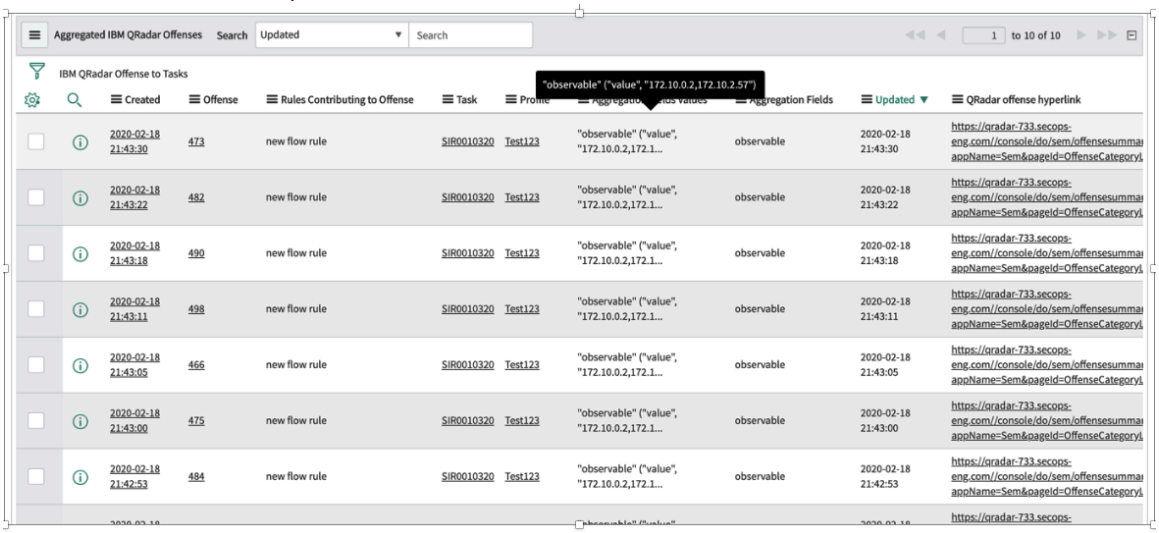
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Infrações agregadas

Clique **Listas relacionadas** > **Infrações agregadas do IBM QRadar** para exibir as infrações agregadas ao incidente de segurança. Clique no hiperlink Ofensão do QRadar para exibir a ofensa no IBM QRadar painel.

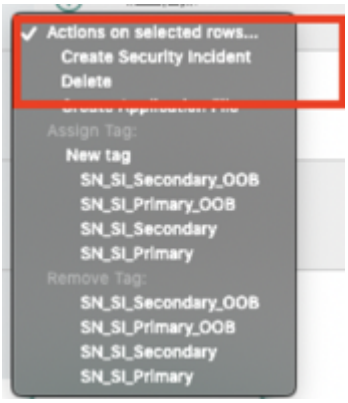


Criar incidente de segurança: Selecione uma infração na lista e clique em **Ações** e clique em **Criar incidente de segurança** . Esta opção cria um incidente de segurança para a infração e esta infração é desagregada do incidente de segurança primário.

Excluir registro de infração: Selecione uma infração na lista e clique em **Ações** e clique em **Excluir** . Esta opção exclui o registro de infração.

Tradução automática

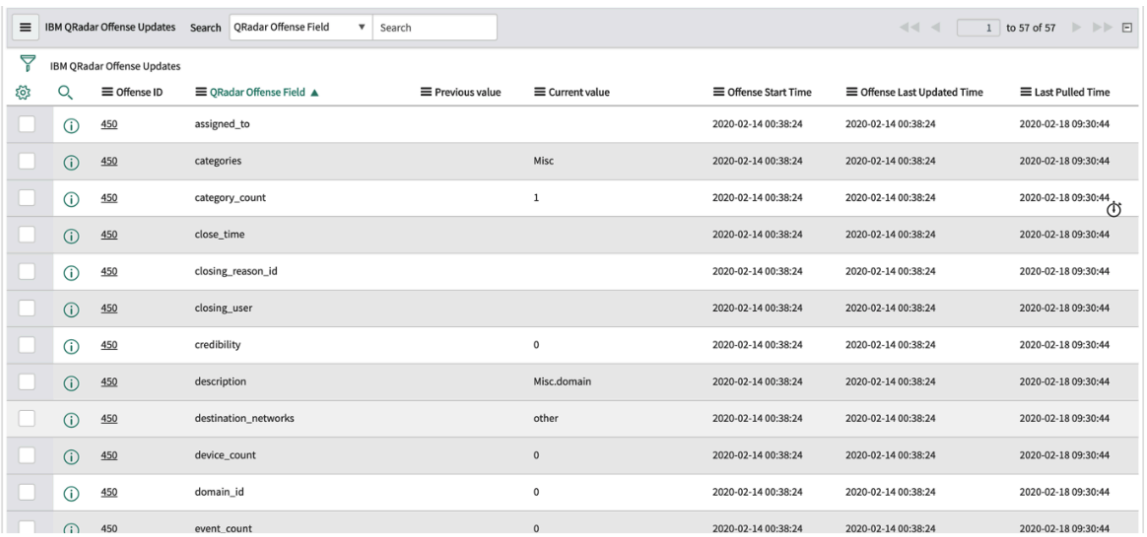
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Atualizações de ofensa do IBM QRadar

Mostra os campos de infração padrão e personalizado e rastreia as mudanças na infração durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir quaisquer atualizações de ofensa diretamente sem navegar até IBM QRadar painel. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.

Para habilitar o recurso de atualizações de infração, navegue até **Integração do IBM QRadar** > **IBM QRadar Integration Settings** e habilitar **Defina esta propriedade para ativar o recurso Atualizações de ofensa** . Por padrão, esta configuração está desabilitada.

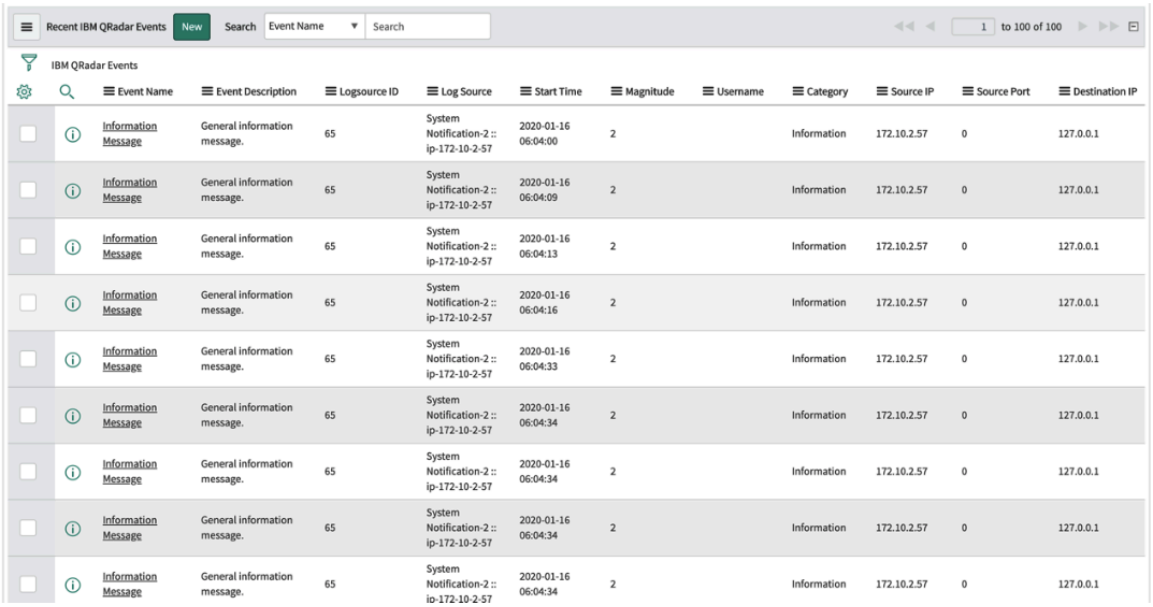


Eventos recentes do IBM QRadar

Clique em **Buscar eventos recentes do IBM QRadar** opção em **Links relacionados** para exibir o mais recente IBM QRadar eventos.

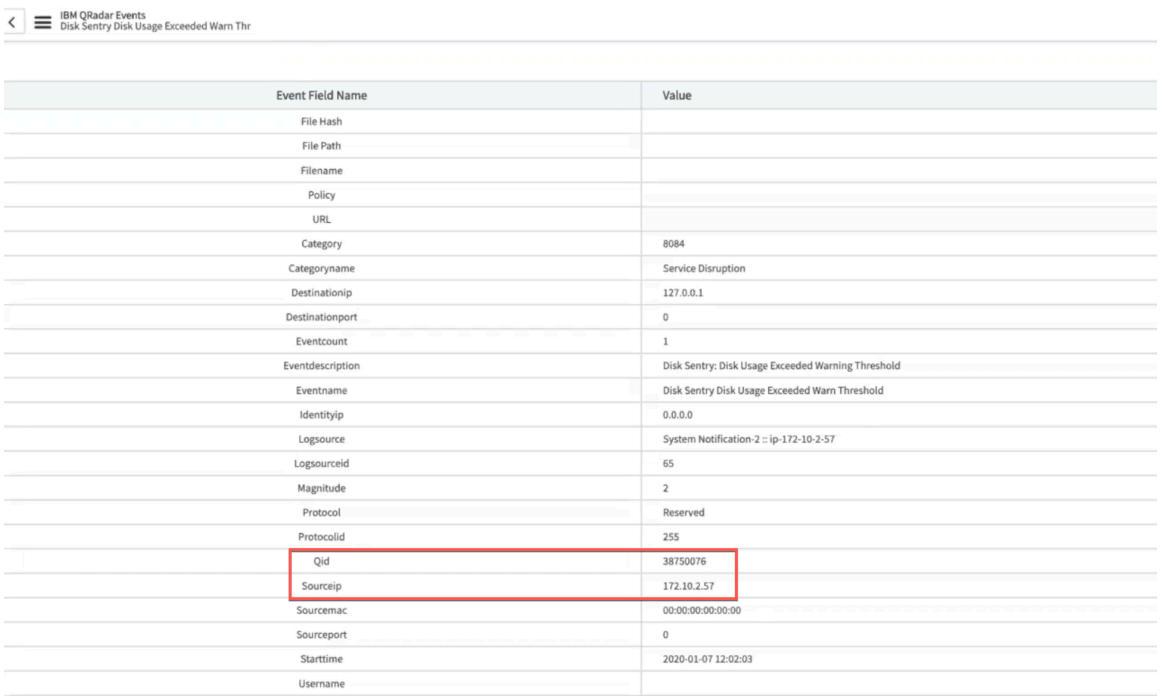
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, um número máximo de 100 eventos é exibido. Você pode modificar esta configuração padrão no Definições de configuração.

Nota: A imagem acima mostra os campos de evento padrão associados à infração. Se você configurou e mapeou campos de evento personalizados (consulte Mapeamento IBM QRadar campos de infração para campos de resposta a incidentes de segurança), você pode exibi-los na Exibição de lista clicando no link Nome do evento.

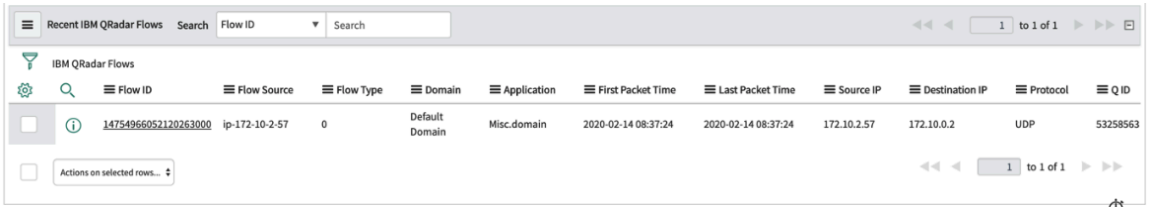


Fluxos recentes do IBM QRadar

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com o. IBM QRadar integração. Ao clicar em **Buscar fluxos recentes do IBM QRadar** Nos links relacionados, os fluxos mais recentes são recuperados. Para exibir esses fluxos, clique em **Fluxos recentes do IBM QRadar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, um número máximo de 100 fluxos é exibido. Você pode modificar esta configuração padrão no Definições de configuração.

Nota: A imagem acima mostra os campos de fluxo padrão associados à infração. Se você configurou e mapeou campos de fluxo personalizados (consulte Mapeamento IBM QRadar campos de infração para campos de resposta a incidentes de segurança), você pode exibi-los na Exibição de lista clicando no link ID de fluxo.

Flow Designer e uso do Integration Hub com integração de ingestão de ofensa do IBM QRadar

Usando a funcionalidade Flow Designer e Hub de integração, vários subfluxos e ações foram criados como parte do IBM QRadar integração de ingestão de ofensa.

A seguir IBM QRadar os subfluxos estão disponíveis:

- Validação de conexão e credencial : É usado no bloco de configuração para validar o host e as credenciais na configuração inicial.
- Recuperação de regras do IBM QRadar : Isso é usado na seção Regras da configuração do perfil para recuperar todas as regras ativas em IBM QRadar. Este subfluxo é acionado de forma assíncrona.
- Buscar dados de infrações de amostra do IBM QRadar : Isso é usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.
- Atualizações de status de infração do IBM QRadar : É acionado por um trabalho agendado a cada minuto e atualiza a infração em IBM QRadar quando o incidente de segurança é criado ou encerrado.
- Perfis de processo de trabalho programado e infrações de fila : Isso é acionado por um trabalho agendado a cada minuto para extrair infrações por perfil com base no intervalo de pesquisa. Extrai as infrações e as coloca na fila da tabela de pesquisa para processamento posterior.
- Processar fila de pesquisa e pesquisa em lotes : Isso é acionado por um trabalho agendado a cada 30 segundos para processar a fila da tabela de pesquisa.
- Buscar fluxos recentes do IBM QRadar : Isso é acionado a partir do link do formulário de incidente de segurança para obter os fluxos de infração mais recentes.
- Buscar eventos recentes do IBM QRadar : Isso é acionado a partir do link do formulário de incidente de segurança para obter os eventos de infração mais recentes.

Para exibir esses subfluxos, faça login como um usuário com `sn_si.admin` e navegue até **Flow Designer** > **Designer**. Clique no link Nome de qualquer um dos subfluxos listados acima para exibir o subfluxo em detalhes.

Solução de problemas IBM QRadar integração de ingestão de ofensa

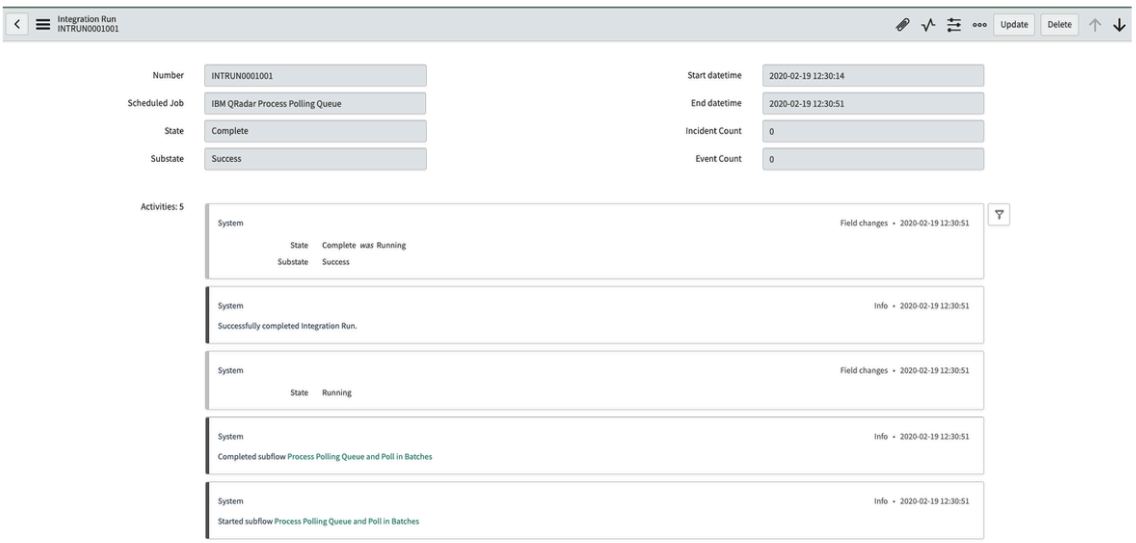
Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas a. IBM QRadar ingestão de ofensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Execução de integração: Quando um trabalho agendado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de infrações extraídas e o número de incidentes criados em uma execução de trabalho programada também são exibidos. Usuários com a função sn_si.analyst podem ver se houve falha na extração de erros/perfis durante a execução da integração.

  As anotações de trabalho na execução de integração fornecem links para os subfluxos executados. Usuários com a função sn_si.analyst podem verificar o. `sn_event_ingestion_integration_run` tabela para todos os erros que ocorreram. Para solucionar quaisquer problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações de trabalho nos registros de execução de integração para cada execução de trabalho programada.



- Problemas de SSL: Ao se conectar ao IBM QRadar Instâncias de nuvem, certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 para obter detalhes.
- Perfil incompleto: Ao configurar o perfil, nas Opções adicionais (Automatize atualizações de infração e fechamento com base no status do incidente SIR), você deve clicar em **Concluir** Botão para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando ingestão.
- Validar perfil: Para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de ofensa, os registros da tabela de ofensa para tarefa.
- Configuração DO MID Server: Se você estiver instalando o. IBM QRadar Aplicação no local, depois de configurar o MID Server, você deve criar uma aplicação do MID Server. O nome da aplicação do MID Server deve ser usado no bloco de configurações de integração em vez do nome do MID Server.

  Nota: O tempo limite do MID Server padrão é de 30 segundos. Para ver instruções sobre como desabilitar o período de tempo limite, consulte <link>. Observe que esta é uma mudança em todo o sistema e pode afetar outras integrações.

- Atualizações de ofensa: Se você habilitou o. *`sn_sec_qradar.get_ofense_updates`* e você percebe um atraso na criação de incidentes de segurança e, em seguida, desabilita

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a propriedade. Não habilite esta propriedade quando o intervalo de pesquisa for baixo e a carga de ofensas no QRadar for alta, pois isso aumenta a carga da fila.

- Evento, dados de fluxo, remote_ip ou dados de usuários ausentes em um incidente de segurança: Se você observar que os dados de evento, dados de fluxo, remote_ip ou usuários estão ausentes em um incidente de segurança, aumente o tempo limite (segundos) para `sn_sec_qradar.sid_ttl` parâmetro. Aumentar a duração atrasa a criação do incidente de segurança até que os AQLs concluam a análise de cada infração.
- Tempos limites: Se você exibir erros de tempo limite nos logs da aplicação, revise e modifique as seguintes ações do Flow Designer:

Ações do Flow Designer

Parâmetros	Ação
Buscar exemplos de infrações Sn_fd.FlowAPI.executeAction(sn_sec_qradar.fire_rest_for_offences', flow_inputs, 60000);	Revise e atualize a duração em milissegundos.
Buscar exemplos de infrações Sn_fd.FlowAPI.executeAction(sn_sec_qradar.fire_rest_for_ofences', flow_inputs);	Adicione um parâmetro para `ExecutoAction` e insira a duração em milissegundos.
Buscar infrações para registros de perfil e fila na tabela de pesquisa Sn_fd.FlowAPI.executeAction(sn_sec_qradar.fire_rest_for_offences', flow_inputs, 180000);	Revise e atualize a duração em milissegundos.
Wrapper para testar REST de conexão REST_outputs: Sn_fd.FlowAPI.executeAction(sn_sec_qradar.test_connection_rest', rest_inputs);	Adicione um parâmetro para `ExecutoAction` e insira a duração em milissegundos.
Wrapper para validar REST de credenciais de API REST_outputs: Sn_fd.FlowAPI.executeAction(sn_sec_qradar.validate_credentials_rest', rest_inputs);	Adicione um parâmetro para `ExecutoAction` e insira a duração em milissegundos.
Etapa REST para atualizações de infração do IBM QRadar Resultado da variável: Sn_fd.FlowAPI.executeAction('sn_sec_qradar.' restStep, inputs,60000);	Revise e atualize a duração em milissegundos.

IBM QRadar - Integração de aprimoramento de incidentes

. IBM QRadar- A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

- Comece a usar IBM QRadar Integração de aprimoramento de incidentes
- Criar registros de configuração de pesquisa de vistas

Usar

- Execute uma Pesquisa de vistas
- Integração de operações de segurança - Fluxo de pesquisa de vistas
- Operações de segurança - Fluxo de pesquisa de vistas do QRadar
- Exibir detalhes da pesquisa de vistas
- Exibir resultados da pesquisa de vistas

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Comece a usar IBM QRadar Integração de aprimoramento de incidentes

IBM QRadarÉ um produto de gestão de eventos e informações de segurança empresarial (SIEM) que se integra facilmente ao Operações de segurança. Antes de poder usar IBM QRadar- Integração de aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicione a URL base da API apropriada e a chave de API.

Antes de Iniciar

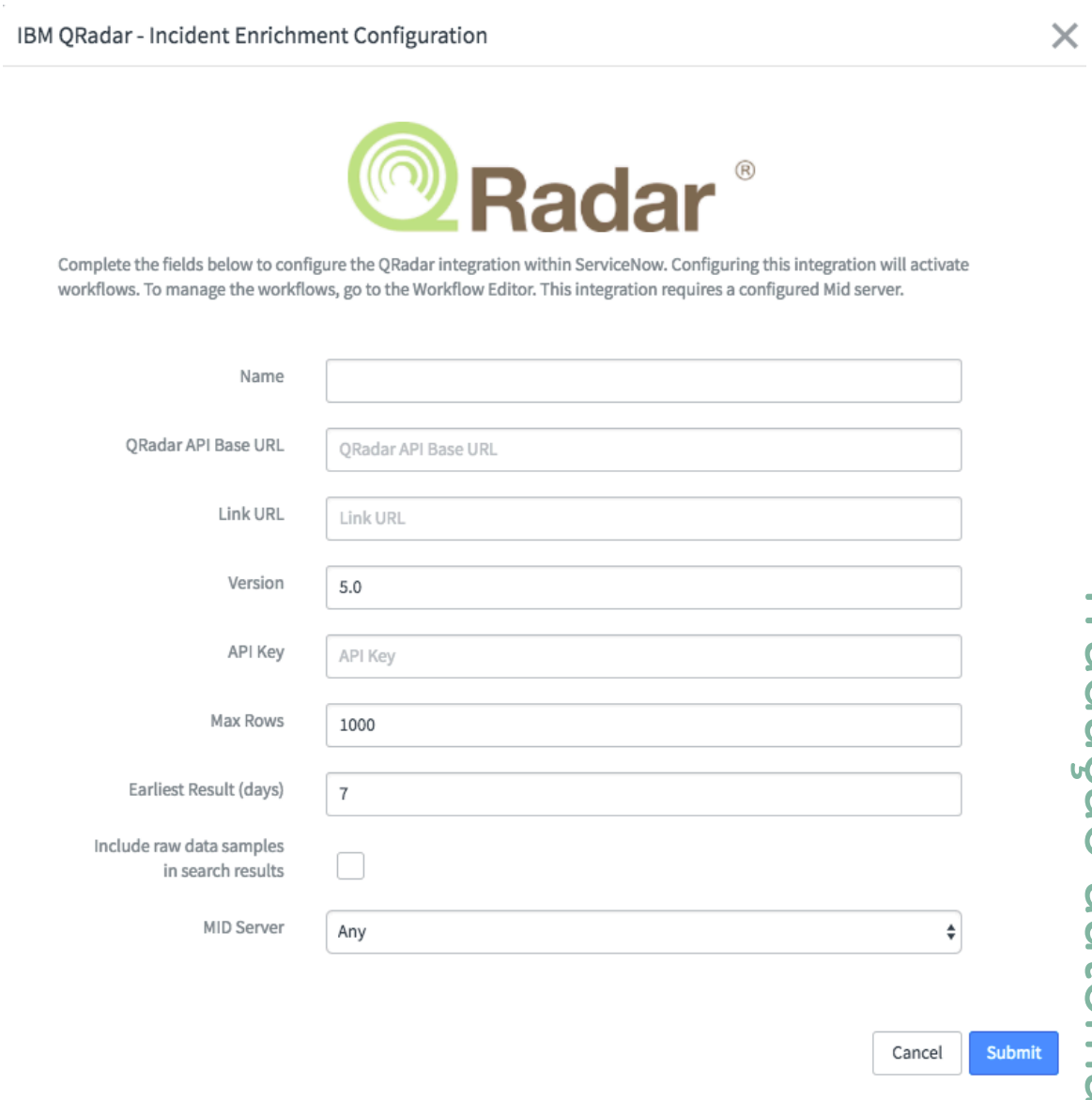
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse IBM QRadar E obtenha o URL base da API e a chave de API em seu IBM QRadar perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. Em IBM QRadar- Cartão de aprimoramento de incidente, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de Base de API do QRadar	O URL base que você adquiriu do IBM QRadar site.
URL do Link	[Opcional] O URL do link vinculado a um IBM QRadar instância, quando disponível.
Versão	. IBM QRadar versão; 5,0 é o padrão.
Chave de API	A chave de API que você obteve do IBM QRadar site.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no **número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

LogRhythm Visão geral

A flexibilidade de mapeamento dessa integração fornece ao analista visibilidade de eventos e dados de alarme relacionados que podem ser integrados ao ServiceNow AI Platform incidentes de segurança para investigação e correção adicionais.

Os perfis de alarme são criados em seu ServiceNow AI Platform instância para personalizar o quão diferente LogRhythm os campos de alarme são exibidos em um ServiceNow AI Platform incidente de segurança. Um mapeamento padrão de campos de alarme é fornecido, que pode ser editado para atender às necessidades específicas do cliente.

A figura a seguir é um exemplo de um ambiente do cliente. Quando um evento aciona a criação de um incidente de segurança no ServiceNow AI Platform® uma solicitação é enviada do seu ServiceNow AI Platform® instância para extrair alarmes do LogRhythm Console do cliente por meio de um MID Server ou até mesmo sem ele.

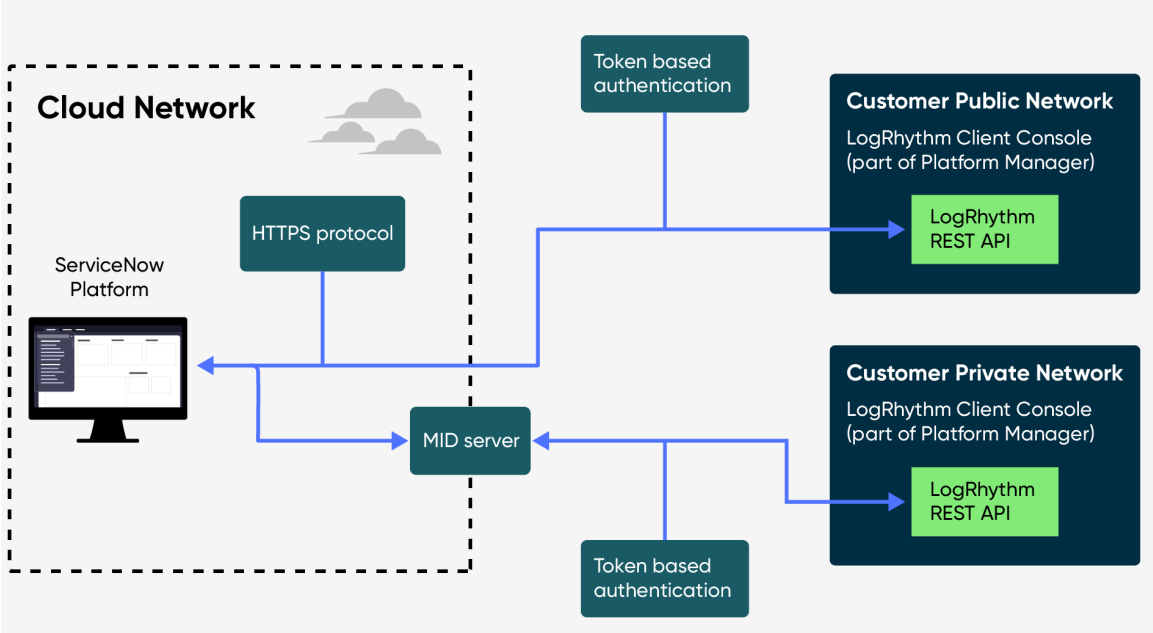
A chave REST API é usada pelo ServiceNow AI Platform® para autenticar com LogRhythm Console do cliente. Esta conexão permite seu ServiceNow AI Platform instância para extrair individual LogRhythm alarmes baseados em perfis configurados.

A REST API é usada para coletar detalhes da mensagem não acessados pela REST API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração com a LogRhythm



Principais recursos

Esta integração inclui os seguintes recursos principais:

- Flexibilidade para criar vários perfis de alarme para diferentes tipos de alarme, como Phishing e. Malware .
- Mapeamento de arrastar e soltar de LogRhythm valores de campo de alarme a associados SIR campos de incidente de segurança.
- Uma visualização do SIR layout de incidente de segurança baseado em LogRhythm alarmes de amostra.
- Ingerir alarmes históricos, bem como alarmes futuros em andamento em intervalos configuráveis.
- Automatizado LogRhythm fechamento do alarme em SIR fechamento do incidente. Um URL para SIR O incidente, bem como um ID de incidente, é fornecido para facilitar a referência.

Versões compatíveis do ServiceNow AI Platform

Esta integração é compatível com Quebec ou versões posteriores do ServiceNow AI Platform®.

Versões compatíveis de LogRhythm

Esta integração é compatível com LogRhythm7,8 ou posterior. As versões anteriores não são compatíveis devido a limitações de API.

Nota: Os tópicos a seguir são numerados. Para uma instalação tranquila e ajudar você a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Configure a REST API para LogRhythm

Você usa LogRhythm Chave REST API para coletar detalhes adicionais do evento para campos de alarme individuais. A chave de API fornece detalhes que não estão disponíveis usando LogRhythm REST API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

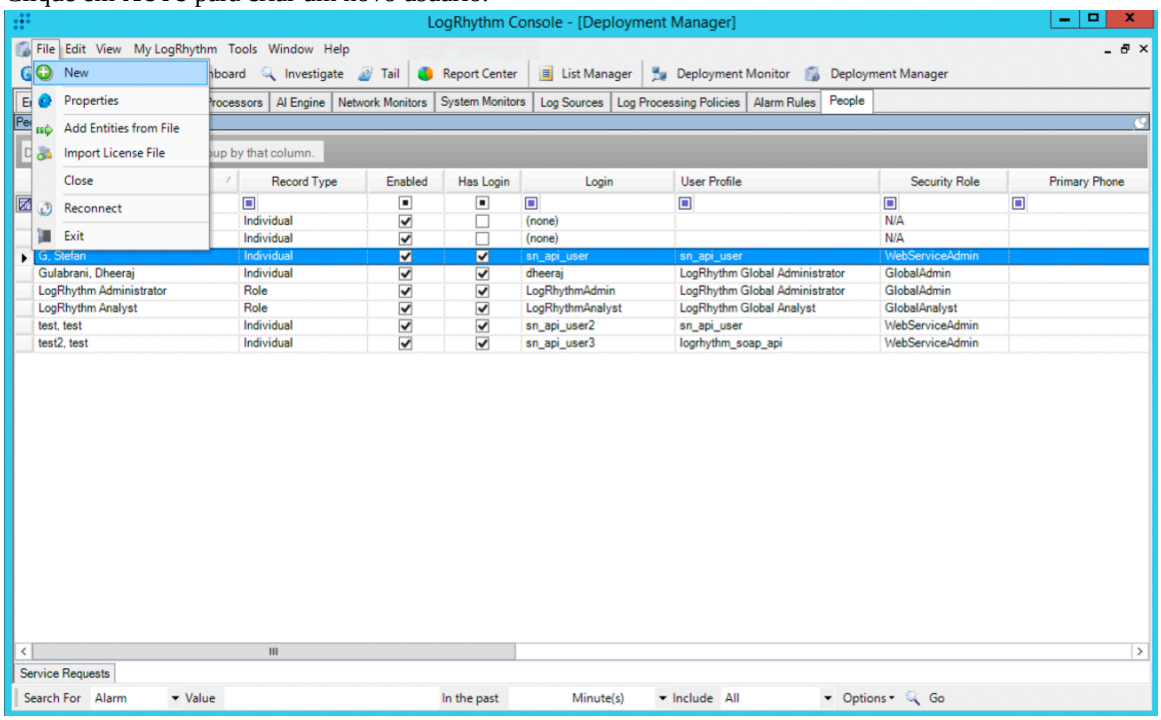
Função necessária: LogRhythm Administrador do gerenciador de plataforma/console do cliente

Por Que e Quando Desempenhar Esta Tarefa

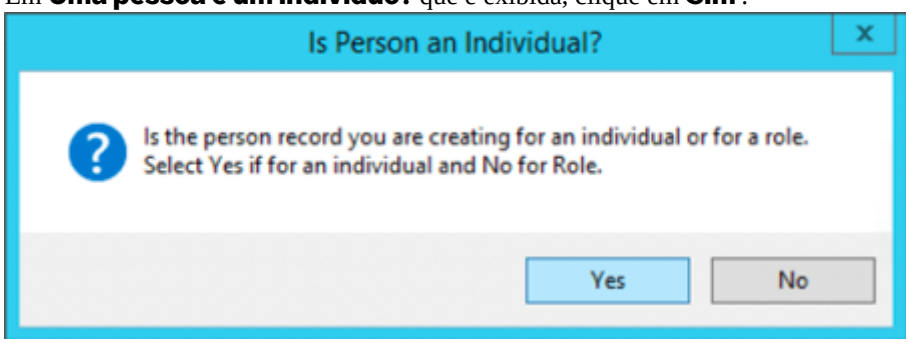
Esta tarefa é executada no LogRhythm Console do cliente. Configure o. LogRhythm REST API antes de instalar o plug-in do ServiceNow Store.

Procedimento

1. Navegue até LogRhythm Console do cliente e selecione **Arquivo** menu.
2. Clique em **Novo** para criar um novo usuário.



3. Em **Uma pessoa é um indivíduo?** que é exibida, clique em **Sim** .

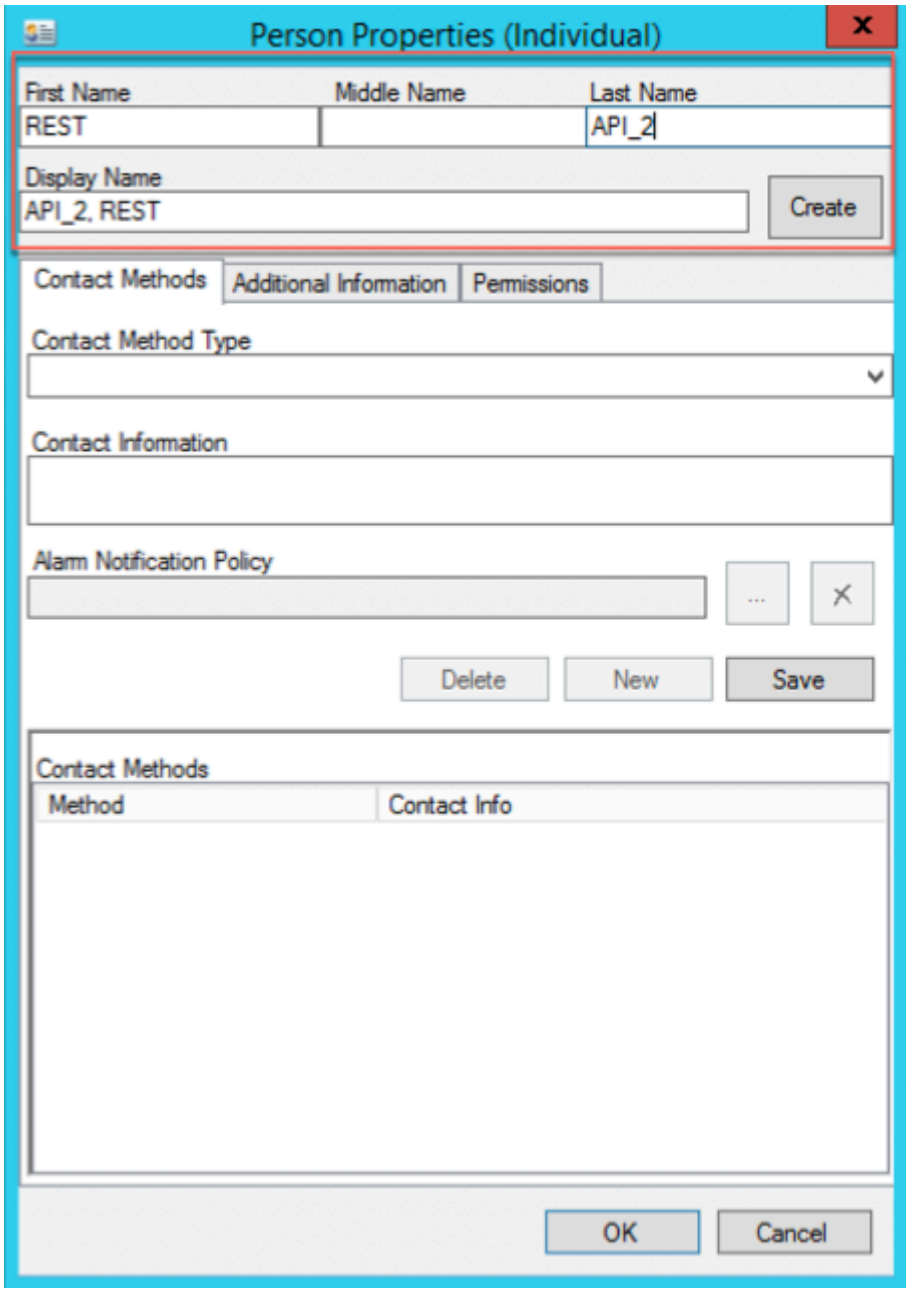


4. Na caixa de diálogo Propriedades da pessoa exibida, preencha os campos Nome.

   Use um nome diferente para LogRhythm REST API do que a usada para criar a REST API, por exemplo, REST API_2 .

Tradução automática

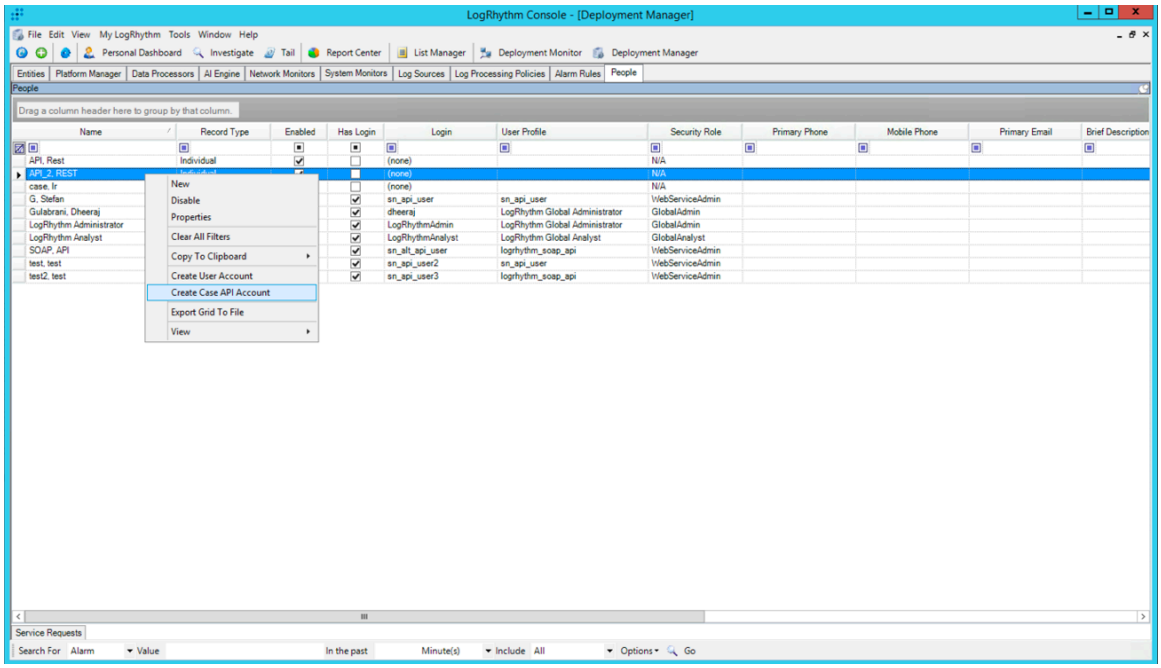
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **OK**.
6. Clique com o botão direito do mouse na nova listagem na coluna Nome (**API_2_REST**) e, na lista de seleção, selecione **Criar conta de API de caso** .

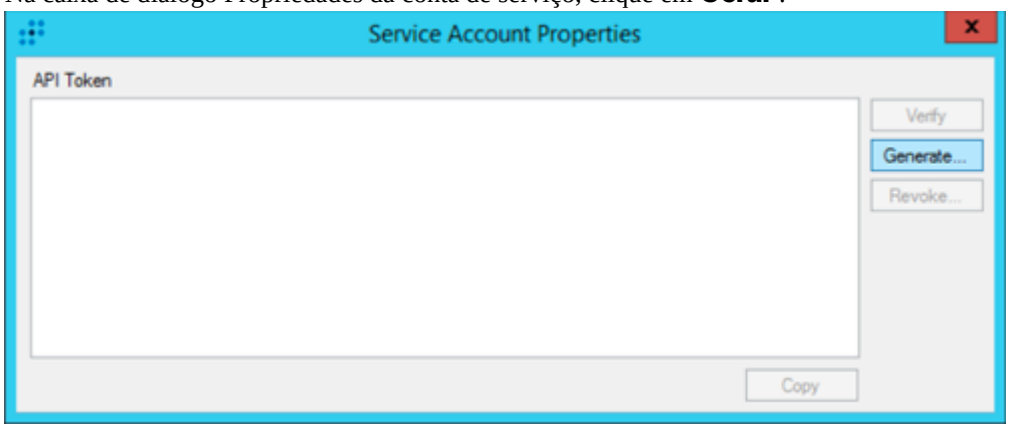
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

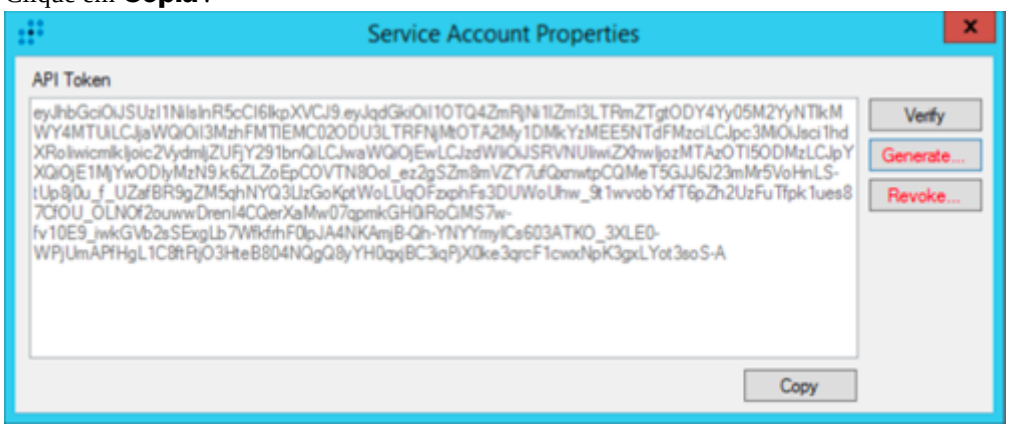


Nota: A API do caso não é usada, mas as credenciais da conta da API do caso e do LogRhythm REST API são iguais.

7. Na caixa de diálogo Propriedades da conta de serviço, clique em **Gerar** .



8. Clique em **Cópia** .



Agora você configurou o. LogRhythm REST API. Cole a cadeia de caracteres copiada na etapa anterior em seu ServiceNow AI Platform instância no LogRhythm Campo Token da REST API durante as etapas de configuração listadas em Instale o plug-in e configure LogRhythm.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você está pronto para Instale o plug-in e configure LogRhythm.

Instale o plug-in e configure LogRhythm

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação se integre corretamente ao Operações de segurança em ServiceNow AI Platform®.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves. Mais recente LogRhythm a versão é 7,8 ou posterior.

Nota: Seus perfis de alarme existentes não serão mais compatíveis com o mais recente LogRhythm, portanto, você precisa criar novos perfis de alarme e executar as configurações necessárias.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform® E Resposta a incidentes de segurança (SIR).	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o plug-in da aplicação e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O (sn_si.admin) supervisiona as seguintes tarefas: ◦ Cria e edita perfis de alarme. ◦ Mapas e filtros de alarmes - Identifica específicos LogRhythm alarmes que criam incidentes de segurança e configuram como esses campos de alarme são mapeados para um ServiceNow AI Platform® incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração. ◦ Ingere alarmes históricos e cronogramas de alarmes extraídos. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Esta função também tem acesso ao Operações de segurança módulo. • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança que são criados com base nas configurações do perfil de alarme.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Obtenha um LogRhythm Nome de usuário e senha da API e verifique se você está usando a versão LogRhythm7,8 ou posterior.	Visite o site do produto para obter informações sobre chaves de API e para criar uma conta: Site da LogRhythm Enterprise . As contas de usuário, credenciais e certificados devem ser configurados corretamente antes de instalar a aplicação. A integração requer LogRhythm versão 7,8 ou posterior e LogRhythm REST APIs. Consulte Configure a REST API para LogRhythm.
Verifique se você instalou e configurou um MID Server.	Um MID Server é necessário em seu ServiceNow AI Platform ambiente. Consulte Site de documentação do produto da ServiceNow Para obter informações sobre como instalar e configurar MID Servers.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Para a versão Rome e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

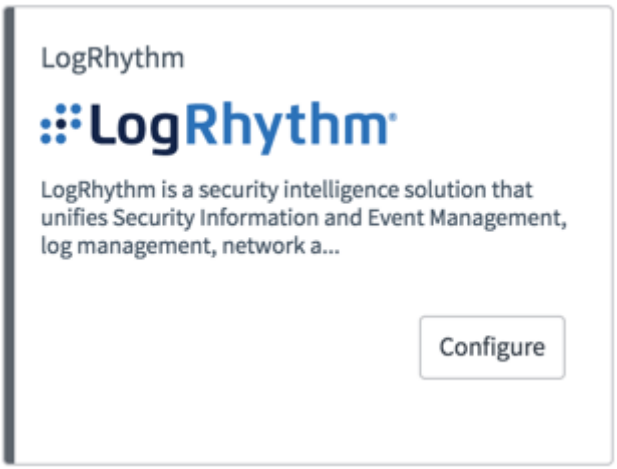
Importante: Se você tiver problemas de conectividade com LogRhythm console do cliente, consulte Verifique a conectividade para LogRhythm.

Tradução automática

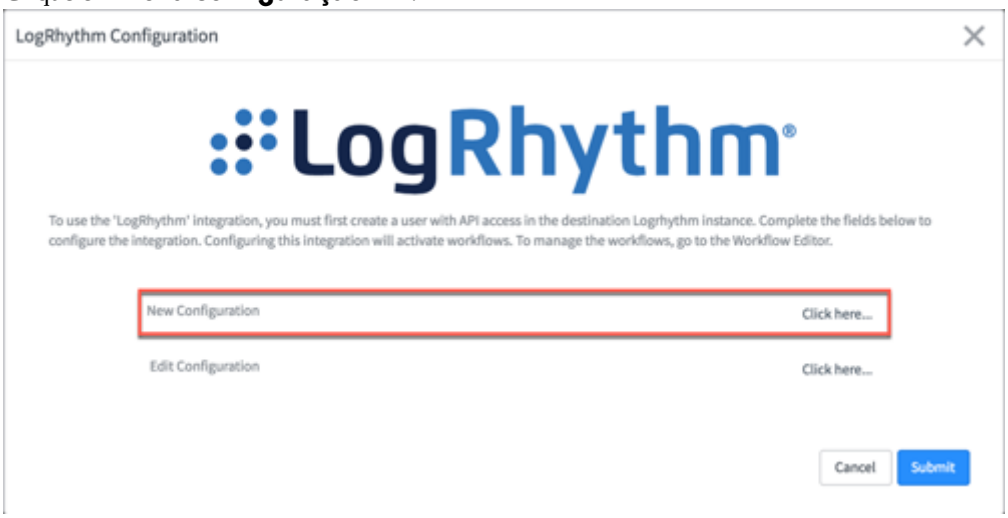
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Quando a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize LogRhythm lado a lado.
3. Clique em **Configurar**.



4. Clique em **Nova configuração** link.



5. No formulário, preencha os campos:

Configuração da LogRhythm

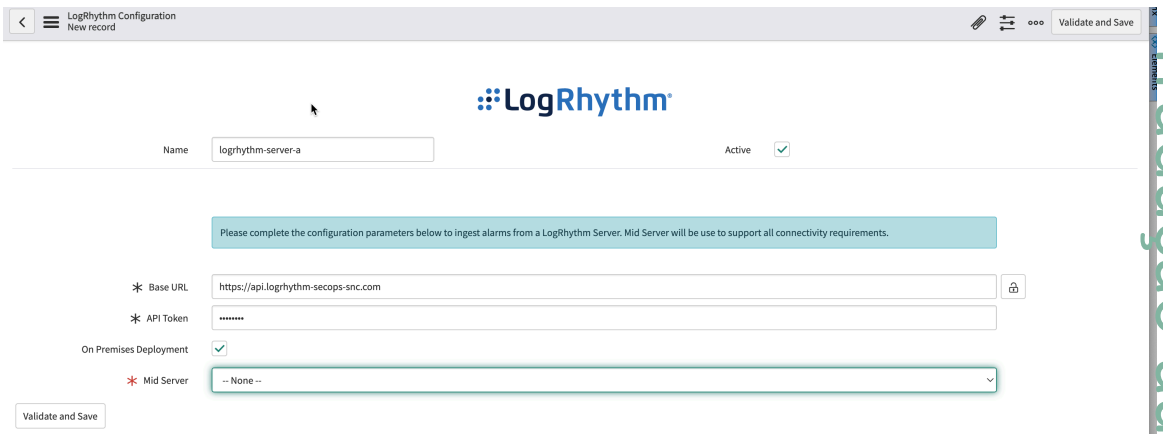
Campo	Descrição
Nome	LogRhythm nome do servidor, por exemplo, logrhythm-server-a. .
URL base	URL base que hospeda o. LogRhythm REST API. O MID Server permite acesso à rede em que o Console do cliente da LogRhythm está hospedado. Este URL é onde LogRhythm o servidor está hospedado nessa rede. Clique no ícone de cadeado na

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	extremidade direita para editar o campo e inserir o texto de um URL, por exemplo, https://logrhythm.secops-eng.com:8501/ .
Token de API	Insira o token associado à REST API que você criou no LogRhythm Console do cliente.
Implantação no local	Opção para selecionar se for um LogRhythm implantação no local.
MID Server	MID Server específico que está configurado em seu ambiente. Somente os MID Servers que estão ativos e foram validados estão disponíveis nesta lista de seleção.

A figura a seguir é um exemplo de um formulário preenchido.



6. Clique em **Valide e salve** .
   Após a validação ser concluída com sucesso, uma mensagem será exibida e o LogRhythm A página de configurações foi recarregada. A próxima etapa é criar um perfil de alarme.

O que Fazer Depois

Depois de concluir a validação com sucesso, a próxima etapa é a. Criando um perfil de alarme para LogRhythm.

Criando um perfil de alarme para LogRhythm

Em um perfil de alarme que você cria e nomeia, você especifica quais alarmes deseja extrair do LogRhythm Console do cliente. Você também define como eles são mapeados para campos em um ServiceNow AI Platform incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Com base no perfil de alarme configurado, um perfil de alarme pode ingerir todos os tipos de alarmes prontos para uso, mas você pode usar critérios de filtro para ingerir tipos específicos de alarmes. Usando isso ServiceNow AI Platform todas as regras de alarme configuradas ou específicas com base no perfil criado são ingeridas. Regras de alarme, como somente alarmes de nível de alto risco, podem ser filtradas para especificar quais alarmes devem criar incidentes de segurança. Antes que os incidentes de segurança sejam criados, os valores de campos individuais nos alarmes filtrados são mapeados

Tradução automática

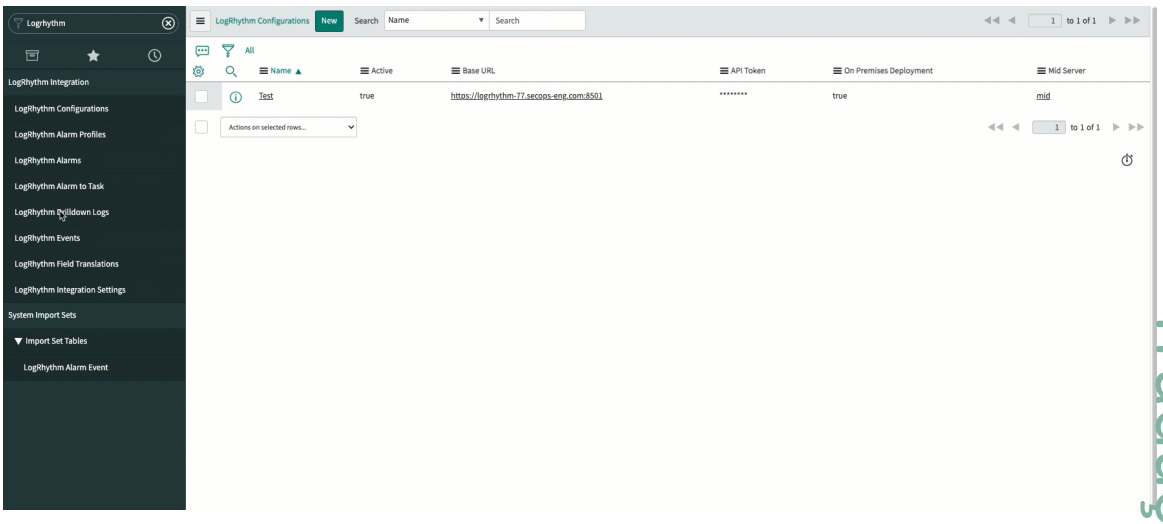
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para os campos correspondentes no ServiceNow AI Platform incidente de segurança. Esta configuração é feita por meio de um perfil de alarme em seu ServiceNow AI Platform instância.

Procedimento

1. Navegar até **Tudo** > **Integração com LogRhythm**.
2. Selecione **Perfis de alarme da LogRhythm** módulo para exibir o. **Perfis de alarme** lista.

Perfil do Alarme



3. Para criar um novo perfil de alarme, clique em **Novo** .
   Um novo formulário de perfil de alarme é exibido. Na parte superior da página na barra de andamento, **Nome** selecionado. Esta barra rastreia seu andamento durante a configuração.
4. No formulário, preencha os campos.

Perfil do Alarme

Campo	Descrição
Nome	Nome do perfil de alarme. Este nome ajuda a identificar os tipos de alarme, como *Acesso não autorizado* (*VPN*), *malware* ou *phishing* .
Descrição resumida	Texto curto para obter informações adicionais sobre o perfil de alarme, que pode incluir o tipo de alarmes ou uma categoria de alarme. Um exemplo de descrição: Todos os alarmes associados a tentativas de acesso não autorizadas ao PowerShell e sudo.
Origem	Servidor de origem na lista de seleção. A lista consiste em LogRhythm configurações que você já definiu, por exemplo, logrhythm-server-a. . Consulte Instale o plug-in e configure LogRhythm.
Ordem	Prioridade do perfil de alarme. Este campo indica a ordem na qual os perfis de alarme são executados quando dois ou mais perfis de alarme compartilham as condições de acionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Esta opção não está selecionada por padrão. Depois de concluir todas as etapas de configuração do perfil de alarme e clique em **Concluir** você será solicitado a marcar esta caixa de seleção para ativar o perfil de alarme. Quando o perfil de alarme está ativo, ele extrai alarmes do LogRhythm Console do cliente automaticamente.

5. Clique em **Continuar** Para salvar seus dados e prosseguir para o formulário Mapeamento.

   Se a validação for bem-sucedida, a página será recarregada e **Mapeamento** o formulário é exibido. Você não pode prosseguir com a configuração até validar com sucesso sua conexão e credenciais.

Tópicos relacionados

Mapeamento

Mapeamento

Depois de selecionar LogRhythm origem que você deseja ingerir, você precisa mapear individual LogRhythm campos de alarme para ServiceNow AI Platform campos de incidente de segurança.

O mapeamento de alarmes inclui as seguintes tarefas:

- Mapa LogRhythm alarmes. Para esta tarefa, você lista e ingira (extrai) alarmes de amostra usando os IDs de alarme ou os alarmes mais recentes do LogRhythm console do cliente.
- Os campos Alarme de amostra são categorizados em três grupos:
  - Campos de alarme : Os campos de alarme que estão disponíveis e seus valores correspondentes são exibidos.
  - Campos de evento : Os campos de evento que estão disponíveis e seus valores correspondentes são exibidos.
  - Campos DrillDowLog : Os campos de log de detalhamento que estão disponíveis e seus valores correspondentes são exibidos.
- Cada ID de alarme que você extraiu é exibido como uma guia. Nas guias ID do alarme, verifique se todos os campos de alarme críticos do Ingestão de amostra de alarme a seção à esquerda do formulário é mapeada para Mapeamento de campo de incidente DO SIR à direita do formulário.
- Depois de mapear os alarmes para Mapeamento de campo de incidente DO SIR , você pode ver a categoria de alarme também sendo exibida no Expressão de entrada campo. Por exemplo, `(Alarme: Alarmid)` .
- Você pode modificar a configuração adicionando ou removendo campos no incidente de segurança. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Você pode filtrar alarmes para especificar quais alarmes são ingeridos na aplicação SIR. Você pode filtrar os alarmes diretamente ou usar as categorias de alarme para detalhar sua pesquisa com base em Alarmes, Eventos ou DrillDowLogs.
- Use o editor de script se quiser formatar valores para os campos Prioridade e Categoria no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A próxima etapa é a. Mapa LogRhythm campos de alarme para campos de incidente de segurança.

Tópicos relacionados

Mapa LogRhythm campos de alarme para campos de incidente de segurança

Use o editor de scripts para formatar LogRhythm valores

Alarmes de filtro para LogRhythm

Mapa LogRhythm campos de alarme para campos de incidente de segurança

Campos de alarme individuais são mapeados para os campos de incidente de segurança. O mapeamento pré-configurado pode ser editado, e a codificação de cores fornecida para os campos ajuda a monitorar os alarmes que você já mapeou. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Se você não estiver familiarizado com LogRhythm alarmes, navegue até LogRhythm Console do cliente e revise alguns IDs de alarme de amostra. Para o exemplo a seguir, LogRhythm alarmes `9468` e. `9474` foram usados para mapear os alarmes para o incidente de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Usando este formulário, você mapeia o. LogRhythm regras de alarme à esquerda para os campos de incidente de segurança à direita.

A figura a seguir mostra o mapeamento padrão de alarmes que é pré-configurado para cada perfil de alarme. Este mapeamento padrão pode ser editado e, com este formulário, você pode personalizar os campos que preenchem o incidente de segurança. Depois de concluir este mapeamento, você poderá ver como adicionar ou remover campos de alarme afeta potencialmente os valores de campo no incidente de segurança.

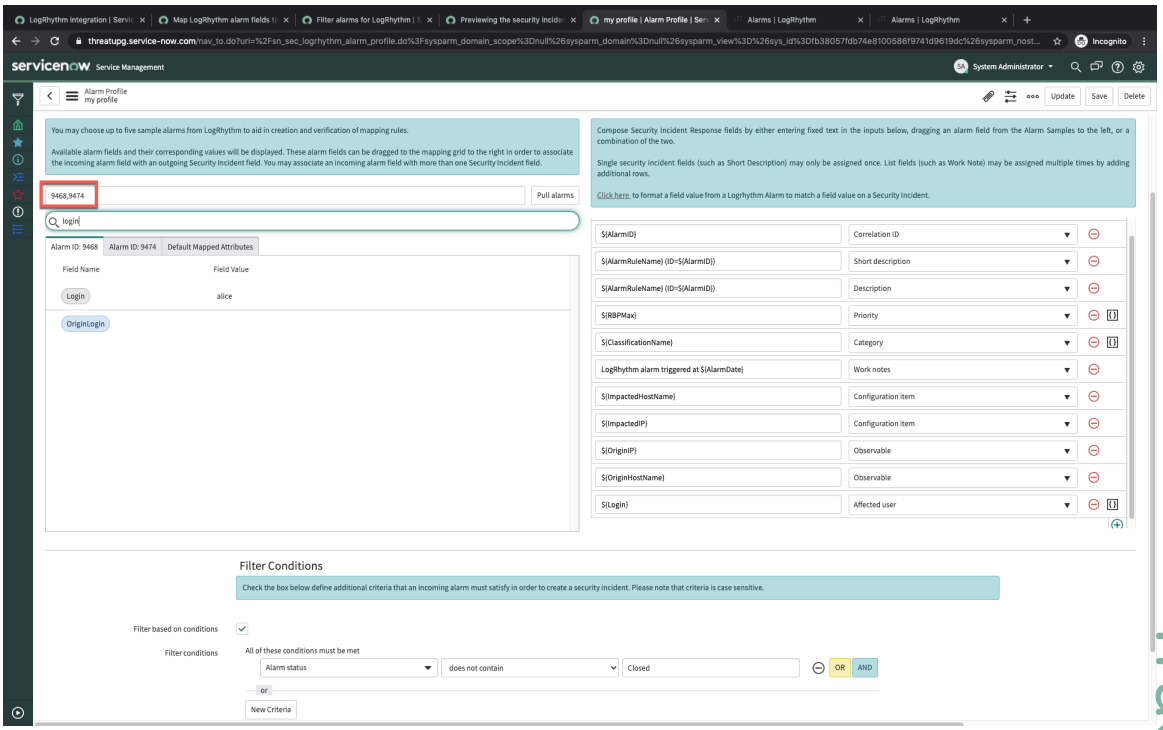
No lado esquerdo deste formulário, na figura a seguir, o. LogRhythm as regras de alarme são descritas. Os valores dessas regras de alarme são mapeados para os campos de incidente de segurança no lado direito do formulário.

Procedimento

1. Depois de criar um perfil de alarme para a LogRhythm, clique em **Mapeamento** na barra de andamento.
2. Em **Ingestão de amostra de alarme** , insira até cinco amostras LogRhythm IDs de alarme separados por vírgulas (`9468,9474`).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Ao lado do campo de alarme, clique em **Extrair alarmes** .

A extração de alarmes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Depois que os IDs de alarme de amostra são enviados e extraídos com sucesso do LogRhythm servidor, os campos de alarme e seus valores correspondentes são exibidos em guias.

Nota: Depois que um ID de alarme é extraído com sucesso, o. ServiceNow AI Platform pode retornar a seguinte mensagem: Os novos campos a seguir estarão disponíveis para filtragem em breve. Recarregue este perfil em alguns minutos se a filtragem com base nesses campos for necessária. itemspacketssout, itemspacketout .

Esta mensagem ocorre quando o alarme único que foi extraído contém nomes de campo não processados anteriormente pelo ServiceNow AI Platform. Esses campos estão disponíveis para mapeamento. No entanto, se esta mensagem for exibida, recarregue o formulário para que esses campos sejam exibidos e disponíveis nas listas de seleção de filtro do construtor de condições quando você estiver pronto para definir condições de filtragem.

Ingerir esses alarmes de amostra na configuração do perfil de alarme ajuda a impedir o mapeamento de campos de alarme para o incidente de segurança que não contêm valores. Também alinha os campos de alarme com valores aos campos apropriados no incidente de segurança. Esta etapa garante que todos os campos de alarme críticos sejam mapeados e que não haja valores de campo ausentes no incidente de segurança.

Para ajudar você a garantir que nenhum alarme seja ignorado ou duplicado no processo de mapeamento, os campos de alarme são codificados por cores. Um campo de alarme azul claro (Conta , ID de regra do alarme , AlarmStatus , etc.) indica que um campo ainda não foi selecionado para mapeamento para um incidente de segurança.

Um campo cinza (AlarmDate , AlarmID e AlarmRuleName) indica que um campo já foi selecionado e foi mapeado para um campo no incidente de segurança. Essa codificação por cores ajuda a rastrear o mapeamento, porque, em determinados casos, um campo

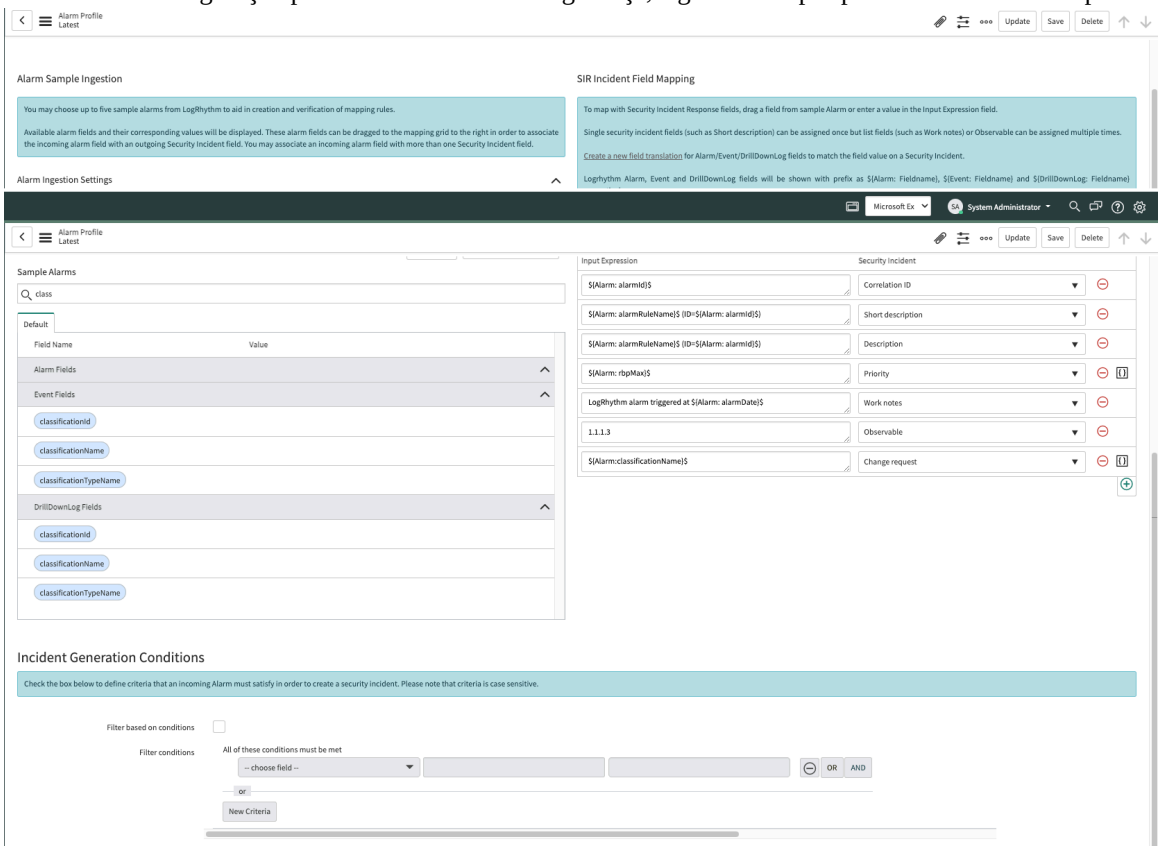
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de alarme pode ser mapeado para mais de um campo em um incidente de segurança. Por exemplo, o. Observáveis e. Anotação de trabalho os campos podem ter mais de um valor.

4. Para limpar os dados de alarme de amostra, clique em **Limpar dados de alarme de amostra** .

5. Para editar a configuração padrão no incidente de segurança, siga estas etapas para adicionar um campo:



a. No canto inferior direito do formulário, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, selecione um campo disponível na lista de seleção.

Na lista de seleção expandida, alguns dos campos estão sombreados. Por exemplo, Categoria tem um fundo cinza, o que indica que ele foi mapeado no incidente de segurança. Semelhante à codificação por cores para LogRhythm campos de alarme, essa codificação de cores para os campos de incidente de segurança garante que os valores dos campos de alarme não sejam mapeados inadvertidamente para o mesmo campo de incidente de segurança.

Na ilustração acima, a regra de alarme Alarme: ClassificationName já está mapeado para Categoria incidente de segurança neste perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo observável pode ser mapeado para mais de campo no mesmo incidente de segurança para que vários observáveis possam ser exibidos. Da mesma forma, o Item de configuração e. Anotações de trabalho os campos podem ser mapeados para exibir vários valores.

No lado Ingestão de amostra de alarme do formulário, azul indica que um campo de regra de alarme não foi mapeado. Cinza indica que ele foi mapeado. Na lista de seleção no lado Mapeamento de campo de incidente SIR do formulário, branco indica que um campo não foi mapeado. Cinza indica que um campo foi mapeado. Use esta codificação por cores para ajudar você a rastrear seu mapeamento de campo.

Na ilustração acima, Usuário afetado foi selecionado na lista de seleção como um novo campo no incidente de segurança.

c. Na seção Ingestão de amostra de alarme no lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID de alarme desejado no campo Expressão de entrada.

Na ilustração acima, Login selecionado.

d. Arraste-o para o campo Limpado e solte-o.
Na coluna esquerda da seção Mapeamento de campo de incidente SIR, o novo valor para Usuário afetado o campo é exibido. Nesse caso, o Login valor do LogRhythm o alarme é exibido no Usuário afetado campo no incidente de segurança.

6. Como alternativa, para inserir manualmente um valor para os campos na coluna Expressão de entrada, coloque o cursor no campo Expressão de entrada e insira um valor de alarme desejado.

Por exemplo, na ilustração acima, outro campo foi adicionado (Grupo de atribuição) para o formulário de incidente de segurança, e. Atribuição de incidente de segurança inserido manualmente no campo.

7. Continue editando o mapeamento pré-configurado conforme necessário.
Se você precisar traduzir valores de LogRhythm campos de alarme para valores compatíveis com os campos no incidente de segurança, você pode usar o editor de scripts. Consulte Use o editor de scripts para formatar LogRhythm valores.

O que Fazer Depois

Depois de concluir o mapeamento de campo, a próxima etapa é Alarmes de filtro para LogRhythm.

Alarmes de filtro para LogRhythm

Definir critérios de filtragem para alarmes depois de mapear campos ajuda a determinar quais alarmes devem ser ingeridos na aplicação SIR. A filtragem de alarmes ajuda a reduzir significativamente o número de alarmes que você ingerem quando o perfil de alarme é ativado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Use as condições de filtragem na parte inferior do formulário de mapeamento para filtrar alarmes específicos ou limitar a ingestão a somente alarmes que atendam a determinados critérios de nível de campo. A filtragem reduz significativamente o número de alarmes que você ingere quando o perfil de alarme é ativado. Use a filtragem para ingerir uma

Tradução automática

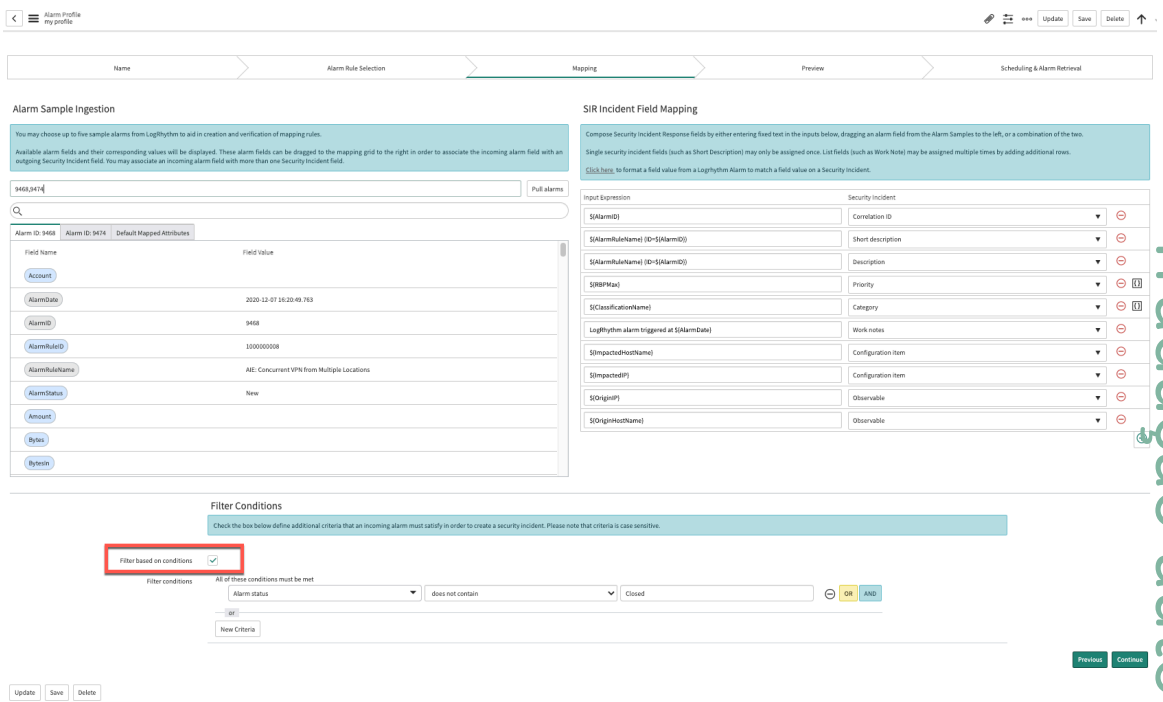
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quantidade gerenciável de alarmes que sua equipe do Centro de operações de segurança (SOC) pode oferecer suporte.

Nota: O exemplo a seguir mostra uma configuração de filtro padrão na qual Alarme status-does-not-contains-closed é a configuração padrão. Este filtro extrai somente alarmes ativos, e esta configuração reduz o número de alarmes extraídos. As etapas a seguir ilustram como adicionar outro filtro útil que inclui somente alarmes com os valores de gravidade ou prioridade mais altos.

Procedimento

1. Para editar os critérios de filtragem, selecione **Filtro com base em condições** caixa de seleção.

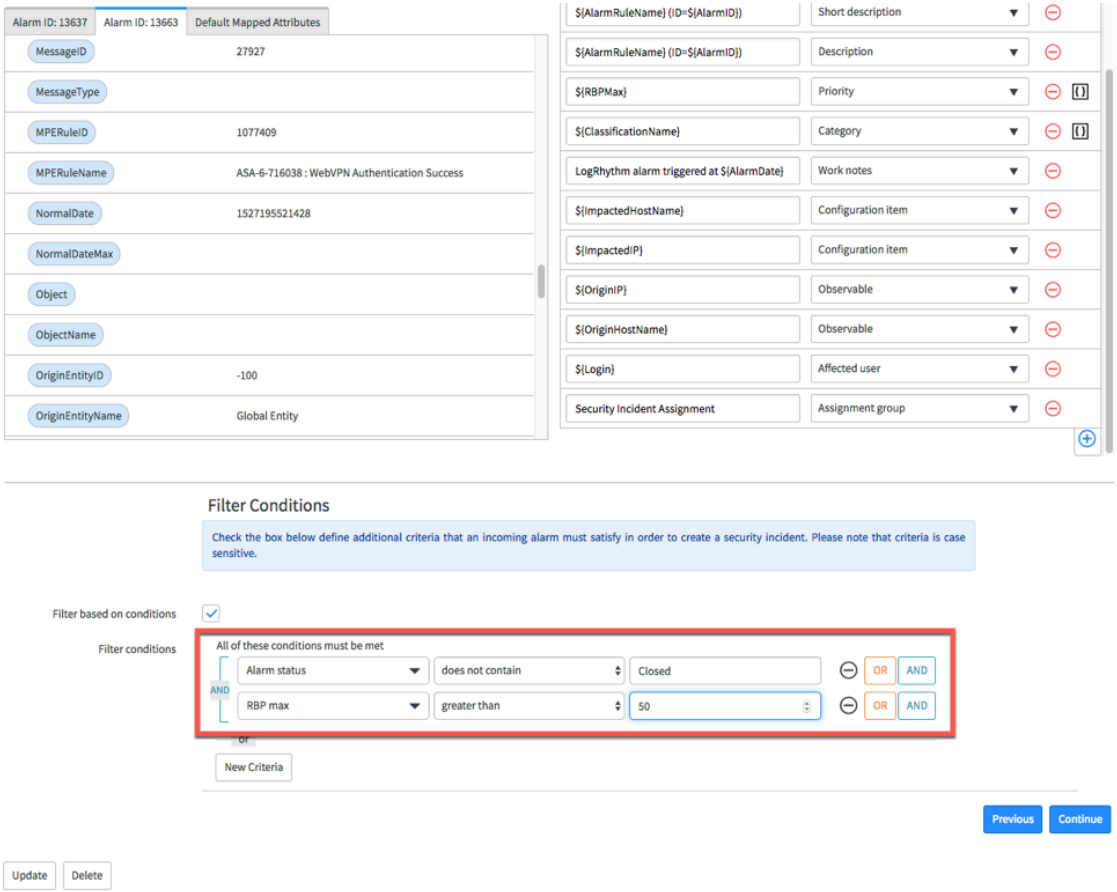


2. À direita do **Condições de filtro** clique em **OU** ou **E.** .
3. Na nova linha exibida, selecione as condições de filtragem nas listas de seleção.

   A imagem a seguir mostra um filtro adicional adicionado aos critérios nos quais a prioridade baseada em risco (RBP máx) é maior que 50 . Somente com esta configuração de filtro LogRhythm alarmes com um valor de prioridade baseado em risco maior que 50 são extraídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Depois de verificar que tudo é crítico LogRhythm os campos de alarme são mapeados para ServiceNow AI Platform incidente de segurança e você definiu critérios de filtragem para limitar a ingestão de alarmes, escolha um para continuar a configuração.

Opção	Descrição
Continuar ou Visualizar	O formulário Visualização do incidente de segurança com sua configuração de mapeamento é exibido. **Visualização** está selecionado na barra de andamento. A próxima etapa é exibir o incidente de segurança com seus alarmes mapeados.
Atualizar	Salve seus dados e retorne ao **Perfis de alarme** lista.
Anterior	O registro do perfil de alarme é exibido.
Excluir	Exclua este perfil de alarme e **Perfis de alarme** a lista é exibida.

O que Fazer Depois

A próxima etapa é visualizar os campos mapeados no incidente de segurança. Consulte Visualizando o incidente de segurança com mapeado LogRhythm valores de alarme.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizando o incidente de segurança com mapeado LogRhythm valores de alarme

Depois de concluir a etapa de mapeamento, visualize os valores mapeados para os campos no incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os críticos LogRhythm campos de alarme que você deseja exibir no incidente de segurança.

Função necessária: sn_si.admin.

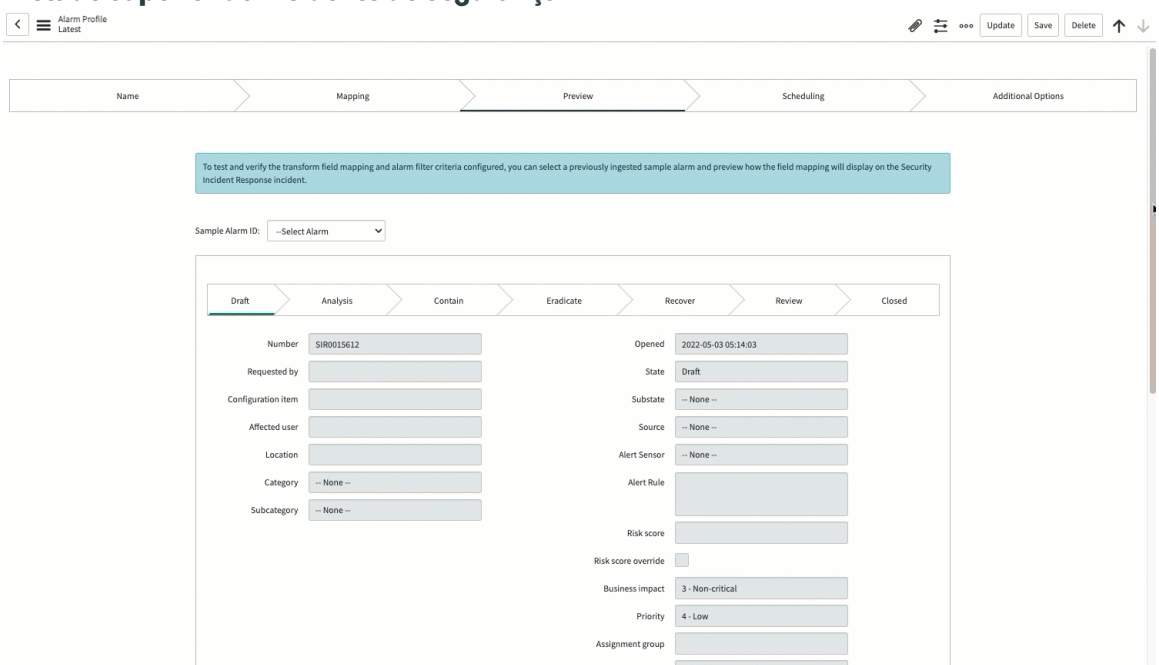
Incidente de segurança

Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.

Um exemplo de visualização para todo ServiceNow AI Platform o incidente de segurança é exibido nas duas figuras a seguir. Este exemplo de visualização do incidente de segurança é preenchido com LogRhythm campos de alarmes mapeados a partir do alarme de amostra 13663 .

Na figura a seguir, o Item de configuração , Usuário afetado , Prioridade , Grupo de atribuição e Descrição resumida os campos do incidente de segurança são preenchidos.

Metade superior do incidente de segurança



Na metade inferior do formulário de incidente de segurança, o. Descrição o campo está preenchido. Na seção Itens relacionados, o. Item de configuração , Observável e Anotação de trabalho os campos são preenchidos com valores. Se vários valores desses campos forem mapeados, cada valor será exibido no incidente de segurança, porque cada um desses campos pode aceitar mais de um valor.

Condições de erro na visualização

As mensagens de aviso a seguir podem ser exibidas ao visualizar o incidente de segurança. Se um alarme de amostra não passar nos critérios de filtragem, todo o incidente de segurança não será preenchido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor de entrada não encontrado

Se o ID do alarme estiver incluído nas condições de filtragem, uma mensagem de aviso ainda poderá ser exibida se valores de entrada específicos não forem encontrados para determinados campos mapeados. Para o exemplo a seguir, na visualização do registro, suponha que não haja nenhum valor em Atribuído a. , embora tenha sido mapeado.

Para este tipo de mensagem, no registro de Mapeamento, verifique se o valor de entrada está correto. Nesse caso, a pessoa no Atribuído a. o campo no incidente de segurança está incorreto em ServiceNow AI Platform instância. Quando este alarme é ingerido e ele cria um incidente de segurança com esta condição, os campos com este valor de entrada (Abel Tuter) são deixados em branco no incidente de segurança.

As mensagens restantes em azul são informativas e indicam que esses campos não têm valor para exibir na visualização. Esta visualização permite que o administrador de incidentes de segurança configure o perfil de alarme para verificar se esses campos não devem ter nenhum valor na fase de criação inicial, porque, em determinados casos, os campos de incidentes de segurança podem ser preenchidos posteriormente automaticamente. Outros erros de mapeamento também são exibidos.

Quando estiver satisfeito com o mapeamento e a visualização do incidente de segurança, escolha um para continuar a configuração.

Opção	Descrição
Clique em **Continuar** ou **Programação** na barra de andamento.	Avançar para **Programação e Recuperação de Alarme** formulário. **Programação e Recuperação de Alarme** está selecionado na barra de andamento. A próxima etapa é programar a recuperação do alarme.
Clique em **Anterior** .	Retorne ao perfil de alarme e continue o mapeamento.
Insira outro ID de alarme em **ID do alarme de amostra** lista de seleção na parte superior do formulário de visualização.	. **ID do alarme de amostra** A lista de seleção é exibida para cada ID de alarme inserido. Você pode selecionar até cinco alarmes. Esta opção permite que você visualize outro LogRhythm ID do alarme em um incidente de segurança.

Depois de visualizar o incidente de segurança e ficar satisfeito com os resultados, a próxima etapa é Programar e recuperar LogRhythm alarmes.

Programar e recuperar LogRhythm alarmes

Depois de visualizar o incidente de segurança com LogRhythm alarmes que você selecionou e mapeou, você está pronto para programar a recuperação do alarme. Depois de concluir esta etapa, o perfil de alarme estará pronto para ser ativado.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A programação permite modificar a programação e os tipos de alarmes selecionados para recuperação. Você filtra os alarmes que ingerem com base em um intervalo de

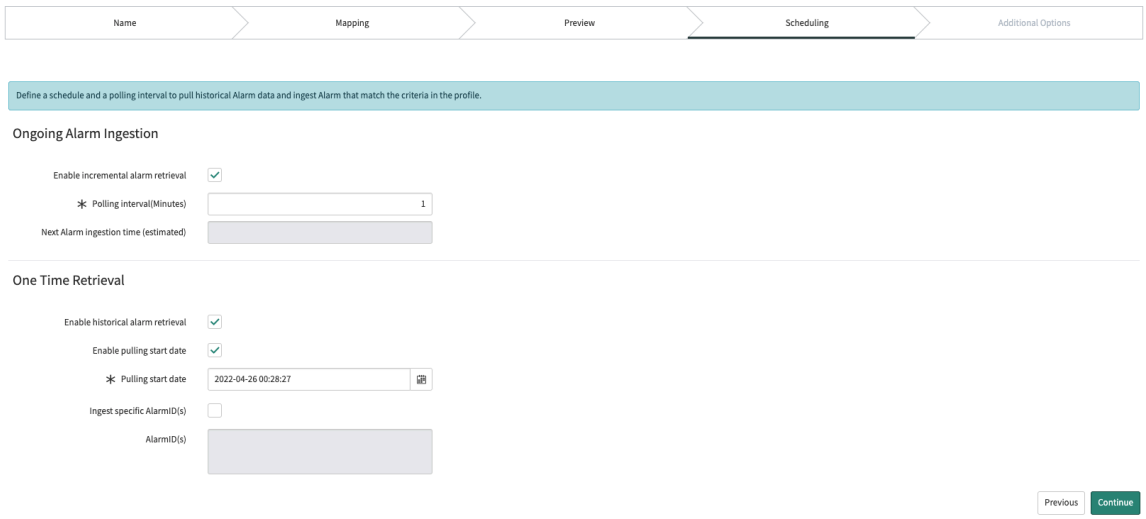
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

datas ou em IDs de alarme específicos. Com esta etapa, você determina se deseja ingerir alarmes históricos e com que frequência pesquisa alarmes futuros que correspondam à configuração do perfil de alarme.

Procedimento

1. Clique em **Programação** etapa na barra de andamento.



2. Escolha uma das seguintes opções para configurar a recuperação do alarme.

Opção	Descrição
Habilitar recuperação de alarme incremental	O padrão é selecionado. Selecione esta opção para recuperar alarmes incrementais.
Intervalo de pesquisa (em minutos)	. ServiceNow AI Platform a instância extrai do LogRhythm Console do cliente para novos alarmes a cada minuto. Se alarmes mape–ados forem encontrados e os critérios de filtragem forem correspondidos, os inci–dentes de segurança serão criados. Esta configuração pode ser alterada, no entanto, a configuração padrão equilibra a ingestão de alarme em relação à carga do servidor e recupera os dados mais atuais.
Próximo período de ingestão de alarmes (estima-do)	Exibe quando ocorrerá a próxima ingestão progra-mada para o perfil de alarme atual. Este é apenas um tempo estimado.
Habilitar recuperação de alarme histórico	O padrão é limpo. Nenhum dado histórico é extraído. Se selecionado, os seguintes campos serão exibidos. Escolha um para configurar a re–cuperação por data ou ID de alarme. **Habilitar data de início de extração** O padrão é limpo. Selecione esta op-ção para habilitar a data de extração. **Data de início da extração**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

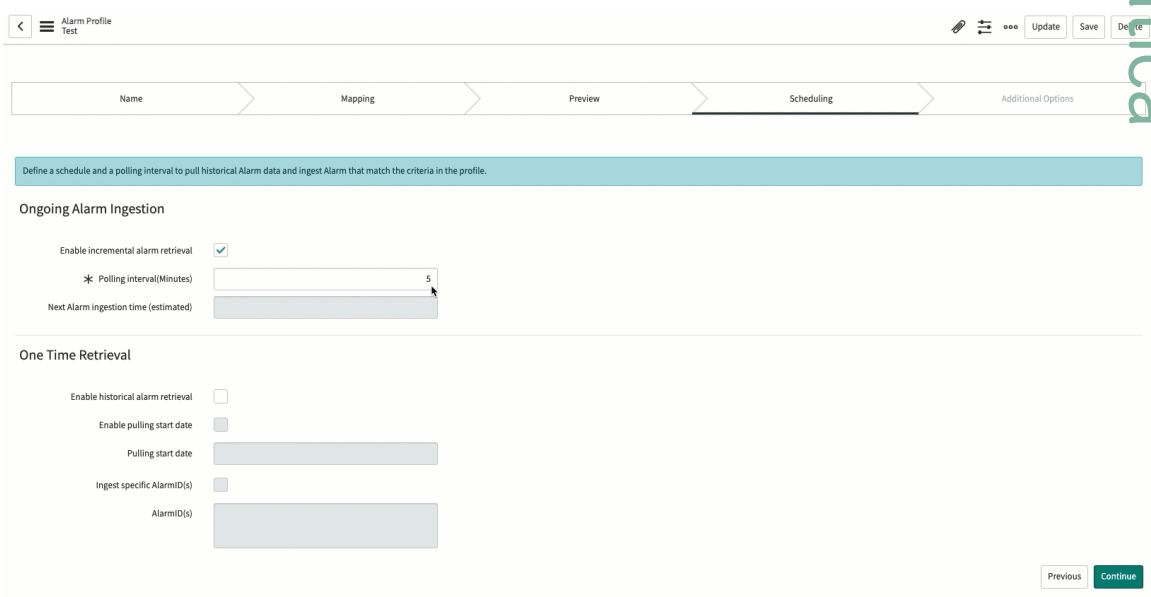
Opção	Descrição
	O padrão é limpo. Selecione esta opção para definir a data de início da extração. Clique no ícone de calendário para inserir uma data e hora. Os alarmes são extraídos da data e hora inseridas até a data atual. **IDs de alarme específicos de ingestão** O padrão é limpo. Selecione esta opção para ingerir IDs de alarme específicos. **ID(s) de Alarme(s)** Insira IDs de alarme específicos. Você extrai os alarmes especificados e pode inserir vários IDs de alarme separados por vírgulas.

Nota: Depois que uma extração única de históricos de alarmes for concluída, esta caixa de seleção será desmarcada. Você precisará marcar esta caixa de seleção novamente antes de executar outra extração única de alarmes históricos.

3. Para editar a recuperação de alarmes históricos, siga estas etapas para inserir uma data para recuperação de alarme ou um ID de alarme específico.

   a. Selecione **Habilitar data de início de extração** e selecione **Extraindo data de início** .

   b. Em **Extraindo data de início** clique no calendário exibido, selecione a data seguida pela marca de seleção verde para salvar sua entrada.



A data é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Como alternativa, selecione **IDs de alarme específicos de ingestão** e no **IDs(s) de alarme** Insira os IDs de alarme específicos para os dados históricos para recuperar IDs de alarme específicos.

É possível inserir até cinco alarmes separados por vírgulas.

d. Clique em **Atualizar**.

4. Escolha uma das seguintes opções para continuar editando ou concluir a configuração.

Opção	Descrição
Atualizar	Salve seus dados e permaneça no formulário.
Opções adicionais (na barra de andamento)	Para ir para a etapa Opções adicionais.
Anterior	Retornar à etapa de Visualização.
Excluir	Exclua este perfil de alarme e a lista de perfis de alarme será exibida.

O que Fazer Depois

Depois de configurar os detalhes de Ingestão de alarme em andamento e Recuperação única, a próxima etapa é Opções adicionais para LogRhythm alarmes.

Opções adicionais para LogRhythm alarmes

. LogRhythm A integração empresarial fornece a capacidade de atualizar ou fechar automaticamente o. LogRhythm alarmes baseados nos incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Quando você habilita a opção Atualizações iniciais do alarme, os alarmes são atualizados automaticamente nos comentários da LogRhythm com as atualizações iniciais do alarme. Da mesma forma, quando você habilita a opção Atualizações de fechamento de alarme, os alarmes são encerrados automaticamente na LogRhythm junto com o Código de fechamento DO SIR e os comentários de fechamento.

. LogRhythm O ID do alarme está conectado ao ServiceNow AI Platform ID do incidente de segurança durante todo o ciclo de vida do incidente. Essa correlação permite que ocorra um fechamento simultâneo e automatizado de incidente/alarme de segurança. . Resposta a incidentes de segurança(SIR o registro de incidente de segurança está encerrado, há um comentário publicado no alarme em LogRhythm console da web. Este comentário indica que o alarme foi encerrado com base no fechamento do ServiceNow AI Platform incidente de segurança. O número do incidente e um URL que se vincula ao incidente de segurança para referência também estão incluídos na seção de comentários em LogRhythm alarme.

Procedimento

1. Clique em **Opções adicionais** etapa na barra de andamento.
2. Para usar a atualização de alarme automatizada para a criação de incidente SIR, escolha uma das seguintes opções para configurar a recuperação do alarme.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Atualizar alarmes da LogRhythm após a criação de incidente de SIR	O padrão é limpo. Selecione esta opção para atualizar automaticamente o. LogRhythm Alarmes quando o incidente SIR é criado.
Comentários iniciais retornados para o alarme da LogRhythm	Indica os comentários iniciais publicados para LogRhythm alarme. Edite o texto padrão exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato"nome do campo" para qualquer campo no formulário de incidente SIR. Por exemplo, O incidente de segurança da ServiceNow relacionado, número, foi criado e atribuído ao grupo de atribuição. Detalhes adicionais podem ser encontrados sobre o incidente de segurança localizado aqui - URL .

3. Para usar a atualização de alarme automatizada para fechamento de incidente SIR, escolha uma das seguintes opções para configurar a recuperação do alarme.

Opção	Descrição
Fechar alarmes da LogRhythm após o fechamento do incidente de SIR	O padrão é limpo. Selecione esta opção para fechar automaticamente o. LogRhythm Alarmes quando o incidente SIR é encerrado.
Comentários de fechamento retornados para o alarme da LogRhythm	Indica os comentários de fechamento publicados para LogRhythm alarme. Edite o texto padrão exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato"nome do campo" para qualquer campo no formulário de incidente SIR. Por exemplo, O incidente de segurança da ServiceNow relacionado foi encerrado pelo analista de SOC com as seguintes anotações de fechamento - notas de fechamento. Detalhes adicionais podem ser encontrados sobre o incidente de segurança localizado aqui - URL .

4. Clique em **Concluir** para salvar o perfil de alarme.

Trouble?
Se você não vir anotações indicando que o alarme foi encerrado com sucesso no incidente de segurança, revise as anotações de trabalho para obter mais informações sobre como proceder para corrigir o problema. Verifique também a conexão do servidor. Se você confirmar ServiceNow AI Platform o incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

foi encerrado e o servidor não atingiu o tempo limite. pode ser necessário fechar manualmente o alarme no LogRhythm Console da Web.

Configurações adicionais para LogRhythm integração

Use LogRhythm Configurações de integração para modificar o sistema predefinido e as propriedades de solução de problemas de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Integração com LogRhythm** > **Configurações da Integração com LogRhythm**.
2. Configure as propriedades do sistema de acordo com seus requisitos.
3. No formulário, preencha os campos.

LogRhythm Propriedades do sistema de integração

Campo	Descrição
O filtro será aplicado antes que os dados sejam salvos nas tabelas da ServiceNow.	Opção para determinar se você deseja aplicar o filtro antes que os dados sejam armazenados nas tabelas da ServiceNow. Por padrão, o valor é definido como Sim.
O número máximo de incidentes de segurança que pode ser criado em um dia	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 2000.
LogRhythm a ingestão periódica pode ter mais de 1000 alarmes, portanto a paginação é usada para ingerir os alarmes. Limite permitido por página para buscar o número de alarmes por página.	Opção para definir o número máximo de alarmes a serem recuperados em uma única página. Por padrão, o valor é definido como 100.
Exclua registros da tabela "Origem para tarefa" mais antigos do que o número de dias especificado.	Opção para excluir registros da tabela Origem para Tarefa quando o número especificado de dias for violado. Por padrão, o valor é definido como 30.

4. Configure as propriedades de solução de problemas de acordo com seus requisitos.
5. No formulário, preencha os campos.

Integração da LogRhythm Propriedades de solução de problemas

Campo	Descrição
Depurar ingestão programada: Habilita logs do sistema no nível de depuração para ingestão feita por trabalho agendado. Registrará todas as mensagens/ exceções geradas pela ingestão programada	Opção para habilitar logs do sistema no nível de depuração para ingestão realizada pelo trabalho agendado. Por padrão, o valor é definido como Não

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ao extrair alarmes/detalhamentos/eventos de LogRhythm.	
Depurar mapa de transformação: Habilita logs do sistema de nível de depuração para o mapa de transformação. Todas as mensagens geradas pelos mapas de transformação serão registradas durante a criação de incidentes de segurança a partir da importação de alarmes. Isso também habilitou a ação de IU na tabela Importação de alarme para executar novamente o mapa de transformação.	Opção para habilitar logs do sistema no nível de depuração para o mapa de transformação. Por padrão, o valor é definido como Não
Depurar ingestão de amostra no perfil de alarme: Habilita logs do sistema de nível de depuração para ingestão de amostra. Todas as mensagens geradas serão registradas enquanto as amostras forem ingeridas.	Opção para habilitar logs do sistema no nível de depuração para ingestão de amostra. Por padrão, o valor é definido como Não
Visualização de depuração no perfil de alarme: Habilita logs do sistema de nível de depuração para a visualização do perfil de alarme. Todas as mensagens geradas serão registradas enquanto a visualização for renderizada para Alarme de amostra.	Opção para habilitar logs do sistema no nível de depuração para a Visualização do perfil de alarme. Por padrão, o valor é definido como Não
Depurar chamadas REST de saída: Habilitar esta propriedade permitirá o registro em log no nível de depuração na tabela Logs do sistema para todas as chamadas REST (solicitação e resposta) que vão com ou sem o MID Server de LogRhythm.	Opção para habilitar o registro em log no nível de depuração na tabela Logs do sistema para todas as chamadas REST que vão com ou sem o MID Server de LogRhythm. Por padrão, o valor é definido como Não

6. Clique em **Salvar**.

Use o editor de scripts para formatar LogRhythm valores

Além dos campos mapeados diretamente dos valores de alarme extraídos e dos valores de alarme inseridos manualmente, você pode usar o editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento, que é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

O editor de script muda os valores de um LogRhythm para que os valores que são mapeados para Prioridade e. Categoria campos no incidente de segurança são compatíveis.

Por Que e Quando Desempenhar Esta Tarefa

Em determinados casos, se LogRhythm os valores de alarme são mapeados para Prioridade e. Categoria no incidente de segurança, convém editar os valores mapeados. Se você quiser traduzir o valor de um LogRhythm alarme para um valor compatível com Prioridade ou Categoria campos no incidente de segurança, use o editor de scripts.

Tradução automática

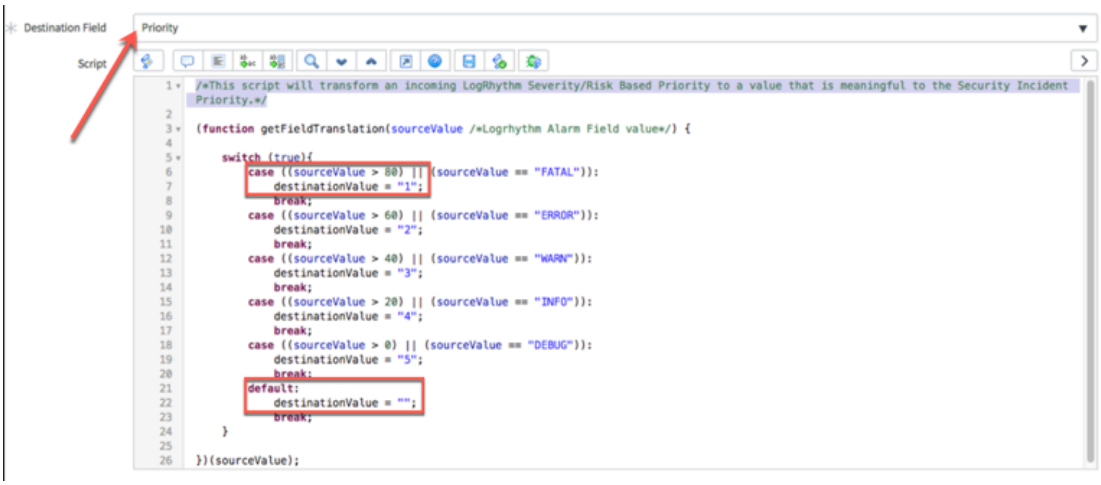
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete [] para abrir o editor de scripts.

Os valores padrão são incluídos para Prioridade e. Categoria campos no incidente de segurança. Você pode editar esses valores.

Para este exemplo, no editor Aberto, verifique isso **Prioridade** é exibido em **Campo de destino** lista de seleção, conforme mostrado na figura a seguir. Observe que este campo é o incidente de segurança *prioridade* . LogRhythm baseado em risco *prioridade* .



Em determinados casos, uma inclusão de script pode ser apropriada para Prioridade campo. Para um LogRhythm alarme, por exemplo, uma pontuação de prioridade baseada em risco recebe um valor entre 0 e 100. No entanto, em ServiceNow AI Platform, o campo prioridade em um incidente de segurança oferece suporte a valores entre 1 e 5. Conforme ilustrado na figura anterior, uma inclusão de script traduz LogRhythm valores de campo de alarme para os valores apropriados compatíveis com o campo no incidente de segurança no ServiceNow AI Platform.

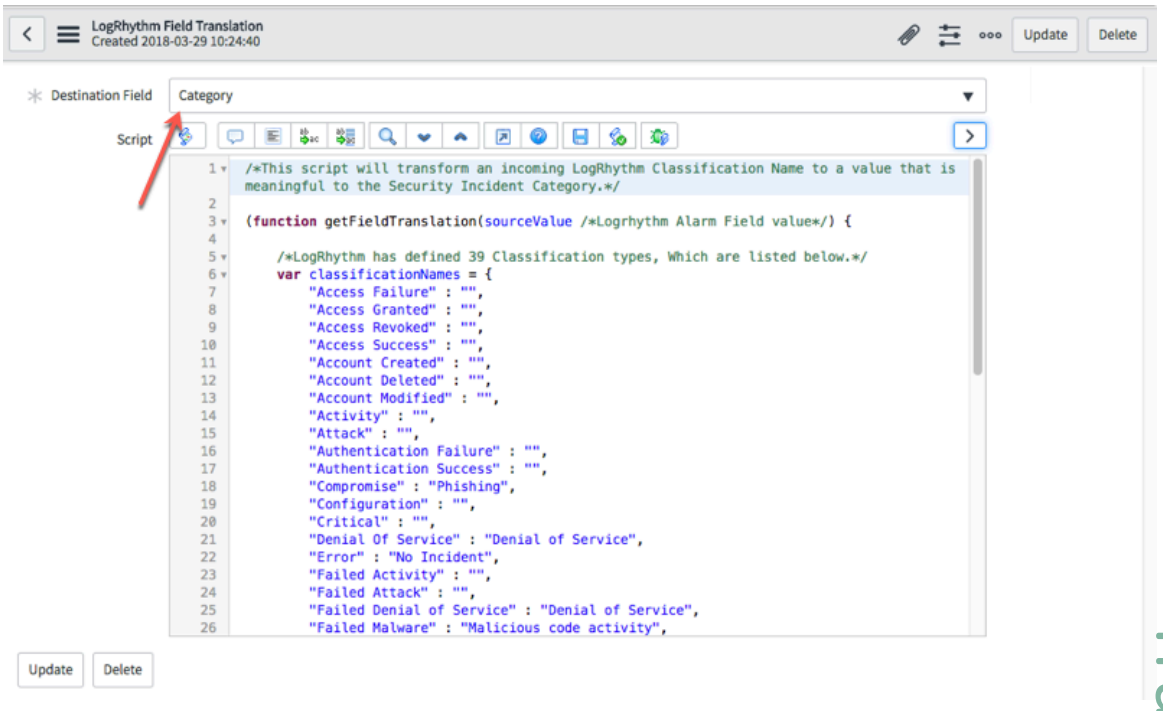
Neste exemplo para Prioridade campo, se for LogRhythm o valor do alarme é 80 ou maior, 1 é exibido no campo de incidente de segurança (Prioridade). Este valor se traduz em um Crítico prioridade no incidente de segurança. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

2. Insira as mudanças e clique em **Atualização** para salvar suas mudanças.
. LogRhythm A tabela Traduções de campo é exibida.
3. Feche a tabela para retornar ao formulário Mapeamento.

A figura a seguir mostra o editor de scripts com Categoria Selecionado na lista de seleção Campo de destino.

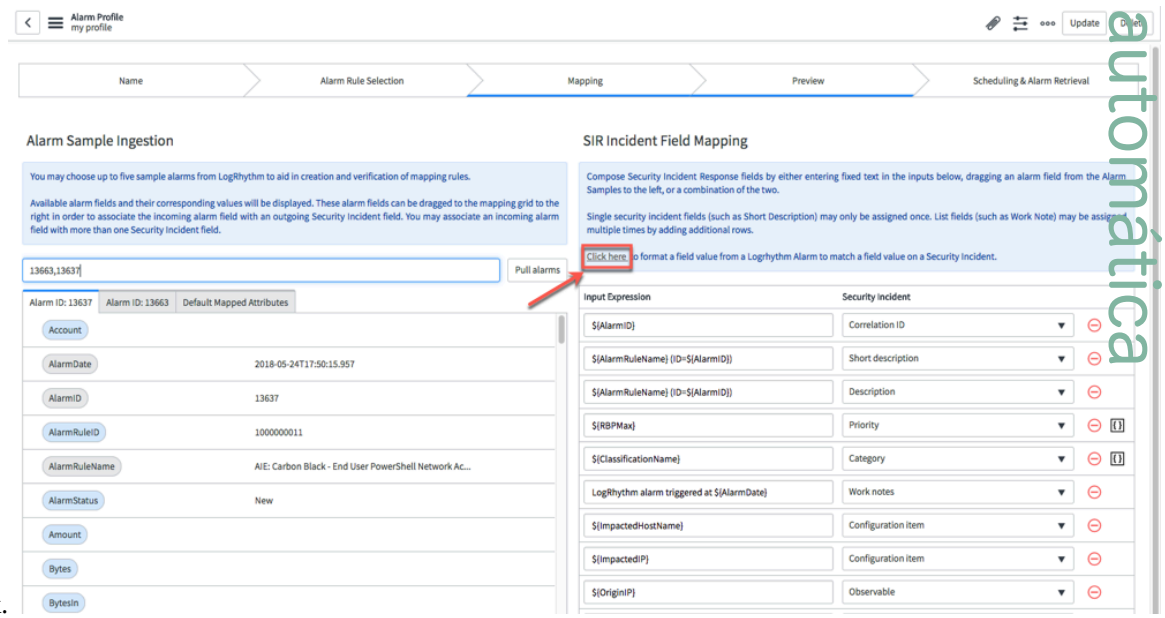
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Se você quiser adicionar um novo campo à lista Traduções de campo, siga estas etapas para adicionar um novo registro.

a. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente SIR, clique em **Clique**



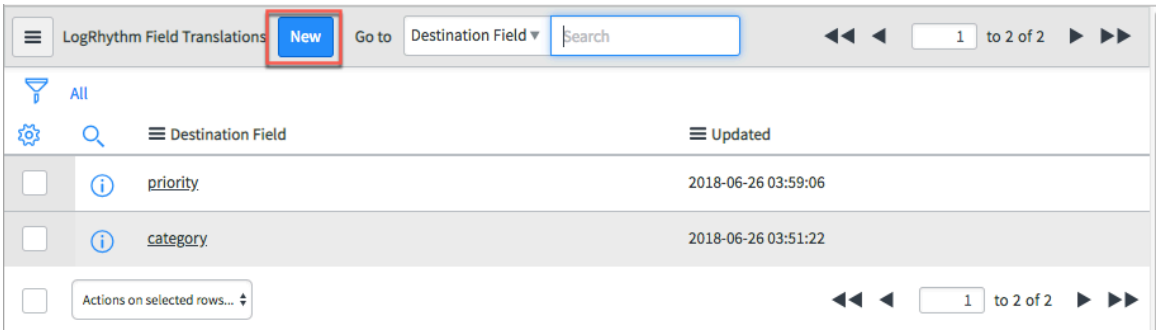
aquilink.

. LogRhythm Lista Tradução de campo com prioridade e. categoria os campos de destino são exibidos.

b. Clique em Novo.

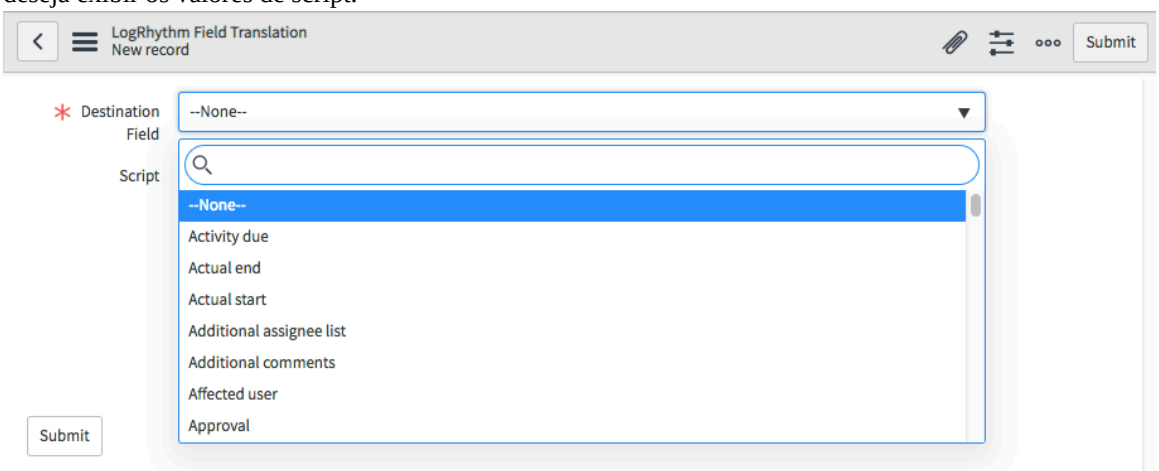
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um novo registro é exibido.

c. Na lista de seleção Campo de destino, selecione um campo de destino no incidente de segurança que você deseja exibir os valores de script.



d. Clique em **Enviar**.
O editor de script é exibido.

e. Insira as mudanças no editor e clique em **Enviar** para salvar suas mudanças.
. LogRhythm A tabela Traduções de campo com seu novo registro é exibida.

5. Feche a tabela para retornar ao formulário Mapeamento.

Copie um perfil de alarme para LogRhythm

Copie um perfil existente e suas configurações associadas em vez de criar um novo perfil de alarme. Se você estiver criando vários perfis de alarme para diferentes tipos de alarmes e quiser reutilizar as configurações de um perfil existente, poderá copiar perfis de alarme para economizar tempo. Este processo é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é definido como inativo para que não seja ativado acidentalmente antes de concluir a configuração.

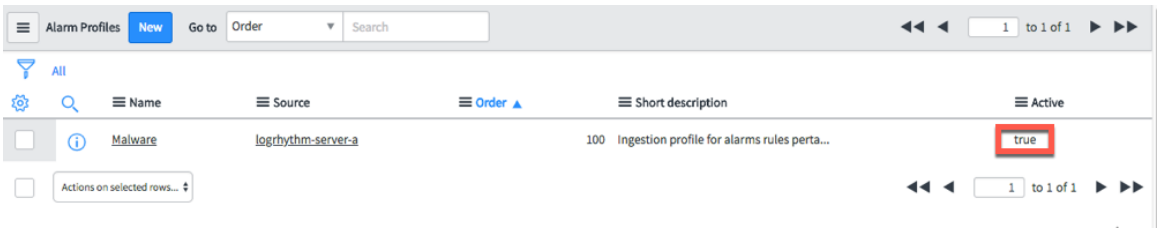
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

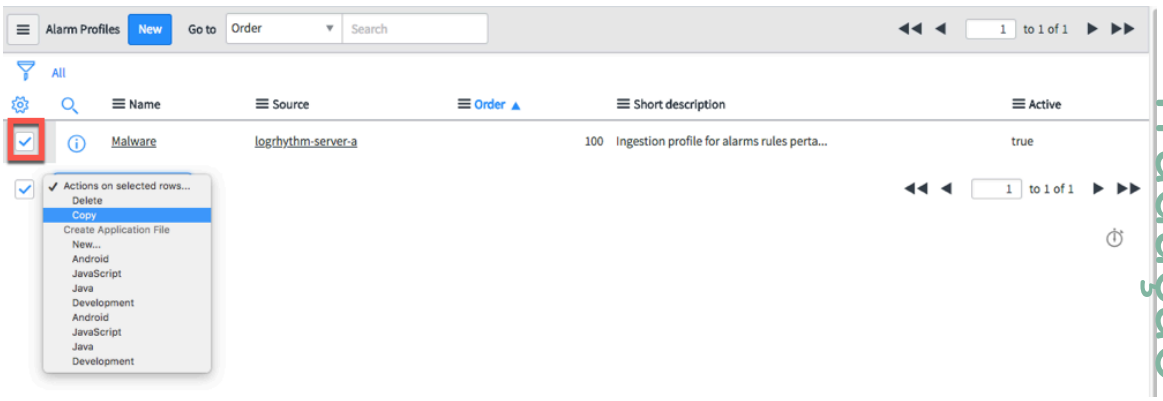
Procedimento

1. Navegar até **Tudo** > **Integração com LogRhythm** > **Perfis de alarme LogRhythm**.

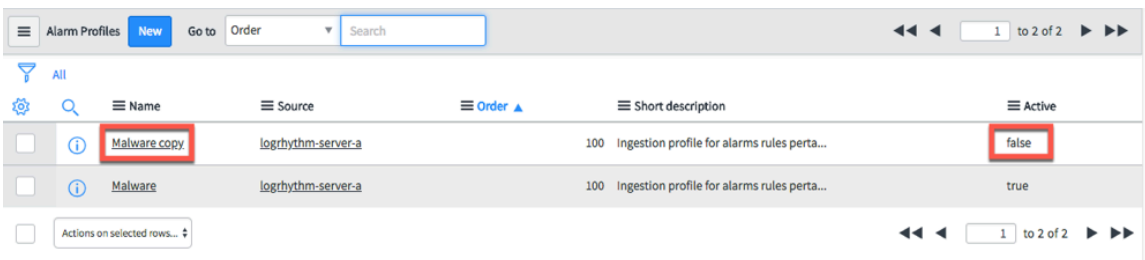
   Na lista exibida, observe Ativo a coluna indica se o perfil está ativo (verdadeiro).



2. No campo à esquerda do **Nome** , selecione o nome do registro.
3. Em **Ações nas linhas selecionadas** lista de seleção, selecione **Cópia** .



Em **Perfis de alarme** , a cópia e o perfil original são exibidos. Embora o registro original esteja ativo, a cópia está inativa neste ponto (falso). Depois de configurá-lo, você ativa este perfil copiado.



Você pode editar valores do perfil copiado e renomeá-lo para que as regras de alarme que você extrai se apliquem ao novo perfil. Você será solicitado a ativar o novo perfil depois que as etapas de configuração forem concluídas.

Tradução automática

Desabilitar fechamento de alarme automatizado para LogRhythm

Desabilite o recurso de fechamento de alarme automatizado se você não quiser mais exibir as informações de fechamento de incidente de segurança no LogRhythm Console da Web. Uma vez desativado, o. ServiceNow AI Platform não fecha mais os alarmes no LogRhythm Console da Web. Este processo é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

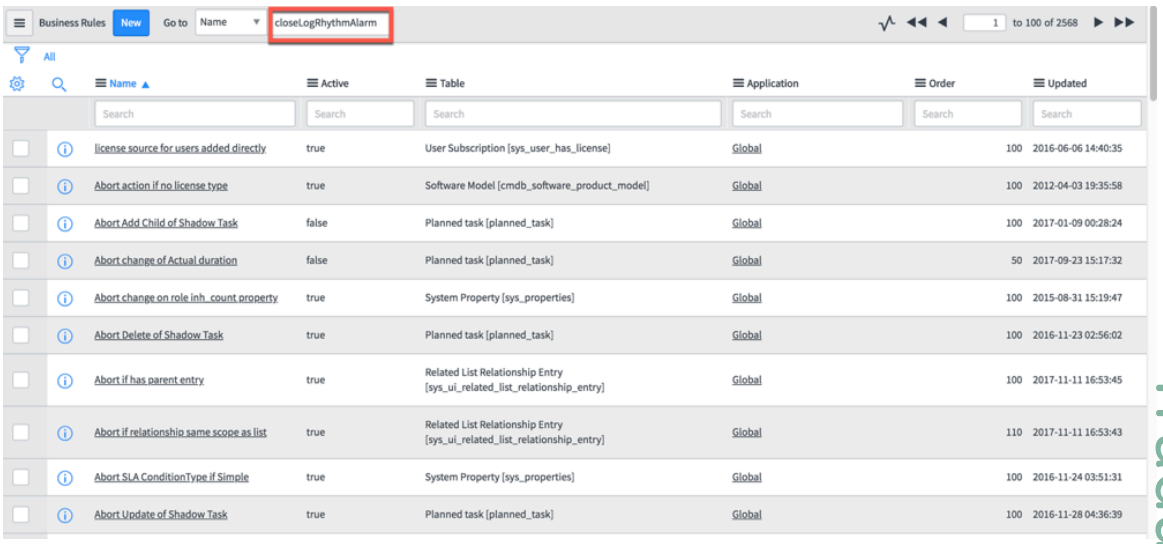
Por Que e Quando Desempenhar Esta Tarefa

Uma vez desabilitadas, as anotações de status e outras informações de fechamento no incidente de segurança não são mais exibidas no LogRhythm Console da Web.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Definição do sistema** > **Regras de negócio** e selecione **Regras de negócio** módulo.
2. Se não for exibido em **Regras de negócio** , insira **Alarme de fechamento da LogRhythm no fechamento do SI** no campo de pesquisa e pressione **Insira** .



3. Em **Nome** , clique em **Alarme de fechamento da LogRhythm no fechamento do SI** link para abrir o registro.
4. No registro exibido, limpe **Ativo** caixa de seleção.
5. Clique em **Atualizar**.
   A capacidade de fechamento de alarme automatizado agora está desabilitada.

Exibir LogRhythm detalhar eventos

Exiba os eventos brutos ou de base relacionados para um LogRhythm alarme no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como analista de segurança, você pode exibir os eventos brutos ou de base relacionados a um LogRhythm alarme sem precisar voltar para LogRhythm console. Você pode fazer isso acessando uma lista relacionada que contém todos os eventos de detalhamento no SIR incidente.

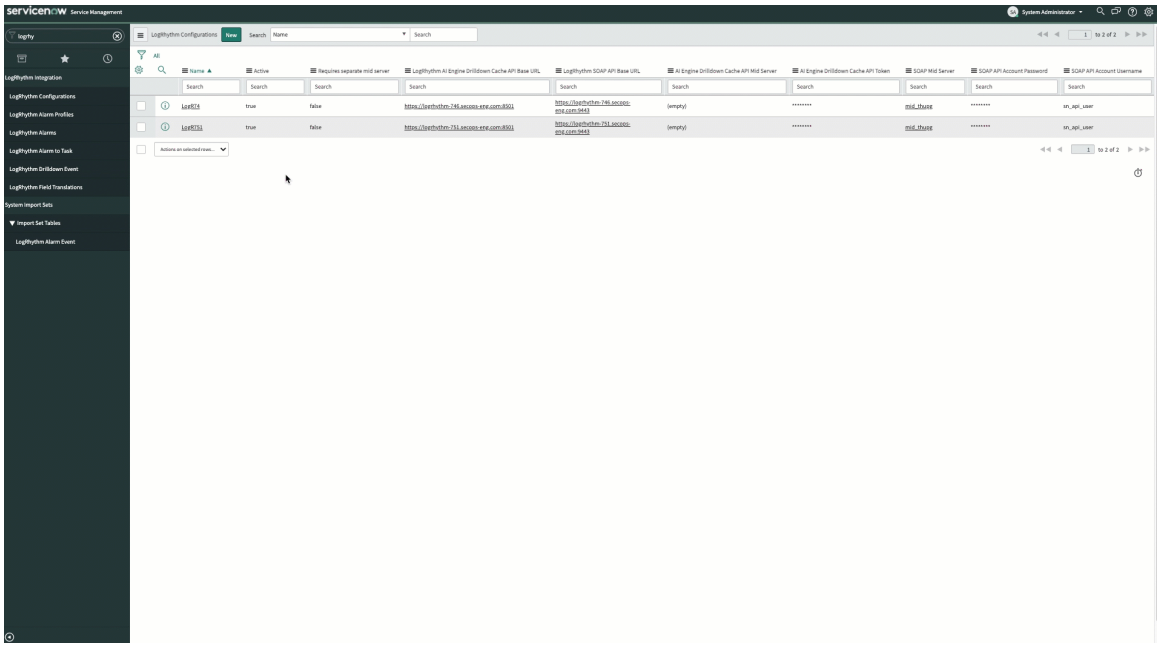
Procedimento

Navegar até **Tudo** > **Integração com LogRhythm** > **Eventos de detalhamento da LogRhythm**.

A ilustração a seguir mostra como navegar até **Eventos de detalhamento da LogRhythm** classifique a lista de eventos por **Agrupar por ID de alarme** e clique no incidente de segurança associado. No incidente de segurança, você pode encontrar **Eventos de detalhamento da LogRhythm** nos links relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solução de problemas da integração da LogRhythm

Solucione problemas de conectividade e ingestão de alarme.

Consulte os seguintes tópicos para solução de problemas:

- Verifique a conectividade para LogRhythm
- Execução de script e log do sistema para LogRhythm

Verifique a conectividade para LogRhythm

Verifique sua conexão com LogRhythm Console do cliente enviando solicitações cURL para testar o. LogRhythm REST API. O processo de verificação é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Para verificar a conexão com LogRhythm O Console do cliente está funcionando corretamente depois que você configura o. LogRhythm REST APIs, enviam duas solicitações cURL do computador que hospeda o MID Server configurado em Instale o plug-in e configure LogRhythm.

. LogRhythm A REST API usa o WSSE para autenticação, o que requer alguns scripts externos para funcionar com Curl e Postman.

. LogRhythm A REST API usa um token para autenticação, para que você possa fazer a chamada de validação real que a integração usa. O "0" no final do URL é A. LogRhythm ID do alarme. . LogRhythm A REST API com uma configuração padrão requer a porta 8501. Este número de porta deve ser incluído no URL que você planeja usar para o teste.

Procedimento

Atualize o URL **LogRhythm REST url>** e token **<api token>** na solicitação curl a seguir e envie-a para validar o. LogRhythm REST API: `Curl -k -i -v --trace-time -o /dev/null -H "Content-Type: Text/json" -H "Authorization: bearer <api token> url" "https://<cache drilldown url>/lr-drilldown-cache-api/drilldown/0"`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para uma conexão bem-sucedida com LogRhythm REST API, você deve receber um HTTP 404, mas o corpo da resposta contém ID do alarme: 0 não encontrado .

Execução de script e log do sistema

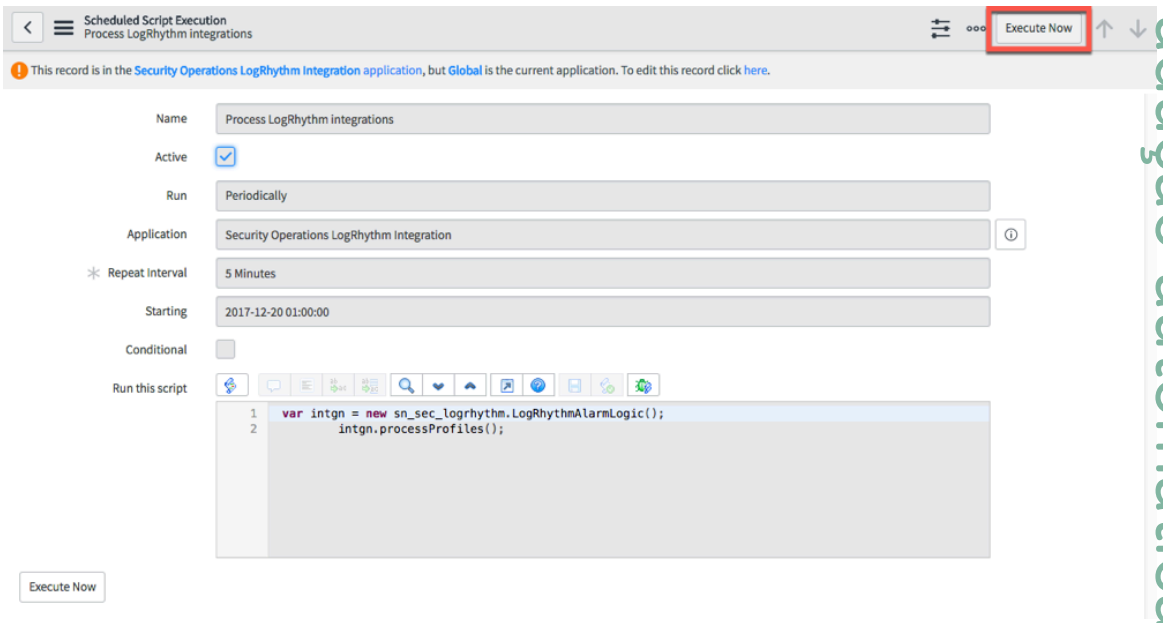
Se você estiver solucionando um problema de ingestão de alarme, poderá substituir o intervalo de pesquisa padrão de cinco minutos para exibir os resultados imediatamente. Neste cenário, chame a execução do script manualmente para executar a pesquisa. Esta execução é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Trabalho programado** > **Trabalhos agendados** e selecione **Trabalhos agendados** módulo.
2. Clique no processo LogRhythm registro de trabalho de integrações.
3. No registro Execução de script programada exibido, clique em **Executar agora** .



Se você precisar de mais ajuda para solução de problemas, poderá acessar o log do sistema do LogRhythm consultas.

4. Para outros problemas gerais de solução de problemas, siga estas etapas para acessar os logs do sistema.

   a. Navegar até **Log do sistema** > **Tudo** e selecione **Todos** .

   b. Defina o filtro (Vá para) a **Origem** e insira `sn_sec_logrhythm` .

   c. Pressione **Enter**.
   Todas as mensagens geradas pela integração são exibidas nesta tabela. As mensagens listadas podem fornecer informações sobre os processos em execução da integração e podem ajudá-lo com a solução de problemas adicional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

McAfee ePO integração

. McAfee ePO Integração do recurso de detecção e resposta de endpoint (EDR) que ajuda os analistas do SOC (Security Operations Center, Centro de operações de segurança) a identificar ameaças virtuais e reparar os danos causados por arquivos maliciosos.

Visão geral

Há dois conjuntos de McAfee ePO recursos usados nesta integração, os recursos que invocam ações, como isolar um host e iniciar uma verificação de malware, e os recursos que executam consultas para coletar detalhes do sistema e eventos de ameaça. Ambos os tipos de recursos, as ações e as consultas, são invocados a partir de ServiceNow AI Platform® instância. Você pode agrupar esses recursos para que eles sejam executados automaticamente quando ocorrer um tipo específico de evento de segurança ou pode invocá-los manualmente de um ServiceNow AI Platform® incidente de segurança.

A seguir McAfee ePO os recursos estão disponíveis para esta integração.

Obter detalhes do sistema

Reúna detalhes do sistema que incluem detalhes do sistema operacional.

Iniciar verificação de malware

Com base na configuração e programação de verificação, inicie uma verificação de um endpoint afetado.

Isolar/desisolar host

Remova um sistema do acesso à rede para investigação e restaure o acesso à rede.

Listar eventos de ameaça

Reúna o status de conformidade e os eventos de ameaça mais atuais.

Principais recursos

Esta integração inclui os principais recursos a seguir.

- Oferece suporte ao acionamento automatizado de McAfee ePO consultas baseadas em condições de incidente.
- Oferece suporte à inicialização do McAfee ePO recursos manualmente de ServiceNow AI Platform® Resposta a incidentes de segurança(SIR incidentes de segurança que executam ações sob demanda.
- A flexibilidade de criar vários perfis para acionar diferentes tipos de McAfee ePO e. ServiceNow AI Platform® Operações de segurança. Esses perfis reúnem informações de eventos de ameaça ou executam ações com base nas condições de categorias de incidente específicas, como malware.
- Valide sua configuração de perfil com uma visualização do McAfee ePO resultados em SIR incidentes de segurança.
- Se a marcação estiver habilitada, os marcadores de segurança identificarão quais McAfee ePO inicialmente, os recursos são iniciados por um fluxo de trabalho e quando as consultas ou ações são concluídas com sucesso.
- Uma trilha de auditoria completa do McAfee ePO consultas e ações são publicadas nas anotações de trabalho em SIR incidentes de segurança e comandos do ServiceNow AI Platform® estão conectados em McAfee ePO console.
- Oferece suporte a vários McAfee ePO consoles.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ServiceNow Plug-ins

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações.

A seguir Operações de segurança as aplicações devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila:

1. Framework de integração de segurança
2. Security Support Common
3. Orquestração do suporte de segurança
4. Resposta a incidentes de segurança
5. Espaço de resposta a incidentes de segurança

Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Configure seu ServiceNow AI Platform instância do McAfee ePO integração.

. ServiceNow plug-in de extensão

. ServiceNow Security Operations Extension para McAfee ePO #o plug-in de extensão é necessário para esta integração. Você instala isso ServiceNow plug-in em seu McAfee ePO console. Para obter mais informações, consulte Configure seu ServiceNow AI Platform instância do McAfee ePO integração.

MID Server

Esta integração requer um MID Server instalado e configurado em seu ServiceNow AI Platform® instância para se conectar ao McAfee ePO servidor (console). Consulte Site de documentação do produto da ServiceNow Para obter mais informações sobre MID Servers.

Versões compatíveis do McAfee

A integração oferece suporte às versões 5.9.1 e 5,10 do McAfee ePO. Compatível com McAfee Agent: MA 5.5.1.388 Para obter mais informações sobre os produtos McAfee e o ePolicy Orchestrator, consulte Site do produto McAfee .

A integração oferece suporte à versão 10,5 do produto McAfee Endpoint Security Threat Prevention. Se você não estiver executando a versão 10,5, consulte seu McAfee ePO administrador para ver se sua versão pode oferecer suporte a verificações sob demanda por meio de ações de marcador.

McAfee ePO marcadores de segurança são usados nesta integração. Você deve criar esses marcadores em seu McAfee ePO console. Para obter mais informações sobre esses marcadores, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referências

Referência	Identificador do documento	Título do documento
1	Site do produto McAfee	Site do produto McAfee
2	McAfee Business Product Documentation para ePolicy Orchestrator Cloud	Documentação do produto McAfee
3	ServiceNow Site de documentação do produto	Site de documentação do produto da ServiceNow

Para obter uma check-list para rastrear seu andamento na configuração, instalação e verificação dos resultados da integração, consulte Check-list para McAfee ePO integração.

Para uma instalação tranquila da aplicação e para ajudá-lo a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Tópicos relacionados

Arquitetura de integração para McAfee ePO

Arquitetura de integração para McAfee ePO

O tópico a seguir é uma visão geral da arquitetura do sistema e lista os principais recursos da integração. Esta seção também fornece informações sobre as etapas de configuração que você deve concluir em ServiceNow AI Platform E no McAfee ePolicy Orchestrator (McAfee ePO) antes de instalar a aplicação do ServiceNow Store.

Termos-chave para McAfee ePO integração

Os termos a seguir são usados em toda a documentação de instalação e configuração da integração.

ServiceNow AI Platform

Uma empresa ServiceNow produto. . ServiceNow AI Platformé a base sobre a qual componentes individuais, como Resposta a incidentes de segurança(SIR IT Service Management, (ITSM) e outros produtos são criados.

Resposta a incidentes de segurança (SIR)

. ServiceNow AI Platform aplicação que rastreia o andamento de incidentes de segurança desde a descoberta e a análise inicial, até contenção, erradicação e recuperação, e até a revisão e fechamento finais pós-incidente.

Plug-in

Plug-ins são componentes de software que fornecem recursos e funcionalidades específicos em seu ServiceNow AI Platform instância. Para obter mais informações sobre a instalação e a configuração dos plug-ins de integração, consulte Instale a aplicação e configure um servidor para McAfee ePO integração.

EPolicy Orchestrator (McAfee ePO)

O console do usuário em que você gerencia os serviços, produtos e configurações da McAfee.

Plug-in de extensão McAfee

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isso ServiceNow o plug-in de extensão é necessário para esta integração. Este plug-in reside em seu McAfee ePO e conecta seu McAfee ePO console para seu ServiceNow AI Platform instância.

Capacidade

Uma atividade automática iniciada a partir de ServiceNow AI Platform instância que é executada no McAfee ePO console para conduzir consultas de aprimoramento e executar ações em seus ativos.

Perfil

Configurações para McAfee ePO capacidades que você configura para especificar quando e sob quais condições os recursos realizam consultas de aprimoramento e executam ações em seus ativos.

MID server

Uma aplicação que facilita a comunicação e a movimentação de dados entre o. ServiceNow AI Platform e aplicações externas, fontes de dados e serviços.

ServiceNow administrador (admin)

Um usuário com esta função baixa e instala o. SIR e. McAfee ePO plug-ins para seu ServiceNow AI Platform instância. Um usuário com esta função também atribui a função de administrador de incidente de segurança conforme necessário.

ServiceNow Administrador de incidentes de segurança (sn_si.admin)

Um usuário com esta função executa a configuração do McAfee ePO integração com Resposta a incidentes de segurança(SIR) no seu ServiceNow AI Platform instância conforme necessário. Um usuário com esta função também atribui a função de analista de incidentes de segurança conforme necessário.

ServiceNow analista de incidentes de segurança (sn_si.analyst)

Um usuário com esta função interage e analisa incidentes de segurança no produto SIR.

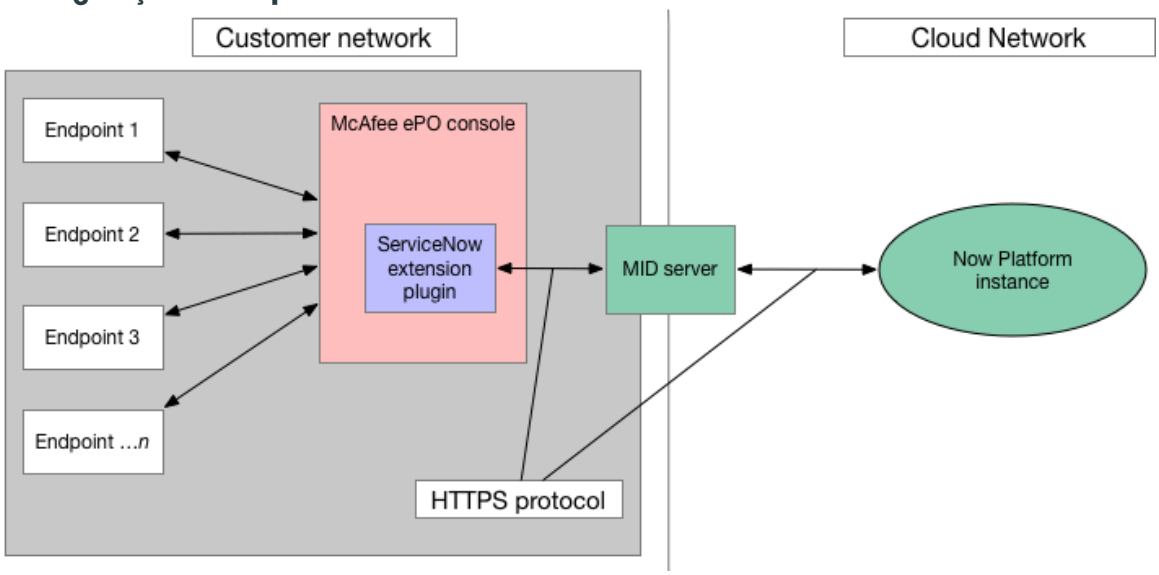
Conexão do sistema e fluxo de dados

A figura a seguir é um exemplo de um ambiente do cliente. . ServiceNow AI Platform O MID Server é necessário para que seu ServiceNow AI Platform a instância pode se conectar a um McAfee ePO servidor (console) por meio de um ServiceNow plug-in de extensão. Depois de conectar, você invoca recursos do seu ServiceNow AI Platform para iniciar verificações de malware, isole as máquinas host e restaure-as em sua rede, recupere os resultados da última verificação e reúna detalhes do sistema sobre seus ativos. Quando esses recursos retornam resultados de seus ativos que correspondem aos critérios de pesquisa, os dados são extraídos por meio do MID Server para seu ServiceNow AI Platform instância. Os dados são exibidos nas listas relacionadas de um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança. A figura a seguir ilustra o fluxo de dados de um grupo de endpoints gerenciados por um McAfee ePO console.

Tradução automática

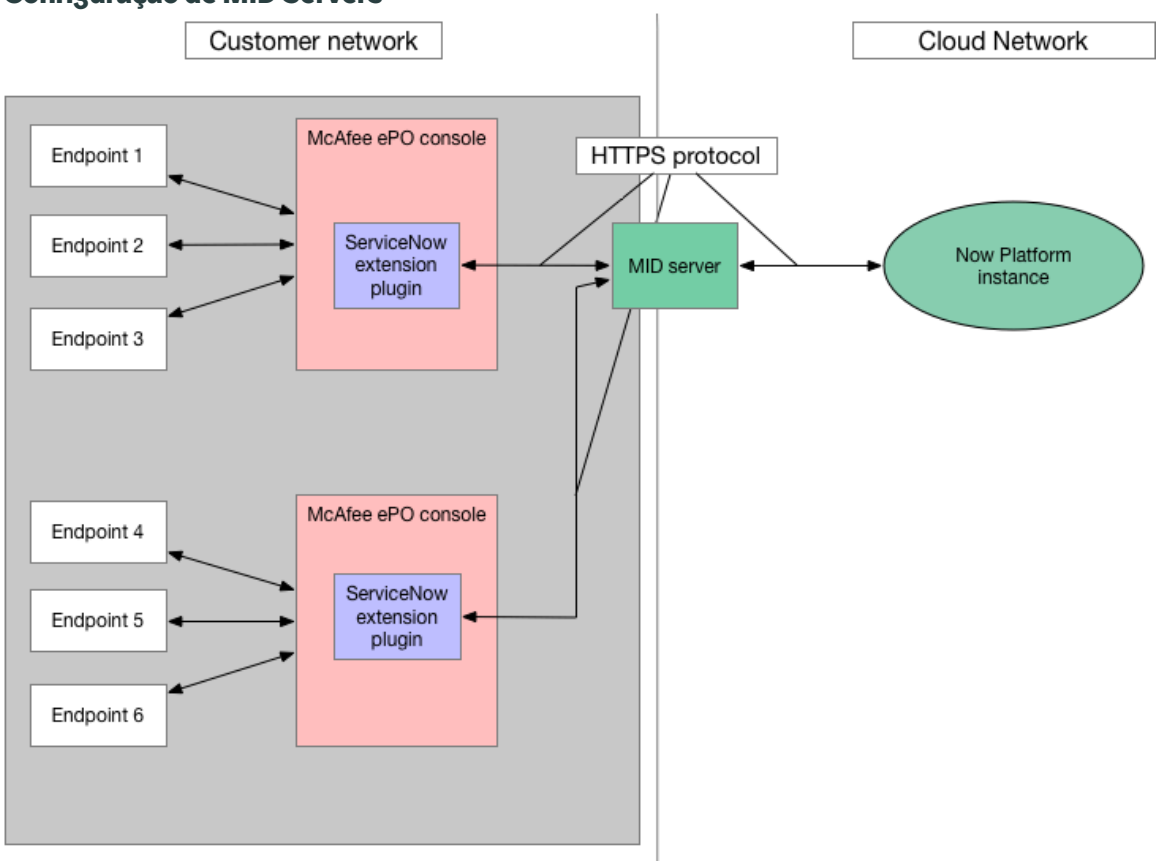
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de endpoint único



Como mostrado na figura a seguir, esta integração pode oferecer suporte a mais de uma McAfee ePO console. Um grupo de endpoints pode ser gerenciado por um McAfee ePO e outro grupo de endpoints gerenciados por outro McAfee ePO console. Dados de vários McAfee ePO Os consoles são extraídos por meio de um único MID Server. No entanto, você também pode preferir configurar vários MID Servers, se exigido pela sua organização.

Configuração de MID Servers



Fluxos de trabalho do McAfee ePO integração

Esta integração inclui os seguintes fluxos de trabalho. Esses fluxos de trabalho são pré-configurados e projetados especificamente para essa integração. Você pode editar esses

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fluxos de trabalho para atender às necessidades da sua organização conforme necessário. Para obter mais informações gerais sobre fluxos de trabalho e como usar o editor de fluxo de trabalho, consulte Introdução aos fluxos de trabalho .

- Integração do McAfee ePO para operações de segurança - Obter detalhes do host
- Integração do McAfee ePO de operações de segurança - Iniciar verificação de malware
- Integração do McAfee ePO para operações de segurança - Isolar host
- Integração do McAfee ePO de operações de segurança - Listar eventos de ameaça
- Integração do McAfee ePO do Security Operations - Remover isolamento

Conexão de sistemas externos

A integração requer que o MID Server se comunique por meio da conexão do protocolo HTTPS com McAfee ePO console.

Check-list para McAfee ePO integração

Use esta check-list para orientá-lo em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem resultados esperados para a integração.

Antes de Iniciar
Função necessária: As funções são listadas para cada etapa.

Por Que e Quando Desempenhar Esta Tarefa
Acompanhe seu andamento com a instalação, a instalação e a configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima etapa. Cada linha da tabela lista tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Procedimento

Siga as etapas na tabela na ordem em que elas são apresentadas.

Check-list

Item	Descrição
☐	Como um usuário com ServiceNow AI Platform® função de administrador, configure seu ServiceNow AI Platform® instância. **a.** Atribuir ServiceNow AI Platform® e. Resposta a incidentes de segurança funções. **b.** Verifique se há ServiceNow Resposta a incidentes de segurança e outros plug-ins compatíveis com a integração são instalados e ativados para sua versão do ServiceNow AI Platform. **c.** Instale e configure um MID Server em seu ServiceNow AI Platform® instância. **d.** Crie um grupo de aprovação se quiser processar solicitações enviadas do analista de incidentes de segurança para isolar o host e iniciar ações de verificação de malware.

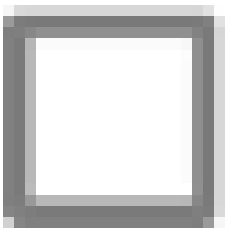
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações, consulte Configure seu ServiceNow AI Platform instância do McAfee ePO integração.
☐	. McAfee ePO administrador, configure seu McAfee ePO console. **a.** Verifique se você está usando a versão 5,9 de McAfee ePO. **b.** Instale o. ServiceNow plug-in de extensão em seu McAfee ePO console. **c.** Verifique se você criou marcadores de segurança em McAfee ePO console para isolar o host e iniciar ações de verificação de malware. Para obter mais informações, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR). Para obter mais informações e obter o arquivo do plug-in de extensão, em seu ServiceNow AI Platform instância, navegue até **Conhecimento** > **Artigos** > **Tudo** E, no campo Pesquisar, insira, ServiceNow Security Operations Extension para McAfee ePO .
☐	Como um usuário com ServiceNow AI Platform função de administrador, instale o. McAfee ePO aplicação do ServiceNow Store, configure um servidor e conecte-se ao McAfee ePO console. Para obter mais informações, consulte Instale a aplicação e configure um servidor para McAfee ePO integração.
☐	Como um usuário com ServiceNow AI Platform função de administrador de incidentes de segurança, edite os nomes dos marcadores de segurança em seu ServiceNow AI Platform® instância para que correspondam aos nomes de marcador que você criou em McAfee ePO console. Para obter mais informações, consulte Edite marcadores de segurança no ServiceNow AI Platform para McAfee ePO integração.
☐	Como um usuário com a função de administrador de incidente de segurança, crie um perfil para McAfee ePO. Para obter informações sobre perfis, consulte McAfee ePO perfis de capacidade de integração. Para obter as etapas necessárias para criar um perfil, consulte Crie um perfil de capacidade.
☐	Como um usuário com a função de administrador de incidentes de segurança, configure um perfil e teste incidentes de segurança. **a.** Revise as informações sobre condições e configurações de acionamento. **b.** Configurar um perfil. **c.** Testar e visualizar incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	d. Localize os resultados da pesquisa e outros detalhes nas listas relacionadas no incidente de segurança. **e.** Crie e configure diferentes tipos de perfis e teste incidentes de segurança para cada tipo. Para obter informações sobre condições de acionamento e o campo de IC alternativo, consulte Definir condições de acionamento com um campo Item de configuração (IC). Para obter as etapas necessárias para configurar um perfil, testar e visualizar incidentes de segurança e exemplos de tipos de perfil, consulte os exemplos a seguir Definir configurações.
	Como um usuário com ServiceNow AI Platform Função de analista de incidentes de segurança, Enviar solicitações adicionais para verificações de malware e listar eventos de ameaça. Para obter mais informações, consulte Gatilho McAfee ePO perfil manualmente a partir de um incidente de segurança. Em ServiceNow AI Platform, como um usuário com uma função de aprovação ou, como membro de um grupo de aprovação, aprovar solicitações para isolar isolamento de host e remover isolamento. Para obter mais informações sobre como processar solicitações de aprovação, consulte Crie um grupo de aprovação.

Você concluiu com sucesso as etapas de configuração, instalou e configurou a aplicação e verificou os resultados esperados para a integração.

Configure seu ServiceNow AI Platform® instância do McAfee ePO integração

A seção a seguir lista as tarefas de configuração que você precisa concluir em ServiceNow AI Platform® instância antes de instalar a aplicação para McAfee ePO integração.

Configurar requisitos

Função necessária: ServiceNow AI Platform administrador (admin). Revise as seguintes informações antes de ServiceNow AI Platform® instância do McAfee ePO integração.

A tabela a seguir é uma lista de requisitos de configuração da aplicação. Verifique se você concluiu essas tarefas antes de instalar a aplicação para a integração do ServiceNow Store.

Configurar tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform® e. Resposta a incidentes de segurança(SIR) funções.	As seguintes funções são necessárias: • Um usuário com a função de administrador do sistema (administrador) para instalar a aplicação. • Um usuário com a função de administrador de incidentes de segurança (sn_si.admin) configura a aplicação e cria, ativa e remove perfis. • Um usuário com a função analista de incidentes de segurança (sn_si.analyst) trabalha com incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefa	Descrição
	As tarefas incluem iniciar manualmente perfis de incidentes de segurança. Se a opção Aprovação for selecionada em um perfil durante a etapa de configuração, os usuários com essa função também enviarão solicitações para isolar hosts e retorná-los à rede.
Verifique se você está usando a versão 5,9 de McAfee ePO.	A integração oferece suporte à versão 10.4.3 do McAfee ePolicy Orchestrator.
Verifique se você instalou o. ServiceNow plug-in de extensão em seu McAfee ePO console.	Instale o. ServiceNow plug-in em seu McAfee ePO console. Para obter mais informações e obter o arquivo de plug-in, em ServiceNow AI Platform instância, navegue até **Conhecimento** > **Artigos** > **Tudo** E, no campo Pesquisar, insira Extensão de operações de segurança da ServiceNow para McAfee ePO .
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	O plug-in Dependência de resposta do incidente de segurança (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Espaço de resposta a incidentes de segurança **3.** Framework de integração de segurança **4.** Security Support Common **5.** Orquestração do suporte de segurança Para obter mais informações sobre como instalar as aplicações principais do Operações de segurança, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefa	Descrição
Verifique se você instalou e configurou um MID Server.	Um MID Server instalado e configurado é necessário em seu ServiceNow AI Platform® instância. Consulte Site de documentação do produto da ServiceNow Para obter mais informações sobre MID Servers.
Se você quiser habilitar o processo de aprovação para perfis, verifique se você criou um grupo de aprovação para processar solicitações.	Há um processo de aprovação opcional disponível para isolar máquinas host e restaurá-las para a rede. Se esta opção estiver habilitada, a aprovação prévia será necessária antes que as máquinas host sejam isoladas e restauradas em sua rede. Se sua organização quiser um nível extra de controle sobre essas ações, habilite o. **Aprovação necessária** opção durante a etapa de configuração de um perfil. Por padrão, a autoridade de aprovação é atribuída ao ServiceNow AI Platform® administrador de incidentes de segurança (sn_si.admin). Esta autoridade pode ser reatribuída a um grupo de aprovação. Qualquer membro do grupo tem permissão para aprovar ou rejeitar solicitações. Você seleciona um grupo de aprovação ativo durante a etapa de configuração da configuração do seu perfil. Para obter mais informações, consulte Crie um grupo de aprovação.

Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR)

A seção a seguir lista as etapas de configuração que você deve concluir em McAfee ePO antes de instalar a aplicação do ServiceNow Store para a integração.

Antes de Iniciar

Função necessária: McAfee ePO administrador

Como um usuário com McAfee ePO permissão de administrador, verifique se você instalou o. Servicenow.zip plug-in de extensão em seu McAfee ePO console. Este plug-in de extensão é necessário para a integração. Para obter mais informações e obter o plug-in, em seu ServiceNow AI Platform instância, navegue até **Conhecimento** > **Artigos** > **Tudo**. No campo Pesquisar, insira Extensão de operações de segurança da ServiceNow para McAfee ePO.

Por Que e Quando Desempenhar Esta Tarefa

. ServiceNow o plug-in de extensão conecta seu ServiceNow AI Platform instância para seu McAfee ePO console. Esta conexão permite que você faça referência aos marcadores de segurança que você cria em seu McAfee ePO isolar host e iniciar ações de verificação de malware para os perfis de capacidade em seu ServiceNow AI Platform instância.

Marcadores de segurança em seu McAfee ePO o console deve corresponder aos marcadores de segurança nos registros de capacidade do seu ServiceNow AI Platform instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As etapas a seguir mostram como instalar o plug-in de extensão, criar um marcador de segurança em seu McAfee ePO e atribua uma ação ao marcador. Para obter mais informações sobre os marcadores de segurança no McAfee ePO console, consulte Documentação do produto McAfee site.

Nota: Os números na seção a seguir são do McAfee ePO console.

Procedimento

1. Se você não instalou o. ServiceNow plug-in de extensão no seu McAfee ePO siga estas etapas para instalá-lo.

   a. Faça login no seu McAfee ePO Console com seu nome de usuário e senha do McAfee.

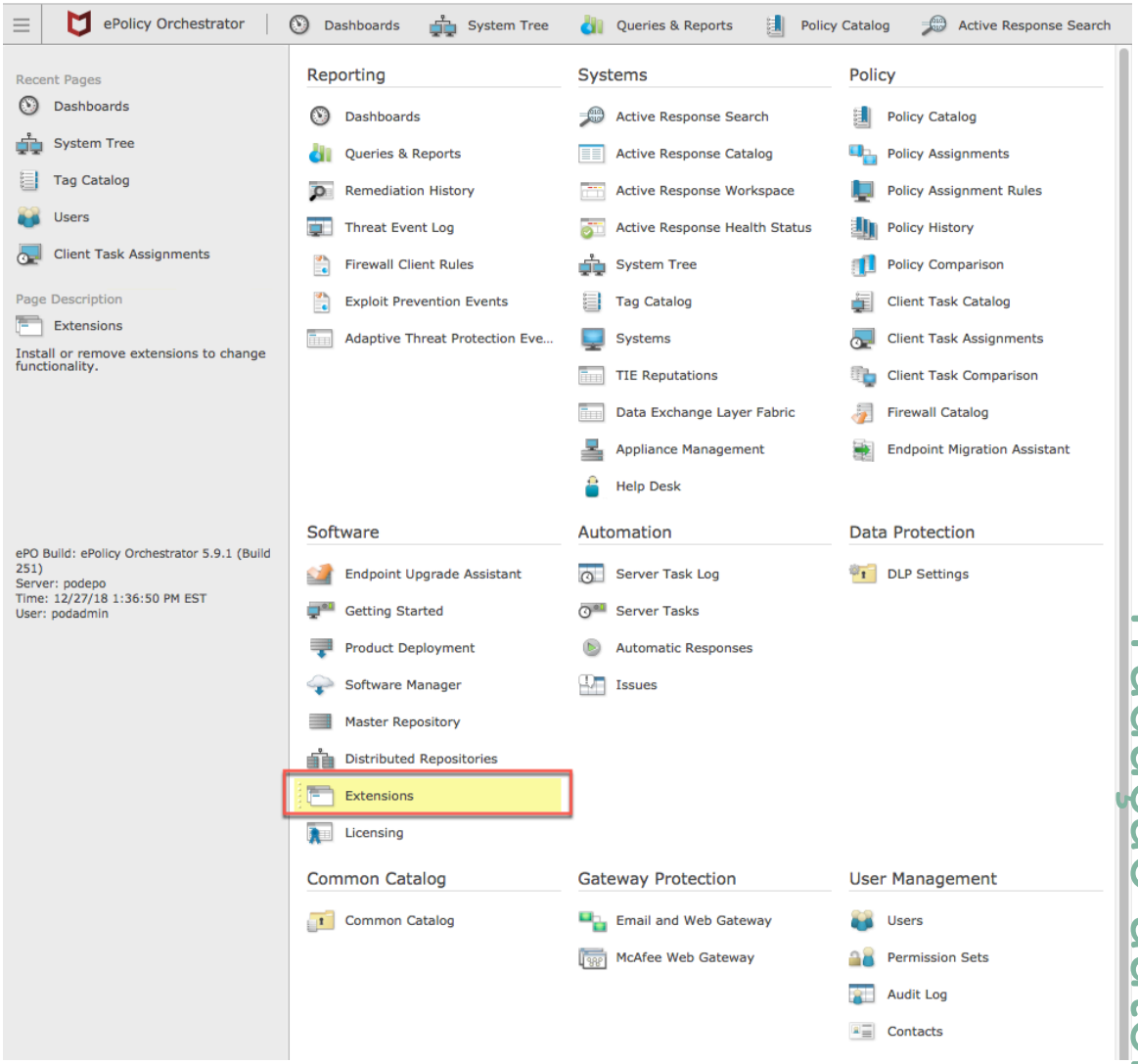


2. Se a página mostrada na figura a seguir não for exibida, no canto superior esquerdo da faixa da página inicial, clique no ícone de menu para exibi-la.

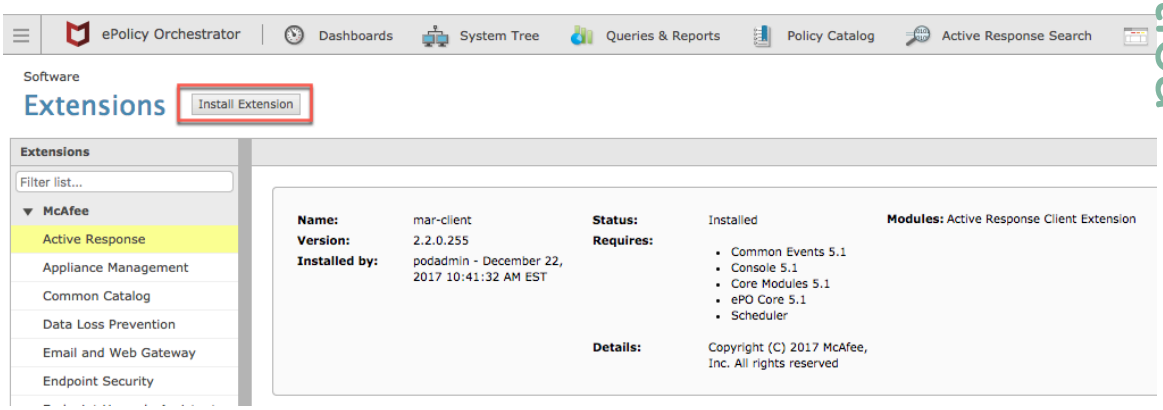
3. Na seção Software, clique em **Extensões** link.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



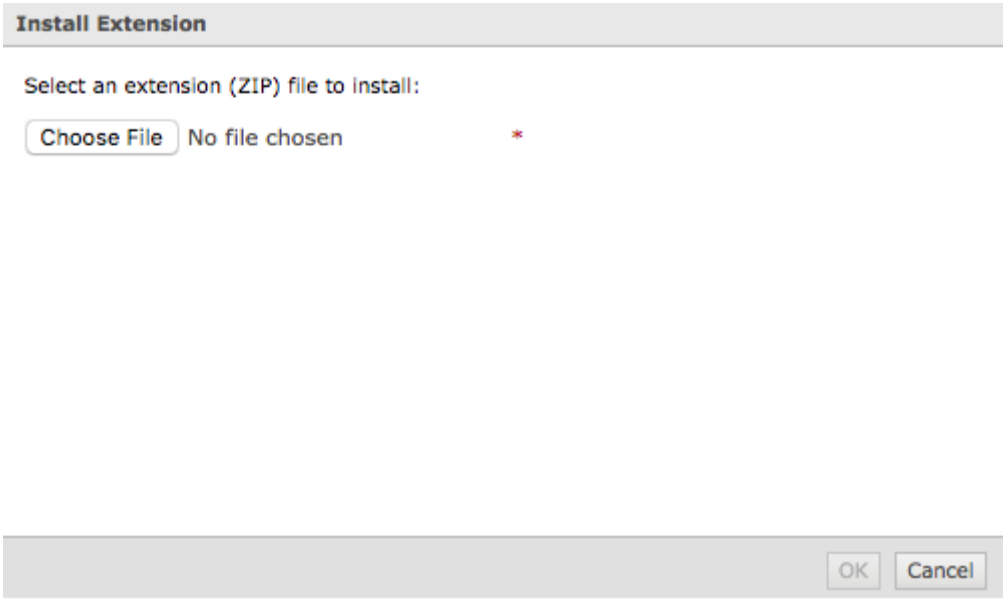
4. Na página Extensões exibida, clique em **Instale a extensão** .



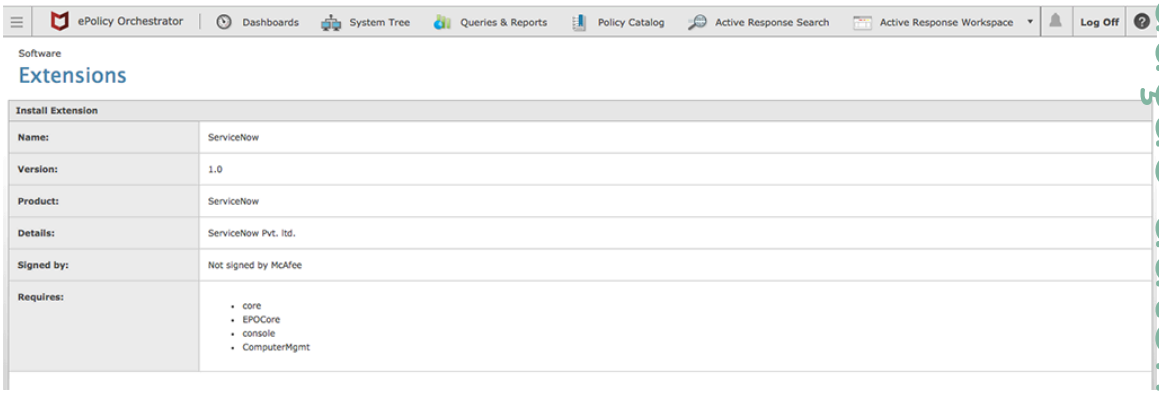
5. Na caixa de diálogo Instalar extensão, clique em **Escolha Arquivo** , navegue até Servicenow.zip em seu sistema e clique em **OK** para baixá-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Após a conclusão do download, a página Extensões de software é exibida com ServiceNow Plug-in de extensão listado.



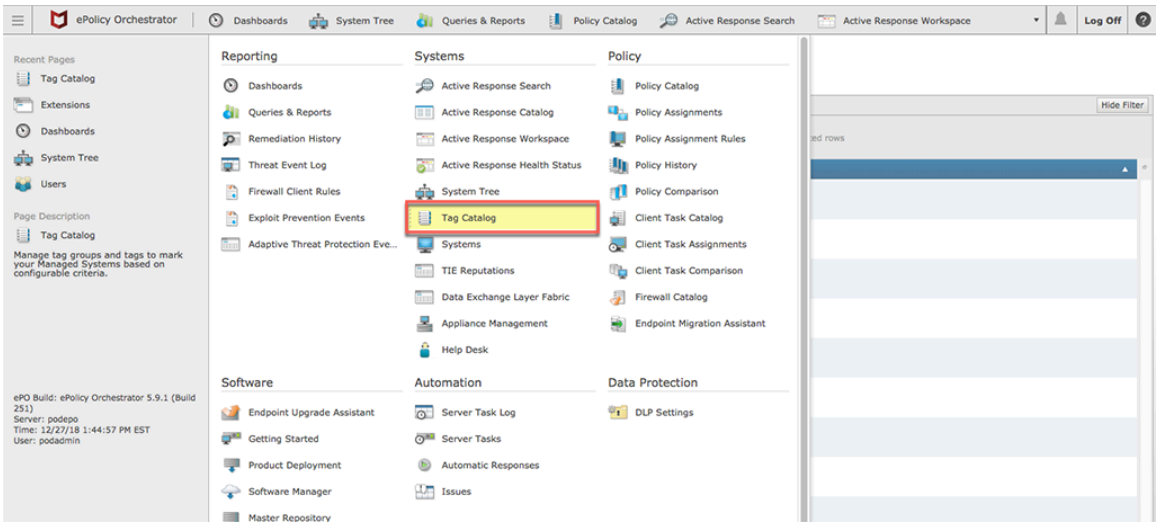
Você instalou com sucesso o. ServiceNow Extensão do plug-in em seu McAfee ePO console.

6. Se você não criou marcadores de segurança em McAfee ePO para iniciar verificação de malware e isolar ações de host, siga estas etapas.

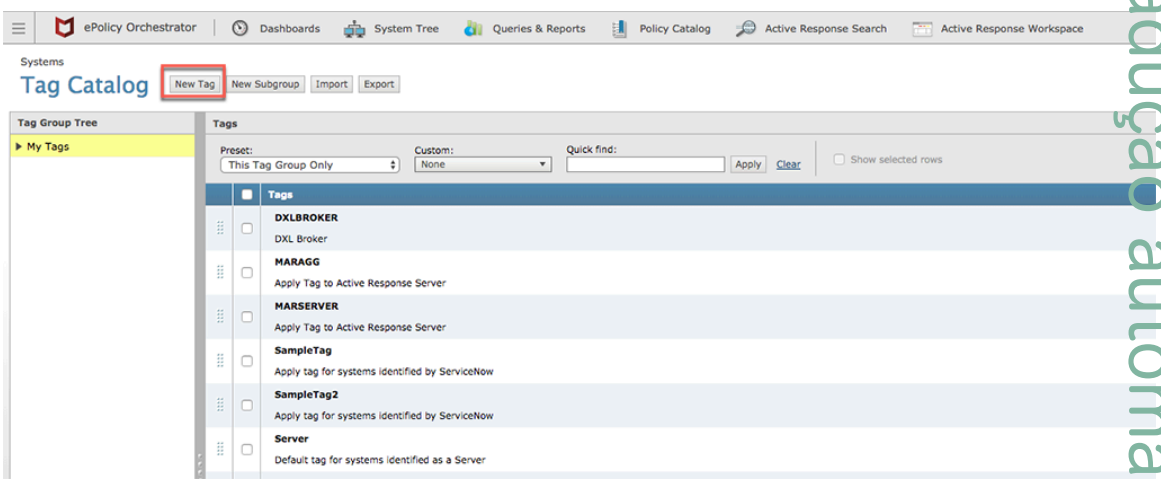
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até a página inicial e clique em **Catálogo de marcadores** link.

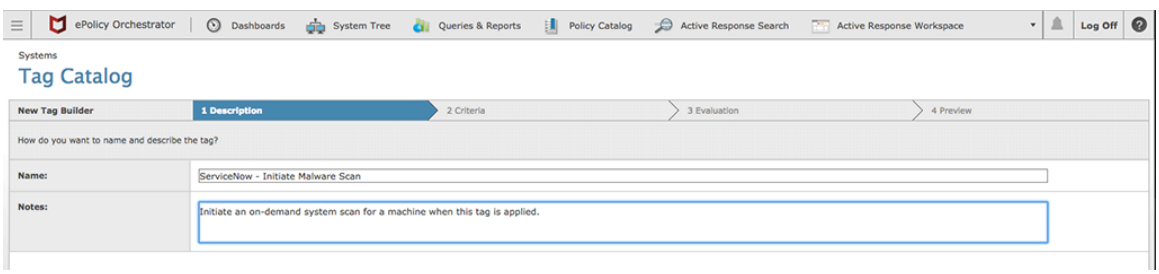


b. Na página Catálogo de marcadores exibida, clique em **Novo marcador** .



c. Com a etapa Descrição selecionada na barra de andamento exibida, insira um nome e uma descrição para o marcador.

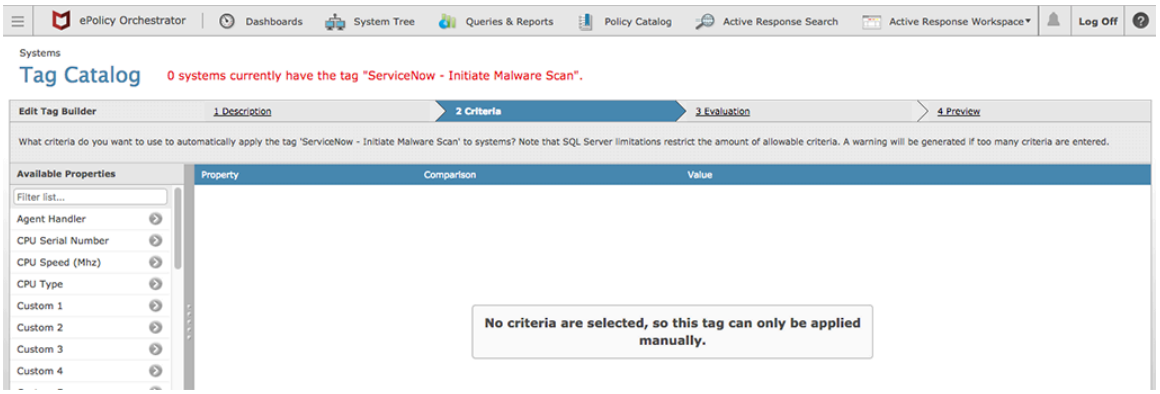
Para este exemplo, um marcador com um nome e uma descrição para o recurso Iniciar verificação de malware é exibido. Este nome de marcador é o que é correspondido e referenciado em seu ServiceNow AI Platform instância.



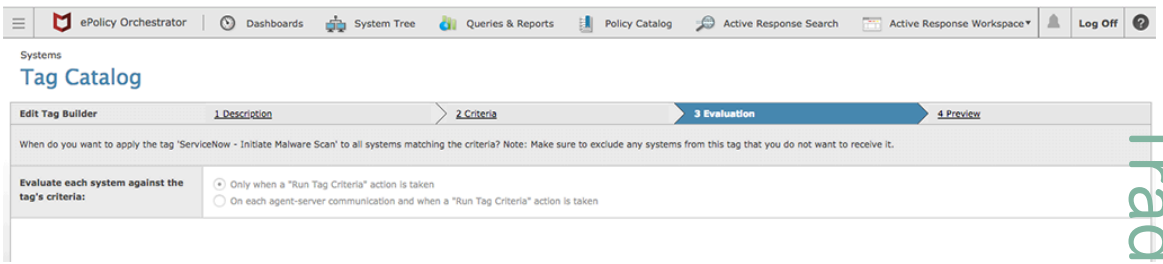
d. Para avançar para a etapa de critérios, clique em **Critérios** na barra de andamento.
As mensagens exibidas indicam que nenhuma ação está atribuída a este marcador no momento e que o marcador só pode ser aplicado manualmente.

Tradução automática

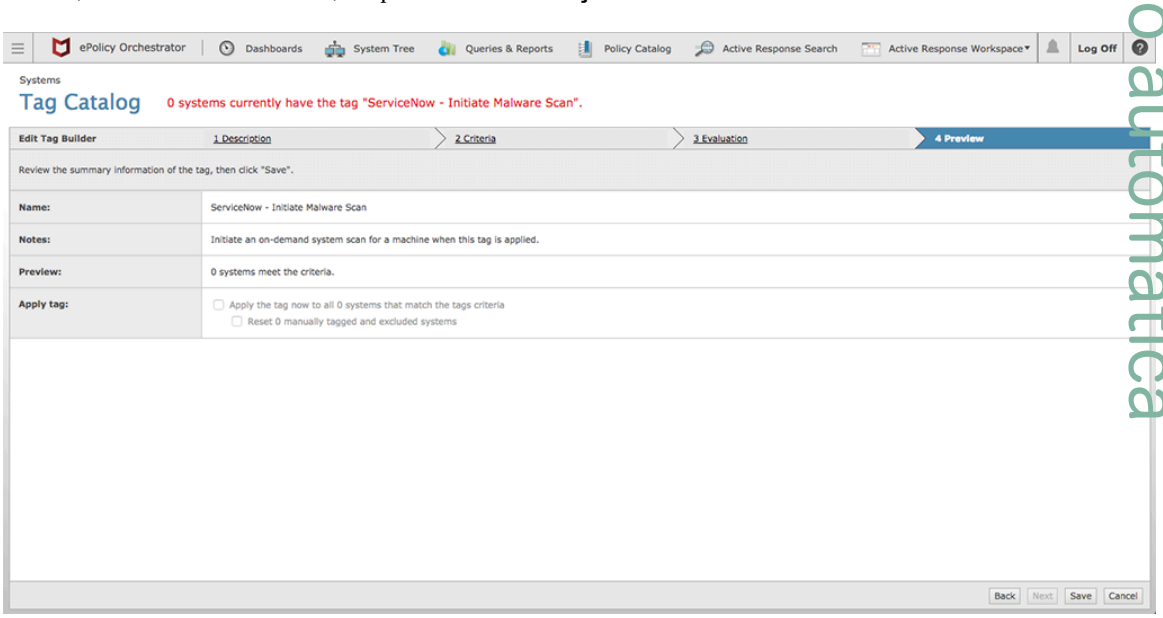
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Clique em **Avaliação** na barra de andamento para continuar.



f. Com a página Catálogo de marcadores da etapa Avaliação exibida, deixe as configurações nesta página em seus padrões e, na barra de andamento, clique em **Visualização** .

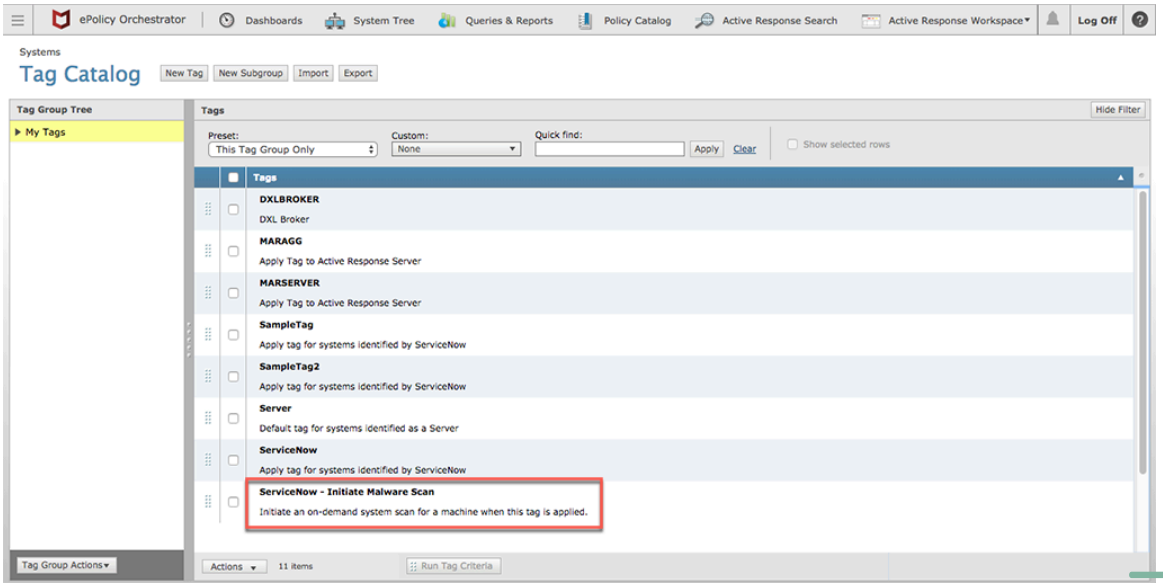


g. Com a página Visualizar exibida, no canto inferior direito da página, clique em **Salvar** para salvar o registro.

Tradução automática

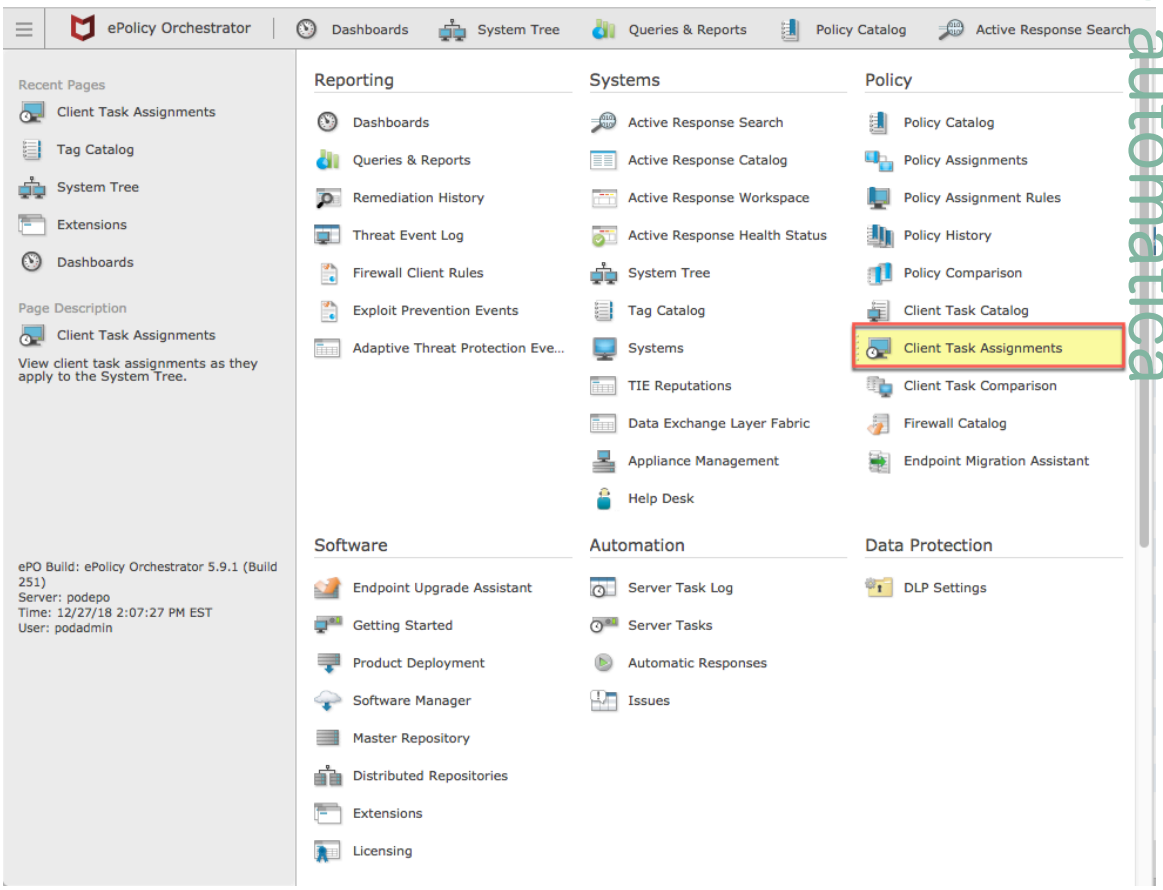
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O novo marcador é exibido no catálogo de marcadores, conforme mostrado na figura a seguir.



7. Repita as etapas anteriores para criar um marcador de segurança para a ação de isolamento do host. Depois de criar os dois marcadores, você estará pronto para atribuir ações aos novos marcadores.
8. Para adicionar uma ação ao seu novo marcador, siga estas etapas.

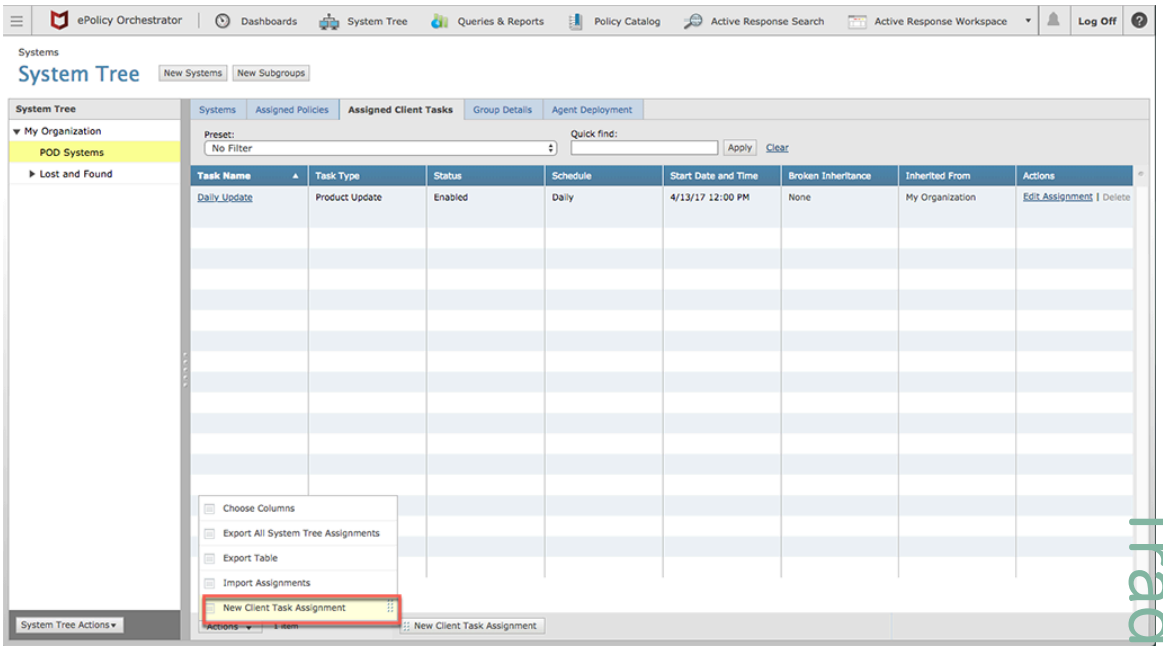
   a. Navegue até a página inicial e, na seção Política, clique em **Atribuições de tarefa do cliente** link.



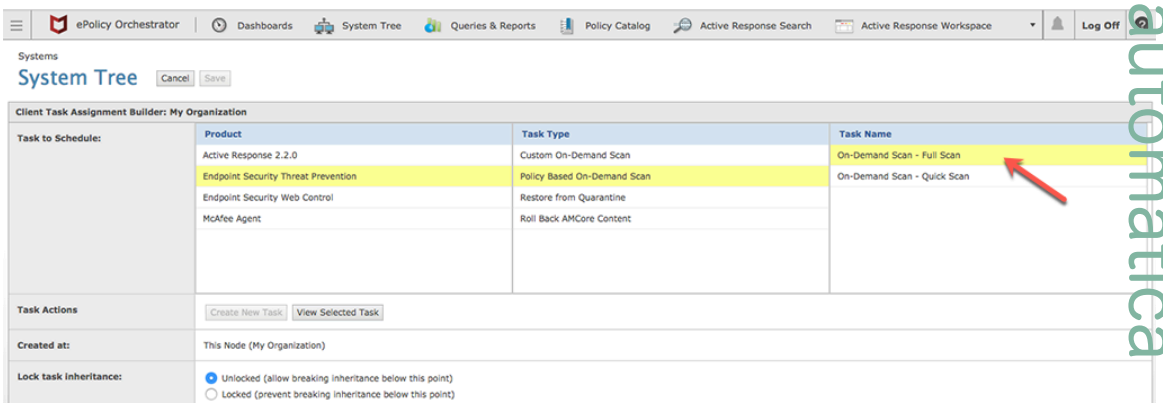
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Na página Árvore do sistema exibida, na parte inferior da página, expanda **Ações** e selecione **Nova atribuição de tarefa de cliente** .



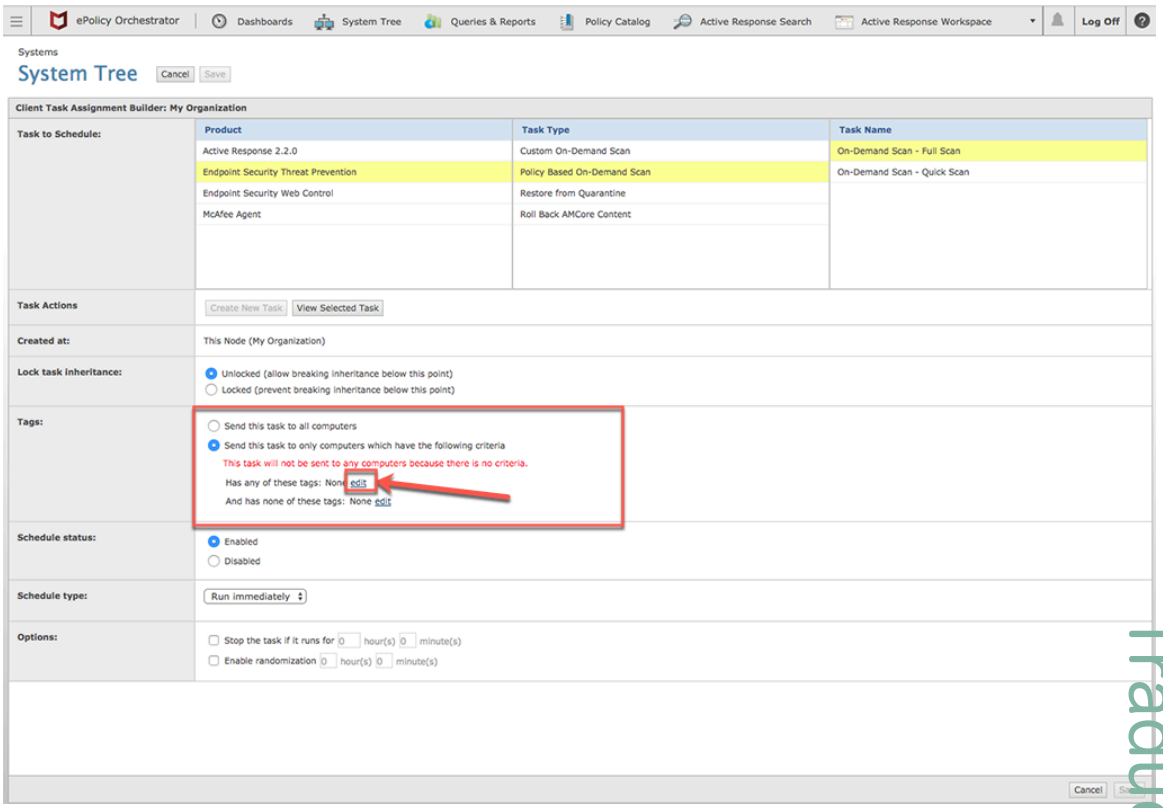
c. Na página exibida, navegue até **Prevenção contra ameaças à segurança de endpoint** > **Verificação sob demanda baseada em política** > **Verificação sob demanda - Verificação completa** selecionando o caminho conforme mostrado na figura a seguir.



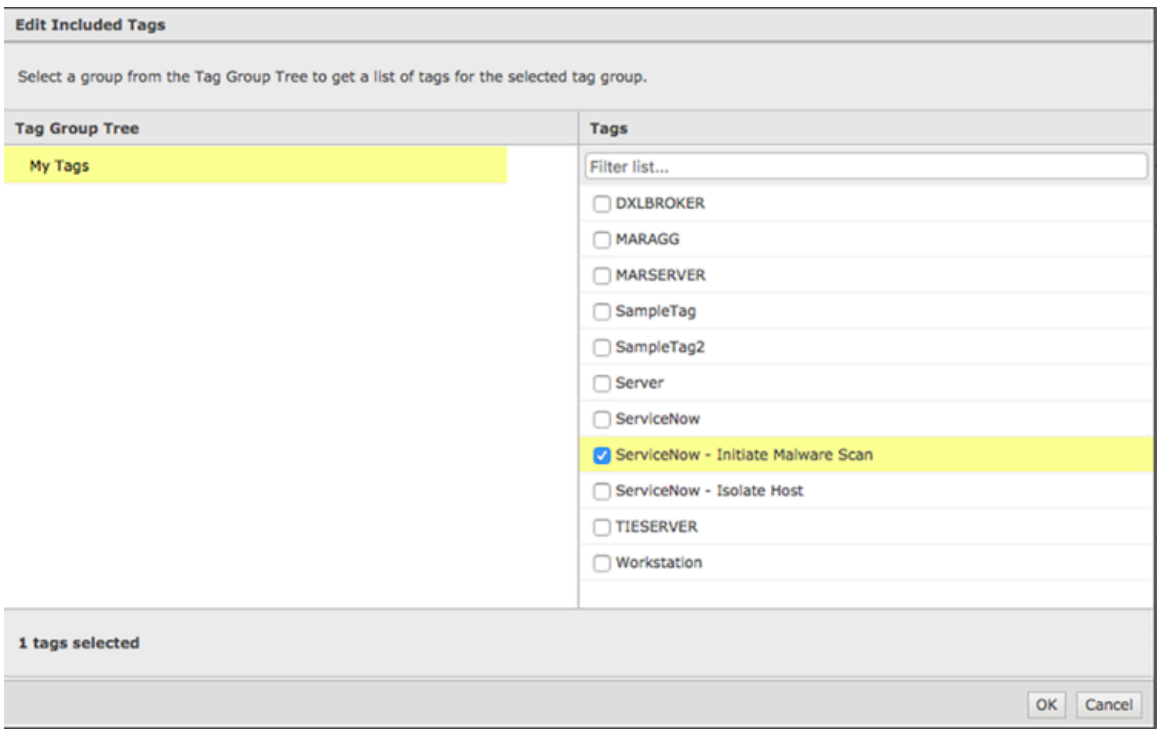
d. Na seção Marcadores, no botão de opção e ao lado de Tem qualquer um destes marcadores: , clique em **editar** link para editar os critérios do marcador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na caixa de diálogo exibida, selecione Iniciar verificação de malware ServiceNow marcador que você criou nas etapas anteriores e clique em **OK** .



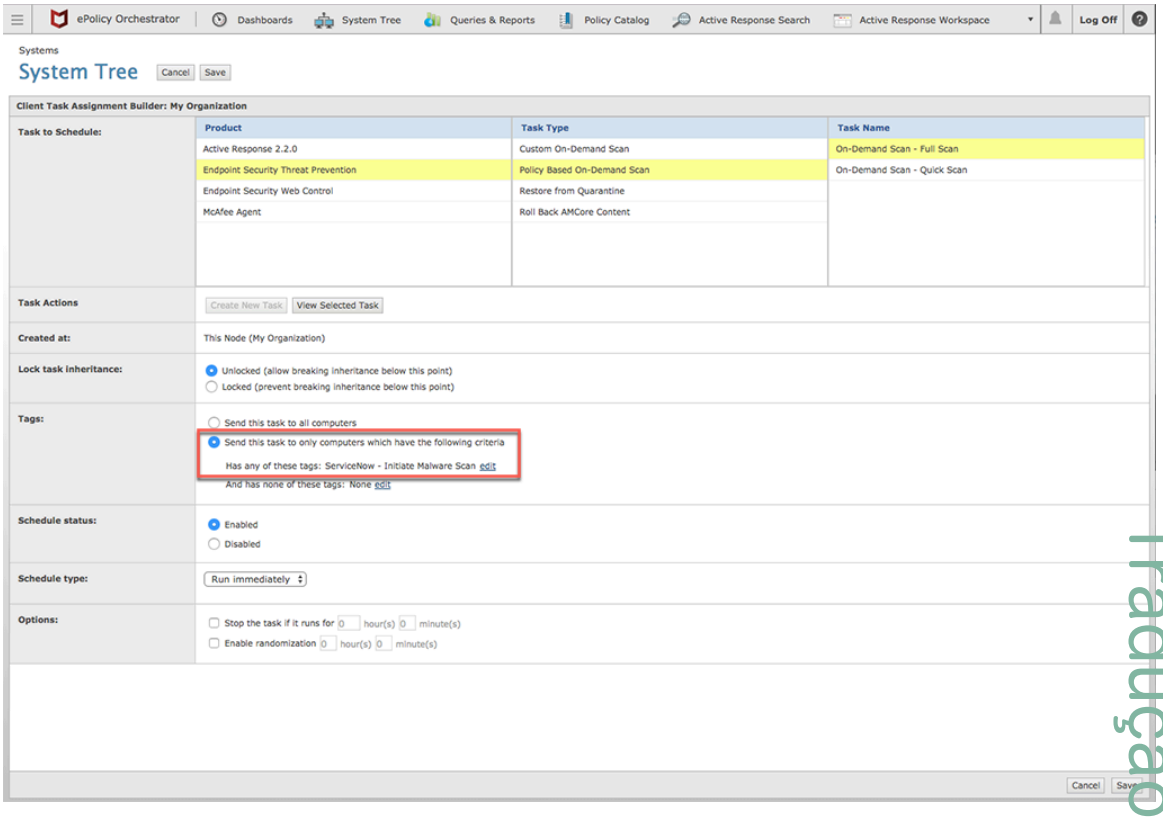
O marcador Iniciar verificação de malware da ServiceNow que você criou é atribuído à ação Verificação sob demanda.

f. Clique em **OK**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

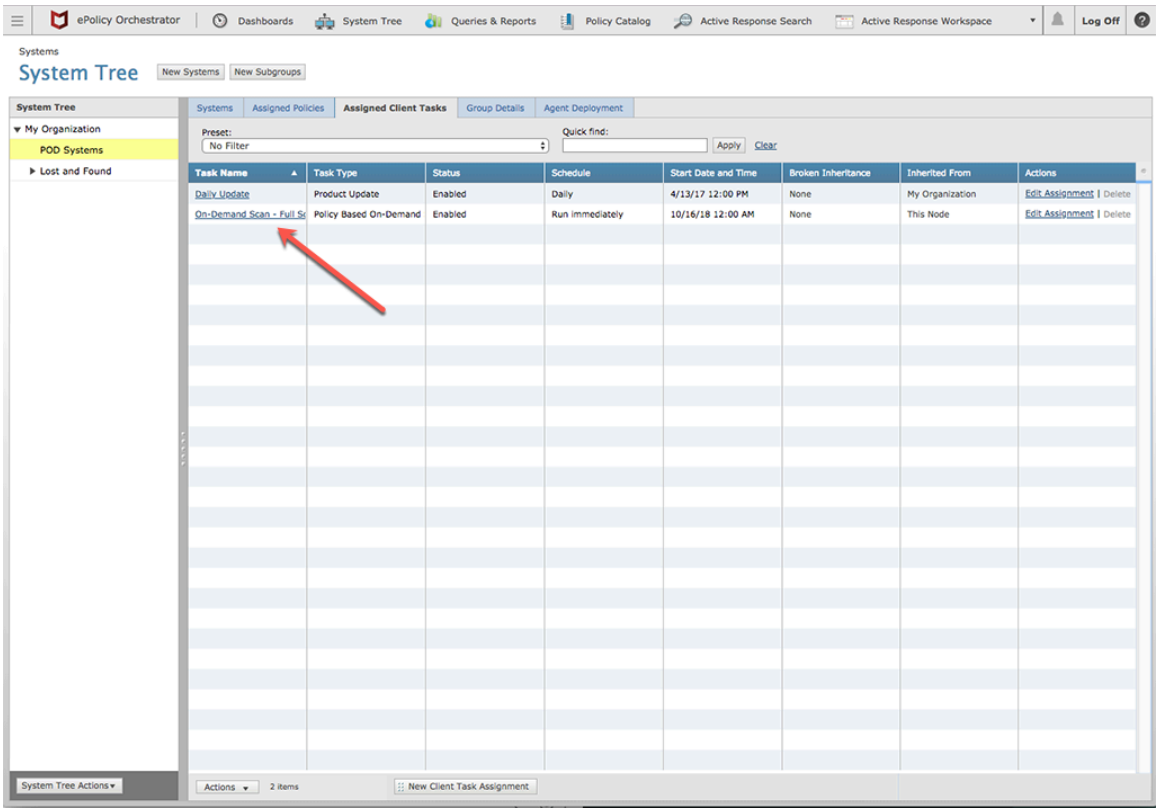
Na seção Marcadores, no botão de opção e ao lado de Tem qualquer um destes marcadores: , O marcador Iniciar verificação de malware é exibido.



g. Clique em **Salvar**.
Na página Árvore do sistema, a tarefa é exibida na lista Tarefas do cliente atribuídas (guia).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



h. Se você não tiver atribuído uma ação à ação Isolar host, repita as etapas anteriores para atribuí-la.

Você instalou o plug-in de extensão com sucesso, criou marcadores de segurança e atribuiu tarefas aos seus marcadores. Você concluiu a configuração da integração em seu McAfee ePO console. A próxima etapa é configurar um servidor em ServiceNow AI Platform instância.

Instale a aplicação e configure um servidor para McAfee ePO integração

Antes de invocar os fluxos de trabalho para a integração, instale e configure o. McAfee ePO aplicação do ServiceNow Store em seu ServiceNow AI Platform instância. A configuração é necessária para se conectar ao McAfee ePO console.

Antes de Iniciar

Função necessária: ServiceNow AI Platform administrador (admin)

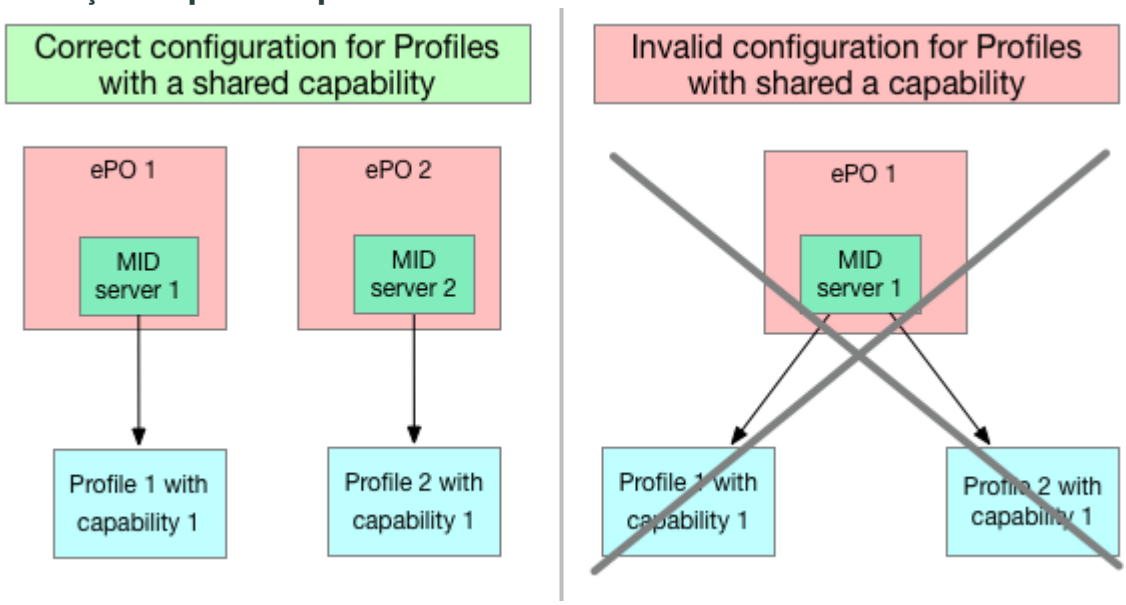
Por Que e Quando Desempenhar Esta Tarefa

A integração oferece suporte a vários servidores, no entanto, para evitar conflitos em perfis que compartilham as mesmas condições de acionamento, você não pode compartilhar um McAfee ePO capacidade com vários perfis que usam o mesmo McAfee ePO servidor. Por exemplo, como mostrado na figura a seguir, você pode ter a capacidade 1 em mais de um perfil, desde que cada um McAfee ePO o servidor é mapeado para um perfil exclusivo que tem capacidade 1.

Tradução automática

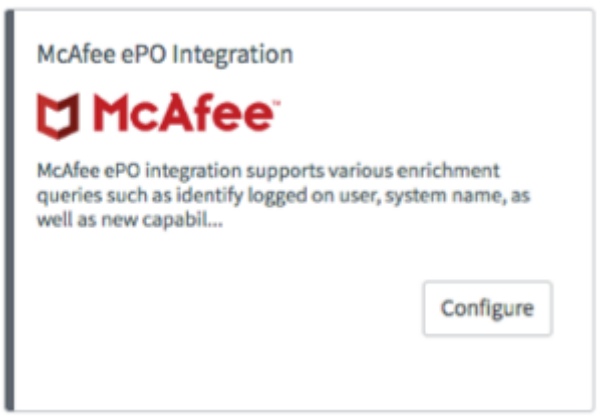
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Limitações do perfil compartilhado do McAfee



Procedimento

1. Baixe o. McAfee ePO para Operações de segurança em ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE McAfee ePO para Operações de segurança bloco de integração e clique em **Configurar** .



4. No formulário, preencha os campos.

Configuração de integração do McAfee ePO

Campo	Descrição
Nome	Nome da integração, por exemplo, demonstração-1 .
Nome do Servidor do ePO	Nome do McAfee ePO servidor. Se você usar um servidor, um exemplo será, McAfee HQ (Matriz da McAfee). Este nome é como o servidor e as credenciais relacionadas são reconhecidos.

Tradução automática

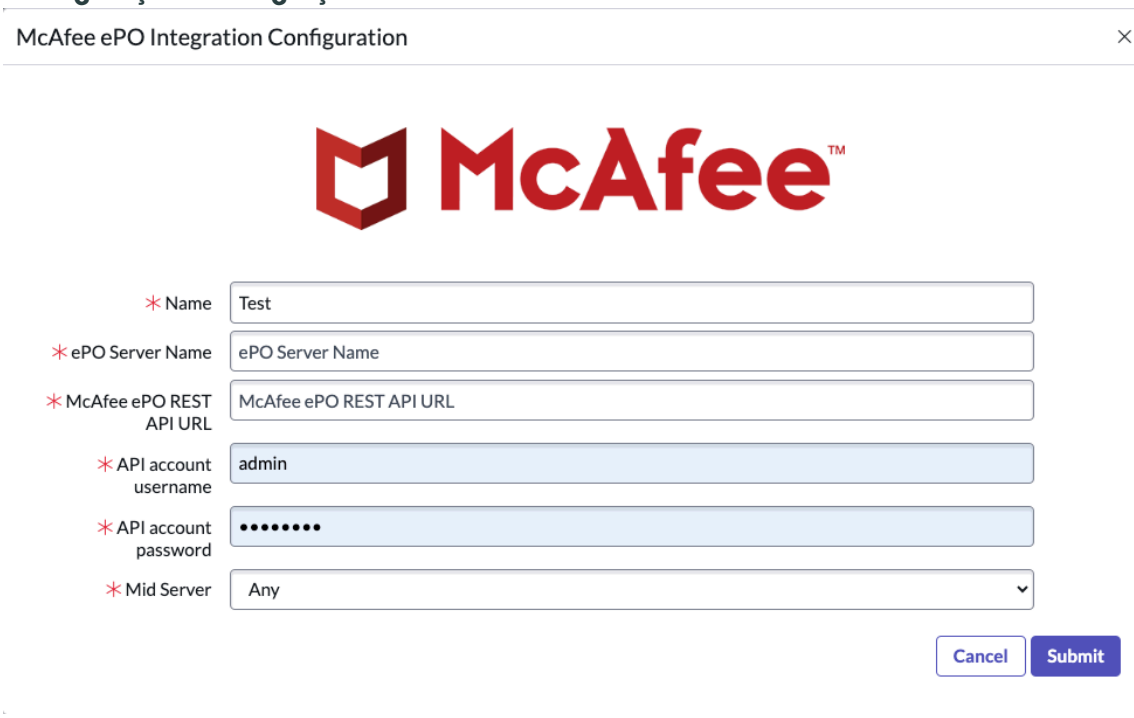
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se sua organização exigir suporte para vários servidores, insira o nome de cada servidor e repita o processo.
URL da REST API do McAfee ePO	URL base que hospeda o. McAfee ePO REST API. Insira o URL com o protocolo https://, por exemplo, `https://corp.epo_server:8443` .
Nome de usuário da conta da API	Nome de usuário exclusivo da conta, por exemplo, `API da ServiceNow` .
Senha da conta da API	Senha exclusiva para a conta da API.
MID Server	Selecione o nome do MID Server que você configurou durante a configuração do ServiceNow AI Platform instância. Você pode selecionar um MID Server específico na lista ou selecionar **Qualquer** Para habilitar uma seleção automática de um MID Server válido na lista para esta integração. **Nota:** ○ O MID Server selecionado durante este tempo de configuração se aplica a toda esta integração. ○ Somente MID Servers ativos e validados são exibidos nesta lista. Por padrão, o valor é definido como **Qualquer** . Um exemplo de nome é, `secops_local_midserver` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de integração do McAfee ePO



5. Clique em **Enviar**.
   A lista Configurações do McAfee ePO é exibida com o novo registro de configuração. Você concluiu com sucesso a configuração de um McAfee ePO servidor.

Nota: Se sua organização exigir suporte para vários servidores, repita as etapas.

Edite marcadores de segurança no ServiceNow AI Platform para McAfee ePO integração

Como parte da configuração da integração, edite os nomes dos marcadores de segurança que você criou em McAfee ePO console em seu ServiceNow AI Platform instância. Edite os nomes dos marcadores em seu ServiceNow AI Platform instância para que correspondam aos nomes dos marcadores em seu McAfee ePO console.

Antes de Iniciar

Função necessária: ServiceNow AI Platform administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Os nomes dos marcadores de segurança em seu McAfee ePO o console das ações iniciar verificação de malware e isolar host deve corresponder aos nomes dos marcadores de segurança nos registros desses recursos do seu ServiceNow AI Platform instância.

Antes de criar um perfil de capacidade para executar suas capacidades, exiba a lista de disponíveis McAfee ePO e edite os marcadores de segurança em seu ServiceNow AI Platform instância para que correspondam aos nomes dos marcadores de segurança em seu McAfee ePO console.

Para obter mais informações sobre como criar os nomes de marcadores de segurança em seu McAfee ePO console, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR).

Tradução automática

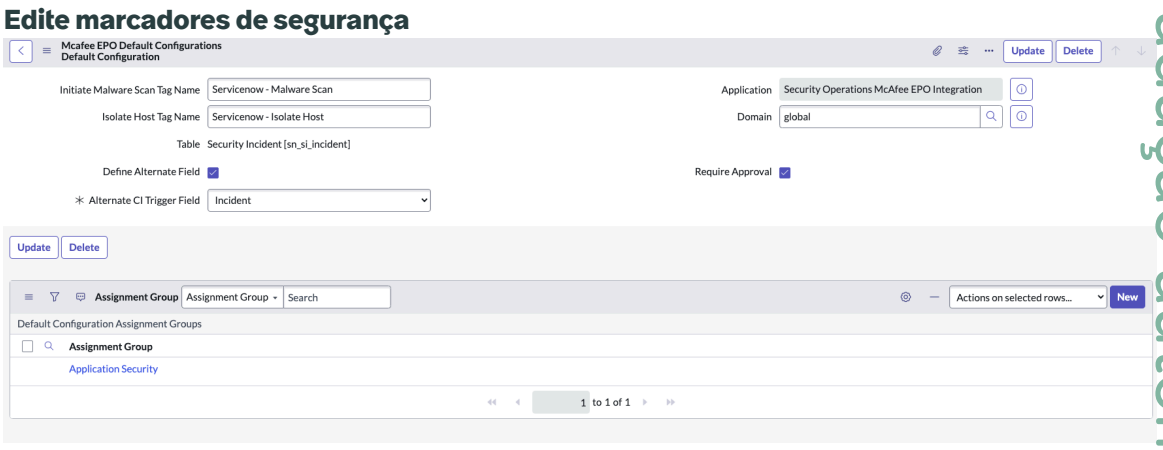
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração do McAfee ePO** > **Configurações padrão**.
2. Para editar o nome do marcador de segurança do McAfee ePO integração, clique em **Configuração padrão** .

   Nota: Certifique-se de executar esta configuração depois de instalar o. McAfee ePO integração.

3. No campo Iniciar nome do marcador de verificação de malware, insira o nome do marcador de segurança que você criou em McAfee ePO console para a ação iniciar verificação.
   Por exemplo, ServiceNow - Verificação de malware
4. No campo Isolar nome do marcador do host, insira o nome do marcador de segurança que você criou em McAfee ePO console para a ação isolar host.
   Por exemplo, ServiceNow - isolar host
5. Se você não quiser usar o campo de gatilho de IC na criação do incidente, selecione **Definir campo alternativo** caixa de seleção.
   Quando esta opção está habilitada, a lista de seleção do campo do gatilho de IC alternativo é exibida.



6. Escolha um campo alternativo na lista de seleção para verificar seus critérios de pesquisa de IC.
   Para este exemplo, como um usuário com a função sn_si.admin, você acredita que o campo IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no IC identificado No incidente de segurança e você seleciona o campo IC identificado como uma alternativa. O IC identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.
7. No campo Domínio, selecione um domínio ou grupo para esta configuração usando a opção de pesquisa.
   Por exemplo, global.
8. No campo Exigir aprovação, selecione **Aprovação necessária** Se você estiver usando os recursos Isolar host e Remover isolamento.

   Nota: Os recursos Iniciar verificação de malware, Listar eventos de ameaça e Obter detalhes do sistema não precisam de aprovação.

9. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Nome do marcador do ePO é atualizado e exibido na lista Configurações padrão do McAfee ePO. O nome do marcador de segurança da ação de verificação de malware em seu ServiceNow AI Platform a instância corresponde ao nome da verificação em seu McAfee ePO console.

Você editou com sucesso os nomes dos marcadores do ePO para a verificação de malware e os recursos de isolar host em seu ServiceNow AI Platform instância. A próxima etapa é criar um perfil para suas capacidades.

Tópicos relacionados

Documentação do produto McAfee

Crie um grupo de aprovação

Crie um grupo de aprovação para McAfee ePO para Operações de segurança integração que pode aprovar solicitações para isolar máquinas host, restaurando-as para a rede.

Antes de Iniciar

Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota: A opção de aprovações no Definir configurações Aparece somente para os recursos Isolar host e Remover isolamento de host.

Função necessária: ServiceNow AI Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

As solicitações de aprovação enviadas pelo analista de incidentes de segurança para isolar máquinas host e remover o isolamento são atribuídas ao usuário com a função sn_si.admin por padrão. Como um usuário com esta função, você pode reatribuir esta autoridade de aprovação durante a etapa de configuração de um perfil. Antes de reatribuir autoridade a um grupo de aprovação, um grupo de aprovação deve estar disponível no Grupos lista em seu ServiceNow AI Platform instância.

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Grupos**.
2. Na lista Grupos, clique em **Novo** .
3. No formulário, preencha os campos.

Formulário do grupo de aprovação

Campo	Descrição
Nome	Nome do grupo exibido quando uma solicitação de aprovação é enviada, por exemplo, Isolamento de host McAfee dos aprovadores .
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo, Mcafeeapproval em ServiceNow .com
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Primário	(Opcional) Outro grupo do qual este grupo é membro, se este grupo tiver um primário.
Descrição	Informações adicionais sobre este grupo.
Incluir membros	Opção para incluir membros a este grupo.
Responsável padrão	Opção para escolher um usuário como designado padrão para este grupo. Use a opção Pesquisar para abrir a lista de usuários.
Funções	Opção para selecionar as funções deste grupo. Use a opção Adicionar e remover para adicionar e remover funções.
Tipo	Opção para escolher uma categoria para este grupo. Use a opção Pesquisar para abrir a lista de tipos de grupo.
Fornecedores	Opção para escolher um fornecedor para este grupo. Use a opção Pesquisar para abrir a lista de fornecedores.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

   Este grupo está disponível para processar solicitações quando você habilita o. **Aprovação necessária** durante a configuração deste perfil.

   Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até **Minhas aprovações** no ServiceNow AI Platform.

McAfee ePO perfis de capacidade de integração

Como um usuário com a função de administrador de incidentes de segurança (sn_si.admin), você cria perfis para McAfee ePO recursos em seu ServiceNow AI Platform® instância. Você agrupa consultas ou ações em perfis e determina quais McAfee ePO capacidades que você deseja executar quando um novo incidente de segurança é criado.

Perfis de capacidade

Você cria perfis ™para que você possa agrupar McAfee ePO e defina as configurações desses recursos no seu ServiceNow AI Platform® instância. Você tem a flexibilidade de criar vários perfis para esses recursos, o que permite determinar quais ações ou consultas são invocadas quando um Resposta a incidentes de segurança(SIR o incidente foi criado. Para atender às necessidades da sua organização, você pode criar um único perfil que executa consultas de detalhes do sistema, inicia verificações de malware e isola máquinas host, por exemplo, ou pode criar vários perfis, cada um com seu próprio, único McAfee ePO capacidade.

Tipos de perfil e obrigatórios McAfee ePO.

Finalidade primária do seu perfil	Configurar requisitos	Recursos do McAfee ePO necessários para este tipo de perfil
Reúna detalhes do sistema	Nenhum(a)	**Obter detalhes do host**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de perfil e obrigatórios McAfee ePO.

Finalidade primária do seu perfil	Configurar requisitos	Recursos do McAfee ePO necessários para este tipo de perfil
Isolar um host	Verifique com seu McAfee ePO administrador que você criou os marcadores de segurança para a ação isolar host em seu McAfee ePO console. Para obter mais informações, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR).	**Isolar Host**
Verifique e pesquise ameaças em seu host	Verifique com seu McAfee ePO administrador que você criou os marcadores de segurança para a ação iniciar verificação de malware em seu McAfee ePO console. Para obter mais informações, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR).	**Iniciar verificação de malware** **Nota:** Como parte do McAfee ePO Verificação de malware, o recurso Listar eventos de ameaça é invocado automaticamente. No entanto, você não precisa adicionar o recurso Listar eventos de ameaça ao perfil com o recurso de verificação de malware. Os resultados da verificação de malware são exibidos na guia Detalhes do evento de ameaça no incidente de segurança.
Remova o isolamento de um host	Verifique com seu McAfee ePO administrador que você criou os marcadores de segurança para a ação isolar host em seu McAfee ePO console. Para obter mais informações, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR).	**Remover isolamento**
Colete dados de aprimoramento de ameaças.	Nenhum(a)	**Listar eventos de ameaça**

Crie um perfil de capacidade

Crie um perfil e selecione McAfee ePO capacidades que você deseja que o perfil execute.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: ServiceNow AI Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Para esta etapa da configuração, você cria um perfil para McAfee ePO. Ao criar perfis, considere a intenção do perfil antes de adicionar McAfee ePO recursos para ti. Consulte a tabela a seguir ao criar perfis.

A tabela a seguir lista os recursos que você precisa adicionar a um perfil se quiser que o perfil execute determinadas consultas ou ações. Crie um único perfil que execute consultas para detalhes do host, inicie verificações de malware, remova o isolamento e isole as máquinas host ou crie vários perfis, cada um com sua própria capacidade única.

Procedimento

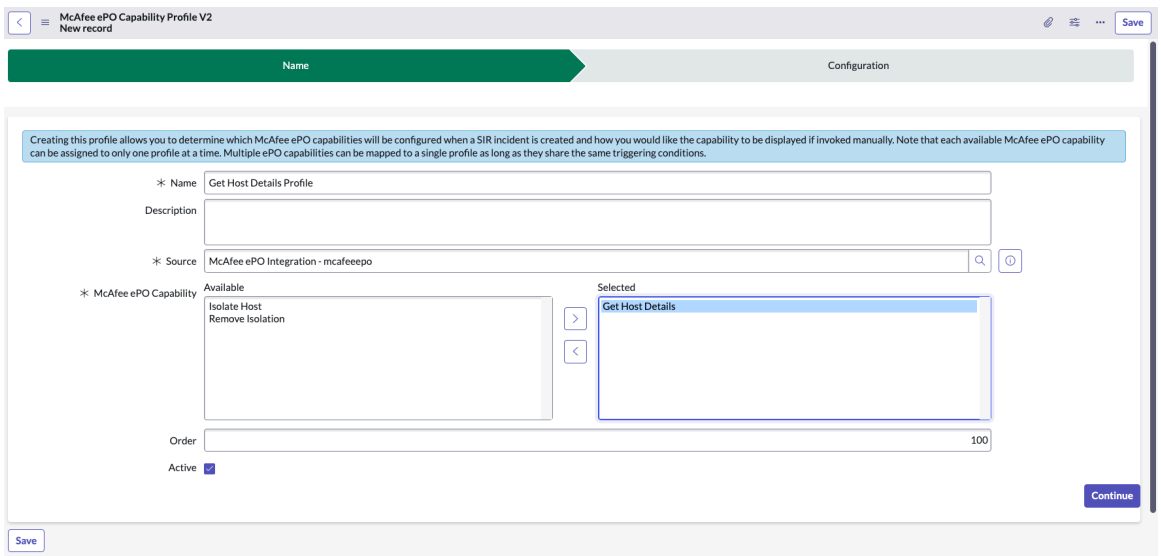
1. Navegar até **Integração do McAfee ePO** > **Perfis de capacidade do McAfee ePO**. . McAfee ePO A lista Perfis de capacidade é exibida.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do McAfee ePO perfil de capacidade. Este nome ajuda a identificar o tipo de perfil e descrevê-lo. Um exemplo de um perfil que executa consultas é Host e Detalhes da ameaça. Este nome também é o nome do marcador de segurança deste perfil por padrão.
Descrição	Informações adicionais sobre o perfil que descrevem melhor as atividades do perfil. Um exemplo de descrição de um perfil que executa consultas é o aprimoramento de ameaças para obter detalhes do sistema e uma lista de eventos de ameaça. Um exemplo de descrição de um perfil que executa ações é Isolar máquina host.
Origem	Nome do McAfee ePO servidor. Somente servidores configurados estão disponíveis na lista de seleção.
Capacidade do McAfee ePO	Recursos do McAfee ePO perfil. O McAfee ePO oferece suporte aos seguintes recursos: ○ Obter detalhes do host ○ Isolar perfil de host ○ Iniciar verificação de malware ○ Remover isolamento ○ Listar eventos de ameaça Selecione os recursos desejados para este perfil em **Disponível** e mova-as para **Selecionado** coluna. Você não pode adicionar Obter detalhes do host, Iniciar verificação de malware e listar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	eventos de ameaça no mesmo perfil e não pode adicionar Remover isolamento e Isolar host no mesmo perfil.
Ordem	Prioridade do fluxo de trabalho. O padrão é 100. O valor deste campo indica a ordem em que os fluxos de trabalho são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	A caixa de seleção é marcada por padrão para indicar que o perfil está ativo. Quando selecionado, o perfil fica ativo e é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem especificadas durante a etapa de configuração. Quando inativo, o perfil não será executado e não estará disponível para ser invocado em uma lista.



4. Para salvar e validar o perfil, clique em **Continuar** .
   Se a validação for bem-sucedida, a página será recarregada e **Configuração** o formulário é exibido.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, você pode preferir revisar os conceitos para configurar perfis e acionar condições. Para obter mais informações, consulte Configure seu McAfee ePO console ao qual integrar Resposta a incidentes de segurança(SIR) e Definir condições de acionamento com um campo Item de configuração (IC).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir condições de acionamento com um campo Item de configuração (IC)

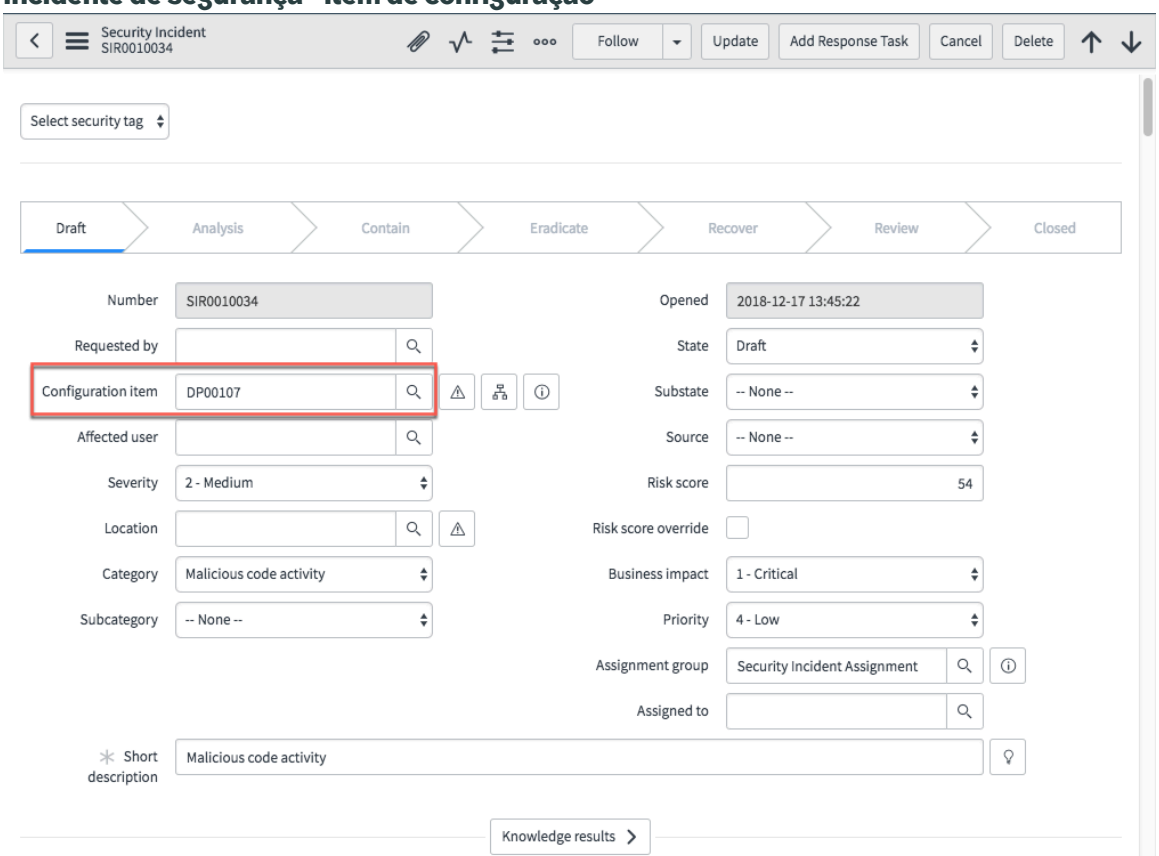
Depois de criar um perfil e selecionar McAfee ePO para executar o perfil, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

Você tem a flexibilidade de definir essas condições de acionamento para que o perfil seja executado automaticamente com base nos valores de campo padrão correspondentes em um ServiceNow AI Platform® Resposta a incidentes de segurança incidente de segurança. Como alternativa, você pode configurar um perfil para que ele pesquise correspondências nos valores de campo que você identifica especificamente no incidente de segurança.

Uma das chaves para a funcionalidade da integração e como um perfil funciona é o campo Item de configuração (IC) no ServiceNow AI Platform® Resposta a incidentes de segurança(SIR incidente de segurança. O valor deste campo é o valor principal em um incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no ServiceNow AI Platform® banco de dados. . SIR Um incidente de segurança é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados em busca de um valor correspondente para um Nome de domínio totalmente qualificado (FQDN), um nome de host ou um endereço IP com base no valor do campo Item de configuração.

Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados podem ser coletados do McAfee ePO console do ativo correspondente, inserido em seu ServiceNow AI Platform® e exibidos nas listas relacionadas de um incidente de segurança. A figura a seguir mostra um exemplo do campo Item de configuração preenchido com um nome de host em um SIR incidente de segurança.

Incidente de segurança - Item de configuração



Nos casos em que o campo Item de configuração (IC) não estiver preenchido no incidente de segurança ou uma correspondência não puder ser encontrada para um FQDN, um nome

Tradução automática

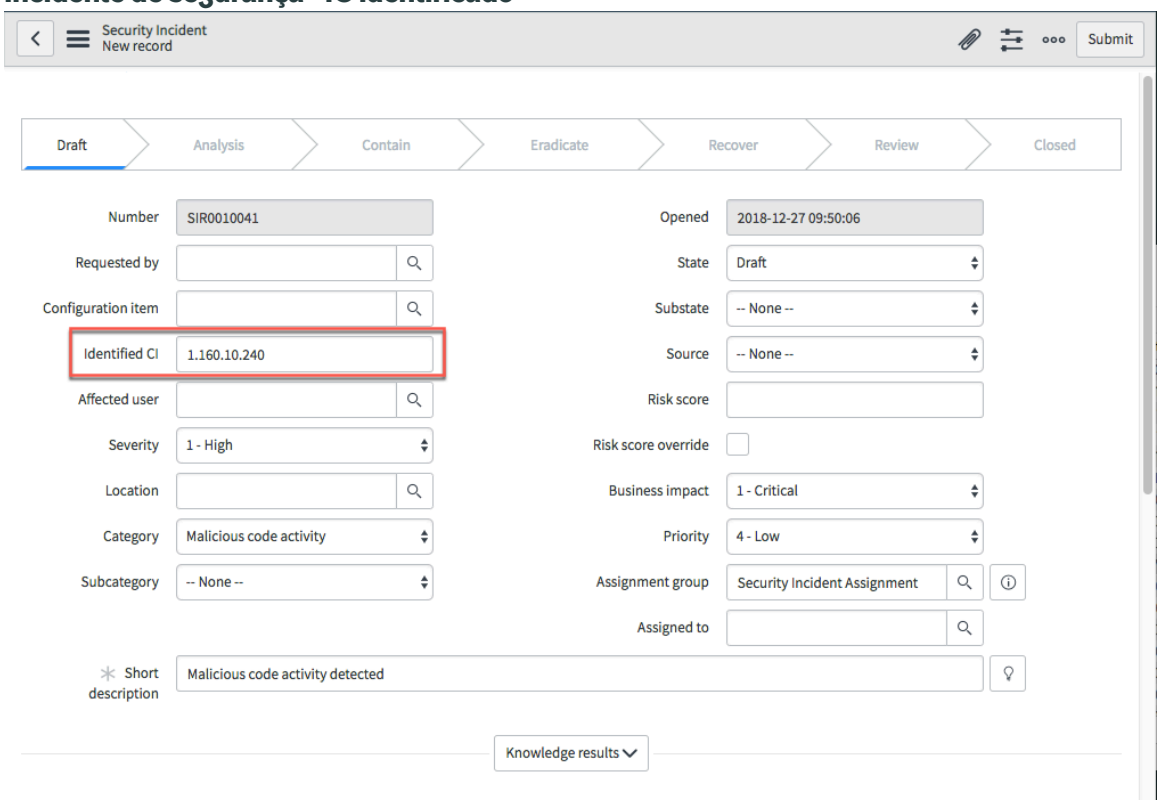
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de host ou um endereço IP que corresponda ao banco de dados, você pode selecionar um campo alternativo no incidente de segurança para exibir quaisquer dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de gatilho de IC alternativo para identificação de endpoint para garantir que os dados de aprimoramento de IC do sejam fornecidos McAfee ePO a pesquisa é preenchida no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que seus perfis sejam executados mesmo que o campo IC não esteja preenchido no incidente de segurança associado após a criação do incidente.

Como exemplo, como analista do SOC (Security Operations Center, centro de operações de segurança), você cria um campo personalizado para um incidente de segurança chamado Endereço IP no meu incidente de segurança. Se você acha que o valor desse campo personalizado não será exibido no campo Item de configuração no incidente de segurança após a criação do incidente, configure o perfil para que ele verifique este endereço IP. Se correspondido, o endereço IP será exibido no incidente de segurança no campo de sua escolha. Na figura a seguir, o IC identificado O campo está selecionado como o campo alternativo para o endereço IP deste exemplo.

Incidente de segurança - IC identificado

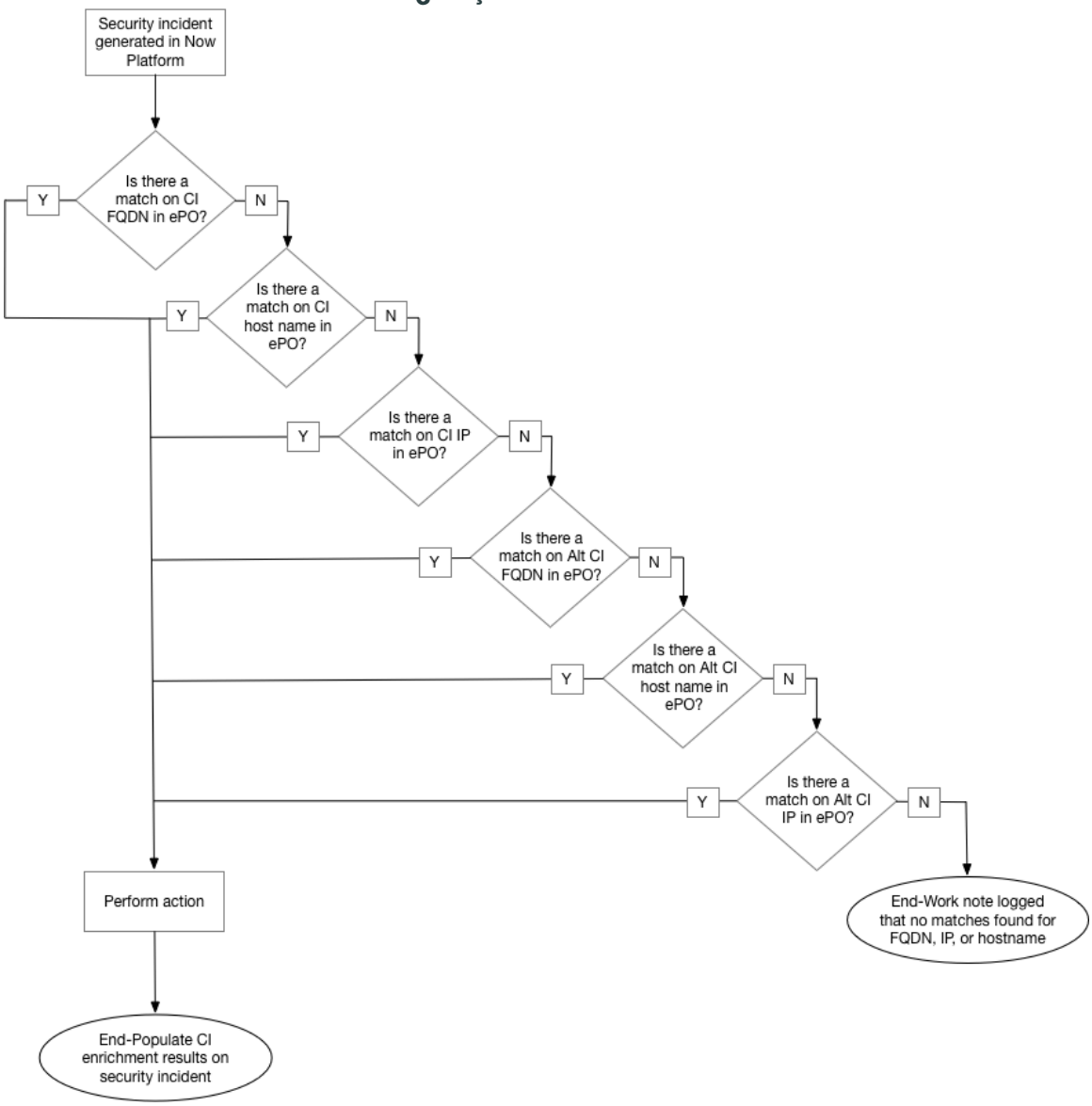


A figura a seguir ilustra como a primeira pesquisa do fluxo de trabalho verifica correspondências para itens de configuração. Se o campo gatilho de IC alternativo estiver habilitado, a segunda pesquisa verificará correspondências para valores alternativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de itens de configuração



Se IDs correspondentes não forem encontrados para o campo IC ou o campo IC alternativo, uma anotação de trabalho será registrada e uma mensagem será exibida no incidente de segurança. Quando nenhuma correspondência é encontrada, nenhum dado de aprimoramento é preenchido nos incidentes de segurança relacionados ao evento.

Você habilita o campo de gatilho de IC alternativo e seleciona o campo em que deseja exibir o ID correspondente durante a etapa de configuração de um perfil. Esta etapa para habilitar o campo de IC alternativo é descrita junto com os outros requisitos de configuração de perfil em Definir configurações.

Definir configurações

Depois de criar um perfil e selecionar McAfee ePO recursos que você deseja que o perfil execute, defina as configurações para que o perfil seja invocado somente sob as condições específicas que você definir.

Configurar um perfil

Nesta etapa, você configura um perfil de capacidade para que ele seja executado somente quando as condições especificadas forem atendidas. Você define quais condições em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

incidentes de segurança acionam automaticamente o. McAfee ePO recursos que você selecionou para o perfil. Você também tem a opção de selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que somente os incidentes de segurança relacionados ao seu evento de gatilho iniciem automaticamente o perfil. A etapa de configuração inclui as seguintes definições no formulário de configuração do perfil.

Campo de gatilho de item de configuração alternativo (IC)

Nos casos em que o campo Item de configuração (IC) no ServiceNow AI Platform® Resposta a incidentes de segurança(SIR) O incidente de segurança não está preenchido com um valor ou uma correspondência não pode ser encontrada no banco de dados, você pode selecionar um campo alternativo no incidente de segurança para exibir quaisquer dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos. Para obter mais informações sobre os campos Item de configuração e Item de configuração alternativo em um incidente de segurança, consulte Definir condições de acionamento com um campo Item de configuração (IC).

Marcadores de segurança

Para ajudar você a rastrear o status de máquinas host isoladas e quando as verificações de malware são iniciadas, um recurso de marcação opcional está disponível. Por padrão, esta opção está desabilitada no formulário de configuração para perfis. Se esta opção estiver habilitada durante a etapa de configuração, os nomes dos marcadores de segurança serão exibidos no formulário de configuração. Estes são os nomes dos marcadores exibidos em incidentes de segurança relacionados. Esses marcadores informam quando uma ação de isolamento de host é iniciada com sucesso e quando é aprovada. Depois que um host é retornado com sucesso para a rede, o marcador de segurança é removido automaticamente do incidente de segurança. Para verificações de malware, um marcador é exibido no incidente de segurança relacionado quando uma verificação é programada. Após a conclusão da verificação, o marcador programado é substituído automaticamente por um marcador que indica que a verificação foi concluída com sucesso.

Gatilho automático com base no incidente

Quando a opção Acionar automaticamente com base no incidente está habilitada, o construtor de condições de filtro está disponível e você precisa definir condições de filtragem que especificam quando o perfil é executado automaticamente. Um filtro comum é A categoria é uma atividade de código mal-intencionado ™e. O impacto nos negócios é 1 - Crítico ™. Com esses filtros, somente incidentes de segurança relacionados a código mal-intencionado e que têm um impacto crítico nos negócios iniciam o perfil. Usar a opção Acionamento automático pode reduzir o número de incidentes de segurança que invocam automaticamente o perfil.

Aprovações

Se sua organização quiser um nível extra de controle sobre ações como isolar máquinas host e iniciar verificações de malware, você poderá habilitar a opção Exigir aprovação durante a etapa de configuração de um perfil.

Por exemplo, se os recursos de aprovação e marcação estiverem habilitados para um perfil, depois que uma solicitação para isolar uma máquina host ou devolvê-la à rede for enviada para aprovação, o incidente de segurança associado será marcado automaticamente de que a ação foi iniciada. As solicitações são enviadas para aprovação a um usuário com a função sn_si.admin por padrão, mas essa aprovação pode ser reatribuída a outro indivíduo ou a um grupo de aprovação para atender às necessidades da sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

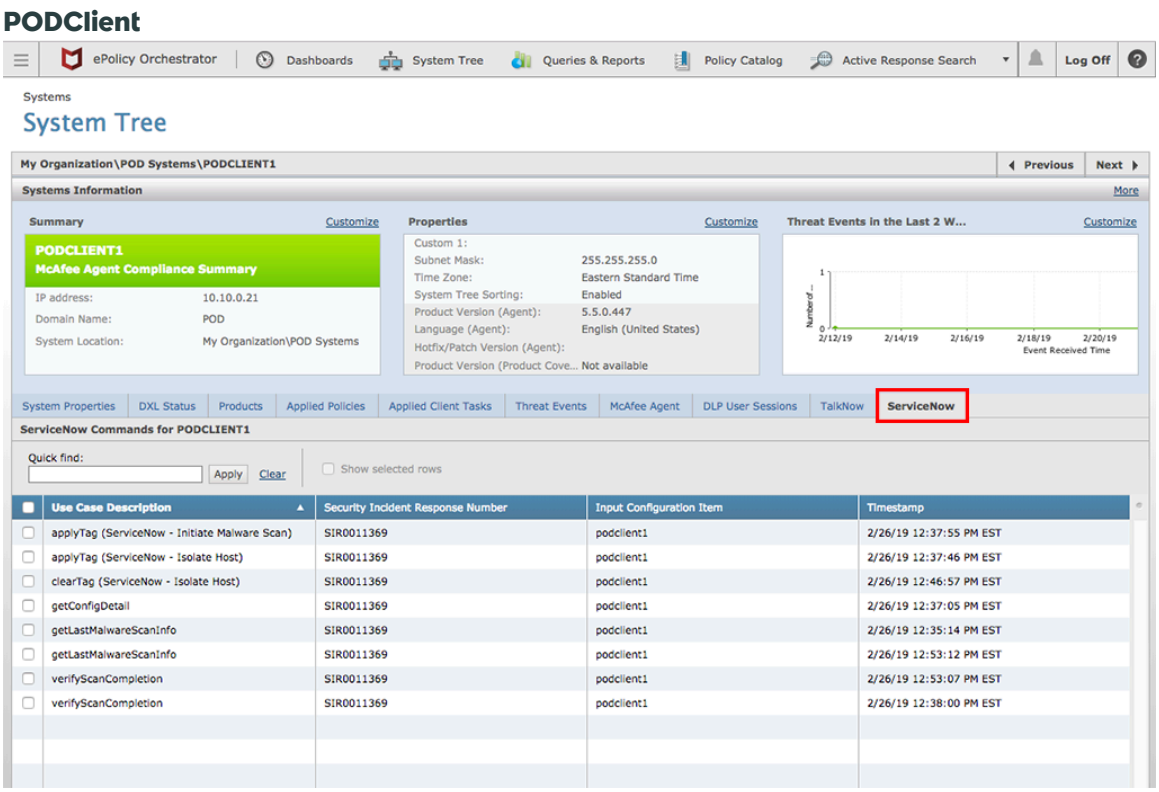
Solicitações de processamento de aprovadores em **Minhas aprovações** em ServiceNow AI Platform® instâncias. Marcadores de segurança são exibidos em incidentes de segurança relacionados. Todas as atividades de fluxo de trabalho também são registradas em anotações de trabalho para criar uma trilha de auditoria.

ServiceNow log de auditoria no McAfee ePO console

Na versão 5.10.0 de McAfee ePO. ServiceNowé exibida com um log de comandos que são iniciados a partir de ServiceNow AI Platform® instância. Depois que uma ação ou uma consulta é invocada a partir de um perfil em seu ServiceNow AI Platform® instância em uma máquina host (endpoint) no McAfee ePO console, um log de auditoria de ServiceNow os comandos são criados no McAfee ePO console. Este log é exibido na árvore do sistema em McAfee ePO e ajuda você a auditar os horários dos comandos enviados para endpoints específicos. Para exibir registrado ServiceNow eventos em máquinas específicas em um McAfee ePO console, siga estas etapas.

1. Navegue até a árvore do sistema em seu McAfee ePO e localize ServiceNow guia.
2. Clique na guia para abrir uma lista de máquinas host.
3. Na coluna Nome, clique em um nome de host para abrir o log de auditoria.

Na imagem a seguir, um exemplo de log para um host (PODCLIENT1) é exibido.



Os eventos iniciados a partir dos perfis em seu ServiceNow AI Platform® as instâncias são registradas e exibidas no log. Verificando o status da máquina host, verifique se os eventos listados no log foram concluídos com sucesso no host.

Perfis de exemplo

Os tópicos a seguir incluem exemplos de como configurar perfis e testar incidentes de segurança. Esses exemplos incluem perfis para todos os McAfee ePO recursos disponíveis para esta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure perfis e incidentes de segurança para consultas de aprimoramento do sistema

Defina suas configurações de perfil para que o perfil seja acionado somente sob as condições definidas por você.

Antes de Iniciar

Função necessária: ServiceNow AI Platform® administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente o. McAfee ePO recursos que você selecionou para o perfil. Você também pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC). Neste campo alternativo, você pode definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Procedimento

1. Se a página Configuração não for exibida, clique em **Configuração** na barra de andamento.
2. No formulário, preencha os campos

Opção	Descrição
Habilitar campo de gatilho de IC alternativo	Campo de gatilho de item de configuração alternativo (IC). O padrão é limpo. Quando esta caixa de seleção está desmarcada e a opção de campo de gatilho de IC alternativo está desabilitada, uma alternativa para o campo de IC não é identificada. Se desabilitado, um valor para o campo IC deve ser preenchido em um SIR incidente de segurança e o valor no campo devem ser reconhecidos pelo McAfee ePO console antes que o perfil colete dados de aprimoramento. Marque esta caixa de seleção se você acredita que o campo IC não será preenchido após a criação do incidente, mas as informações de IC serão preenchidas em outro campo no incidente de segurança. Quando esta opção está habilitada, a lista de seleção do campo do gatilho de IC alternativo é exibida. Escolha um campo alternativo na lista de seleção para verificar seus critérios de pesquisa de IC. Para obter mais informações sobre o campo do gatilho de IC alternativo, consulte Definir condições de acionamento com um campo Item de configuração (IC).
Marcadores de exibição	Marcadores de segurança são exibidos em incidentes de segurança. O padrão é limpo. Quando esta caixa de seleção está desmarcada e a opção de marcação está de-

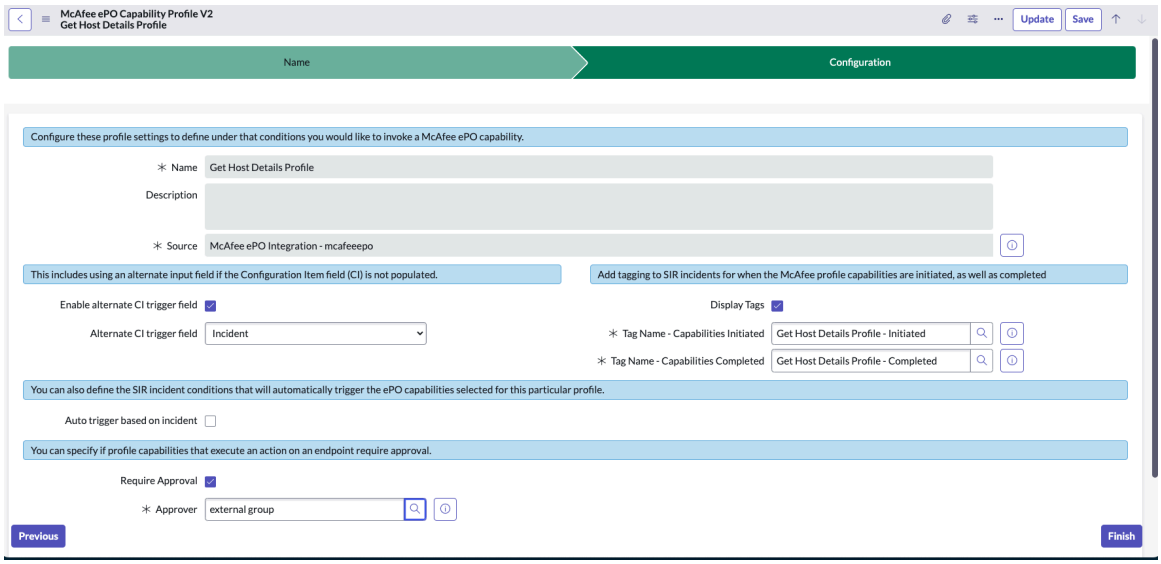
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	sabilitada, nenhum nome de marcador de segurança é exibido no formulário de configuração e os marcadores não são exibidos em incidentes de segurança relacionados. Para este exemplo, a opção de marcadores de segurança está desabilitada.
Gatilho automático com base no incidente	Condições de filtro. O padrão é limpo. Quando a caixa de seleção está desmarcada e a opção está desabilitada, o perfil deve ser invocado manualmente a partir de um incidente de segurança. Quando esta opção está habilitada, o Construtor de condição de filtro é exibido. Você deve definir as condições de filtragem para especificar quando o perfil será executado automaticamente após a criação do incidente. Um exemplo comum de um filtro para um perfil que executa consultas de aprimoramento é A categoria é uma atividade de código mal-intencionado e. O impacto nos negócios é 1-Crítico . Essas condições de filtro ajudam a localizar os incidentes relacionados a tipos específicos de eventos de segurança e ajudam a limitar o número de incidentes de segurança que você precisa revisar. Essas configurações de filtro permanecem salvas até que você as altere e elas ficam disponíveis para edição durante a etapa de visualização e teste do incidente da configuração.
Requer aprovação	Opção de aprovação da solicitação. O padrão é limpo. Esta opção de aprovação está disponível para qualquer perfil. Normalmente, as aprovações são usadas para recursos que invocam ações como isolamento de host e verificações de malware. Quando a caixa de seleção está desmarcada e esta opção está desabilitada, nenhuma solicitação de aprovação é enviada. Para este exemplo, nenhuma permissão prévia é necessária para consultas de aprimoramento do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para habilitar a opção de campo de IC alternativo e definir as condições de filtragem que invocam automaticamente este perfil, siga estas etapas.

a. Selecione **Habilitar campo de gatilho de IC alternativo** caixa de seleção.
O campo do gatilho de IC alternativo é exibido. Para este exemplo, como um usuário com a função sn_si.admin, você acredita que o campo IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no IC identificado No incidente de segurança e você seleciona o campo IC identificado como uma alternativa. O IC identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.

b. Em **Gatilho de IC alternativo** lista de seleção de campo exibida, selecione **IC identificado** campo.

Todos os campos disponíveis no incidente de segurança são exibidos na lista, incluindo todos os campos personalizados. No campo Gatilho de IC alternativo, IC identificado é exibido.

Quando este perfil é invocado e o campo IC não é preenchido no incidente de segurança associado no gatilho de evento inicial, o perfil usa alternativamente o valor do campo IC identificado na pesquisa.

c. Selecione **Gatilho automático com base no incidente** caixa de seleção.
O construtor de condições de filtro é exibido. Com esta opção, defina condições de filtragem e especifique quando o perfil será invocado automaticamente após a criação de um incidente de segurança.

d. Defina as condições de incidente SIR que acionarão automaticamente os recursos do ePO selecionados para este perfil específico.

e. Se os recursos de perfil que executam uma ação em um endpoint exigirem aprovação, selecione **Aprovação necessária** caixa de seleção.

f. Selecione uma aprovação usando o ícone de pesquisa.

4. Clique em **Concluir**.
Você configurou o perfil com sucesso para que ele seja acionado automaticamente após a criação do incidente e um campo alternativo é usado para preencher os resultados de IC correspondentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure um perfil para iniciar a verificação de malware

Depois de criar um perfil com o recurso Iniciar verificação de malware e qualquer outro McAfee ePO recursos que você deseja que o perfil execute, defina as configurações do perfil para que ele seja invocado sob as condições específicas que você definir.

Antes de Iniciar

Função necessária: sn_si.admin

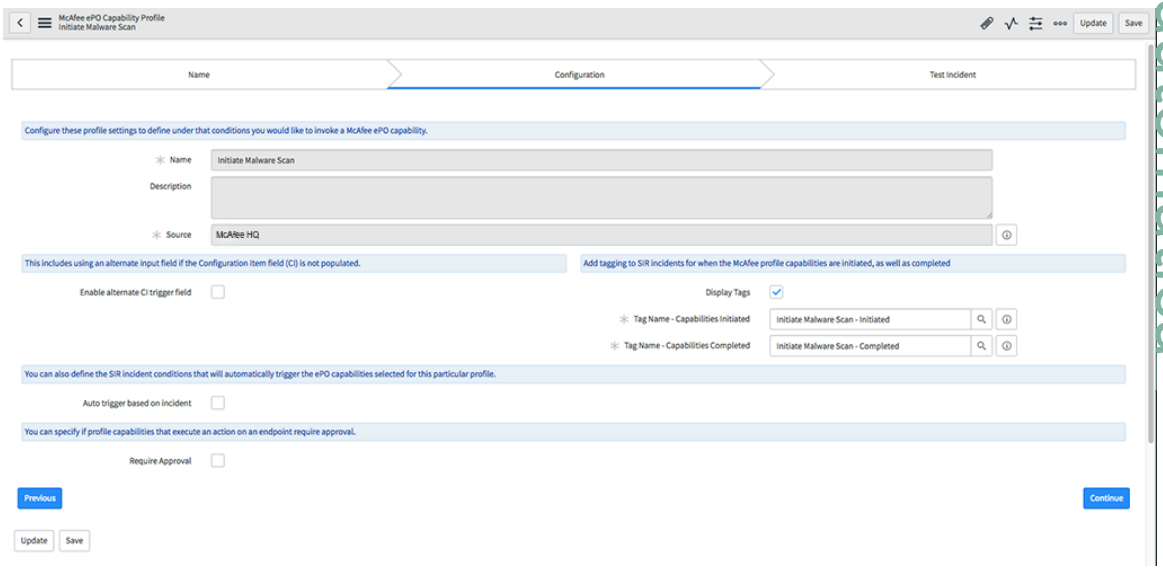
Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, configure o perfil para que ele programe uma verificação somente quando as condições especificadas forem atendidas em ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança. Você define quais condições em incidentes de segurança acionam a verificação. Qualquer outro McAfee ePO as capacidades selecionadas para o perfil compartilham as condições de acionamento. As opções para selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem estão disponíveis. Você pode preferir definir a filtragem para que somente esses SIR os incidentes de segurança relacionados ao seu evento de gatilho invocam automaticamente o perfil.

Da mesma forma que ocorre com a ação Isolar host, você pode iniciar uma verificação sob demanda diretamente de um SIR incidente de segurança. Para obter mais informações sobre como iniciar uma verificação manualmente, consulte Gatilho McAfee ePO perfil manualmente a partir de um incidente de segurança.

Procedimento

1. Se a página Configuração não for exibida, clique em **Configuração** na barra de andamento.



O formulário Configuração é exibido.

2. Preencha o formulário.

Opção	Descrição
Habilitar campo de gatilho de IC alternativo	Campo de gatilho de item de configuração alternativo (IC). O padrão é desabilitado. Para este exemplo, a caixa de seleção está desmarcada. Quando esta caixa de seleção está desmarcada e a opção de campo de gatilho de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	IC alternativo está desabilitada, uma alternativa para o campo de IC não é identificada. Se desabilitado, um valor para o campo IC deve ser preenchido em um SIR incidente de segurança e o valor no campo devem ser reconhecidos pelo McAfee ePO console antes da execução do perfil. Quando esta caixa de seleção é marcada e esta opção está habilitada, a lista de seleção do campo do gatilho de IC alternativo é exibida. Escolha qualquer campo desta lista como um campo alternativo para o IC. Para obter mais informações sobre o campo do gatilho de IC alternativo, consulte Definir condições de acionamento com um campo Item de configuração (IC) e. Crie um perfil de capacidade.
Marcadores de exibição	Marcadores de segurança em incidentes de segurança. O padrão é desabilitado. Quando esta caixa de seleção está desmarcada e a opção de marcação está desabilitada, nenhum nome de marcador de segurança é exibido no incidente de segurança. Deixe esta caixa de seleção desmarcada se você não quiser que marcadores de segurança sejam exibidos em incidentes de segurança relacionados. Quando a caixa de seleção é marcada e a opção de marcação está habilitada, os nomes dos marcadores de segurança são exibidos no formulário de configuração. Estes são os nomes dos marcadores exibidos em incidentes de segurança relacionados. Verificações de malware podem ser programadas fora do horário comercial e levar tempo para serem concluídas. Na parte superior do incidente de segurança, quando a marcação está habilitada, um marcador de segurança é exibido indicando que a verificação está programada. Depois que a verificação é concluída com sucesso, o marcador programado é substituído automaticamente por um marcador que indica que a verificação foi concluída com sucesso. Nomes e cores de marcador podem ser editados. Para obter mais informações,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	consulte Edite marcadores de segurança no ServiceNow AI Platform para McAfee ePO integração.
Gatilho automático com base no incidente	Condições de filtro. O padrão é desabilitado. Quando a caixa de seleção está desmarcada e a opção está desabilitada, o perfil não inicia automaticamente uma verificação de malware. O perfil deve ser iniciado manualmente a partir de um incidente de segurança. Quando a caixa de seleção está marcada e a opção de gatilho automático está habilitada, o Construtor de condição de filtro é exibido no formulário. Você deve definir as condições de filtragem para especificar quando o perfil será executado automaticamente após a criação do incidente. Para este exemplo, filtra para A categoria é uma atividade de código mal-intencionado e. O impacto nos negócios é 1 - Crítico são usados. Para obter mais informações sobre o construtor de condições de filtro, consulte Crie um perfil de capacidade.
Requer Aprovação	Requer aprovação antes de iniciar a verificação. O padrão é desabilitado. Quando a caixa de seleção está desmarcada e a opção Aprovação está desabilitada, um usuário com a função sn_si.analyst inicia uma verificação de malware sem solicitar aprovação prévia. Marque esta caixa de seleção e habilite esta opção se quiser que um usuário com a função sn_si.analyst solicite aprovação antes de iniciar uma verificação de malware.

Para este exemplo, as opções de aprovação e marcação estão habilitadas para o perfil. Para obter mais informações sobre como configurar o. Habilitar campo de gatilho de IC alternativo e o. Gatilho automático com base no incidente opções, consulte Configure perfis e incidentes de segurança para consultas de aprimoramento do sistema.

3. Escolha uma opção para continuar.

Opção	Descrição
Anterior	Retorne à etapa Nome se quiser editar o perfil.
Salvar	Salve suas mudanças e permaneça nesta página. Para salvar suas mudanças, na faixa cinza na parte superior da tela, clique com o botão direito do mouse. No menu exibido, clique em **Salvar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Continue ou selecione Testar incidente na barra de andamento	Prossiga para a etapa Testar incidente e visualização. Se você sair da página sem salvar suas mudanças antes, suas edições não serão salvas.
Excluir	Exclua este perfil do McAfee ePO Lista de perfis de capacidade.

Você configurou o perfil com sucesso para que uma verificação de malware seja acionada automaticamente após a criação do incidente. Um campo de IC alternativo é usado para preencher os resultados de IC correspondentes da verificação. A próxima etapa é visualizar e testar incidentes de segurança para este perfil.

Gatilho McAfee ePO perfil manualmente a partir de um incidente de segurança

Acionar um perfil de capacidade manualmente a partir de um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Nota: A opção de aprovações no Definir configurações Aparece somente para os recursos Isolar host e Remover isolamento de host.

Por Que e Quando Desempenhar Esta Tarefa

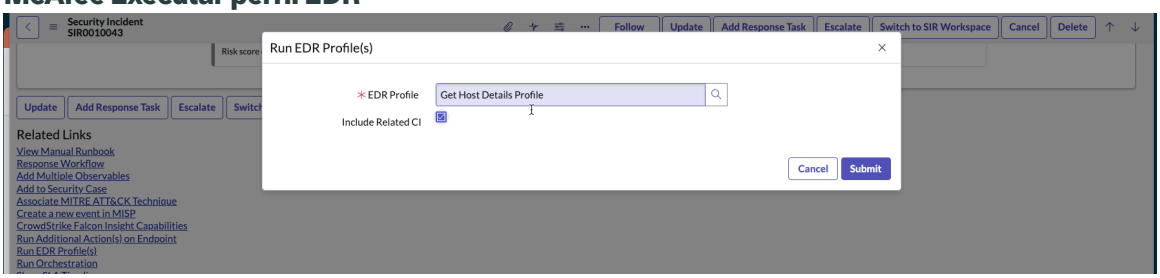
Você pode invocar uma solicitação para Obter detalhes do host, Isolar máquina host ou Remover isolamento de uma máquina automaticamente se as condições de acionamento especificadas no perfil corresponderem às condições em incidentes de segurança. Se você quiser enviar uma solicitação manualmente, envie a solicitação diretamente de um incidente de segurança.

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta no ServiceNow AI Platform incidentes de segurança. McAfee ePO As integrações também permitem que você execute recursos individuais em Itens de configuração (ICs) sem usar um perfil.

Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com McAfee ePO informações.
3. Na seção Listas relacionadas, selecione **Executar perfil(s) EDR** .

McAfee Executar perfil EDR



4. Procure e selecione um perfil na lista de perfis disponíveis.
   A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina do host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.
5. Selecione **Incluir IC relacionado** Para executar este perfil em todos os ICs relacionados do perfil.

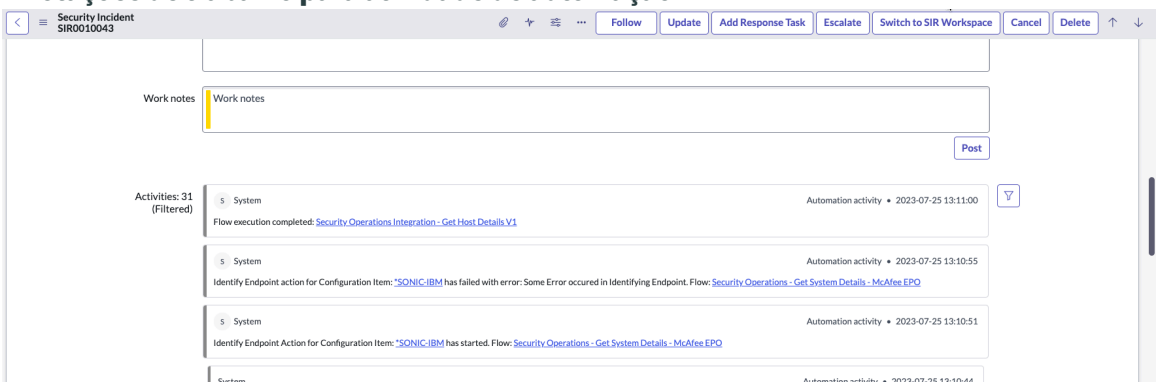
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.

6. Clique em **Enviar**.
   O perfil selecionado é acionado manualmente. Você pode revisar a seção Anotações de trabalho e atividades e os marcadores de perfil iniciado e perfil concluído na seção Anotações de trabalho.

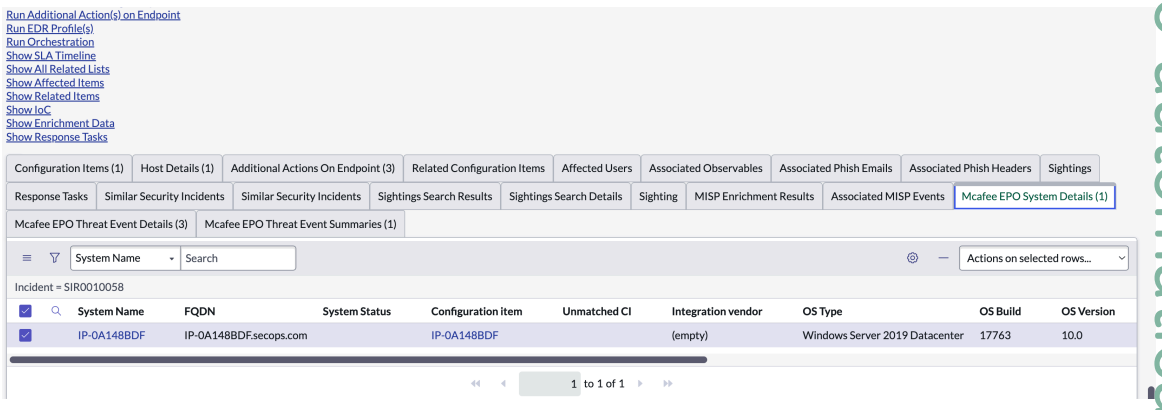
Anotações de trabalho para atividade de automação



Os resultados aparecem na forma de listas relacionadas, como Obter detalhes do host, Isolar máquina host ou Remover isolamento.

Nota: Todas as tabelas de lista relacionada estendem as tabelas base. Neste exemplo, Detalhes do sistema McAfee epo é uma tabela estendida da tabela base Detalhes do host.

Listas relacionadas da McAfee



7. Para executar capacidades individuais em um Item de configuração (IC), execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique em **Ações nas linhas selecionadas...** E selecione a capacidade necessária que você deseja executar para o IC selecionado.
   Por exemplo, Isolar host.

   c. Clique em **Isolar host** Para executá-lo no IC selecionado.
   O IC selecionado é isolado da rede.

Acionar ações adicionais em McAfee ePO integração

Os recursos Listar eventos de ameaça e Iniciar verificação de malware podem ser acionados em Executar ações adicionais.

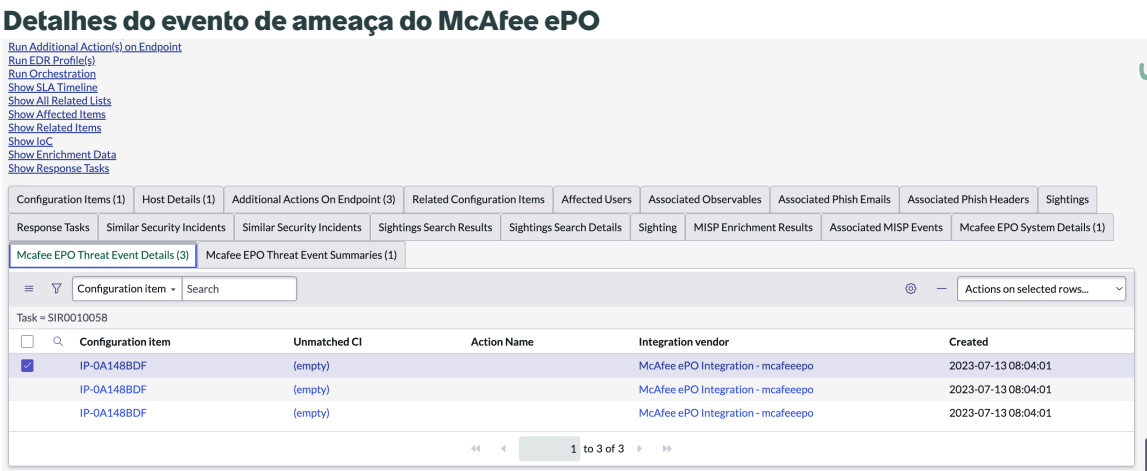
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode configurar e acionar ações adicionais no McAfee ePO a integração permite usando **Executar ações adicionais no endpoint** , que incluem McAfee ePO Listar eventos de ameaça e. McAfee ePO Iniciar recursos de verificação de malware.

Procedimento
1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar as ações adicionais.
3. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint** .
4. Procure e selecione a implementação de capacidade que você deseja acionar na lista de ações adicionais. Por exemplo, McAfee ePO Listar eventos de ameaça.
5. Selecione **Incluir IC relacionado** Para executar esta ação adicional em todos os ICs relacionados do perfil. Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique em **Executar ações adicionais** .



Nota: Todas as tabelas de lista relacionada estendem as tabelas base. Neste exemplo, a tabela Detalhes do evento de ameaça do McAfee ePO é uma tabela estendida da tabela base Ações adicionais no endpoint.

7. Exiba e valide os Detalhes do evento de ameaça do McAfee ePO nas listas relacionadas.

Usando McAfee ePO Integração no Espaço do analista

Use McAfee ePO integração para aproveitar o. McAfee ePO Recursos no Espaço do analista SIR.

Antes de Iniciar
Função necessária: sn_si.admin

Antes de usar McAfee ePO Integração No espaço Resposta de incidentes de segurança, você deve baixá-lo do ServiceNow Store e configure-o. Para obter mais informações, consulte Configure seu ServiceNow AI Platform instância do McAfee ePO integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

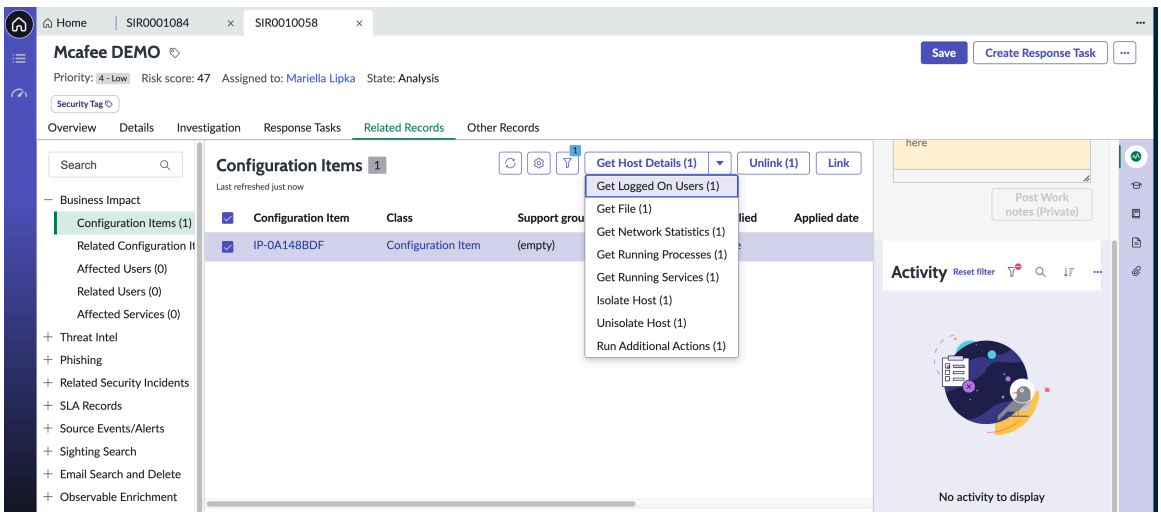
Você pode usar McAfee ePO integração para fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o. Resposta a incidentes de segurança espaço.

. McAfee ePO a integração permite que os analistas usem o seguinte McAfee ePO recursos no Resposta a incidentes de segurança Espaço do analista:

- **Obter detalhes do host**
- **Isolar Host**
- **Remover isolamento**
- **Executar ações adicionais no endpoint**

Procedimento

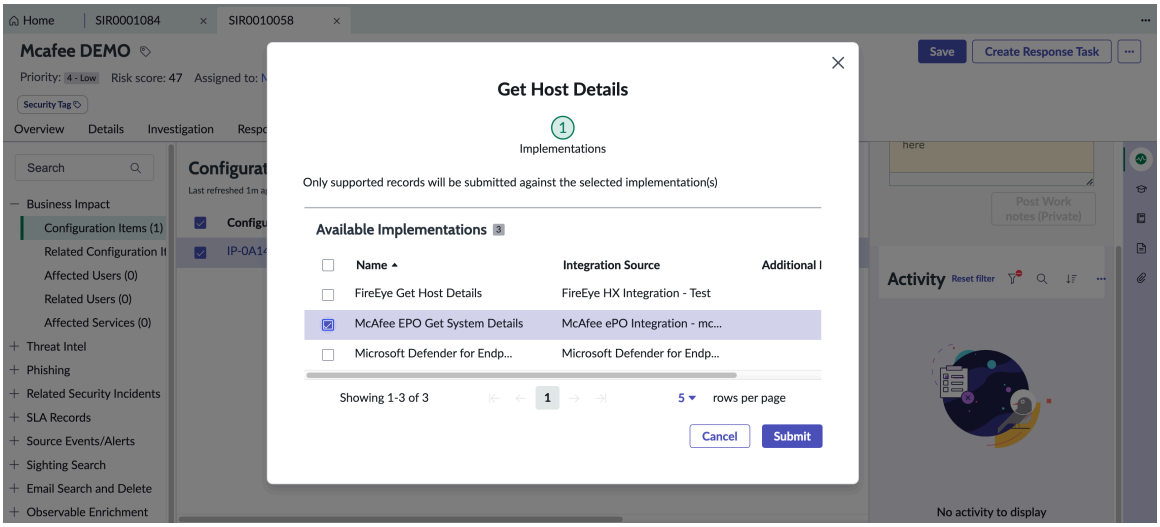
1. Para abrir o incidente de segurança no espaço SIR, clique em **Alterne para o Espaço SIR** no incidente de segurança.
2. No espaço SIR, selecione **Registros relacionados** guia.
3. Selecione Qualquer **Item de configuração** E escolha um recurso do McAfee ePO para acionar na ação suspensa da lista relacionada.
   Por exemplo, Obter detalhes do host.



4. No pop-up Obter detalhes do host, selecione **McAfee ePO** implementação.

Tradução automática

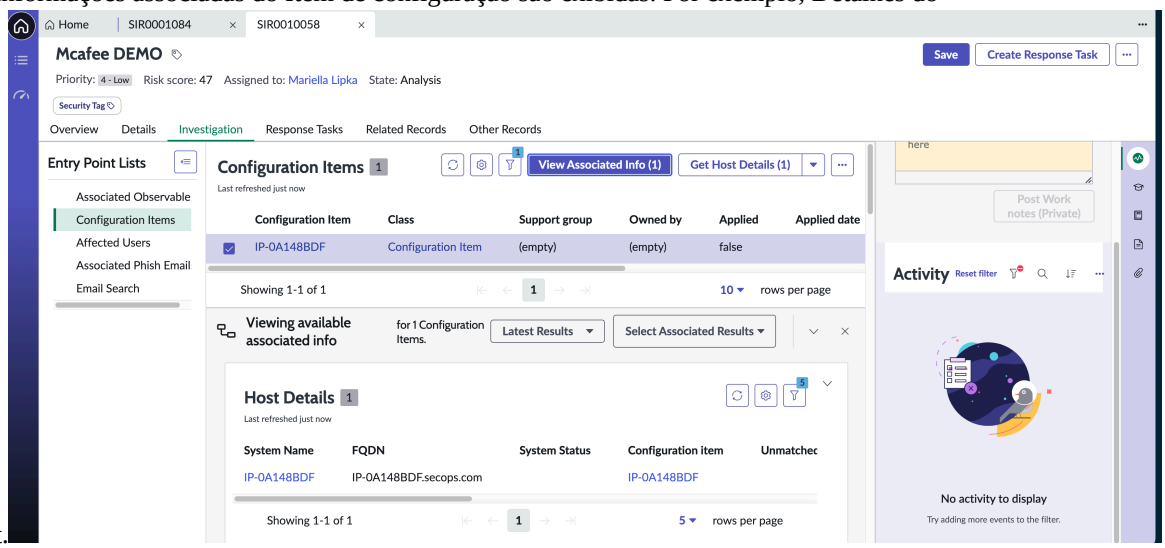
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   O recurso Obter detalhes do host é invocado no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.

6. Para exibir os dados da capacidade acionada, selecione **Investigação** guia.

7. Selecione **Item de configuração** e clique em **Exibir informações associadas** ação.
   As informações associadas do Item de configuração são exibidas. Por exemplo, Detalhes do host.



8. Clique em **Item de configuração** para exibir os detalhes do host.
   Da mesma forma, você pode tentar usar o outro recurso do McAfee ePO para incidentes de segurança no SIR Analyst Workspace.

9. Você pode usar os recursos do McAfee ePO no **Detecção e resposta de endpoint (EDR)** lista relacionada para análise.

10. Procure e selecione um perfil na lista de perfis disponíveis.
    A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina do host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.

11. Selecione **McAfee ePO** implementação e clique em **Enviar** .

Teste incidentes de segurança para iniciar a verificação de malware

Depois de configurar um perfil para a verificação de malware, teste o perfil e exiba os incidentes de segurança que correspondem às configurações do seu perfil. Visualize os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

resultados da verificação nas listas relacionadas de um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Antes de Iniciar

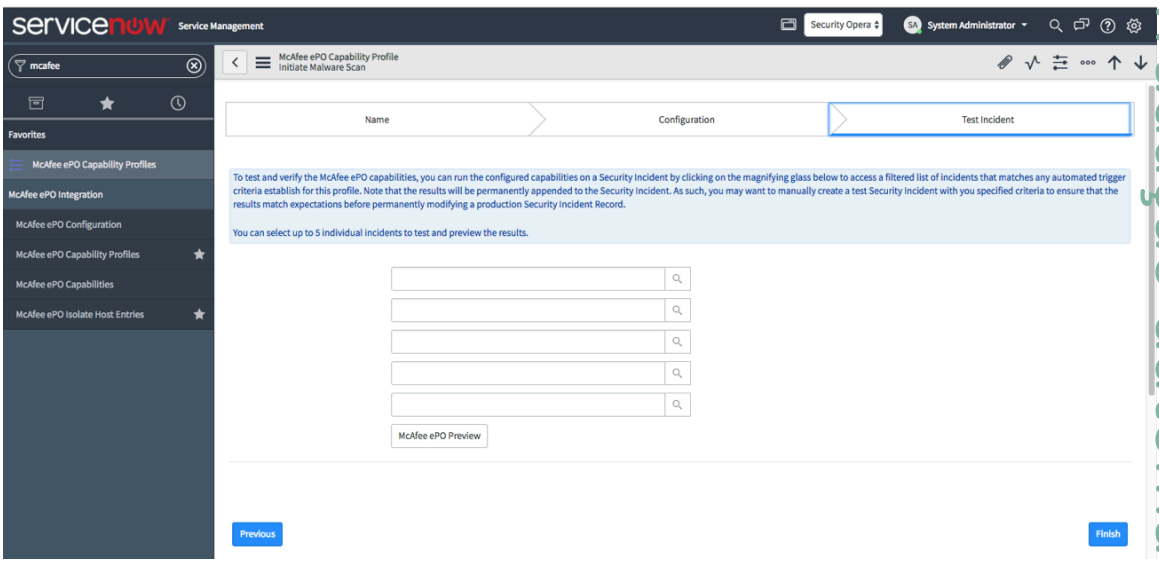
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

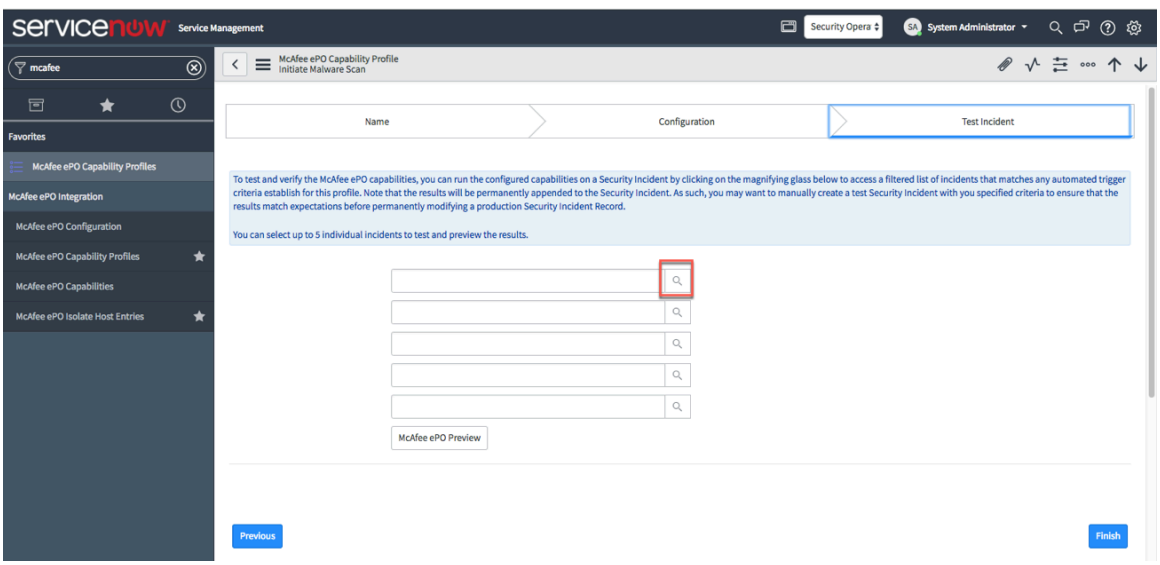
Como um usuário com a função sn_si.admin, verifique se o perfil com o recurso de verificação de malware foi invocado e se os resultados da pesquisa de verificação correspondem ao esperado com uma visualização das listas relacionadas em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança. A visualização permite validar se os resultados da verificação são retornados conforme o esperado para o perfil.

Procedimento

1. Se a página Testar incidente não for exibida, clique em **Incidente de teste** na barra de andamento.
   A página Testar incidente é exibida para o seu perfil. Para este exemplo, o perfil Iniciar verificação de malware que você criou e configurou nas seções anteriores é exibido.



2. À direita do campo superior, clique no ícone de pesquisa para selecionar um incidente de segurança a ser exibido na visualização.

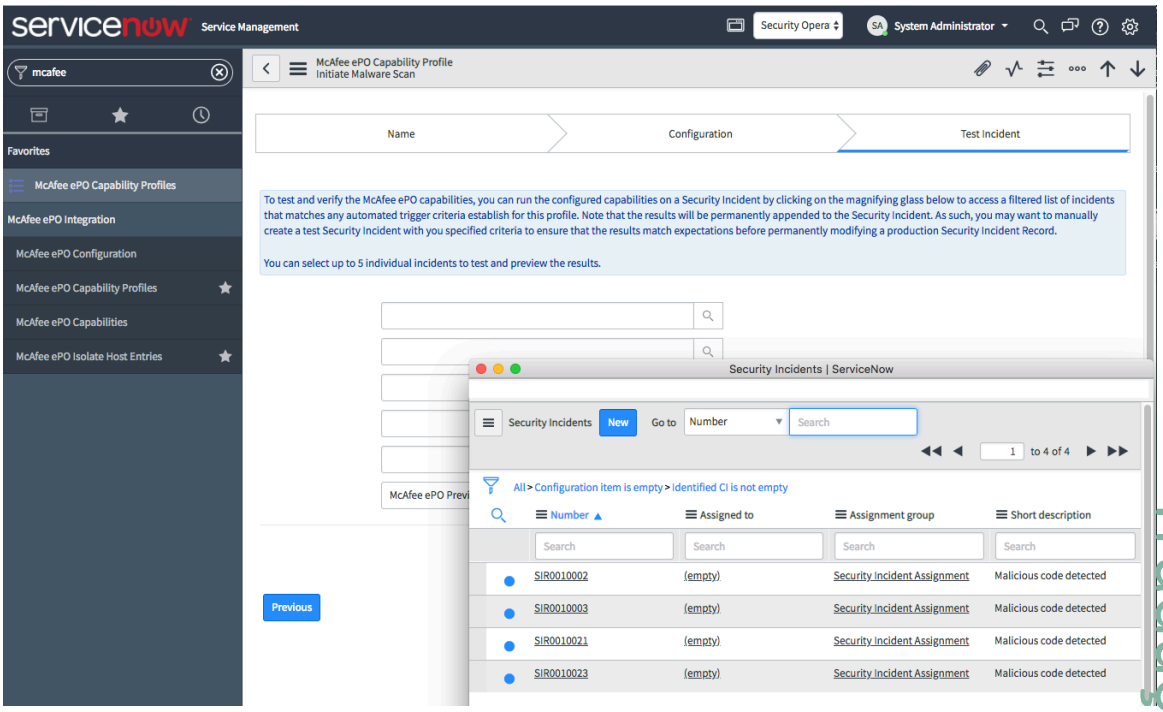


Tradução automática

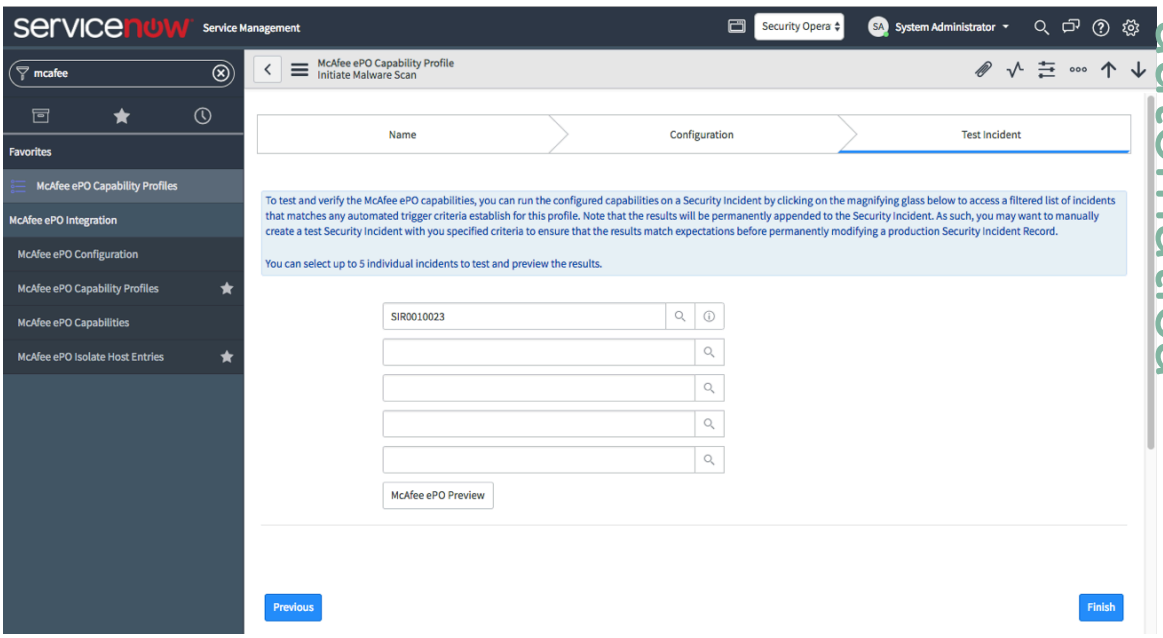
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Somente incidentes de segurança que correspondem aos critérios de perfil são exibidos.

3. Na coluna Número da lista exibida, selecione um item que você deseja exibir na visualização.



O número do incidente de segurança é exibido no campo.

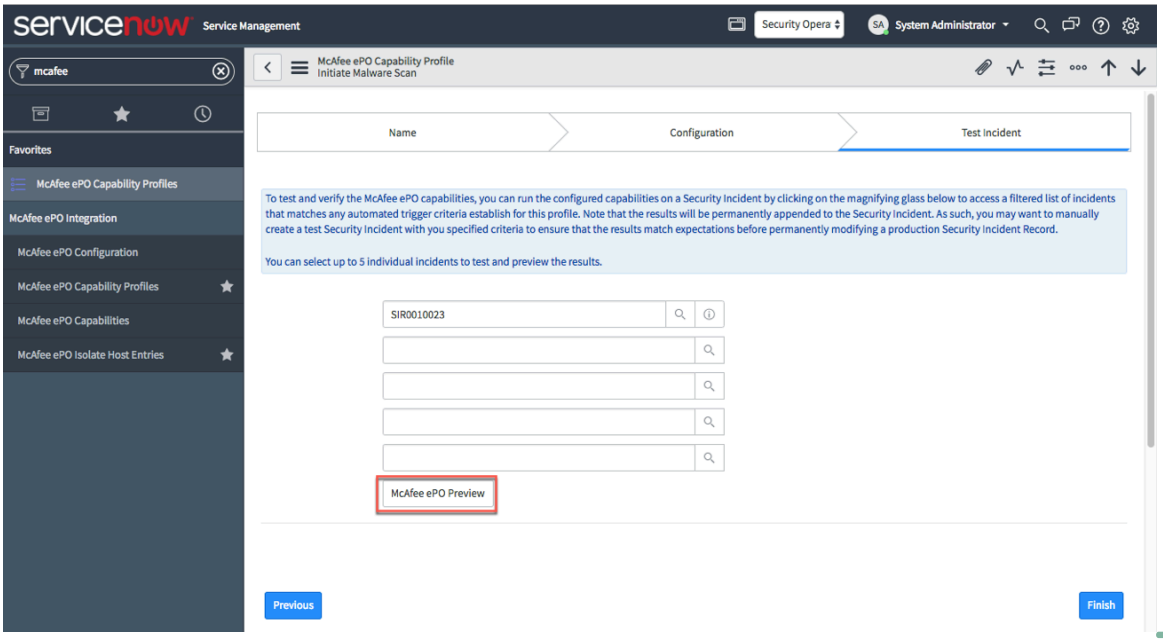


4. Repita as etapas 2 e 3 até que todos os incidentes que você deseja visualizar sejam exibidos nos campos. Selecione até cinco incidentes de segurança para a visualização.

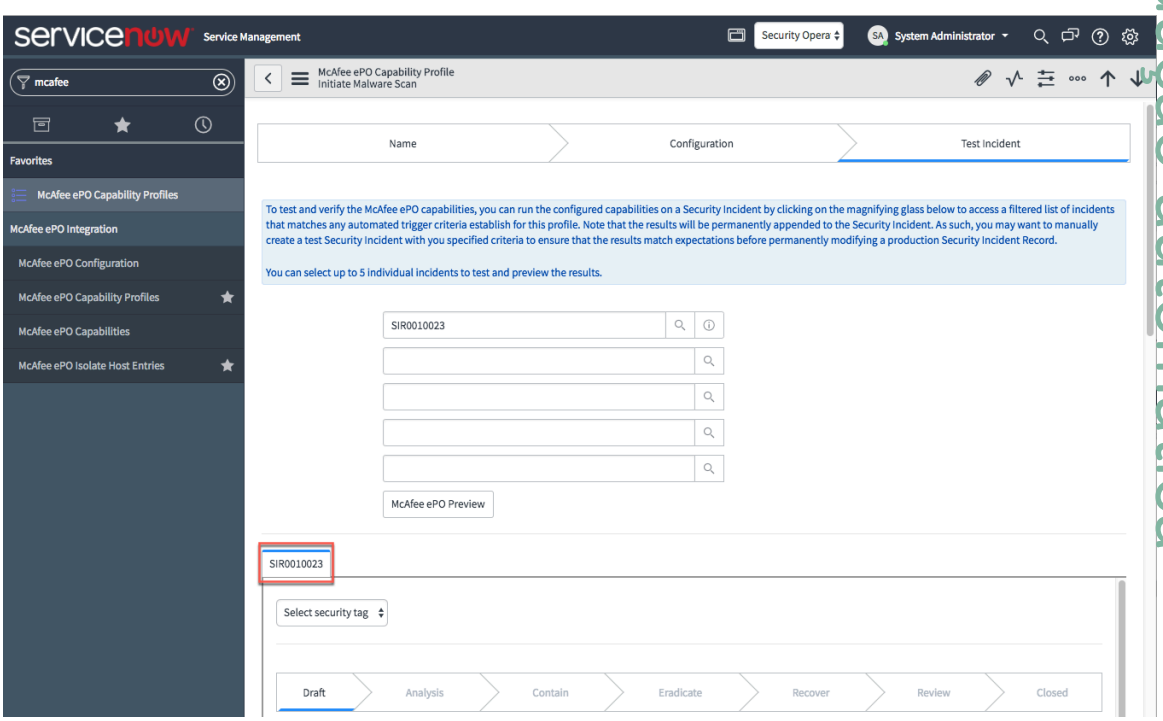
5. Clique em **Visualização do McAfee ePO** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os incidentes de segurança que correspondem às condições de evento do seu perfil são exibidos. Depois que a página for carregada, na parte inferior da página, serão exibidas guias para cada incidente de segurança.

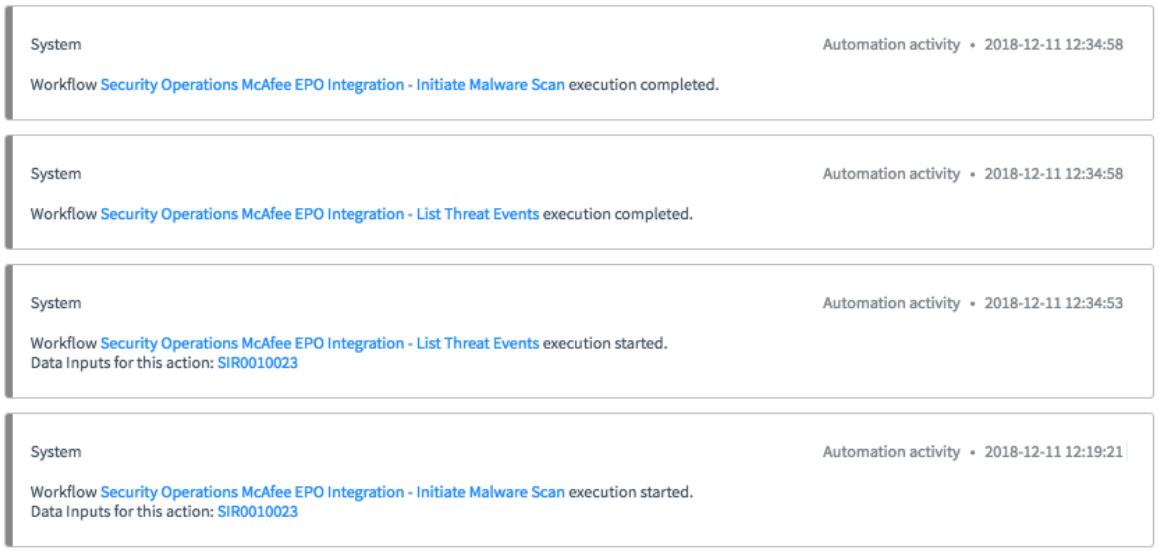


6. Role para exibir as anotações de trabalho.

Nota: O fluxo de trabalho de eventos de ameaça da lista faz parte da verificação. Para obter mais informações sobre como criar um perfil com o recurso de verificação de malware, consulte Crie um perfil de capacidade.

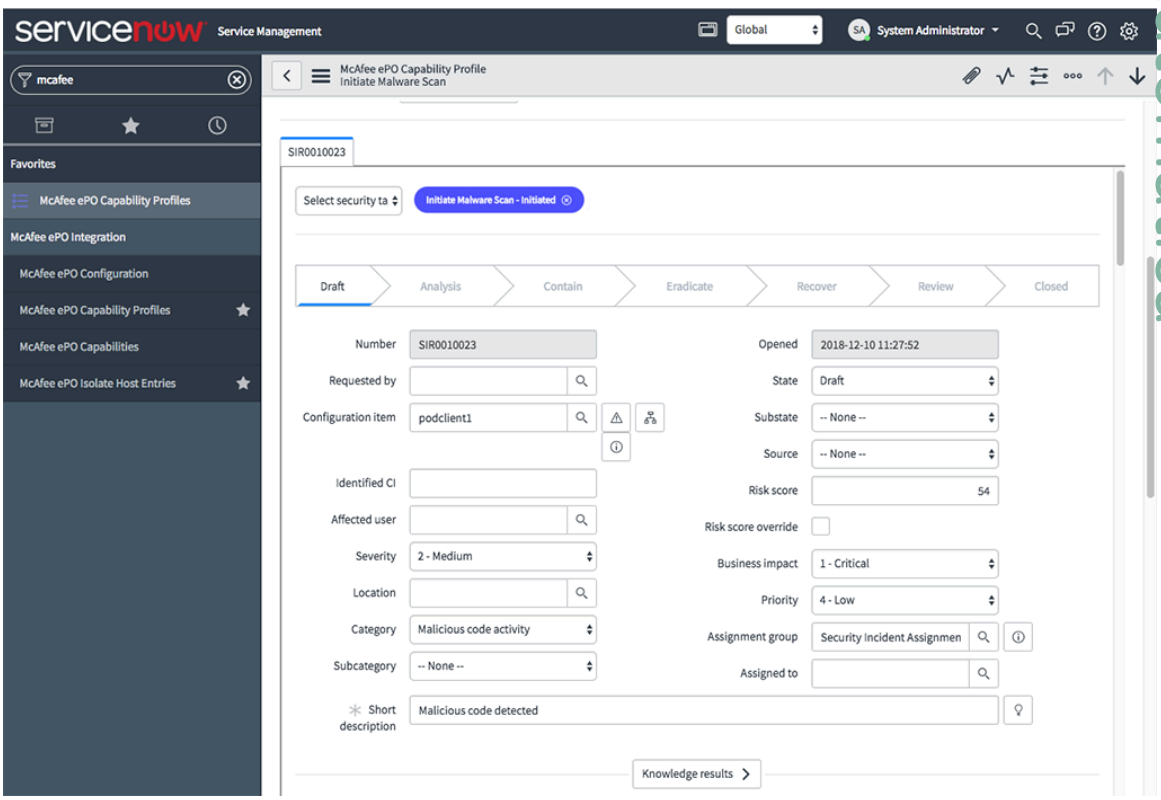
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Às vezes, as verificações são programadas para serem executadas após o horário de trabalho de pico para minimizar o impacto para os usuários na rede. A verificação pode não ser concluída imediatamente. Nesse caso, na parte superior do incidente de segurança, um marcador de segurança é exibido indicando que a verificação está programada. Consulte as anotações de trabalho para obter o status no fluxo de trabalho. A lista de anotações de trabalho quando os fluxos de trabalho são iniciados e concluídos com sucesso. Para este exemplo, as anotações de trabalho na figura a seguir mostram que a verificação foi iniciada e concluída com sucesso. O recurso Listar eventos de ameaça também foi iniciado e concluído com sucesso como parte da verificação.

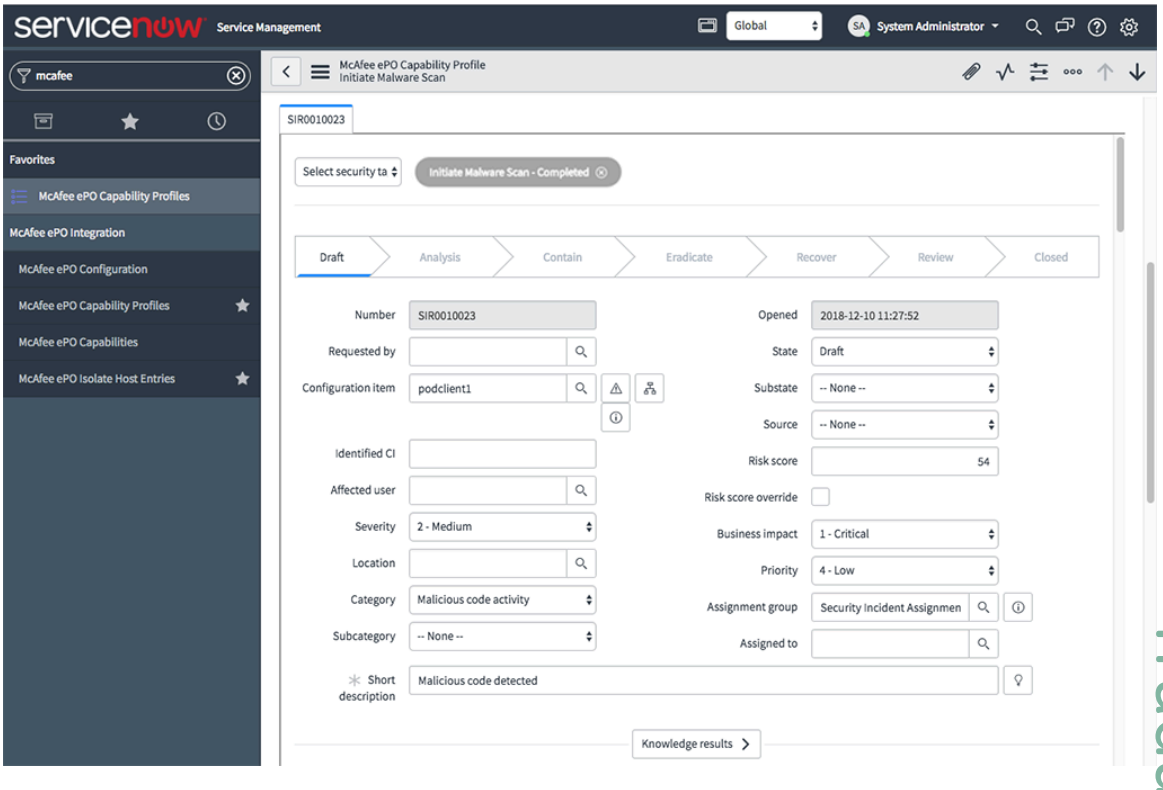
A figura a seguir mostra um exemplo de um marcador de segurança no incidente de segurança relacionado.



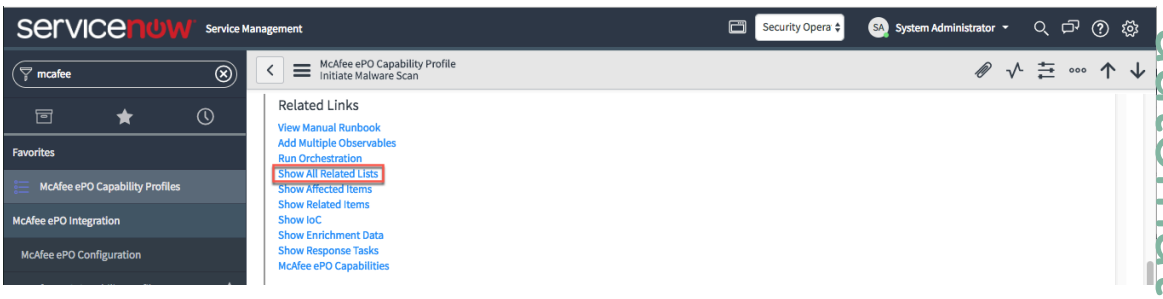
No incidente de segurança, depois que a verificação é concluída com sucesso, o marcador programado é substituído automaticamente pelo marcador Concluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

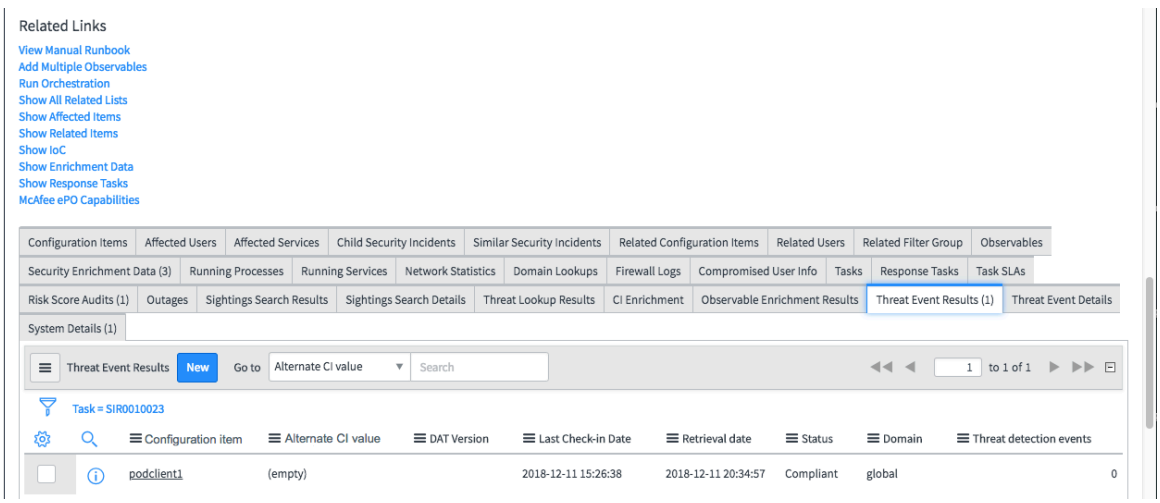


7. Depois de verificar se a verificação foi concluída com sucesso, no incidente de segurança, role para exibir os links relacionados e clique em **Mostrar todas as listas relacionadas** .



Os resultados do evento de ameaça e a lista Detalhes do evento de ameaça são exibidos como guias.

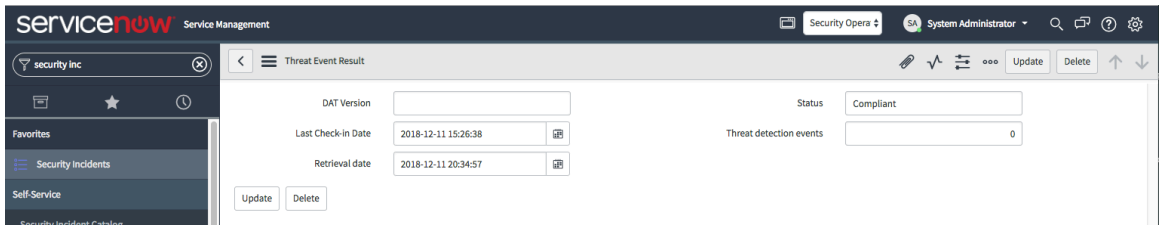
8. Se a lista Detalhes do evento de ameaça não estiver selecionada, selecione-a para exibir os resultados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Clique em um item na coluna Origem para abrir um registro e exibir os dados de aprimoramento.



Os dados de aprimoramento incluem as seguintes informações.

- O valor do campo de IC que foi correspondido durante a verificação.
- Data do último check-in com fuso horário. Esses dados se referem a quando, no horário local, os dados mais atuais foram extraídos do McAfee ePO console.
- Dados brutos

Você verificou com sucesso se o fluxo de trabalho de verificação foi concluído com sucesso para incidentes de segurança que corresponderam aos critérios de gatilho automático definidos para este perfil.

10. Escolha um para continuar.

Opção	Descrição
Anterior	Retorne à etapa Configuração do perfil. Se você não estiver satisfeito com os resultados de teste e visualização, continue definindo as configurações de perfil.
Encerrar	Conclua a configuração. Você será solicitado a confirmar a ativação.

Testar incidentes de segurança e aprovar solicitações para o host isolado

A etapa de teste e visualização permite validar se os resultados do fluxo de trabalho de isolamento de host e remover isolamento de host são retornados conforme esperado para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Durante esta etapa da configuração, como um usuário com a função sn_si.admin, verifique se o perfil configurado com o recurso Isolar host retorna incidentes de segurança e IDs de ativos correspondentes conforme o esperado. Exibir o real ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança criados quando ocorrem condições de evento de segurança que correspondem às configurações do seu perfil.

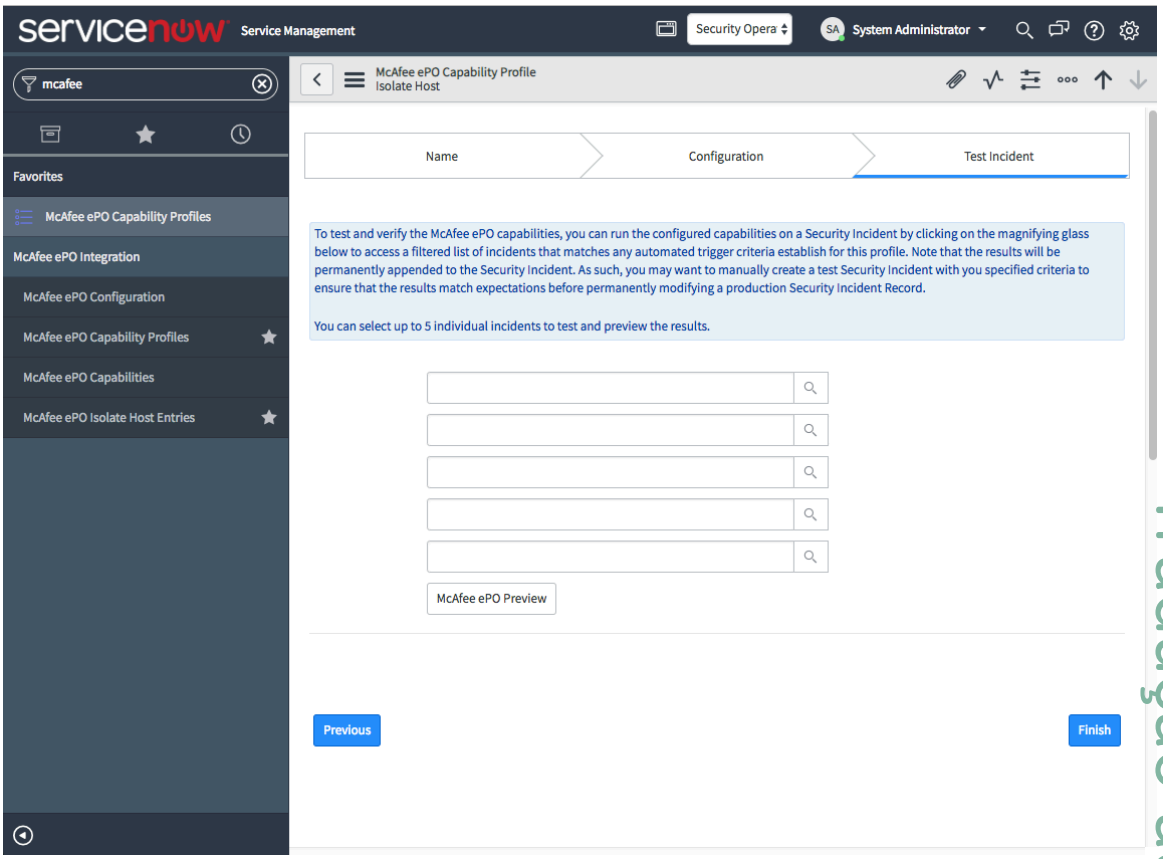
Depois que uma solicitação para isolar uma máquina host é enviada, como um usuário com uma função de aprovador, processe a solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a página Testar incidente não for exibida, clique em **Incidente de teste** na barra de andamento.

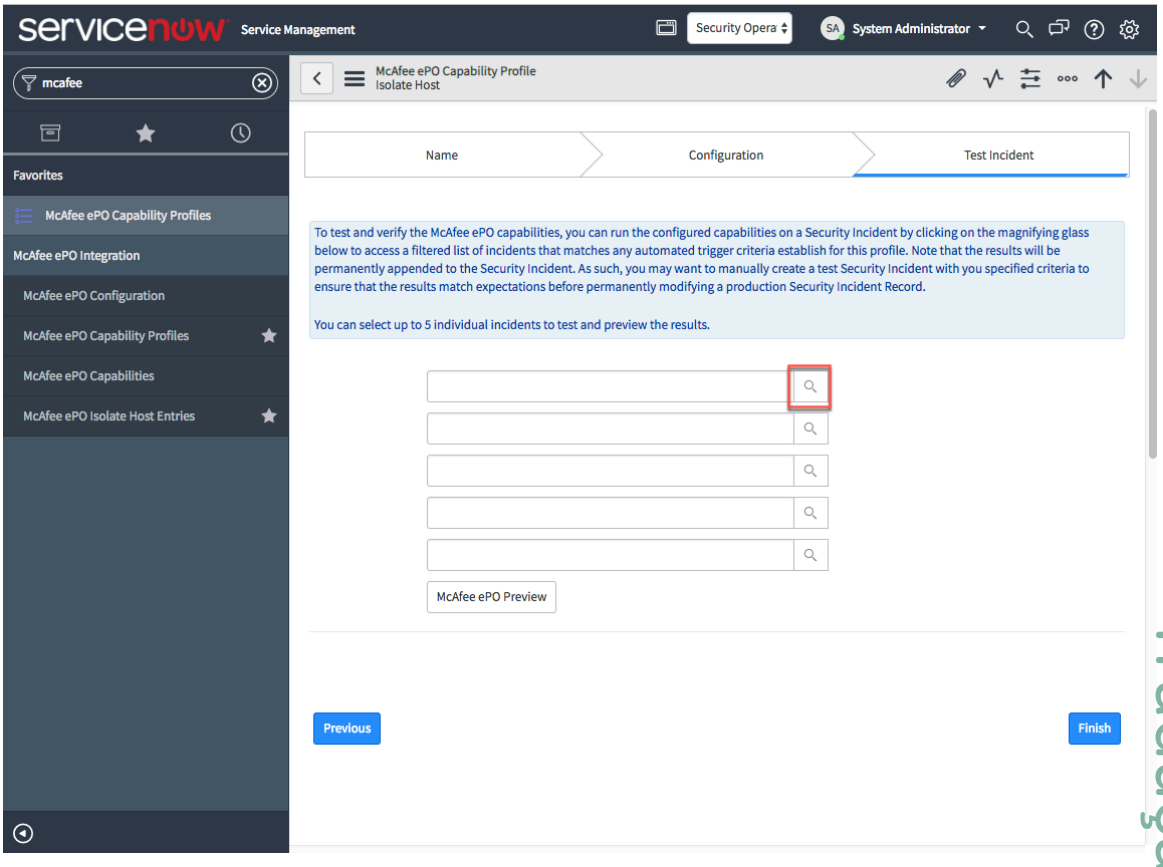


A página Testar incidente é exibida para o seu perfil. Para este exemplo, Isolar host ™o perfil que você criou e configurou nas seções anteriores é exibido.

2. À direita do campo superior, clique no ícone de pesquisa para selecionar um incidente de segurança para visualizar.

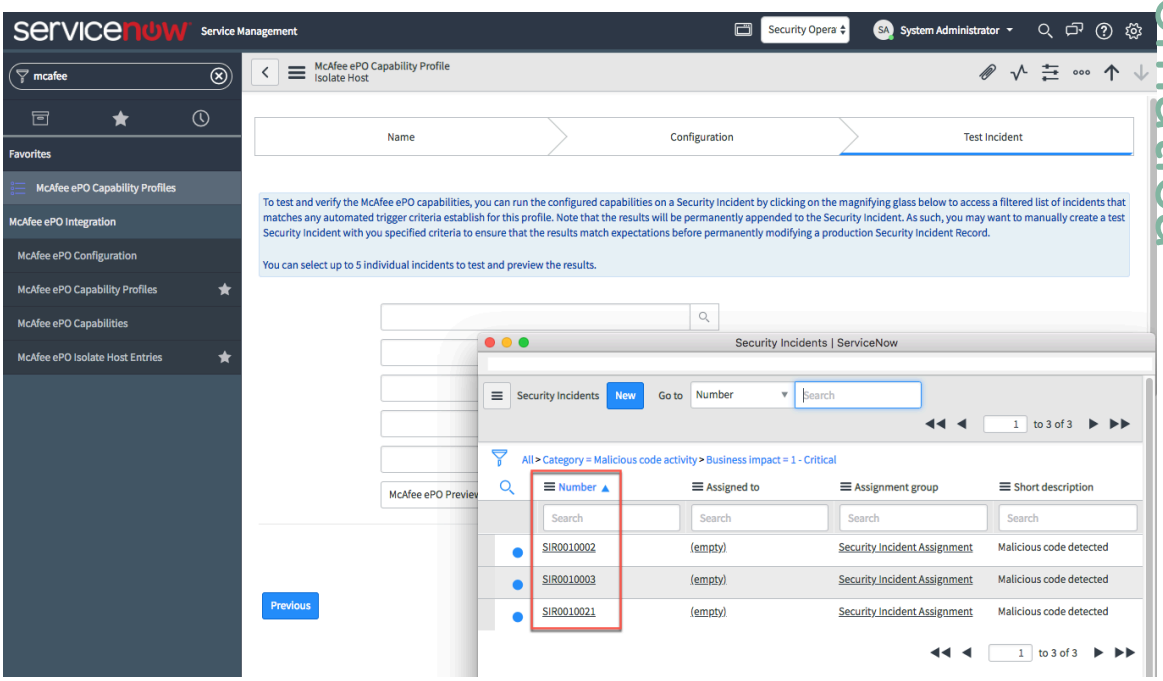
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na coluna Número da lista exibida, selecione um item que você deseja exibir na visualização.

Somente incidentes de segurança que correspondem aos critérios definidos para o perfil são exibidos.



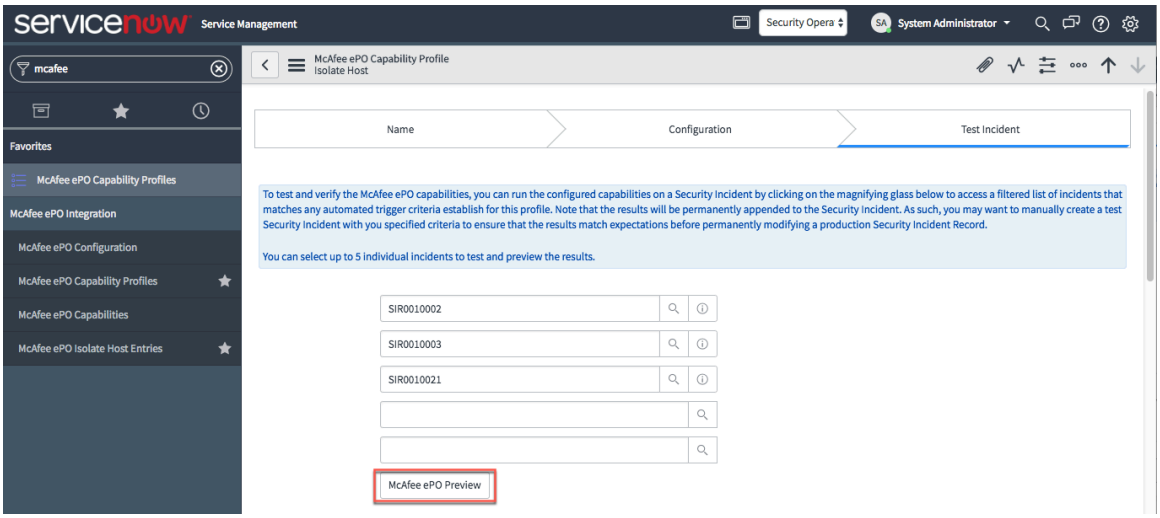
Os incidentes de segurança são exibidos na página .

4. Repita as etapas 2 e 3 até que todos os incidentes que você deseja visualizar sejam exibidos nos campos. Selecione até cinco incidentes de segurança para a visualização.

Tradução automática

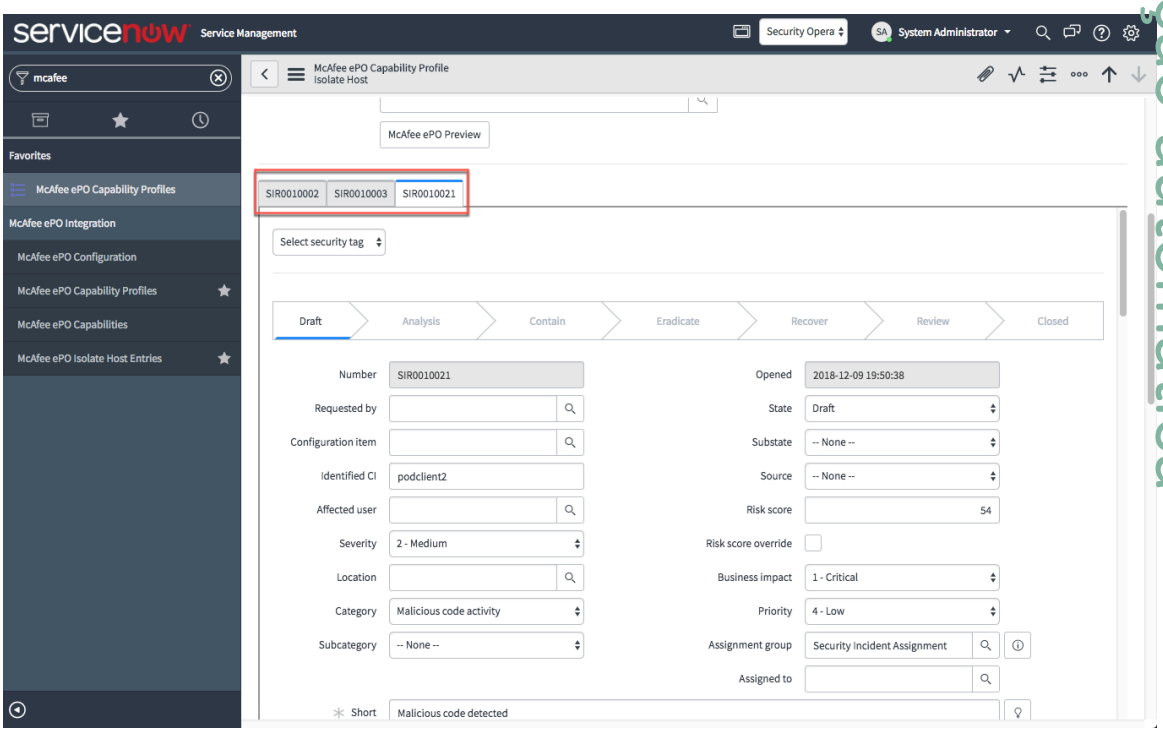
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Visualização do McAfee ePO** para exibir os incidentes de segurança.



Os incidentes criados para as condições de evento de segurança que correspondem ao seu perfil são exibidos em guias.

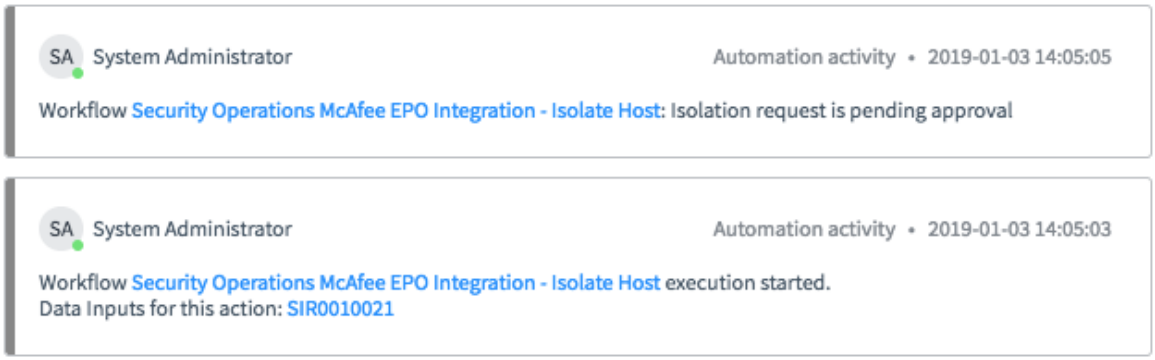
Nota: Se você sair da página Testar incidente neste momento, seus incidentes de segurança serão limpos desses campos.



6. Selecione uma guia e, no incidente de segurança, role para exibir as anotações de trabalho.

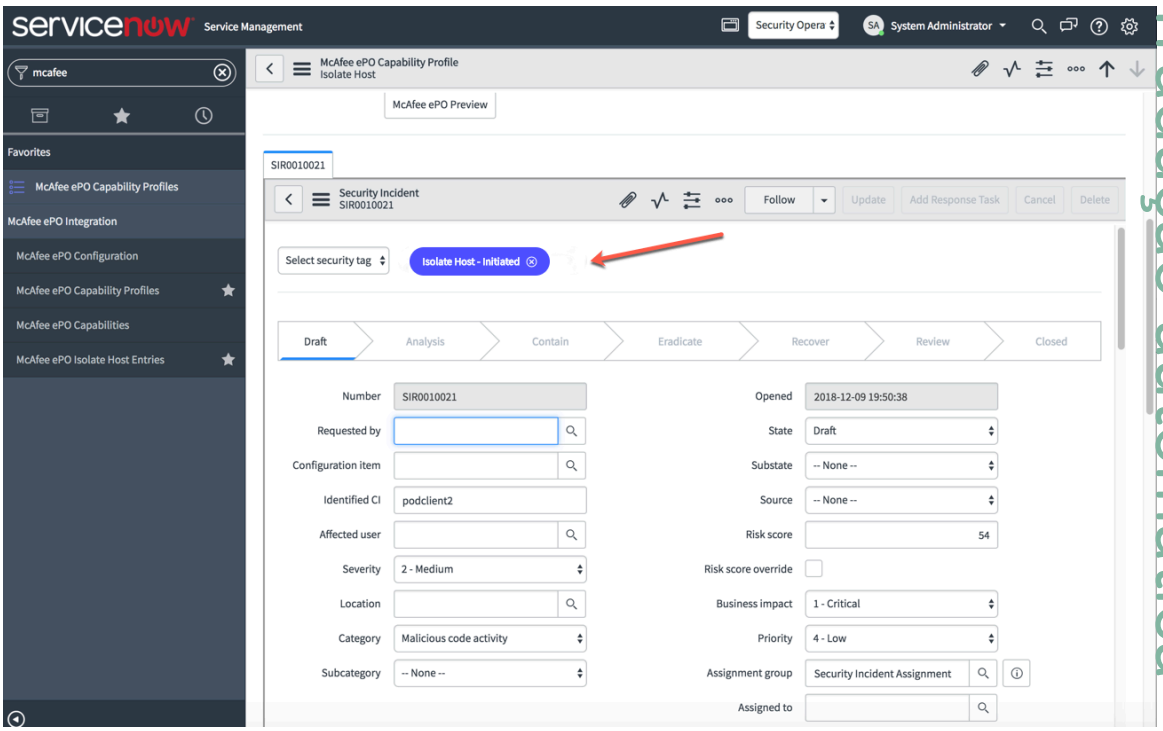
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Para este exemplo, SIR0010021 da imagem anterior está selecionado. As anotações de trabalho listam em que o fluxo de trabalho Isolar do host foi iniciado. . **Aprovação necessária** para este perfil, as anotações de trabalho indicam que a solicitação é aprovação pendente .

Na parte superior do incidente, o marcador de segurança é exibido indicando que a solicitação foi iniciada (Isolar host - Iniciado).



Tradução automática

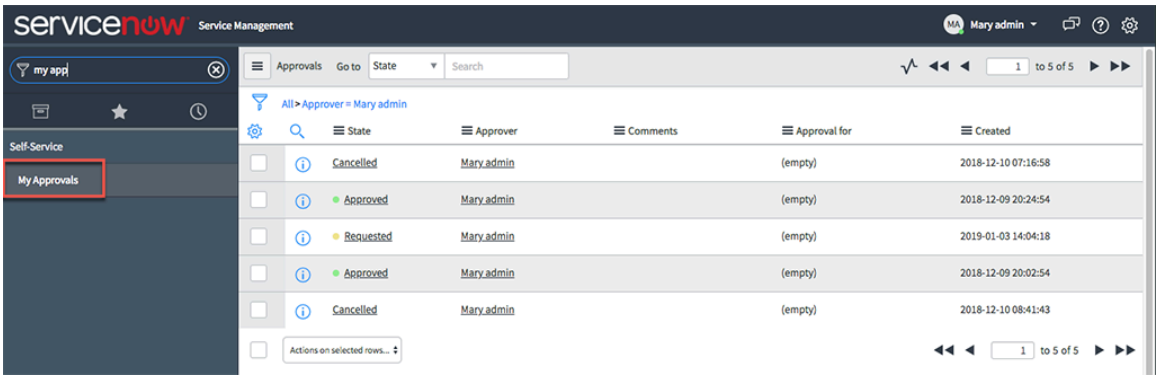
Você localizou com sucesso incidentes de segurança que correspondem ao seu perfil para o recurso Isolar host e visualizou um incidente de segurança.

7. Se você for um usuário em um grupo de aprovação, siga estas etapas para processar uma solicitação.

a. Navegue até **Minhas aprovações** em sua instância.

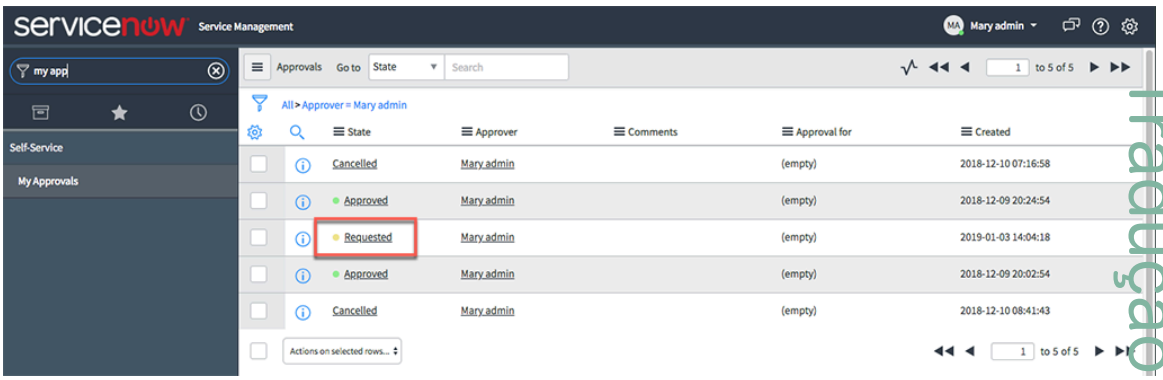
Para este exemplo, o nome de usuário do aprovador é Mary, administrador ™.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

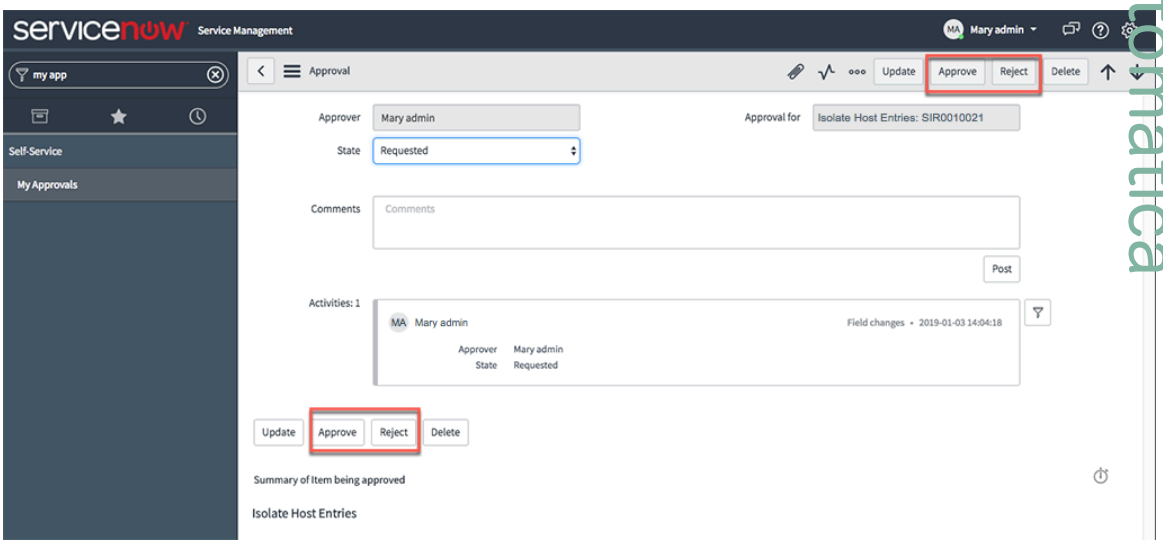


A lista de aprovações é exibida.

b. Na coluna Estado, clique em um item para abrir o registro de aprovação.



c. No registro de aprovação exibido, clique em **Aprovar** ou **Rejeitar** .



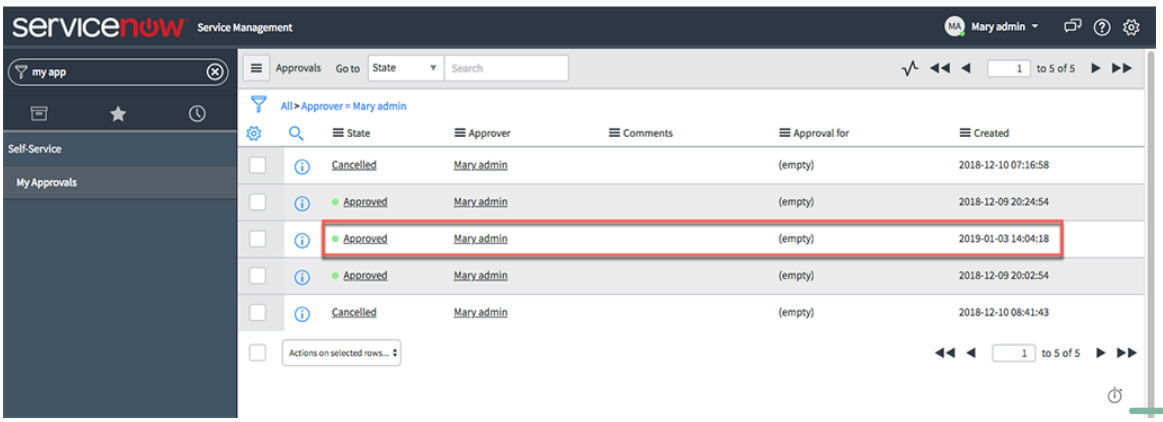
Depois de processar a solicitação, o fluxo de trabalho pode levar alguns minutos para ser executado. No registro na parte superior, uma mensagem será exibida, conforme mostrado na figura a seguir, se a transação demorar mais de alguns segundos.



Tradução automática

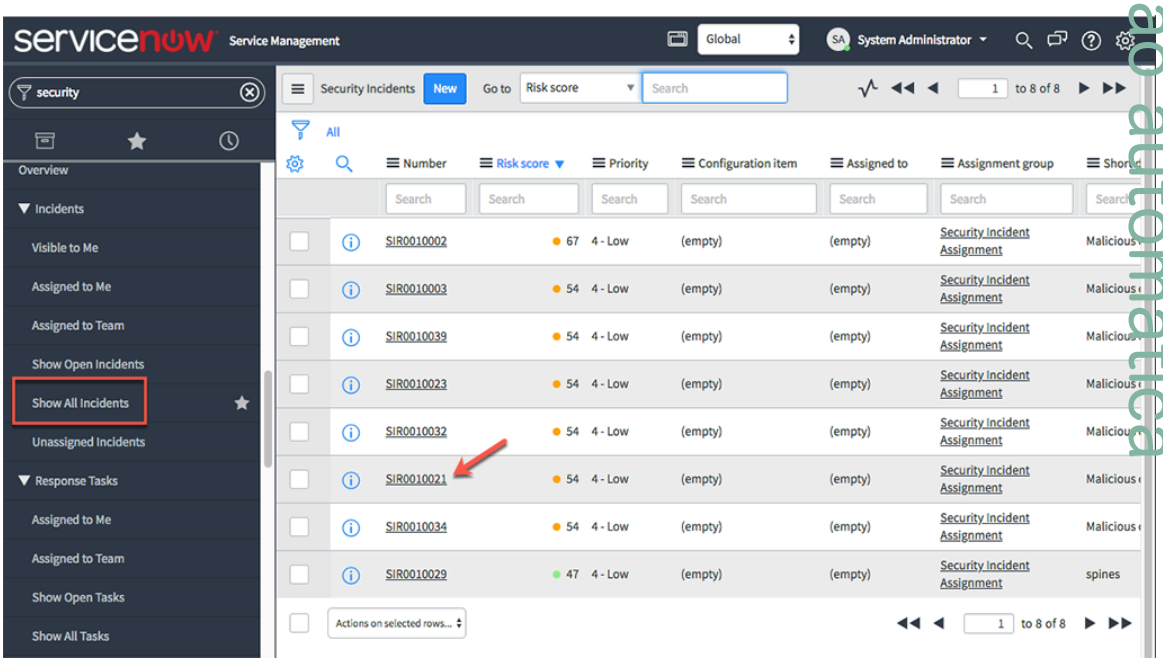
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após alguns momentos, no registro de aprovação exibido, a coluna Estado muda de Solicitado . Aprovado . Nenhuma aprovação adicional é necessária para isolar a máquina host desta solicitação. Se a solicitação for rejeitada, o host não será isolado e a solicitação permanecerá pendente. Como um usuário com a função sn_si.analyst, se a solicitação for rejeitada, você deverá enviar uma nova solicitação se ainda quiser isolar o endpoint.



A solicitação para isolar a máquina host na figura anterior foi aprovada.

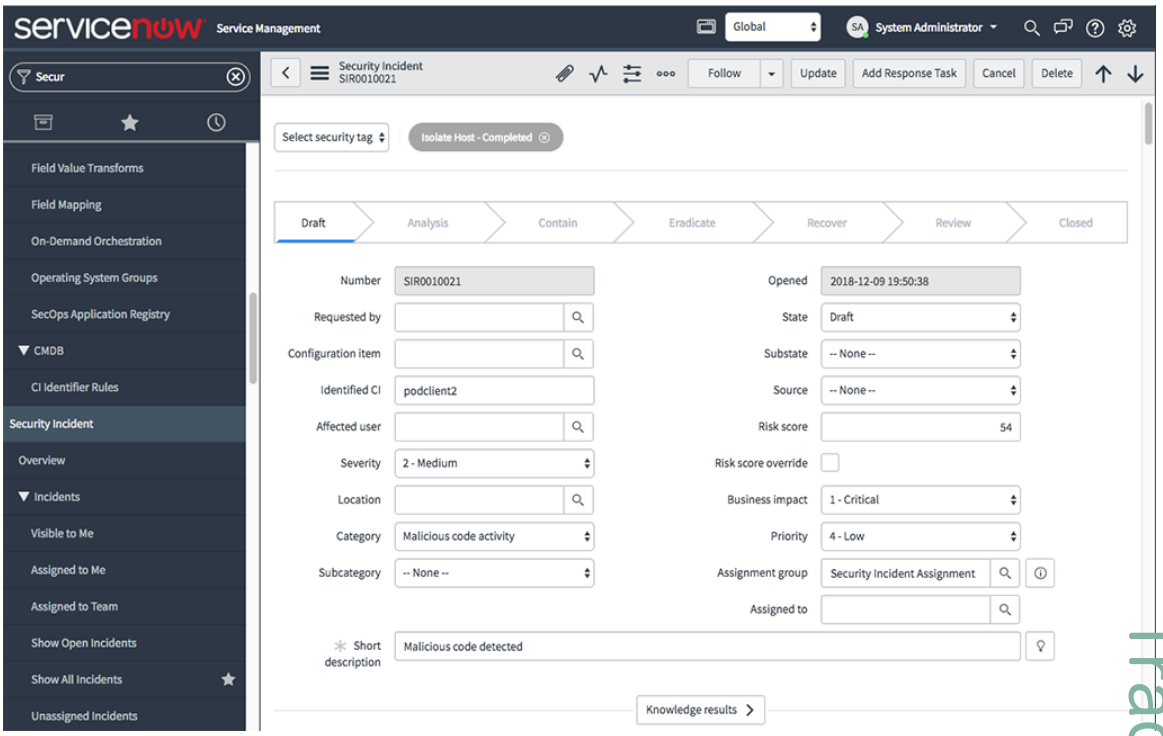
d. Navegar até **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes** E, na coluna Número, clique em uma entrada para abrir o incidente de segurança com o qual você está trabalhando.



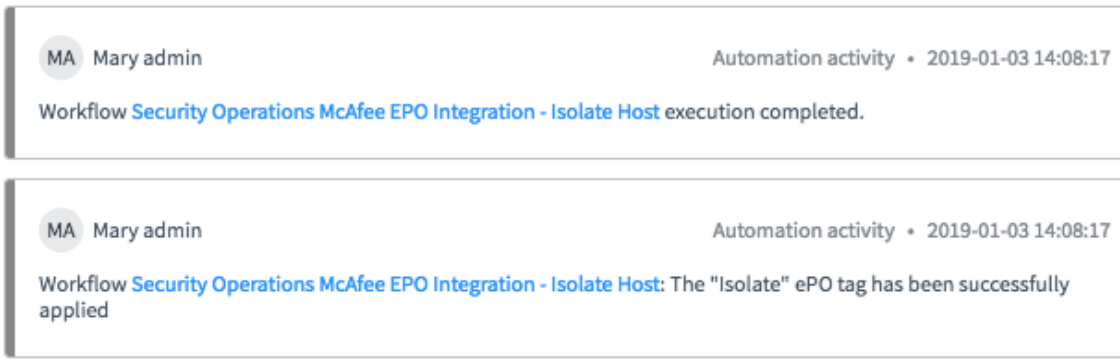
No incidente de segurança exibido, o. Isolar host - Concluído ™ o marcador substitui Isolar host - Iniciado ™ marcador. O fluxo de trabalho de isolamento de host para este exemplo foi bem-sucedido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As anotações de trabalho sobre o incidente de segurança também indicam que o isolamento do host foi concluído e o aprovador, Mary, administrador ™está listado.



Importante: Embora o marcador de segurança e as anotações de trabalho no incidente de segurança indiquem que um fluxo de trabalho de isolar host bem-sucedido foi concluído, retorne ao McAfee ePO console e verifique se a máquina host está isolada da sua rede.

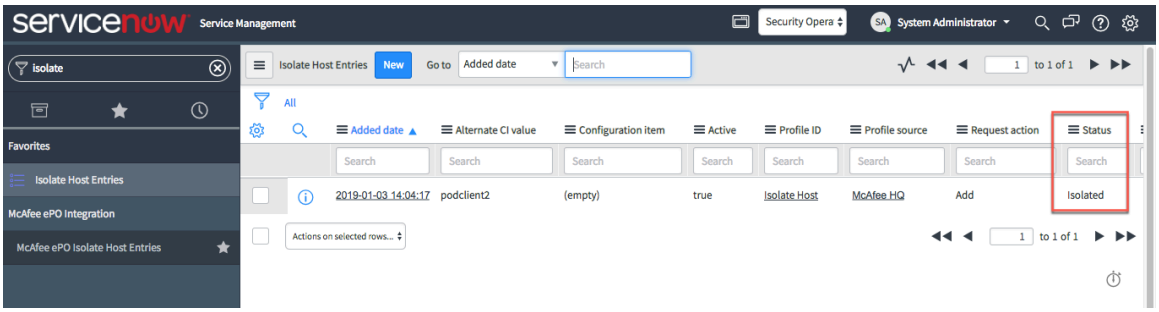
Depois de concluir sua investigação no ativo, inicie o fluxo de trabalho Remover isolamento do Entradas de isolamento de host ™tabela em seu ServiceNow AI Platform® instância para retornar o host à rede.

8. Para remover o host da quarentena e devolvê-lo à rede, siga estas etapas.

Tradução automática

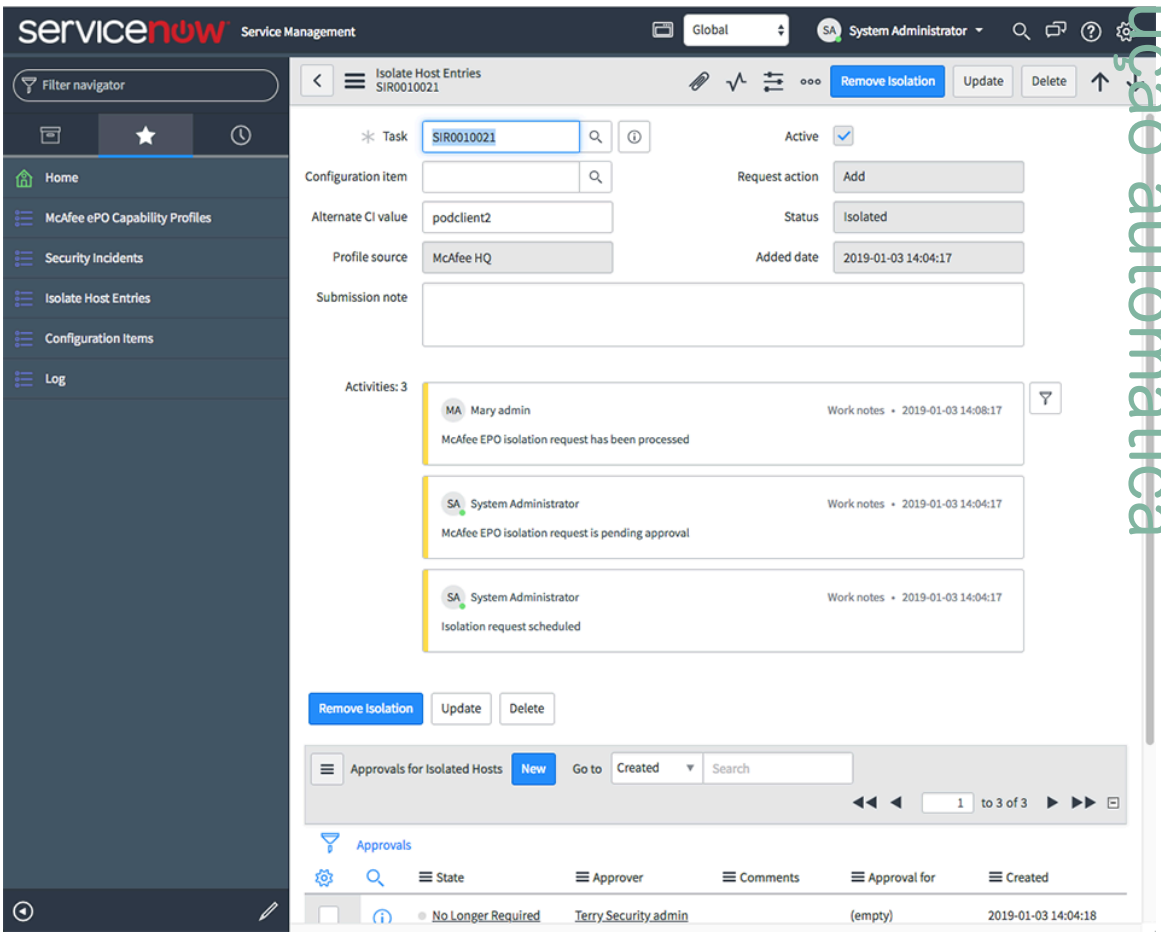
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. . McAfee ePO A tabela Isolar entradas de host não é exibida, navegue até **Integração do McAfee ePO** > **Isolar entradas de host da integração do McAfee ePO**.



A lista Isolar entradas de host é exibida. Na parte superior da lista na coluna Status, pesquise o ativo isolado.

b. Na coluna Data adicionada, clique no item para abrir o registro.
O registro Isolar entradas de host é exibido. Uma trilha de auditoria para todas as ações associadas ao incidente de segurança é exibida nas anotações de trabalho. Na figura a seguir, a última entrada nas anotações de trabalho é um isolamento de host bem-sucedido. A data em que a quarentena foi concluída é exibida em **Data adicionada** campo (2019-01-03 14:04:17).

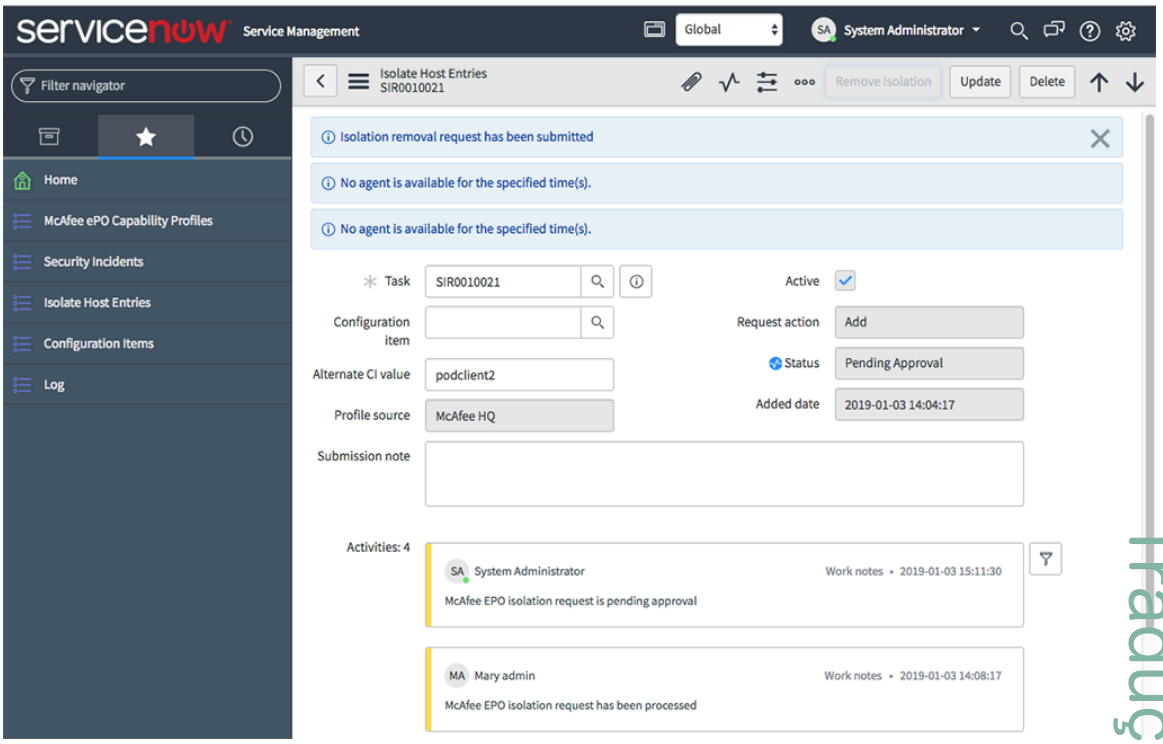


c. Clique em **Remover isolamento** para iniciar o fluxo de trabalho para restaurar a máquina para a rede.
O registro Isolar entrada de host é exibido. Na parte superior do registro, uma mensagem indica que a solicitação foi enviada. O Status muda de **Isolado** . **Aprovação pendente** e uma anotação de trabalho

Tradução automática

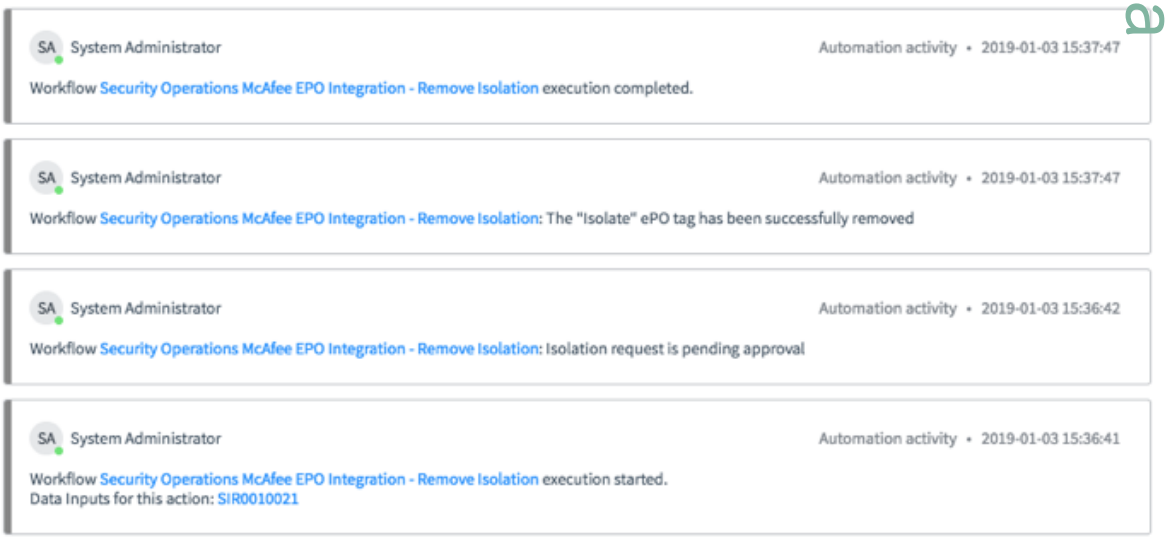
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é registrada em log. Nesse caso, o administrador do sistema solicitou que a máquina seja restaurada para a rede.



d. Depois de ser notificado sobre a solicitação, como um usuário com permissão de aprovação para isolamento de host, navegue até **Minhas aprovações** em sua instância e abra o registro da solicitação de remoção de isolamento.

e. Clique em **Aprovar** para aprovar a solicitação e retornar o ativo para a rede.
Como alternativa, clique em **Rejeitar** para manter a solicitação no estado de aprovação pendente. Se uma solicitação for rejeitada, uma nova solicitação deverá ser enviada para isolar o host. Depois de aprovar a solicitação para remover o isolamento do host, o marcador no incidente de segurança é removido. As anotações de trabalho criam uma trilha de auditoria para a solicitação de remoção de isolamento. Para este exemplo, o administrador do sistema iniciou e aprovou a solicitação.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O marcador de segurança e as anotações de trabalho no incidente de segurança indicam que o fluxo de trabalho de remoção de isolamento do host foi concluído com sucesso. Para verificar se o host está de volta na rede, retorne ao McAfee ePO console e verifique se a máquina host agora está ativa.

9. Escolha um para continuar.

Opção	Descrição
Anterior	Retorne à etapa Configuração do perfil. Se você não estiver satisfeito com os resultados de teste e visualização, continue definindo as configurações de perfil.
Encerrar	Conclua a configuração. Você será solicitado a confirmar a ativação.

Edite os nomes e as cores dos marcadores de início e conclusão

Você pode preferir editar os nomes e as cores dos marcadores de início e conclusão para os recursos Iniciar verificação de malware e isolar host. Os marcadores de início e conclusão ajudam a identificar rapidamente quais recursos são invocados ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança.

Antes de Iniciar

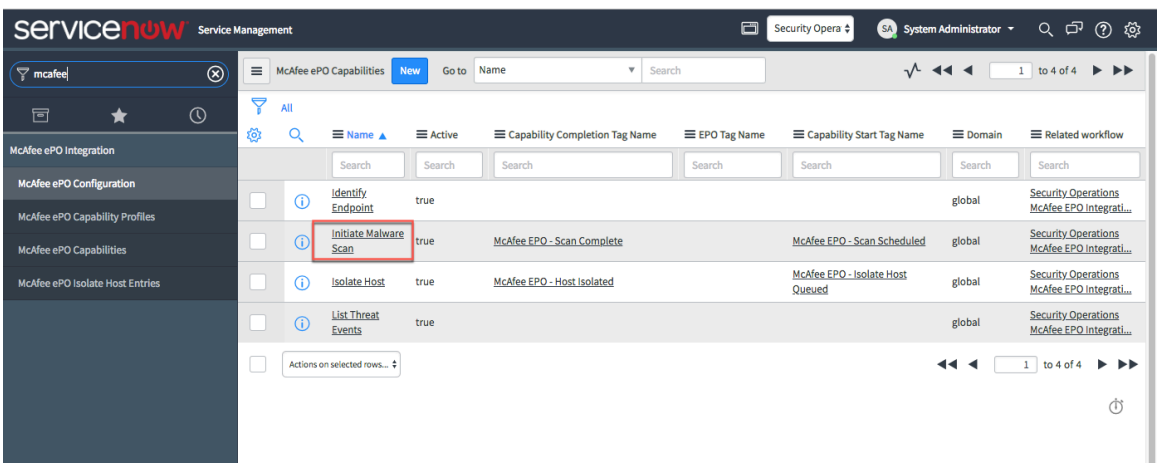
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, você pode preferir editar as cores e os nomes dos marcadores de segurança exibidos no SIR incidentes de segurança. Você também pode atribuir marcadores a grupos de marcadores de segurança para ajudá-lo a organizá-los em seu ServiceNow AI Platform® instância. Por exemplo, você pode mudar as cores dos marcadores para que o marcador de início de um recurso seja uma cor e o marcador de conclusão seja outra cor. Essas cores diferentes podem ajudá-lo a identificar rapidamente quando as digitalizações começam e são concluídas com sucesso. Para obter mais informações sobre como configurar grupos e marcadores de marcadores de segurança, consulte Configurar grupos de marcadores de segurança e marcadores .

Procedimento

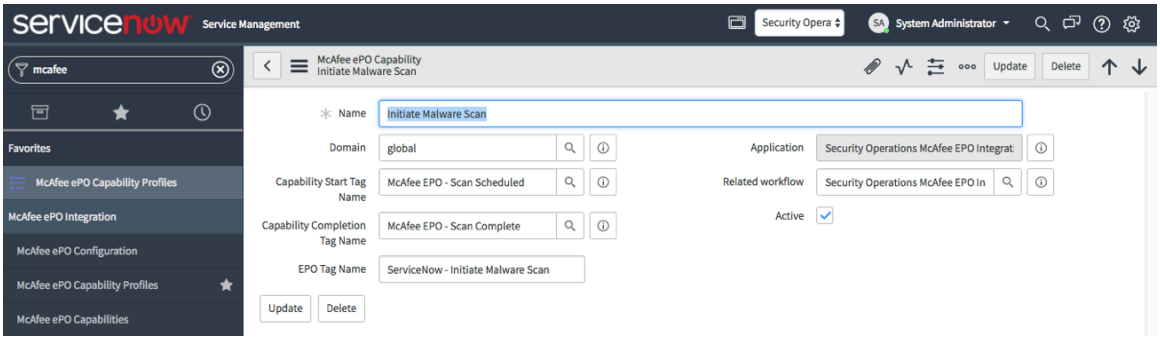
1. Para editar os nomes e as cores dos marcadores de segurança, navegue até **Recursos do McAfee ePO** E, na coluna Nome, clique em um item na lista.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro da capacidade é exibido.



2. Para editar um marcador, à direita de um nome de marcador, clique no ícone de informações e abra o registro do marcador.

No registro exibido, edite os campos.

Campo	Descrição
Nome	Insira um nome para a etiqueta de segurança.
Cor	Cor do marcador de segurança. Selecione uma cor na lista de seleção.
Grupo de marcadores de segurança	Insira um nome do grupo de marcadores de segurança. Clique no ícone de informações para exibir os grupos disponíveis. O padrão é Grupo Metatag.
Impor acesso restrito	Marque esta caixa de seleção para atribuir funções de leitura e gravação necessárias para que os usuários leiam ou gravem em registros que tenham este marcador de segurança. O padrão é limpo.
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista. O padrão é 100. Para definir a ordem na lista, insira um valor. Por exemplo, 100, 200, 300, 400. O marcador com o menor número é exibido primeiro na lista. O perfil com o número mais alto é exibido por último.
Ativo	Ativar ou desativar o marcador.
Descrição	Uma descrição do marcador.

3. Escolha um para continuar.

Opção	Descrição
Atualizar	Atualize a página com novas mudanças.
Excluir	Exclua este registro de marcador do recurso McAfee ePO.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

McAfee ESM - Integração do analisador de e-mail

A integração ESM - Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configure a integração McAfee ESM - Analisador de e-mail

A integração McAfee ESM - Analisador de e-mail usa notificações por e-mail do ESM para impulsionar o aprimoramento e fluxos de trabalho de resposta.

Antes de Iniciar

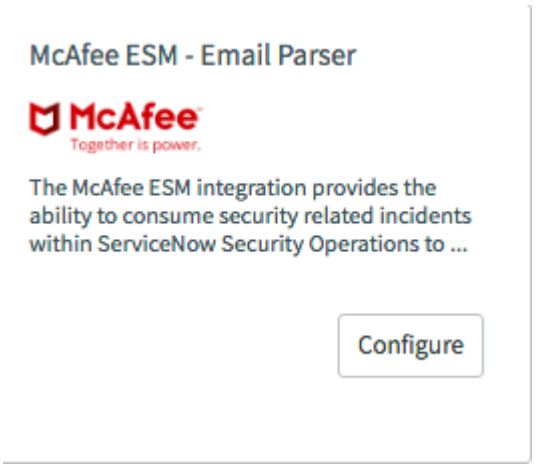
Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa

Um modelo de analisador de e-mail McAfee ESM é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão McAfee ESM - Analisador de e-mail, clique em **Configurar** .
3. Em **McAfee ESM - Configuração do analisador de e-mail** na caixa de diálogo, clique em **Configure o analisador de e-mail** link.
4. Clique em **McAfee ESM** link para editar as configurações no analisador de e-mail do modelo fornecido. No mínimo, preencha O e-mail é de campo. Para criar seu próprio analisador de e-mail, consulte Crie analisadores de e-mail em Operações de segurança.
5. Verifique **Ativo** caixa.
6. Clique em **Atualização** em **Analisador de e-mail** formulário.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração** .

McAfee ESM - Integração de aprimoramento de incidentes

McAfee ESM - A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos incidentes de segurança.

Explorar **Configurar**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Resposta a incidentes de segurança

- Comece a usar McAfee ESM Integração de aprimoramento de incidentes
- Criar registros de configuração de pesquisa de vistas

Usar

- Execute uma Pesquisa de vistas
- Integração de operações de segurança - Fluxo de pesquisa de vistas
- Operações de segurança - Fluxo de pesquisa de detecções do McAfee ESM
- Exibir detalhes da pesquisa de vistas
- Exibir resultados da pesquisa de vistas

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Comece a usar McAfee ESM Integração de aprimoramento de incidentes

McAfee ESM Protege endpoints contra vírus, spyware, cavalos de Tróia e outras ameaças de malware e se integra facilmente ao Operações de segurança. Antes de poder usar McAfee ESM- Integração de aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicione a URL base da API apropriada e as credenciais de login.

Antes de Iniciar

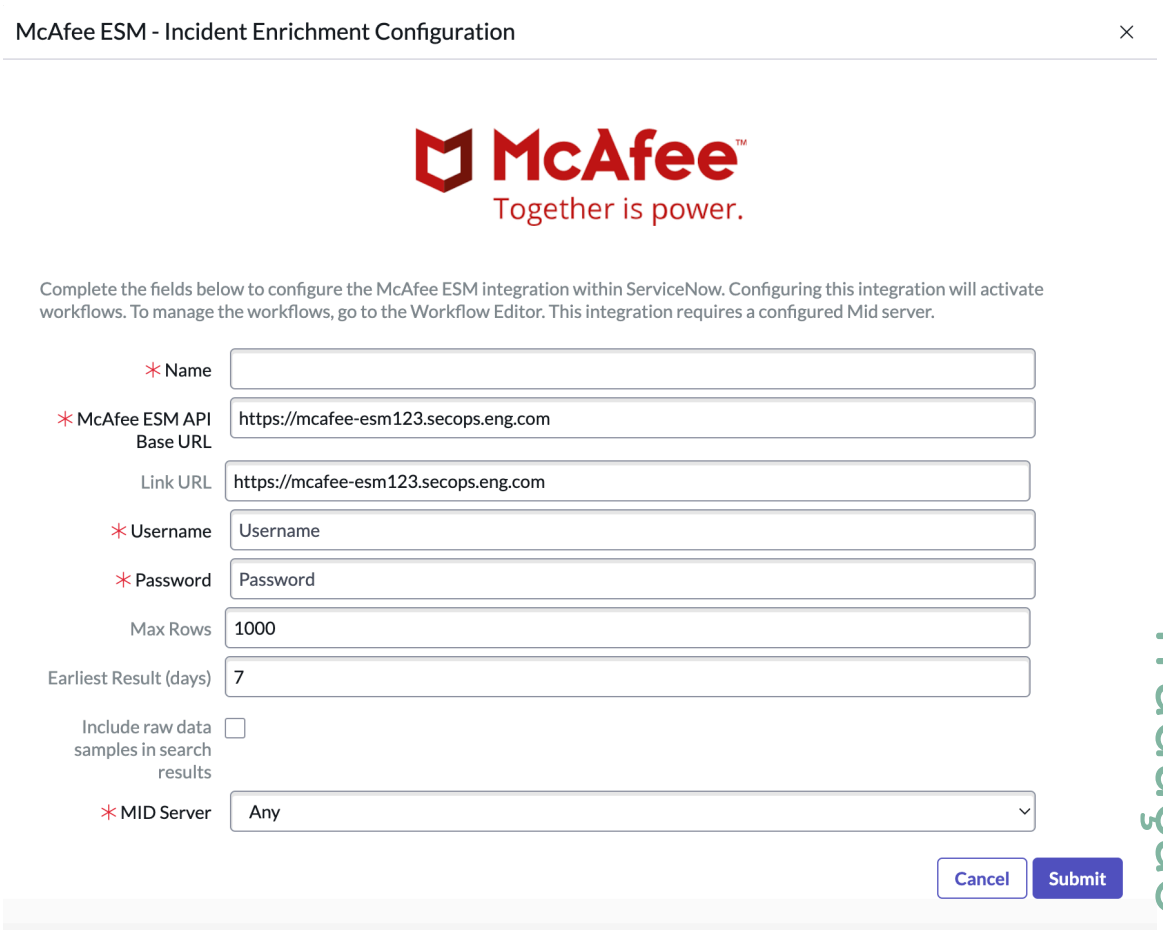
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. Em McAfee ESM- Cartão de aprimoramento de incidente, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL Base da API McAfee ESM	O URL base que você adquiriu no site do McAfee ESM.
URL do Link	[Opcional] O URL do link que vincula uma instância do McAfee ESM, quando disponível. **Nota:** Se você estiver recebendo um erro, use o URL base da API McAfee ESM.
Nome do usuário	Seu nome de usuário do McAfee ESM.
Senha	Sua senha do McAfee ESM.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
nos resultados da pesquisa	**número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Microsoft Azure Sentinel integração

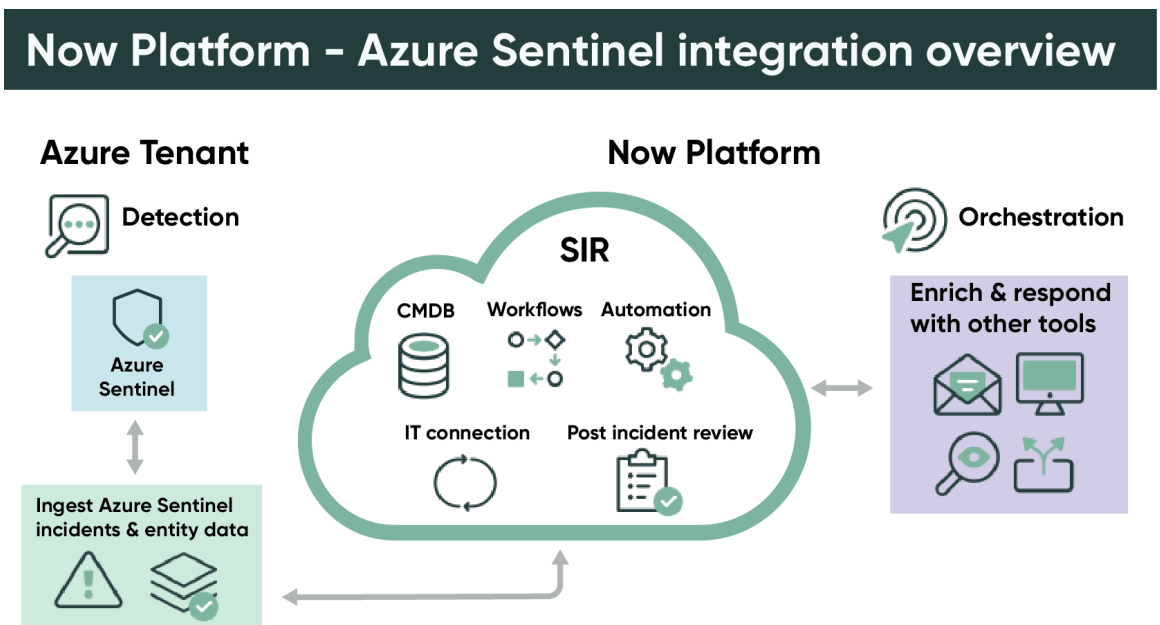
Microsoft Azure Sentinel É uma solução de Security Information Event Management (SIEM) e Security Orchestration Automated Response (SOAR) baseada em nuvem. Você pode usar Microsoft Azure Sentinel Integração para ingerir incidentes do Azure Sentinel e criar automaticamente incidentes de segurança no Resposta a incidentes de segurança.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

Consulte o diagrama a seguir para saber como Microsoft Azure Sentinel integra-se ao ServiceNow AI Platform Operações de segurança aplicações.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

Use os principais recursos desta integração para executar as seguintes ações:

- Descobrir Microsoft Azure Sentinel incidentes que são candidatos a incidentes de segurança e automatizam a criação desses incidentes de segurança.
- Mapa Microsoft Azure Sentinel campos incidente e entidade para SIR campos de incidente de segurança.
- Filtro Microsoft Azure Sentinel incidentes.
- Agregue incidentes a incidentes de segurança em aberto existentes para que você não precise criar incidentes de segurança duplicados.
- Automatizar Microsoft Azure Sentinel Atualizações de status do incidente para Resposta a incidentes de segurança para que você possa criar e fechar incidentes de segurança.

  Nota: ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes baseados na criação ou fechamento do incidente de segurança. Esta atualização também inclui comentários de incidentes agregados e novos incidentes.

- Programe a ingestão de incidentes para criar incidentes de segurança periodicamente.
- Sincronizar Microsoft Azure Sentinel comentários do incidente com SIR Anotações de trabalho.

Conheça esta integração

Identificador do documento	Título do documento
Microsoft site de documentação do produto	Site de documentação do produto da Microsoft
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece com Microsoft Azure Sentinel integração

Ativar e configurar o. Microsoft Azure Sentinel – Ingestão de incidentes Para o plug-in Operação de segurança para fazer interface com seu ServiceNow AI Platform instância e. Resposta a incidentes de segurança produto.

Antes de poder usar Microsoft Azure Sentinel, você deve baixá-lo do ServiceNow Store.

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário.

Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração tranquila.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.ingestion_profile_admin. • A função sn_si.ingestion_profile_admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria perfis de incidente. ◦ Mapeia o. Microsoft Azure Sentinel campos de dados de incidente para os campos de incidente de segurança. ◦ Agenda a ingestão de incidentes em andamento. ◦ Habilita atualizações de incidentes quando um Resposta a incidentes de segurança o incidente foi criado ou encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst).
Atribua o. Microsoft Azure funções necessárias.	As funções a seguir são necessárias em Microsoft Azure para registrar e configurar sua aplicação: • Desenvolvedor de aplicações para registrar a aplicação. • Administrador de locatário para conceder permissões à aplicação chamando o endpoint de consentimento do administrador.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você configurar esta integração.	. ServiceNow IntegrationHub Instalador do pacote inicial [o plug-in com.glide.hub.integrations] é necessário. . Resposta a incidentes de segurança o plug-in (com.snc.security_incident) é obrigatório. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	instalar e ativar cada aplicação uma de cada vez na seguinte ordem para garantir uma instalação tranquila: **1.** Resposta a incidentes de segurança **2.** IU Resposta a incidentes de segurança **3.** Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) **4.** Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Registre e configure sua aplicação no Microsoft Azure portal.	Registre sua aplicação no Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação .

Registre e configure o. Microsoft Azure portal

Registre sua aplicação no Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação .

Antes de Iniciar

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário

Procedimento

1. Entre no Microsoft Azure portal.
2. PESQUISE e selecione **Registros de aplicações** .
3. Clique em **Novo registro** .
4. No formulário, preencha os campos.

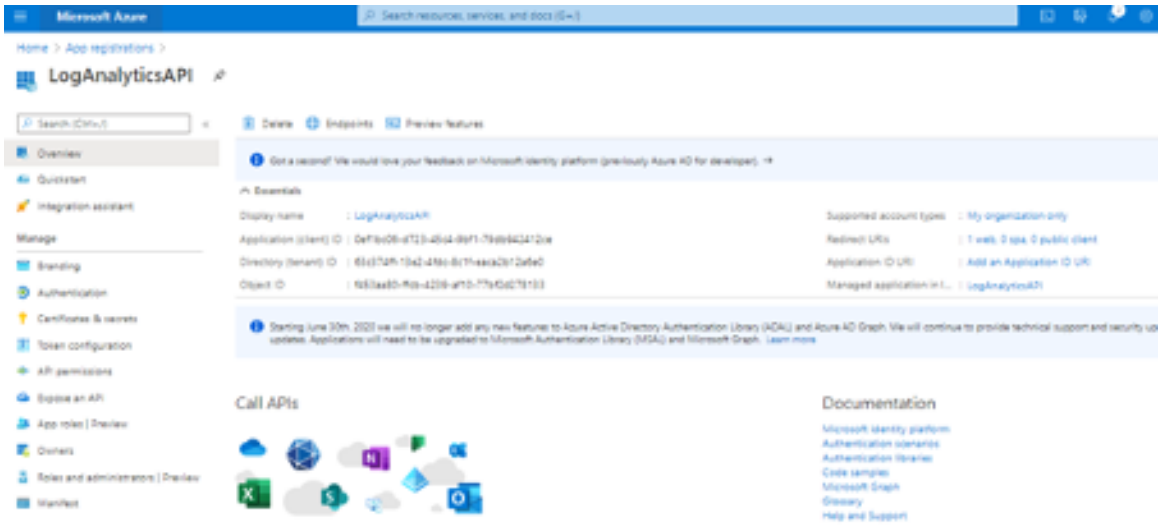
Registrar um formulário de candidatura

Campo	Descrição
Nome	Nome de exibição voltado para o usuário da aplicação. Por exemplo, LogAnalyticsAPI.
Tipos de conta compatíveis	Tipo de conta que pode usar esta aplicação ou acessar a API.
URI de redirecionamento	URI de redirecionamento. A resposta de autenticação é direcionada para este URI após autenticar um usuário com sucesso.

5. Clique em **Registrar**.
   Depois de registrar a aplicação com sucesso, você verá a página Visão geral.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Navegar até **Gerenciar** > **Certificados e segredos**.
7. Na seção Segredos do cliente, clique em **Novo segredo do cliente** .
   Você não pode exibir o segredo do cliente mais tarde, portanto, copie e salve o segredo do cliente agora nesta etapa. Se você esquecer o segredo do cliente, poderá gerar um novo segredo seguindo as instruções nas etapas 4 e 5.
8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique em **Adicione uma permissão** .
10. Na janela Solicitar permissões da API, clique em **APIs que minha organização usa** guia.
11. PESQUISE e selecione **API de análise de log** nome da aplicação.
12. Em Permissões da API Análise de log, selecione **Permissões da aplicação** .
    Habilitar esta permissão garante que a aplicação seja executada como um serviço em segundo plano ou daemon sem um usuário conectado.
13. Na seção Dados, selecione **Data.Read**
14. Clique em **Adicionar permissões** .
    As permissões são atualizadas.
15. Habilite o. **Conceda consentimento do administrador para o diretório padrão** Opção para a permissão da API Data.Read que você habilitou na etapa 13.
16. PESQUISE e selecione **Espaços de Análise de log** .
17. Selecione seu espaço de Análise de log do Sentinel.
    Agora você vê a página Visão geral do espaço Análise de log do Sentinel.
18. Navegar até **IAM (controle de acesso)** > **Atribuições de função**.
19. Clique em **Adicionar** e selecione **Adicionar atribuição de função** .
20. No formulário, preencha os campos.

Formulário Adicionar atribuição de função

Campo	Descrição
Função	Tipo de conta que pode usar esta aplicação. Selecione **Azure Sentinel Respondente** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuir acesso a.	Escopo de permissões que você define. Selecione **Usuário** , **grupo** ou **entidade de serviço** .
Selecionar	Aplicação que você criou anteriormente na etapa 4. Por exemplo, LogAnalyticsAPI.

21. Clique em **Salvar**.

Instale e configure o. Microsoft Azure Sentinel integração

Instale e configure o. Microsoft Azure Sentinel integração do ServiceNow Store em seu ServiceNow AI Platform Instância para começar a ingerir incidentes do Azure Sentinel.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Baixe o. Microsoft Azure Sentinel integração do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE Microsoft Azure Sentinel lado a lado e clique **Configurar** .
4. No formulário, preencha os campos.

Microsoft Azure Sentinel Formulário Configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome do Nuvem do Microsoft Azure configuração da instância.
URL de identidade	URL de identidade do Nuvem do Microsoft Azure locatário. Por exemplo, login.microsoftonline.com . Para obter informações adicionais, consulte Documentação do Microsoft Azure .
Azure Resource Manager	Endpoint do Azure Resource Manager para Nuvem do Microsoft Azure locatário. Por exemplo, management.azure.com . Para obter informações adicionais, consulte Documentação do Microsoft Azure .
ID de locatário	Microsoft Azure Sentinel ID do locatário. Esta é a instância da qual todos os incidentes no Microsoft Azure os portais são recuperados.
ID de cliente	ID do cliente da aplicação que você registrou no Microsoft Azure portal.
Segredo do cliente	Segredo do cliente para sua aplicação registrada.
ID de Assinatura	ID de assinatura da sua aplicação registrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do grupo de recurso	Nome do grupo de recursos para sua aplicação registrada.
Nome do espaço	Nome do espaço para sua aplicação registrada.

5. Clique em **Enviar**.

Resultado
Depois de validar e enviar a configuração com sucesso, cada configuração do servidor de ingestão de incidentes será salva na página Integrações de segurança como um bloco.

Crie um perfil para Microsoft Azure Sentinel

Crie um perfil de incidente em seu ServiceNow AI Platform e determinar o. Microsoft Azure Sentinel incidentes adequados para criar incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa
A integração permite que você crie diferentes tipos de incidentes, como tentativas de acesso não autorizado e malware. Esses incidentes são criados com base nos perfis que você configura no ServiceNow AI Platform instância. Inicialmente, todos os incidentes são criados para um tipo de incidente configurado em um perfil. Os incidentes criados podem ser filtrados ainda mais para especificar quais incidentes criam incidentes de segurança.

Todos os incidentes que atendem aos critérios de seleção em seu Microsoft Azure locatário, e estão disponíveis sobre Microsoft Azure Sentinel Inicialmente, são ingeridas em seu ServiceNow AI Platform instância.

Procedimento

1. Navegar até **Tudo** > **Integração do Microsoft Azure Sentinel** > **Perfil de incidentes do Azure Sentinel**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Microsoft Azure Sentinel Formulário Configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda você a identificar o tipo de perfil e também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Indicador de que o perfil está ativo. Quando o perfil está ativo, isso implica que ServiceNow AI Platform Está pesquisando ativamente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	incidentes do Azure Sentinel e se os incidentes de segurança correspondentes são criados em SIR quando as condições de filtragem são correspondidas.
Origem	Microsoft Azure locatário que você configurou para ingerir incidentes. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de incidente que você planeja ingerir para o perfil.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Descrição	Texto extra para ajudá-lo a distinguir este perfil de outros perfis.

4. Para mover para a seção Mapeamento, clique em **Continuar** .

O que Fazer Depois

Mapear indivíduo Microsoft Azure Sentinel campos de incidente para os campos no ServiceNow AI Platform SIR incidente de segurança.

Mapeie o. Microsoft Azure Sentinel campos de incidente

Mapeie o indivíduo Microsoft Azure Sentinel campos de incidente para os campos no SIR incidente de segurança para que você possa criar incidentes com os dados mapeados.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Na página de mapeamento, na seção Mapeamento de campo do Azure Sentinel, selecione um dos métodos de ingestão de amostra.

Métodos de ingestão de amostra

Campo	Descrição
Todos os campos Incidente padrão e Entidade	Use este método de ingestão para exibir a lista estática de todos os incidentes e campos de entidade. Este método contém somente nomes de campo padrão sem valores.

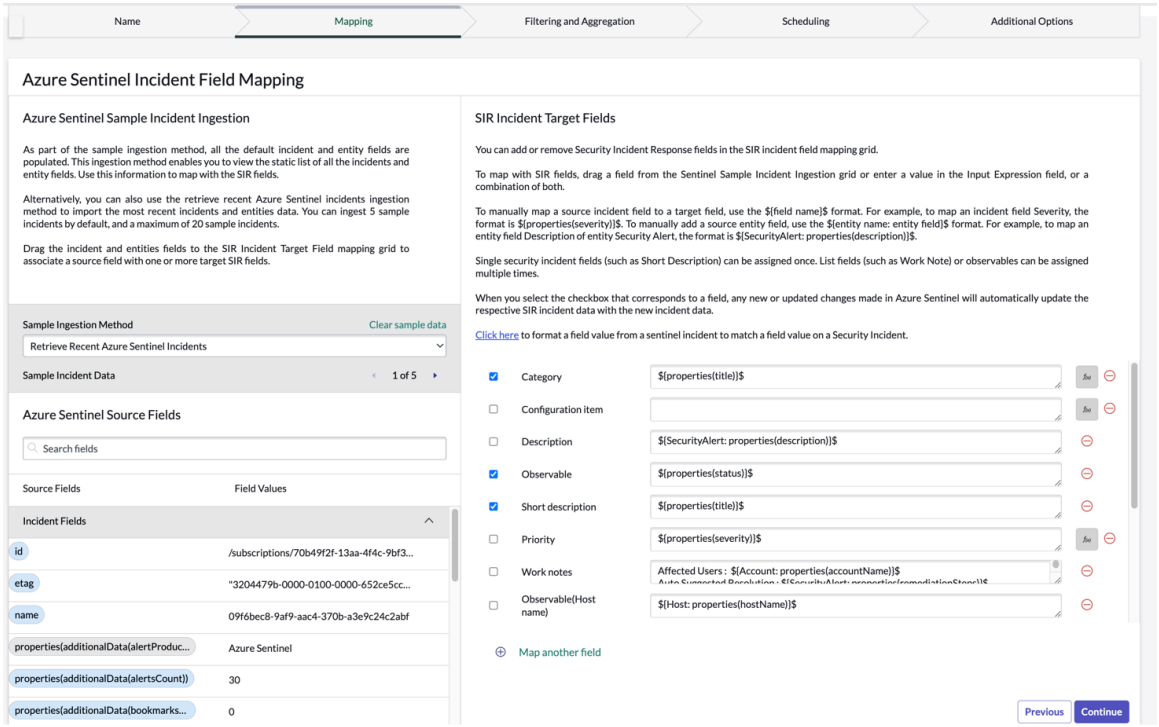
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Você pode usar essas informações para mapear com SIR campos.
Recupere incidentes recentes do Azure Sentinel	Use este método de ingestão para importar os dados de incidentes e entidades mais recentes. Se o incidente do Azure Sentinel contiver os dados da entidade, os dados da entidade serão recuperados e estarão disponíveis para mapeamento na seção Campos de origem do Azure Sentinel. Às vezes, o incidente do Azure Sentinel pode não conter os dados da entidade e, portanto, os campos da entidade não estão disponíveis para mapeamento em tal cenário. Se o incidente do Azure Sentinel contiver vários alertas, o alerta mais antigo que faz parte do incidente será mostrado na seção de mapeamento. Os valores de campo de alerta de segurança mais antigos serão usados durante a ingestão. Você pode ingerir 5 incidentes de amostra por padrão e um máximo de 20 incidentes de amostra. Os valores do campo de incidente de amostra são preenchidos quando o perfil ingere os incidentes de amostra. Você pode mapear esses incidentes para **Campos de destino do incidente SIR** . Os campos e os valores do incidente aparecem como guias individuais.
Importar dados de amostra	Clique em **Importar dados de amostra** Para importar incidentes de amostra do Azure Sentinel. Este botão aparece quando você seleciona o método de ingestão Recuperar incidentes recentes do Azure Sentinel. Recuperando incidentes de amostra de Microsoft Azure Sentinel o servidor pode demorar um momento. Mapeie esses incidentes recuperados para **Campos de destino do incidente SIR** . Os campos e os valores do incidente aparecem como guias individuais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Para adicionar campos aos campos padrão exibidos no incidente de segurança, execute as seguintes ações:

a. Na seção Campos de destino do incidente SIR, clique em ⊕ Map another field Botão Mapear outro campo.
Mostra uma lista de SIR campos, a partir dos quais você pode selecionar um campo para que um novo campo seja exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Nota: Vários observáveis podem ser exibidos no mesmo incidente de segurança. Por exemplo, o. **Observável** o campo pode ser mapeado várias vezes com valores diferentes. Da mesma forma, o **Item de configuração** e. **Campos de anotações de trabalho** suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, verá uma mensagem de erro informando que este campo não oferece suporte a vários valores. Da mesma forma, se um campo em um incidente de segurança tiver uma lista da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista, o campo não será preenchido no incidente de segurança.

c. Na seção Campos de origem do Azure Sentinel, arraste e solte o campo para mapeá-lo para o novo campo.

d. Quando você marca a caixa de seleção que corresponde a um campo, todas as mudanças novas ou atualizadas feitas no Azure Sentinel atualizarão automaticamente os respectivos dados do incidente SIR com os novos dados do incidente.

Nota: No sistema de base, a propriedade do sistema sn_sec_sentinel.incident_updates é definida por padrão como verdadeira para receber Microsoft Azure Sentinel Atualizações relacionadas a novos alertas vinculados ao SIR.

- Por padrão, os campos Usuários afetados, Itens de configuração e Observáveis são verificados. Sempre que houver novos observáveis ou itens de configuração associados, ou usuários afetados que são adicionados ao incidente, essas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

informações serão extraídas e preenchidas automaticamente nas respectivas listas relacionadas na Resposta a incidentes de segurança (SIR) durante esse intervalo de pesquisa.

- Para quaisquer outros campos, você deve marcar a caixa de seleção que corresponde a um campo para todas as mudanças novas ou atualizadas feitas no registro de incidente do Azure Sentinel no Azure Sentinel. Isso atualizará automaticamente os respectivos dados do incidente SIR com os novos dados do incidente.

Importante: A due diligence deve ser feita antes de selecionar esta funcionalidade, pois a substituição dos dados existentes pode resultar em dados instáveis para o analista trabalhar e qualquer outra automação definida até mesmo pelos valores de campo do incidente de segurança também pode ser afetada. Portanto, é muito importante fazer a due diligence antes de selecionar qualquer funcionalidade de substituição.

3. Para remover um campo, use Botão Remover item ao lado do campo Expressão de entrada na seção Campos de destino do incidente SIR.
4. Para mapear um valor de campo da seção Campos de origem do Azure Sentinel para um campo na seção Campos de destino do incidente SIR, use uma das seguintes ações:

   a. Arraste o nome do campo (por exemplo, id) e solte-o ao lado de um nome de campo na coluna Campos de destino do incidente SIR.

   Você pode corresponder qualquer valor da seção Campos de origem do Azure Sentinel a um campo na seção Campos de destino do incidente SIR. Os campos são codificados por cores para que você não ignore ou duplique os campos de incidente no processo de mapeamento. Campos azuis claros indicam que um campo de incidente ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de incidente de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Dessa forma, você pode visualizar quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de incidente importante restante permanece não mapeada.

   b. Você pode adicionar uma combinação de texto e campo.
   Por exemplo, `O nome do incidente é` . Aqui `O nome do incidente é` pode ser inserido manualmente enquanto `(nome)` É mapeado na seção Campos de origem do Azure Sentinel.

   c. Você pode inserir e mapear manualmente diretamente um incidente de origem ou campo de entidade para um campo de destino.

   - Para mapear manualmente um campo de incidente de origem, use oformato "nome do campo". Por exemplo, para mapear a gravidade de um campo de incidente, o formato é `(propriedades(severidade))` .
   - Para adicionar manualmente um campo de entidade de origem, use `nome da entidade: campo da entidade` formato. Por exemplo, para mapear um campo de entidade Descrição do alerta de segurança da entidade, o formato é `SecurityAlert: Properties(description)` .

Esta integração classifica determinados subtipos observáveis. Ao mapear um campo Azure Sentinel com o campo observável SIR, o. ServiceNow AI Platform classifica automaticamente o observável. Se você quiser mapear genericamente o Observable do Azure Sentinel de entrada para o tipo de observável em SIR, Em seguida, arraste e solte o campo Azure Sentinel no campo Observável. No entanto, se você souber do tipo de observável para o observável do Azure Sentinel de entrada em SIR, em seguida, mapeie especificamente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para SIR Campo de tipo de observável. Alguns exemplos de tipos de observáveis específicos em SIR Incluir Observable (nome do domínio), Observable (endereço de e-mail), Observable (endereço IP (V4)) e Observable (nome do host).

Se os campos de entrada do Azure Sentinel contiverem algum MITRE-ATT&CK e mapeie-as para MITRE-ATT&CK Campo de técnica. Certifique-se de que o campo Azure Sentinel de entrada contenha MITRE-ATT&CK ID da técnica ou nome da técnica.

Às vezes, valores de campo de incidente em Microsoft Azure Sentinel Não pode ser traduzido diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos.

5. Para formatar uma tradução de campo para um novo campo de um incidente do Azure Sentinel para corresponder a um valor de campo em um Incidente de segurança, clique em **Clique aqui** link no **Campos de destino do incidente SIR** cabeçalho.

6. Para modificar os campos compatíveis com a tradução de campo, clique em  ícone de tradução de campo de formato de script.
   Os campos compatíveis com a tradução de campo são **Categoria** , **Item de configuração** e **Prioridade** .
   Por exemplo, clique em  Ícone ao lado da Categoria. O editor de script de Tradução de campo do Azure Sentinel é aberto.

7. Insira as mudanças no script e clique em **Atualização** Para salvar as mudanças e retornar à página Mapeamento.
   Por exemplo, para Categoria, defina o seguinte no editor de scripts:

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
   ```

   Este mapeamento garante que um perfil use somente categorias configuradas.

8. Continue seu mapeamento adicionando ou removendo valores de campo.
   Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um incidente de entrada deve atender para criar um incidente de segurança.

9. Para ir para a seção Filtragem e agregação, clique em **Continuar** .

O que Fazer Depois

Defina e defina condições de filtro para que você possa especificar quais incidentes devem criar incidentes de segurança. Você pode usar os mesmos valores de campo (definidos na seção Mapeamento) no construtor Condições de geração de incidentes (na seção Filtragem e agregação) para definir critérios adicionais que um incidente de entrada deve atender para criar um incidente de segurança.

Definir critérios de filtro e agregação

Você pode definir e definir condições de filtro para especificar qual entrada Microsoft Azure Sentinel os incidentes devem criar incidentes de segurança. Você também pode definir critérios de campo de incidente adicionais que permitem que um incidente de entrada seja anexado a um incidente de segurança aberto em vez de criar um incidente.

Defina as condições de filtragem para incidentes de segurança

Defina as condições de filtragem para que os incidentes de segurança sejam criados somente quando as condições de filtragem corresponderem.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda você a isolar incidentes de segurança e limita o número de incidentes de segurança que você cria. Se você definir critérios de filtragem adicionais, somente os incidentes necessários serão ingeridos sem precisar mudar a consulta ou a configuração do incidente acionado.

Procedimento

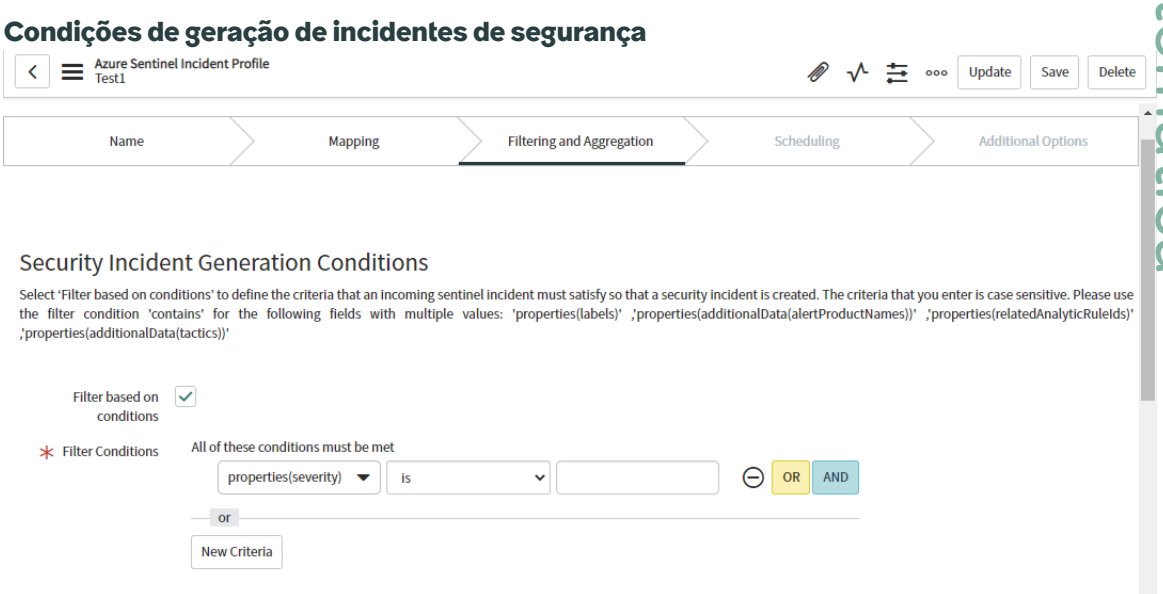
1. Para definir os critérios que um de entrada Microsoft Azure Sentinel para que um incidente de segurança seja criado, selecione **Filtro com base em condições** .

   As opções no primeiro campo em Condições de filtro correspondem aos campos exibidos na seção Ingestão de incidente de amostra do Azure Sentinel para o incidente que você ingeriu. Esses campos são dinâmicos e mudam dependendo do incidente que você ingerir. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios que você define correspondem aos valores do incidente.

   Use a condição de filtro *contém* para os seguintes campos com vários valores:

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar *contém* condição de filtro para os campos acima para garantir que os dados sejam filtrados corretamente.



2. Usando as listas e os campos do construtor de condições, defina os filtros para a primeira linha.
3. Para adicionar mais condições, clique em **E.** ou **OU** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **E.** selecionado, todas as condições devem ser correspondidas.
- Se **OU** está selecionado, qualquer condição pode ser correspondida.

4. Para definir uma segunda condição de filtro, clique em **Novos critérios** .

Definir condições de agregação

Defina critérios de agregação de incidentes adicionais que agreguem um incidente de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Quando você usa critérios de valor de correspondência de campo para cada perfil, essa agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de incidentes relacionados em um único incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa
Se um novo incidente corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o incidente será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os incidentes agregados adicionados em uma lista relacionada em um incidente de segurança.
Todos os incidentes agregados em um incidente de segurança são exibidos na lista relacionada Incidentes agregados do Azure Sentinel. Esta lista detalha os carimbos de data/hora associados e os valores de campo agregados. Essas informações ajudam você a entender por que os incidentes são adicionados aos incidentes de segurança existentes.

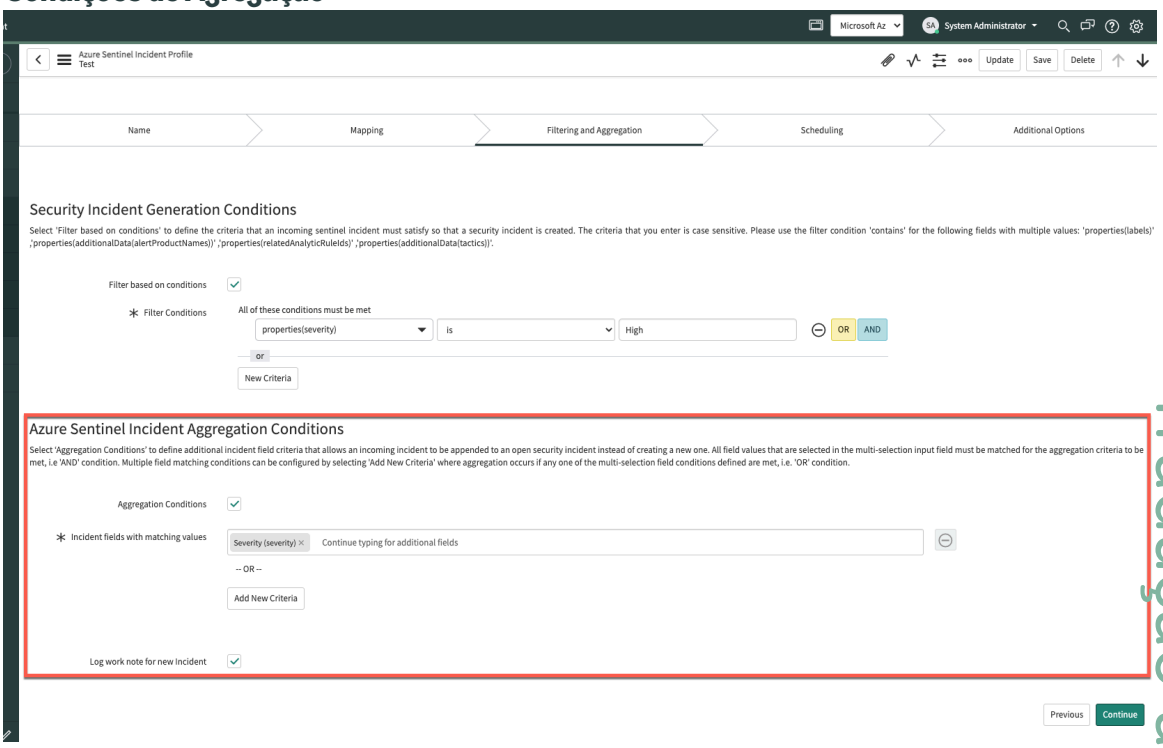
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Para definir critérios de campo de incidente adicionais que permitem uma entrada Microsoft Azure Sentinel incidente a ser anexado a um incidente de segurança em aberto em vez de criar um novo incidente, selecione **Condições de agregação** opção conforme mostrado na figura a seguir.

Condições de Agregação



2. Em **Campos de incidente com valores correspondentes** campo, insira os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform instância. Todos os valores de campo selecionados no campo de entrada de seleção múltipla devem corresponder para que os critérios de agregação sejam atendidos e que este incidente de entrada possa ser anexado a um incidente de segurança existente. Esta seleção implica que é um *E.* Condição em que campos, como Observáveis e Itens de configuração que podem ter vários valores de campo, são mapeados para eles. Se somente um subconjunto dos valores for correspondido, as condições de agregação de Incidente do Azure Sentinel não serão atendidas e um novo incidente de segurança será criado.
3. Para adicionar várias condições de correspondência de campo, clique em **Adicionar novos critérios** A agregação ocorrerá se qualquer uma das condições do campo de seleção múltipla que você definir for atendida. Esta seleção implica *OU* condição.
4. Para atualizar a anotação de trabalho de um novo incidente quando ela for adicionada a um incidente de segurança, selecione **Anotação de trabalho em log para o novo incidente** .

   A anotação de trabalho registra em log que um novo incidente foi adicionado e inclui um link para os detalhes do incidente. A anotação de trabalho de log também atualiza mais detalhes que você adiciona ao campo de anotação de trabalho na seção de mapeamento.
5. Para configurar a programação, clique em **Continuar** .

O que Fazer Depois

Defina uma programação para recuperar os dados do incidente e os incidentes ingeridos que correspondam aos critérios no perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programe o. Microsoft Azure Sentinel recuperação de incidentes

Defina uma programação para recuperar os dados do incidente e ingerir o. Microsoft Azure Sentinel incidentes que correspondem aos critérios no perfil.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que deseja pesquisar para o futuro Microsoft Azure Sentinel incidentes que correspondem à configuração do perfil de incidente.

Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. Para definir uma data e hora específicas para a ingestão inicial, habilite **defina o tempo de ingestão do incidente** . A ingestão subsequente é baseada no período de intervalo de pesquisa.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho do Microsoft Azure Sentinel integração de incidentes. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente. Um valor padrão de um minuto é definido para todos os perfis. Você pode modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Todos os alertas adicionados ao incidente em um intervalo de pesquisa específico, haverá um processo executado e anexado às listas relacionadas aos alertas do Azure Sentinel e a anotação de trabalho também será publicada.

Procedimento

1. No formulário de programação, preencha os campos.

   Configure a programação para definir como e quando você extrai incidentes do Microsoft Azure locatário.

Formulário de programação

Campo	Descrição
Ingestão de incidentes em andamento	Ingestão de incidentes em andamento que o ServiceNow AI Platform a instância extrai do Microsoft Azure locatário para novos incidentes. Os incidentes de segurança serão criados se incidentes acionados forem encontrados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos.
Definir tempo de ingestão do incidente	Ingestão de incidente baseada na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tempo de adição do incidente de entrada	Data e hora especificadas para a ingestão do incidente.
Recuperação Única	Marque esta caixa de seleção para permitir a recuperação única de incidentes históricos do Azure Sentinel e, em seguida, faça a reconciliação dos dados. Ao selecionar este checkox, a aplicação extrairá todos os incidentes do Azure Sentinel abertos e encerrados pelo período de até aproximadamente 6 meses. Ao processar os dados, os incidentes em andamento e os dados históricos são extraídos, mas o processamento dos incidentes em andamento tem precedência sobre a extração histórica e, caso contrário, a extração histórica pode levar algum tempo com base na duração e no número de incidentes que você está ingerindo. **Nota:** Os incidentes históricos recuperados do Azure Sentinel passam por verificações de desduplicação para evitar duplicatas na aplicação Resposta de incidentes de segurança.
Desde a data	A data desde quando os incidentes históricos são ingeridos do Azure Sentinel. **Nota:** Os dados do incidente são extraídos aproximadamente dos últimos 6 meses.

A página de programação permite que você defina como e quando os incidentes são extraídos do Microsoft Azure locatário.

2. Para navegar até a página Opções adicionais, clique em **Continuar** .

Automatize as atualizações e fechamentos de incidentes pelo SIR status do incidente

Automatize as atualizações e fechamentos de incidentes pelo SIR status do incidente. . Microsoft Azure Sentinel a integração tem uma interface bidirecional que permite que os incidentes criem incidentes de segurança e atualizem os incidentes depois que o incidente de segurança é criado ou encerrado.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. No formulário, preencha os detalhes.
   Siga as instruções para concluir a configuração para atualizar incidentes ao criar ou fechar um incidente de segurança em SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Automatizando atualizações de incidentes

Categoria	Campo	Descrição
Atualizações de criação de incidente	Atualize o status de incidentes do Azure Sentinel após a criação do incidente SIR	Opção que permite que você use a funcionalidade de atualização automatizada de incidentes. . Microsoft Azure Sentinel o status do incidente é atualizado em Microsoft Azure incidente com os comentários após SIR o incidente é criado em ServiceNow AI Platform.
	Atualização de status de incidente inicial	Status do incidente inicial que é atualizado em Microsoft Azure Sentinel ambiente. Você pode selecionar **Novo** ou **Ativo** como o status.
	Comentários iniciais retornados para o incidente	Comentários iniciais que são publicados no incidente em Microsoft Azure Sentinel ambiente. Edite o texto padrão que é exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato"nome do campo" para qualquer campo no SIR formulário incidente.
Atualizações de fechamento de incidentes	Feche incidentes do Azure Sentinel após o fechamento do incidente SIR	Opção que permite que você use a funcionalidade de atualização automatizada de status do incidente. Microsoft Azure Sentinel os incidentes são encerrados no Microsoft Azure incidente com os comentários fornecidos após SIR o incidente está encerrado em ServiceNow AI Platform.
	Atualização de status de incidente de fechamento	Atualização de status no Microsoft Azure Sentinel incidente quando o incidente é encerrado em SIR.
	Comentários de fechamento retornados para o incidente	Comentários publicados no incidente em Microsoft Azure Sentinel incidente quando o incidente é encerrado em SIR. Edite o texto padrão que é exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato"nome do campo" para qualquer campo no SIR formulário incidente.
	Classificação de incidente e motivo do fechamento	Método para a classificação do incidente e o motivo do fechamento que é usado para fechar o incidente no Microsoft Azure Sentinel ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

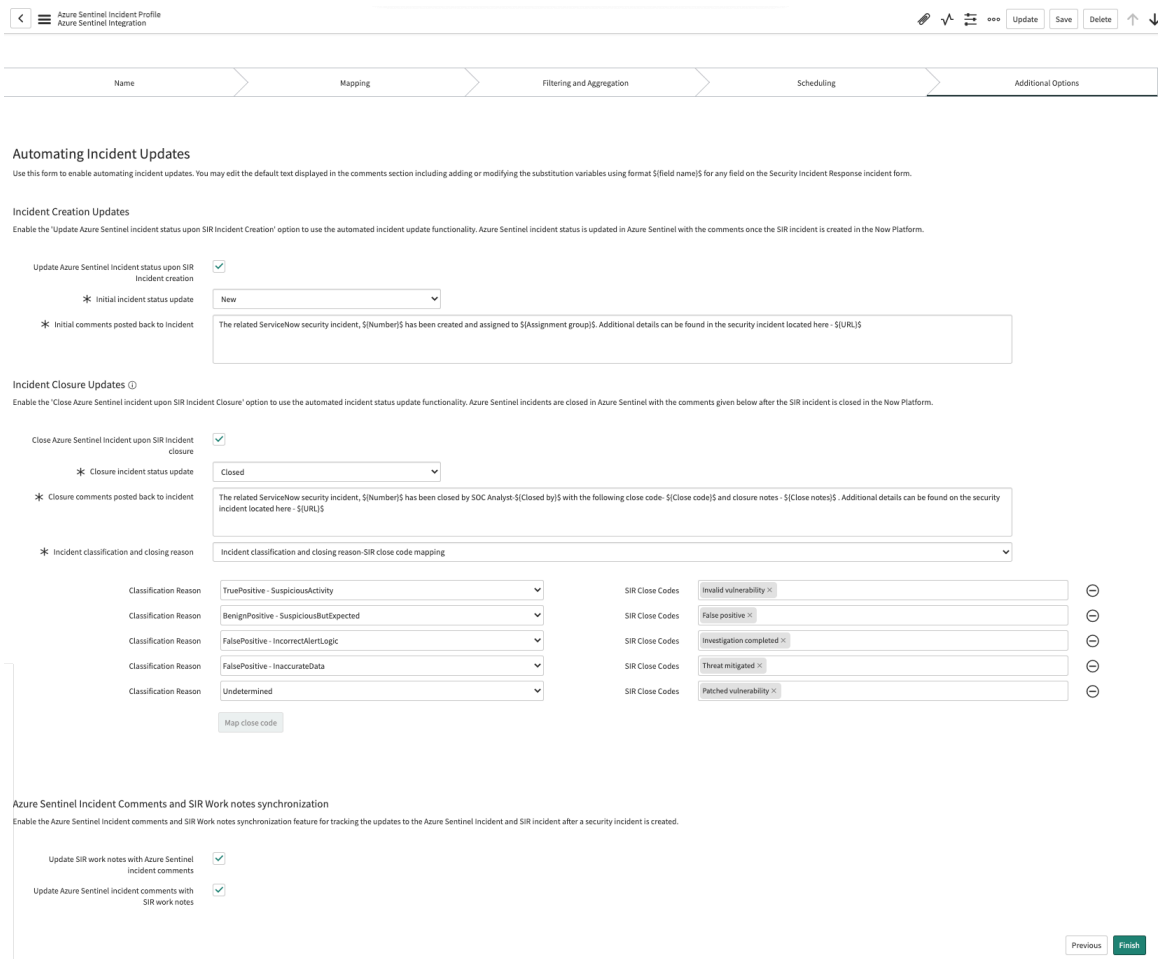
Categoria	Campo	Descrição
		Selecione **Classificação de incidente padrão e motivo de fechamento** método para fechar o incidente no Microsoft Azure Sentinel ambiente. Ao selecionar este método, você deve definir **Classificação de incidente padrão e motivo de fechamento** . Quando você fecha um incidente no SIR, o status do incidente no Azure Sentinel também é Encerrado com o especificado **Classificação de incidente padrão e motivo de fechamento** . Selecione **Mapeamento de código de fechamento do SIR de classificação de incidente e motivo de fechamento** método para fechar os incidentes e mapear os motivos da classificação com SIR códigos de fechamento. Você pode mapear vários SIR códigos de fechamento para um único motivo de classificação. Depois de fechar um incidente em SIR Usando o código de fechamento, o status do incidente no Azure Sentinel também é Encerrado com a classificação de incidente mapeada e o motivo do fechamento. Se o motivo da classificação e. SIR Códigos de fechamento não são mapeados ou uma correspondência não foi encontrada, então o incidente é encerrado usando o motivo de classificação padrão como "Indeterminado" em Microsoft Azure Sentinel ambiente.
Sincronização de Anotações de trabalho de SIR e comentários de incidente do Azure Sentinel	Atualizar anotações de trabalho SIR com comentários de incidentes do Azure Sentinel	Opção que você pode selecionar para atualizar seu Microsoft Azure Sentinel comentários em SIR anotações de trabalho. O comentário em SIR as anotações de trabalho aparecem com o prefixo `Comentário do Sentinel` . O comentário também contém o ID do Sentinel, os detalhes do analista e o carimbo de data/hora.
	Atualizar comentários de incidentes do Azure Sentinel	Opção que você pode selecionar para atualizar seu SIR anotações de trabalho

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
	com anotações de trabalho SIR	no Microsoft Azure Sentinel comentários do incidente. O comentário em Microsoft Azure Sentinel aparece com o prefixo *`Comentário da ServiceNow .`*

O exemplo a seguir mostra as opções de configuração disponíveis para automatizar atualizações de incidentes.



2. Clique em **Concluir**.

O que Fazer Depois

O perfil é movido para o estado Aguardando. Quando a mensagem de confirmação mostrar que a instalação e a configuração estão concluídas, você pode ativar o perfil.

Copie um Microsoft Azure Sentinel perfil

Copie um perfil existente e suas configurações associadas em vez de criar um perfil. Ao criar vários perfis, você pode reutilizar as configurações de um perfil existente copiando esses perfis.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

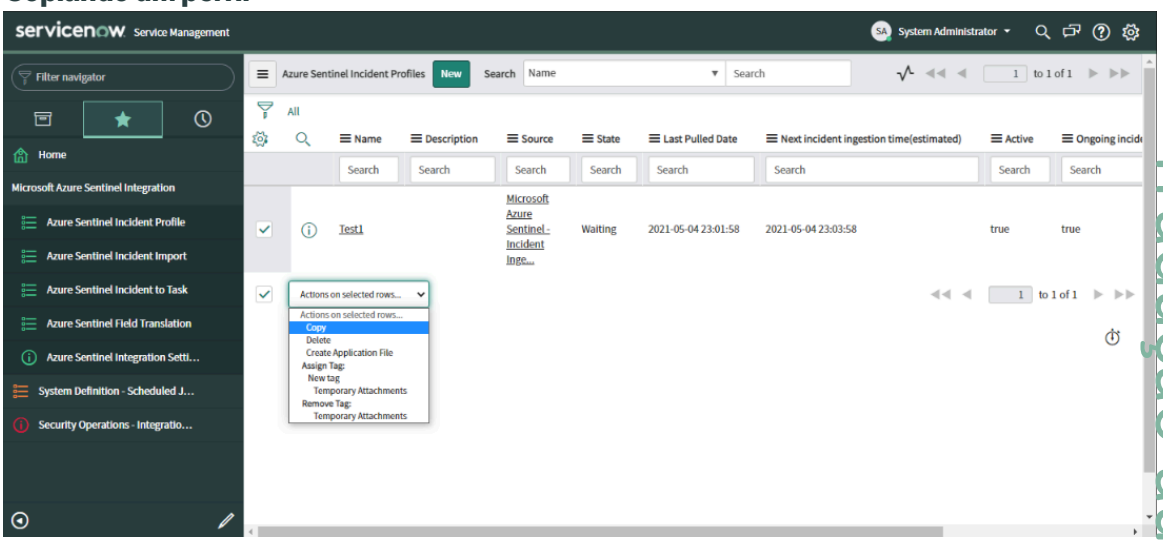
Por Que e Quando Desempenhar Esta Tarefa

Quando você copia um perfil, o nome do perfil é modificado inicialmente para evitar a criação de perfis duplicados. O perfil copiado também é desativado (definido como falso) para garantir que você não o ative acidentalmente antes de concluir a configuração. Você pode copiar os perfis e usar mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Tudo** > **Integração do Microsoft Azure Sentinel** > **Perfil do Azure Sentinel**.
2. Na lista Perfis do Azure Sentinel, selecione um perfil que você deseja copiar e, na lista Ações nas linhas selecionadas, clique em **Cópia** conforme mostrado no exemplo a seguir.

Copiando um perfil

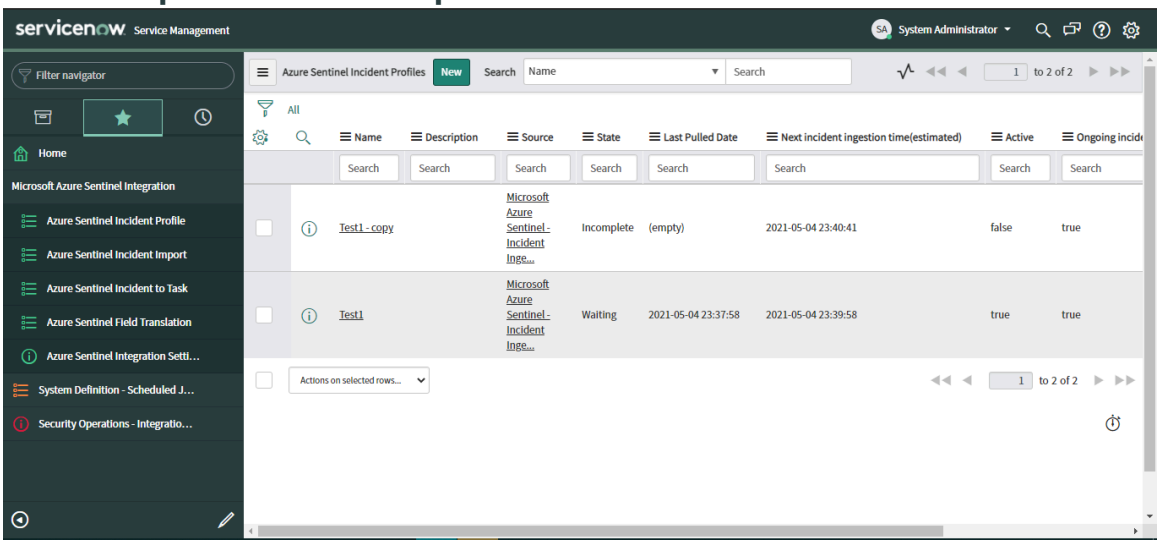


O perfil é copiado e exibido na lista, conforme mostrado no exemplo a seguir. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém a palavra "copiar". Embora o perfil original esteja habilitado (verdadeiro), a cópia está desativada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-los para que as definições de configuração se apliquem ao novo perfil conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibindo os perfis de incidente copiados



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. O status da coluna Ativo é definido como falso, o que significa que o perfil deve ser ativado.

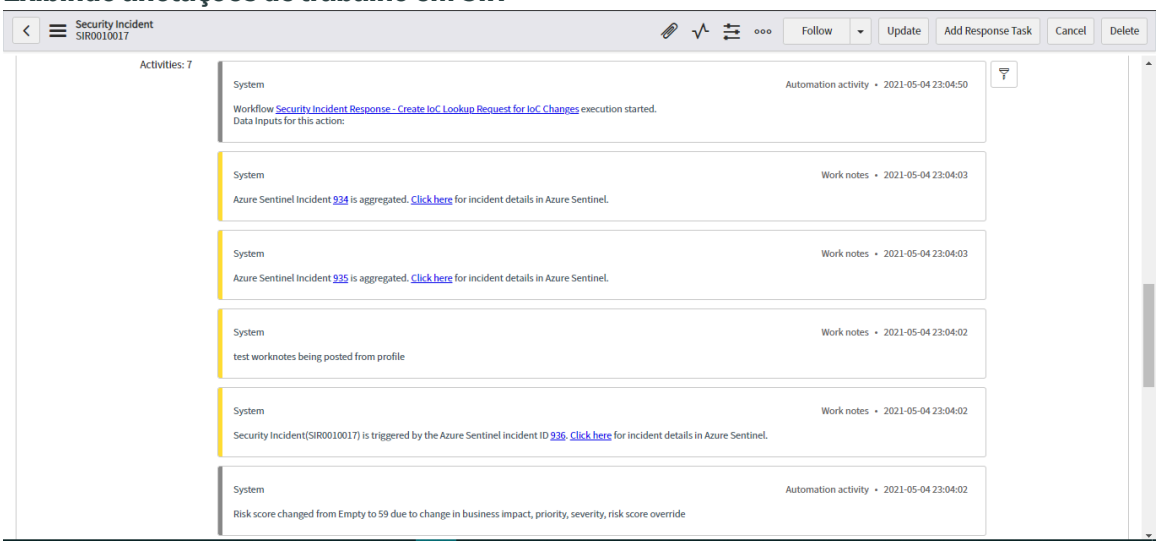
SIR formulário após uma ingestão de incidente

Após ServiceNow AI Platform ingere o. Microsoft Azure Sentinel um incidente de segurança é criado e as atualizações são feitas nesse registro de incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada quando um incidente é agregado e se você configurou o. **Anotação de trabalho em log para o novo incidente** . Critérios de agregação de incidentes . O exemplo a seguir mostra as anotações de trabalho em SIR.

Exibindo anotações de trabalho em SIR



Ao clicar no número do incidente, você pode exibir o registro de importação de incidente interno que contém os dados brutos do incidente. O exemplo a seguir mostra os dados brutos do incidente em SIR.

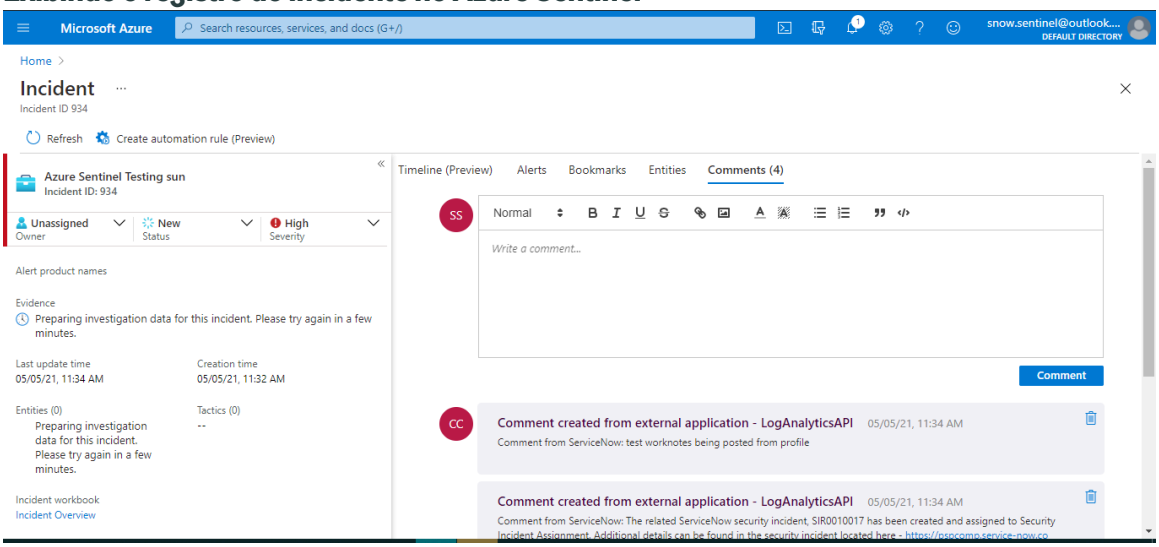
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibindo os dados brutos do incidente em SIR



Ao clicar em **Clique aqui** , você pode exibir o registro no Microsoft Azure Sentinel ambiente. O exemplo a seguir mostra o registro no Microsoft Azure Sentinel ambiente.

Exibindo o registro do incidente no Azure Sentinel

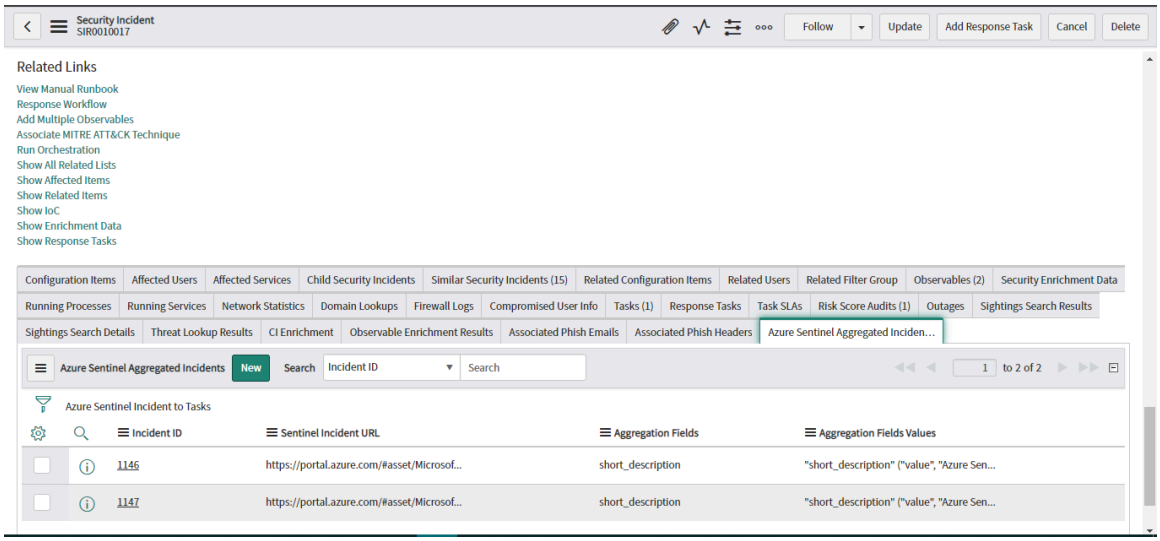


Incidentes do Sentinel agregados

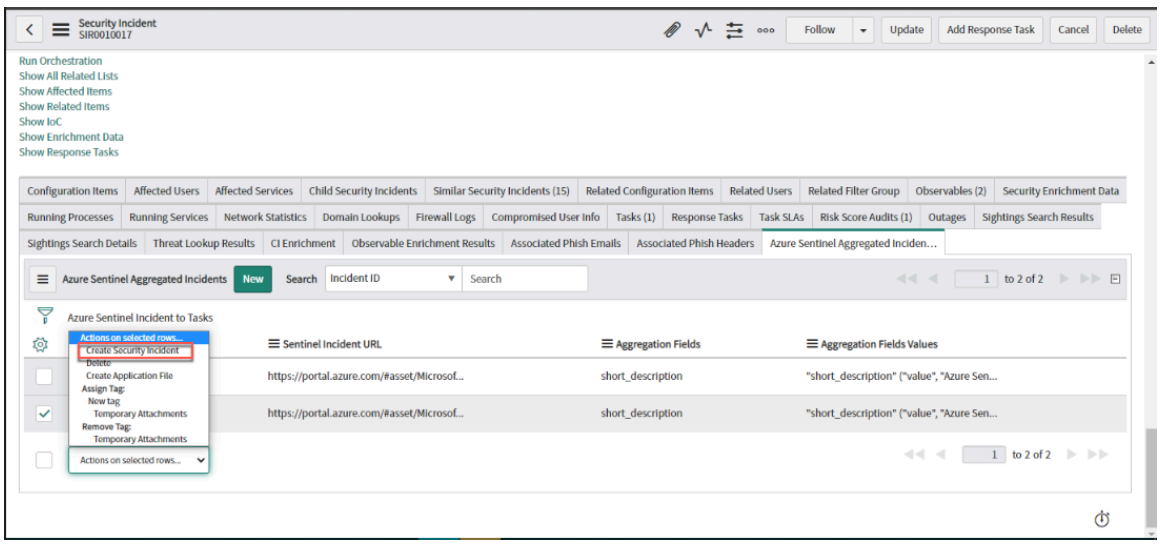
Exibir incidentes do Sentinel agregados: Exiba os incidentes agregados ao incidente de segurança. Navegar até **Mostrar todas as listas relacionadas** > **Incidentes agregados do Microsoft Azure Sentinel**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar incidente de segurança: Selecione um incidente na lista e clique em **Ações** e, em seguida, clique em **Criar incidente de segurança** . Esta opção cria um novo incidente de segurança para o incidente e este incidente é desagregado do incidente de segurança primário.



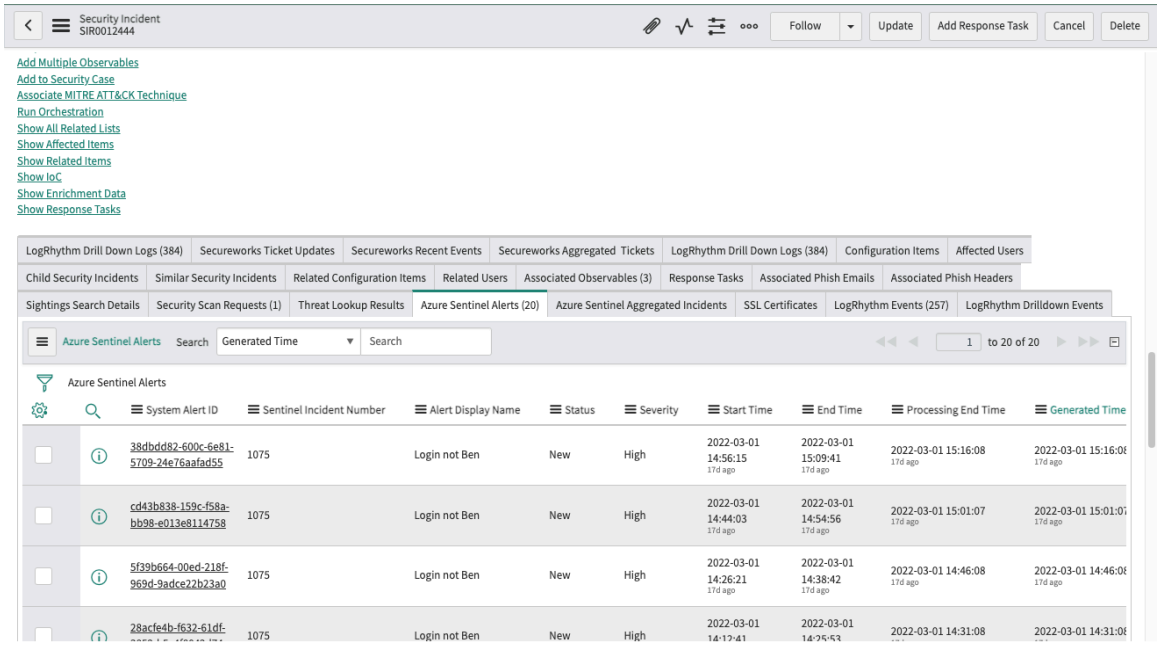
Alertas do Azure Sentinel

Para exibir os alertas associados ao Incidente Sentinel que acionou o incidente de segurança, navegue até **Mostrar todas as listas relacionadas** > **Alertas do Azure Sentinel**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alertas do Azure Sentinel



Revise Microsoft Azure Sentinel configurações de integração

Revise Microsoft Azure Sentinel configurações de integração para que você possa modificar as propriedades do sistema para se adequar ao seu ambiente.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Navegar até **Tudo** > **Integração do Microsoft Azure Sentinel** > **Configurações de integração do Azure Sentinel**.
2. Modifique as configurações a seguir conforme necessário.

Microsoft Azure Sentinel Configurações de integração

Nome da Propriedade	Descrição
Impor um limite no número de dias para os quais os dados de amostra podem ser obtidos. sn_sec_sentinel.max_num_of_days_for_sample_data	Número máximo de dias para os quais você pode buscar dados de amostra do Microsoft Azure Sentinel ambiente. Tipo: inteiro Valor padrão: 7
Receba atualizações relacionadas a novos alertas vinculados ao SIR. sn_sec_sentinel.incident_updates	Ative a opção para receber atualizações de incidentes. Tipo: booleano Valor padrão: Verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
O caractere delimitador no qual dividir os valores Microsoft Azure Sentinel mapeamentos de campo. sn_sec_sentinel.delimiter	O caractere delimitador no qual dividir os valores Microsoft Azure Sentinel mapeamentos de campo. Tipo: cadeia de caracteres Valor padrão: ', ' (vírgula com espaço)
Impor um limite no número de incidentes de amostra que podem ser obtidos. sn_sec_sentinel.max_num_of_sample_incident_per_call	Número máximo de incidentes de amostra que você busca do Microsoft Azure Sentinel ambiente para ingestão. Tipo: inteiro Valor padrão: 5 Valor máximo da amostra: 20
Impor um limite no número de incidentes sentinela que podem ser agregados a um único incidente. sn_sec_sentinel.max_aggregations_per_si	Limite de agregação de incidentes para um incidente de segurança. Por exemplo, se houver 102 incidentes, os primeiros 100 serão agregados a security incident_1 e os 2 restantes a security incident_2. Tipo: inteiro Valor padrão: 100
Impor um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_sentinel.max_si_per_day	Número máximo de incidentes de segurança que podem ser criados em um período de 24 horas no ServiceNow AI Platform. Tipo: inteiro Valor padrão: 1000
Limite máximo de paginação para buscar os dados do incidente em uma chamada REST. sn_sec_sentinel.max_page_size	Limite de paginação para buscar os dados do incidente em uma chamada REST do Microsoft Azure Sentinel ambiente. Tipo: inteiro Valor padrão: 100
Valor da versão da API para incidentes. sn_sec_sentinel.sentinel_security_incident_api_version	A versão da API da Microsoft para recuperar incidentes do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para Alertas. sn_sec_sentinel.sentinel_security_alert_api_version	A versão da API da Microsoft para recuperar alertas do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para entidades.	A versão da API da Microsoft para recuperar entidades do Sentinel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
sn_sec_sentinel.sentinel_security_entities_api_version	Valor padrão: 2021-10-01
sn_sec_sentinel.logging.detalhamento	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** Valor padrão: **informações** .

3. Clique em **Salvar**.
   Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation

Domain Separation é compatível com esta aplicação. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Microsoft Azure Sentinel integração

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função sn_si.admin no respectivo domínio.

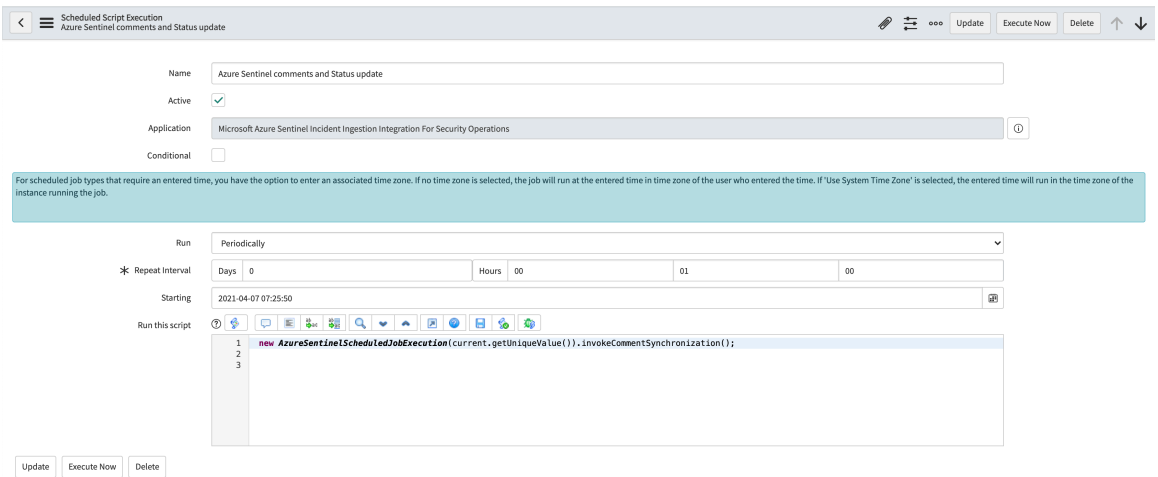
Nota: Ao criar o perfil, use o seletor de domínio para selecionar um domínio. Não crie o usuário no domínio primário e altere posteriormente o domínio do perfil. Cada domínio do seu perfil deve ter um usuário com a função sn_si.admin. Use este usuário para criar ou modificar configurações no perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desabilitar trabalhos agendados existentes.
- Replique os seguintes trabalhos agendados para cada domínio:
  - Azure Sentinel buscando alertas e entidades
  - Sincronização de comentários do Azure Sentinel
  - Atualização de status do Azure Sentinel
  - Processo de perfil do Azure Sentinel
  - Dados brutos do processo do Azure Sentinel
  - Limpeza de dados do Azure Sentinel
  - Extração de comentários históricos do Azure Sentinel
- Mude **Executar como** do usuário do sistema para o usuário com a função sn_si.admin no respectivo domínio e execute o trabalho agendado.

O exemplo a seguir mostra como replicar os comentários do Azure Sentinel e o trabalho de atualização de status e executar o trabalho como um usuário do sistema.



Tópicos relacionados

Domain Separation para provedores de serviço

Comparando Microsoft Azure Sentinel e. API de segurança do Microsoft Graph integrações com SIR

Você pode exibir as diferenças entre Microsoft Azure Sentinel e. API de segurança do Microsoft Graph e escolha a integração certa com seu ServiceNow AI Platform instância.

Visão geral Microsoft Azure Sentinel – Ingestão de incidentes

Microsoft Azure SentinelÉ uma solução de gestão de eventos de segurança da informação (SIEM) e resposta automatizada de orquestração de segurança (SOAR) baseada em nuvem. Microsoft Azure Sentinel fornece análise de segurança inteligente e inteligência contra ameaças em toda a empresa. Ele fornece uma solução única para detecção de alertas, visibilidade de ameaças, busca proativa e resposta a ameaças.

Tradução automática

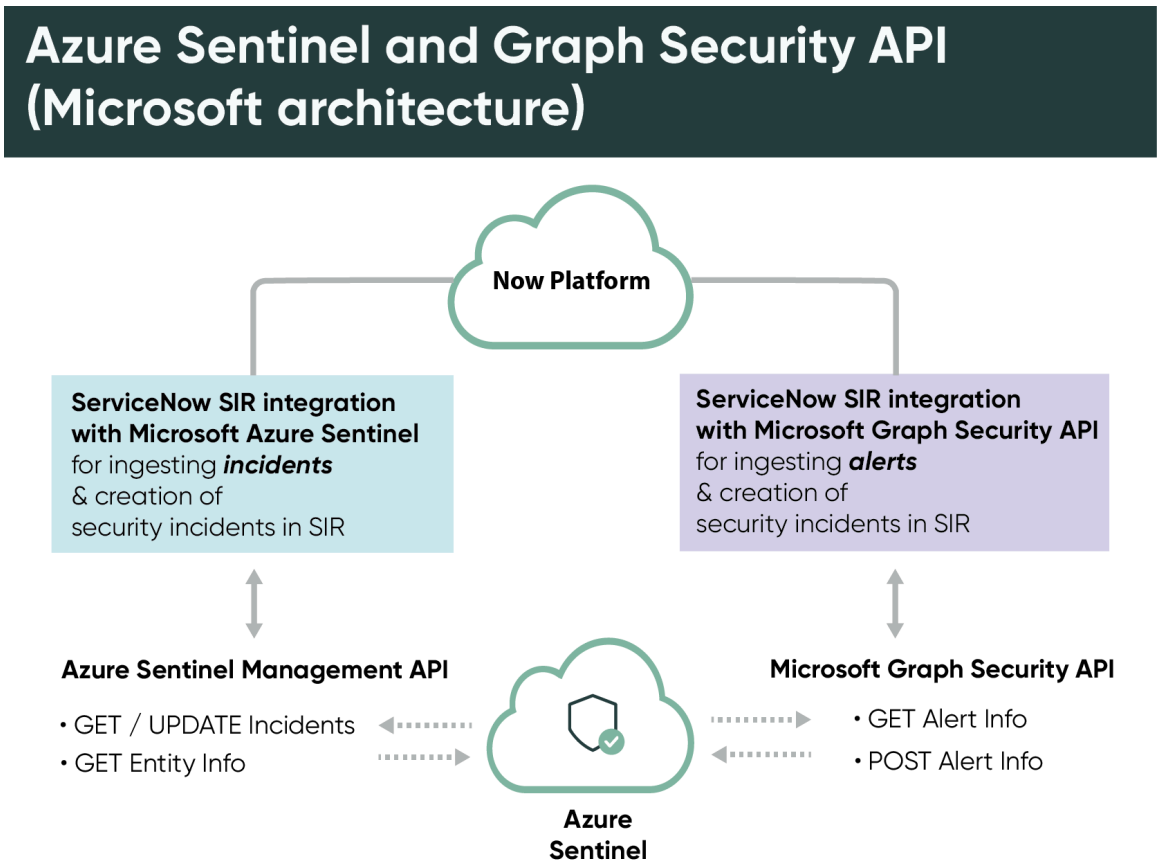
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral API de segurança do Microsoft Graph

. API de segurança do Microsoft GraphÉ um serviço intermediário (ou agente) que fornece uma interface programática única para conectar vários provedores de segurança (nativo da Microsoft, bem como ServiceNow Parceiros).

. API de segurança do Microsoft Graph a integração resolve esses problemas usando API de segurança do Microsoft Graph Para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Microsoft Defender Advanced Threat Protection e Azure Advanced Threat Protection. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente no Resposta a incidentes de segurança.

Resumo das diferenças de recursos



Microsoft Azure Sentinel vs API de segurança do Microsoft Graph

Microsoft Azure Sentinel	API de segurança do Microsoft Graph
Ingere Microsoft Azure Sentinel junto com as informações da entidade (quando disponíveis) e automatiza a criação de incidentes de segurança em SIR.	Ingere alertas de vários provedores de segurança (incluindo o Azure Sentinel) em um esquema padrão e automatiza a criação de incidentes de segurança em SIR.
Automatiza Microsoft Azure Sentinel Atualizações de status do incidente para Resposta a incidentes de segurança para que você possa criar e fechar incidentes de segurança.	Oferece suporte a atualizações de alerta (mudança de status de alerta e fechamento de alerta) para provedores de segurança selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Azure Sentinel vs API de segurança do Microsoft Graph

Microsoft Azure Sentinel	API de segurança do Microsoft Graph
Nota: ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes baseados na criação ou fechamento do incidente de segurança.	**Nota:** Para obter mais informações sobre API de segurança do Microsoft Graph provedores de segurança compatíveis, exiba Documentação da Microsoft .
Use esta integração se o seu cenário incluir as seguintes condições: • A investigação de incidente preliminar está em Microsoft Azure Sentinel e a investigação subsequente está em SIR • Ingerir Microsoft Azure Sentinel incidentes para SIR	Use esta integração se o seu cenário incluir as seguintes condições: • Execute investigação de incidente em SIR. • Ingerir Microsoft Azure Sentinel alertas em SIR. • Os incidentes não são criados em Microsoft Azure Sentinel.
Alerta é uma entidade em Microsoft Azure Sentinel. Você não pode recuperar alertas autônomos ou específicos usando Microsoft Azure Sentinel API de gestão. Você só pode recuperar os dados de alerta associados a um incidente. Os dados de alerta disponíveis usando esta integração são mais avançados do que os dados de alerta disponíveis usando o. API de segurança do Microsoft Graph.	. Microsoft Azure Sentinel dados de alerta normalizados estão disponíveis. . Microsoft Azure Sentinel campos de alerta mapeados internamente em API de segurança do Microsoft Graph e estão disponíveis em API de segurança do Microsoft Graph estão disponíveis para uso nesta integração.
	Não é possível atualizar alertas em Microsoft Azure Sentinel usando esta integração.

Microsoft Defender for Endpoint integração

. Microsoft Defender for Endpoint o permite inspecionar, analisar e conter proativamente ameaças conhecidas e desconhecidas em qualquer endpoint.

. Microsoft Defender for Endpoint A integração ajuda os analistas de segurança a investigar e corrigir incidentes de segurança com eficiência sem precisar navegar entre as ferramentas.

Você pode usar esta integração para criar configurações para recuperar os detalhes do host, detalhes dos usuários conectados, detalhes das máquinas relacionadas e outros recursos de aprimoramento. Você pode solicitar o isolamento de qualquer máquina de acessar as redes ou remover as máquinas do isolamento. As solicitações podem ser aceitas ou rejeitadas pelos aprovadores.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Microsoft Defender for Endpoint tem os seguintes recursos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Execute a Pesquisa de segurança corporativa para detectar possíveis observáveis mal-intencionados em endpoints e tomar ações de correção.
- Executar ações de resposta, como isolar host, Remover isolamento, Restringir execução de app, Executar verificação antivírus, Remover restrição de app, e Parar e colocar arquivo em quarentena.
- Criar ou atualizar indicadores.
- Realizar o aprimoramento do observável e recuperar dados relacionados aos indicadores.

Microsoft Defender for Endpoint

Explorar	Instalar	Configurar
Comece a usar o Microsoft Defender para Endpoint	Instale a aplicação e configure uma origem para a integração	Configure perfis e incidentes de segurança para o Microsoft Defender para Endpoint
Perfil de capacidade	**Configurações adicionais**	**Diversos**
Crie um perfil de capacidade para a integração do Microsoft Defender for Endpoint.	Configurações adicionais que você pode executar no Microsoft Defender para Endpoint	Crie e configure um perfil para pesquisa de vistas e indicadores com o Microsoft Defender para Endpoint.

Registre e configure o. Microsoft Defender for Endpoint em Microsoft Azure portal

Registre o. Microsoft Defender for Endpoint No portal do Microsoft Azure e conceda acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: Desenvolvedor de aplicações, administrador de locatário.

Procedimento

1. Faça login no portal do Microsoft Azure.
2. Insira Registros de aplicações Na caixa Pesquisar e clique em **Clique em Novo registro** .
3. Insira um nome para sua aplicação e o URI de redirecionamento e clique em **Registre-se** .
   Um exemplo de nome é Microsoft Defender para Endpoint . O URI de redirecionamento é usado ao fornecer consentimento do administrador para a aplicação.
4. Em **Registros de aplicações** , selecione a aplicação que você registrou na Etapa 3.
5. Em Gerenciar, selecione **Certificados e segredos** .
6. Para criar um segredo do cliente, selecione **Novo segredo do cliente** .
7. Copie o segredo do cliente e salve-o.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso você tenha esquecido o segredo do cliente, poderá gerar um novo segredo do cliente.

8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique em **Adicione uma permissão** .
10. Na janela Solicitar permissões da API, clique em **APIs que minha organização usa** guia.
11. PESQUISE e selecione **WindowsDefenderATP** .
12. Em Permissões WindowsDefenderATP, selecione **Permissões da aplicação** .
    Habilitar esta permissão garante que a aplicação seja executada como um serviço em segundo plano ou daemon sem um usuário conectado.
13. Adicione as seguintes permissões no nível da aplicação e conceda o consentimento do administrador para as permissões de API recém-adicionadas.

Permissão	Nome de exibição da permissão
Ler.Tudo.Máquina	Leia todos os perfis de máquina
User.Read.All	Ler perfis de usuário
Máquina.Isolar	Isolar máquina
Execução.RestrictExecution	Restringir execução de código
Machine.Scan	Máquina de verificação
ParoeQuarentena	Parar e colocar em quarentena
URL.Ler.Tudo	URLs de Leitura
Arquivo.Read.All	Perfis de arquivo de leitura
Read.All.IP	Perfis de endereço IP de leitura
ReadWrite.All	Indicadores de leitura e gravação

Comece a usar Microsoft Defender for Endpoint integração

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar o. Microsoft Defender for Endpoint Da ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform E Resposta a incidentes de segurança (SIR).	As seguintes funções são necessárias: 1. Você deve ter a função de administrador do sistema (administrador) para instalar a aplicação para a integração. 2. Você deve ter a função de administrador de incidentes de segurança (sn_si.admin) para configurar a integração, criar, ativar e remover perfis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	3. Você deve ter a função de analista de incidentes de segurança (sn_si.analyst) para trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer um dos recursos disponíveis na integração.
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação uma de cada vez na seguinte ordem para garantir uma instalação tranquila: 1. Resposta a incidentes de segurança 2. Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) 3. Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las de volta à rede e executar ações adicionais no endpoint. Se sua organização quiser um nível extra de controle sobre essas ações, habilite a opção Exigir aprovação durante a configuração dos perfis. Em um cenário em que o perfil está disponível, a configuração de perfil para aprovação tem precedência. Em um cenário em que o perfil não está disponível, as aprovações são tratadas com base nas configurações padrão. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um grupo de aprovação deve estar disponível na lista Grupos em sua instância. Para monitorar e processar solicitações enviadas pelos usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações no ServiceNow AI Platform®. Como alternativa, os aprovadores podem encontrar as solicitações enviadas exclusivamente para Microsoft Defender for Endpoint Integração no módulo Aprovações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre como criar um grupo de usuários, consulte Crie um grupo de usuários .

O que Fazer Depois

Você configurou com sucesso seu ServiceNow AI Platform® instância do Microsoft Defender for Endpoint integração. A próxima etapa é instalar o. Microsoft Defender for Endpoint Aplicação da ServiceNow Store para a integração.

Instale a aplicação e configure Microsoft Defender for Endpoint integração

Instale e configure o. Microsoft Defender for Endpoint integração do ServiceNow Store em seu ServiceNow AI Platform instância. Comece a criar perfis de capacidade usando as configurações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe a integração do Microsoft Defender para Endpoint do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE o bloco Microsoft Defender para Endpoint e clique em **Configurar** .
4. No formulário, preencha os campos a seguir.

Configure o Microsoft Defender para Endpoint

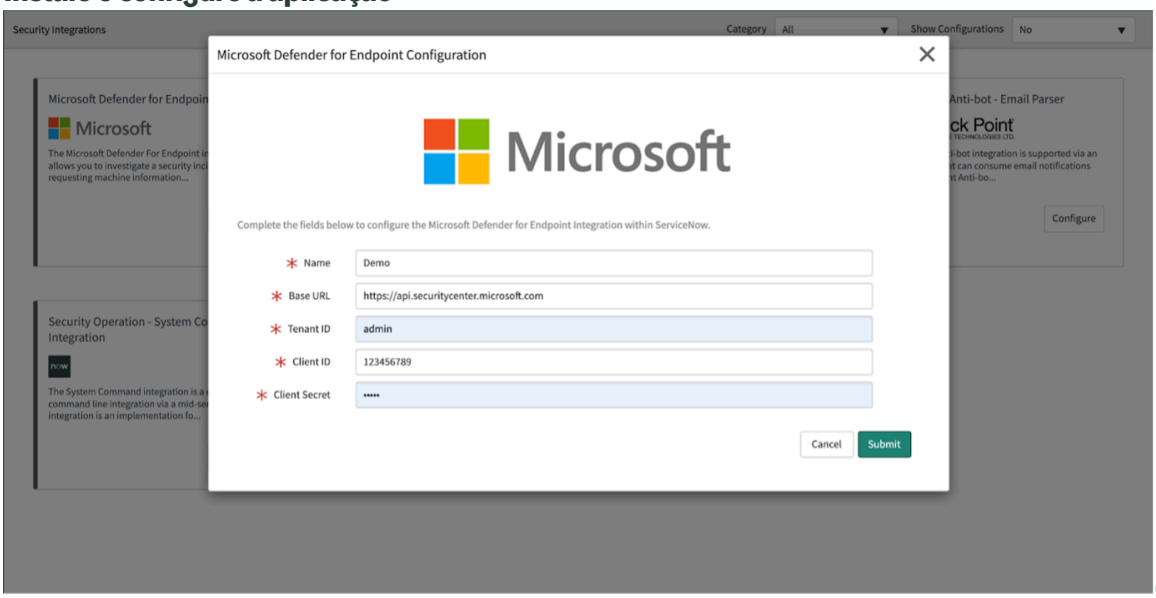
Nome	Nome do Microsoft Defender for Endpoint configuração da instância.
URL base	O URL da base de serviço para Microsoft Defender for Endpoint
ID de locatário	. Microsoft Defender for Endpoint ID do locatário. Todas as ações seriam executadas nesta instância.
ID de cliente	ID do cliente da aplicação que você registrou no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente para sua aplicação registrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.

Instale e configure a aplicação



Resultado

. Microsoft Defender for Endpoint a lista de configurações é exibida com seu novo registro de configuração. Você concluiu a configuração do Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint Configurações padrão

Há definições de configuração adicionais que você deve executar depois de concluir a instalação.

Depois de concluir a instalação, você pode encontrar o módulo Configurações padrão em Microsoft Defender for Endpoint no painel de navegação esquerdo. Ele contém as configurações padrão para diferentes Microsoft Defender for Endpoint funcionalidades.

Funções necessárias: sn_si.admin, sn_si.analyst (somente leitura).

Configurações adicionais

As definições de configuração adicionais são apresentadas a seguir:

- **Aprovação** : Esta aprovação é especificamente para a ação Isolar host, Remover isolamento de host e ações adicionais, como Restringir execução de app, Remover restrição de app e Executar verificação antivírus. Você pode usar esta aprovação somente quando as ações são acionadas diretamente da lista relacionada e se não houver perfis existentes. Se houver perfis existentes para esses recursos, a configuração de aprovação no perfil terá precedência.
  - **Aprovação necessária** : Quando você habilita **Aprovação necessária** , O campo Aprovadores está disponível no formulário.
  - **Aprovadores** : Lista de grupos de aprovadores. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.
- **IC alternativo** Habilitar esta caixa de seleção fornece a lista de campos disponíveis para passar um IC alternativo para a capacidade. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente ao recurso Executar ações adicionais no endpoint. Use esta configuração para definir um campo de entrada de IC alternativo para o recurso Executar ações adicionais somente

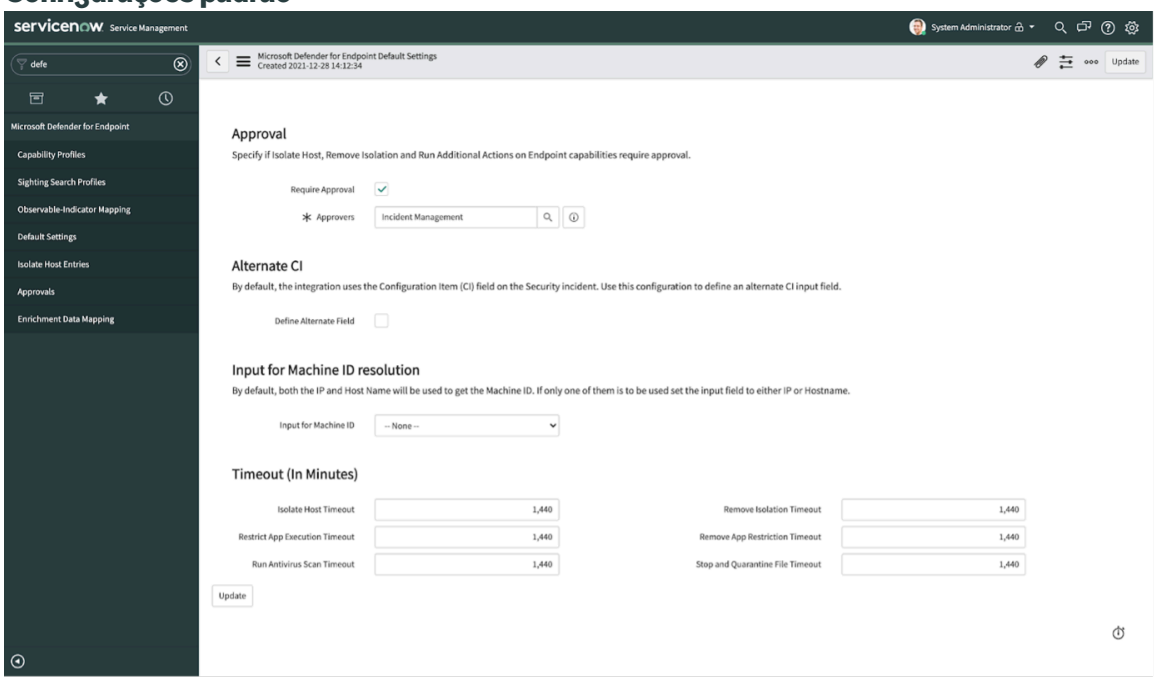
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no endpoint. Para os outros recursos, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, os recursos usarão o campo IC do formulário Incidente de segurança.

- **Entrada para resolução do ID do agente** : Por padrão, o IP e o nome do host são usados para obter o ID do agente. Se você for usar apenas um deles, defina o campo de entrada como IP ou Nome do host.
- **Tempo limite** :
  - **Isolar tempo limite do host (em minutos):** Indica o limite de execução para os recursos Isolar host.
  - **Remover tempo limite de isolamento (em minutos):** Indica o limite de execução do recurso Remover tempo limite de isolamento.
  - **Restringir tempo limite de execução da aplicação (em minutos):** Indica o limite de execução para o recurso Restringir execução de apps.
  - **Remover tempo limite de restrição do app (em minutos):** Indica o limite de execução do recurso Remover restrição de app.
  - **Tempo limite de execução da verificação antivírus (em minutos):** Indica o limite de execução do recurso Executar verificação antivírus.
  - **Parar e colocar em quarentena tempo limite do arquivo (em minutos):** Indica o limite de execução para o recurso Interromper arquivo e quarentena.

Configurações padrão



Mapeie o. Microsoft Defender for Endpoint tipos de indicador

Mapeie o tipo de observável da ServiceNow com Microsoft Defender for Endpoint tipo de indicador. Este mapeamento seria usado no aprimoramento do observável e em Criar ações de indicador no Microsoft Defender.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst (somente leitura)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

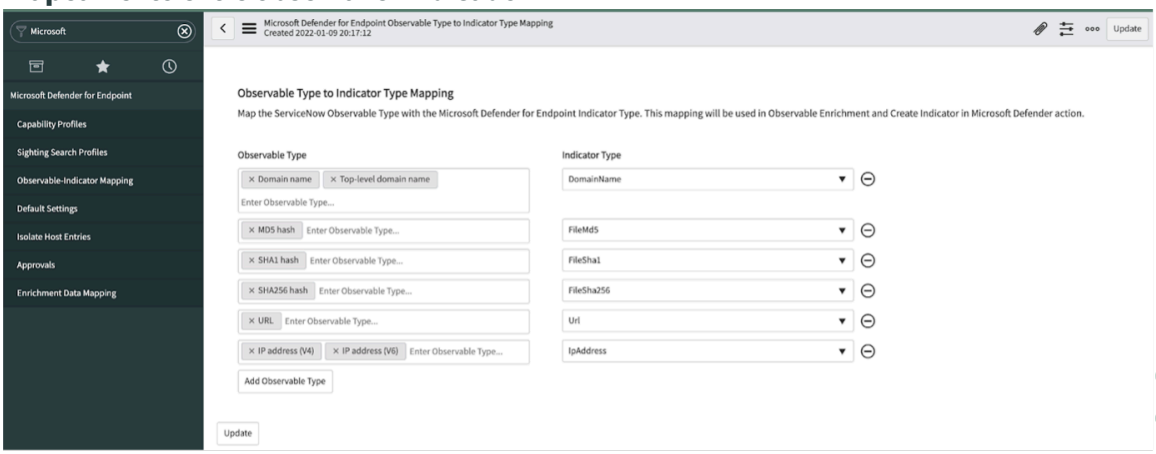
Por Que e Quando Desempenhar Esta Tarefa

Em um cenário em que o tipo de observável não é mapeado para um tipo de indicador, esses observáveis não estão qualificados para aprimoramento de observável e criação de indicador no Microsoft Defender for Endpoint.

Procedimento

1. Navegar até **Endpoint do Microsoft Defender** > **Mapeamento entre observável-indicador**.

Mapeamento entre observável-indicador



2. Adicione ou atualize um tipo de observável de uma das seguintes maneiras:
   - Para adicionar um novo mapeamento, clique em **Adicionar tipo de observável** .
   - Para atualizar o observável para o mapeamento do tipo de indicador, clique em qualquer linha existente.
3. Para salvar o mapeamento, clique em **Atualização** .

Crie um perfil de capacidade para Microsoft Defender for Endpoint integração

Crie um perfil e selecione Microsoft Defender for Endpoint capacidades que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Os perfis são criados para agrupar ou agrupar os recursos, o que ajudaria os analistas a executar a investigação ou correção facilmente. Você pode adicionar os seguintes recursos ao perfil:

- Obter detalhes do host
- Obter usuários conectados
- Isolar Host
- Remover isolamento

Você não pode associar os recursos Isolar host e Remover isolamento de host com outros recursos ao criar um perfil. Os perfis para esses recursos precisam ser criados individualmente. Por outro lado, os recursos Obter detalhes do host e Obter usuários conectados podem ser agrupados. Você pode criar perfis individualmente ou clubbing-los em cheio ou em partes conforme sua exigência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

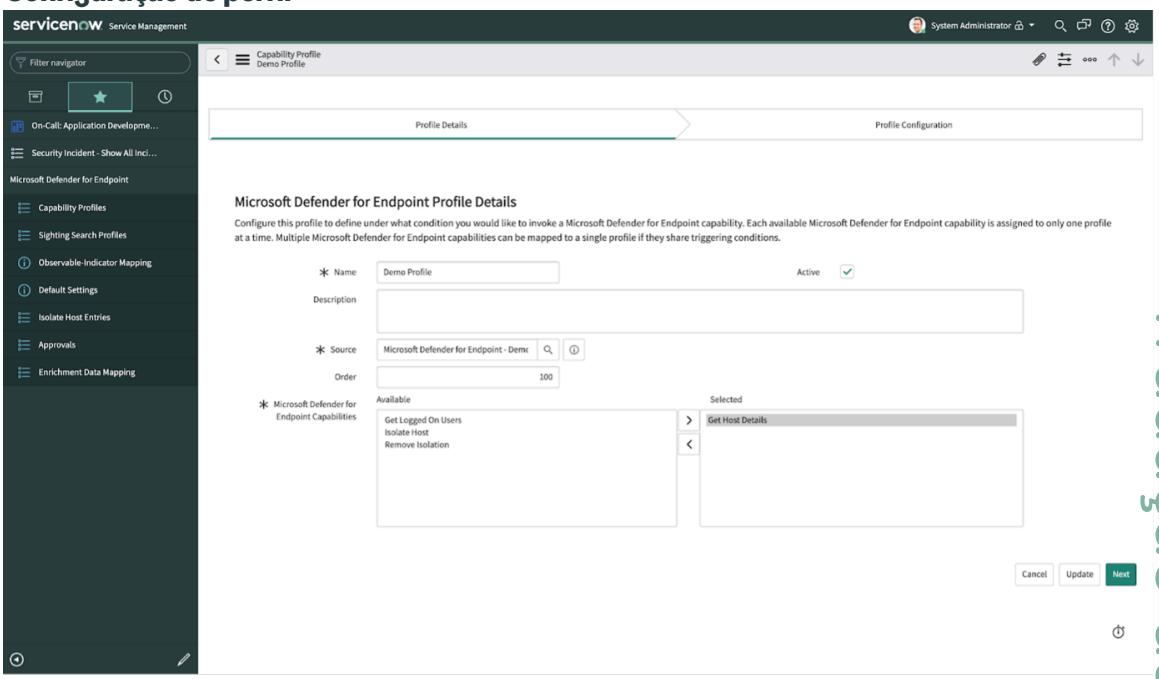
Nota: Depois que uma capacidade é incluída em um perfil, ela não pode ser incluída em nenhum outro perfil da mesma origem.

Procedimento

1. Navegar até **Endpoint do Microsoft Defender** > **Perfis de capacidade**.

   A lista de perfis de capacidade do Microsoft Defender para endpoint é exibida.

Configuração de perfil



2. Clique **Novo(a)**.
3. No formulário, preencha os campos.

Formulário Perfil de capacidade

Campo	Descrição
Nome	Nome do Microsoft Defender for Endpoint perfil de capacidade. Este nome ajuda a identificar o tipo de perfil e descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome do Microsoft Defender for Endpoint origem. Somente fontes configuradas estão disponíveis na lista.
Microsoft Defender para recursos de endpoint	Recursos do Microsoft Defender for Endpoint perfil. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Opção para indicar que o perfil está ativo. Após o perfil está ativo, o perfil é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem especificadas na configuração.

4. Para continuar para a Configuração de perfil, clique em **Próxima**.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, você pode preferir revisar os perfis de como e as condições de acionamento e configuração. Para obter mais informações, consulte Acionar condições em um item de configuração.

Acionar condições em um item de configuração

Depois de criar um perfil e selecionar Microsoft Defender for Endpoint recursos que você deseja que o perfil execute, defina as configurações do perfil para que o perfil seja executado somente quando um conjunto de condições específicas for atendido.

Como acionar condições em um item de configuração

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança for criado que corresponda à condição do gatilho. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados manualmente clicando no formulário Executar perfil(s) EDR no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no ServiceNow AI Platform Configuration Management Database (CMDB). Quando um incidente de segurança é criado e um perfil é executado automaticamente ou manualmente, o. CMDBÉ pesquisado para recuperar o nome do host ou o endereço IP com base no valor do campo IC. O nome do host ou IP é usado para resolver o ID do agente em Microsoft Defender for Endpoint para identificar o endpoint.

Em um cenário ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do Microsoft Defender for Endpoint console para o ativo correspondente. Os dados de vários recursos são extraídos para seu ServiceNow AI Platform Configuration Management Database (CMDB) e exibidos nas listas relacionadas de um incidente de segurança. Quando o campo Item de configuração (IC) não é preenchido no incidente de segurança com um nome de host com ou um endereço IP que corresponda ao banco de dados, você pode selecionar um campo alternativo no incidente de segurança que contém o nome do host ou o IP para executar a resolução do ID do agente.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação de endpoint para garantir que você possa identificar o endpoint em Microsoft Defender for Endpoint. Você pode selecionar qualquer campo no incidente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que seus perfis sejam executados mesmo que o campo IC não esteja preenchido no incidente de segurança associado na criação do incidente.

Nota: Os campos de IC alternativos são considerados somente para recursos que podem ser adicionados a um perfil. Esses recursos incluem Obter detalhes do host, Obter usuários conectados, Isolar host e Remover isolamento. Para todas as ações adicionais, o IC alternativo deve ser configurado no módulo Configurações padrão.

Configure perfis e incidentes de segurança para Microsoft Defender for Endpoint integração

Crie um perfil e selecione Microsoft Defender for Endpoint capacidades que você deseja que o perfil execute. Você precisa definir as configurações para que o perfil possa ser acionado somente sob as condições definidas.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Se necessário, você pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atenda às condições do gatilho for criado.

Nota: Você pode navegar até a página Configuração do perfil somente depois de inserir a página Detalhes do perfil.

Procedimento

1. Navegar até **Endpoint do Microsoft Defender** > **Perfis de capacidade**.
2. Depois de concluir a seção Detalhes do perfil, clique em **Próxima**.
   Revise e configure as seções.
3. Na seção Definir critérios de incidente (automação), selecione **Definir critérios de incidente** opção para acionar automaticamente Microsoft Defender for Endpoint recursos no perfil.
   Definir critérios de incidente (automação) : Defina as condições de incidente de segurança que acionariam automaticamente os recursos do Microsoft Defender para Endpoint para o perfil. Se você não selecionar **Definir critérios de incidente** , o perfil e os recursos subjacentes podem ser invocados manualmente a partir do incidente de segurança.

   Nota: Isolar host e remover os recursos de isolamento de host não podem ser acionados automaticamente.

   a. Em **Condições de filtro** , selecione o campo necessário.
   b. Adicionar **Novos critérios** e também definem **OU** ou **E.** condição.
4. Na seção Aprovações, selecione **Aprovação necessária** caixa de seleção para fornecer um nível extra de controle.

   Se você selecionar esta opção, terá mais controle ao usar os recursos do Microsoft Defender for Endpoint para isolar máquinas host, restaurá-las para a rede e obter arquivos.

   A opção Aprovações na configuração do perfil aparece somente para os recursos Isolar host e Remover isolamento de host, respectivamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na seção Configuração adicional, selecione **Definir campo alternativo** opção para definir um campo de entrada alternativo.
   Configuração adicional : Quando o campo Item de configuração (IC) não é preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você pode selecionar um campo alternativo no incidente de segurança para consultar o Microsoft Defender para APIs de endpoint.

   Nota: Para obter mais informações, consulte Acionar condições em um item de configuração.

   a. Selecione **Definir campo alternativo** opção.

   b. Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.

6. Na seção Marcadores, selecione **Marcador de exibição** para habilitar a marcação de incidentes de segurança, o nome do perfil é prefixado na habilitação do marcador.

   Opcionalmente, você pode marcar incidentes de segurança com marcadores para marcadores de perfil iniciado, perfil concluído e perfil com falha. Por padrão, esta opção está desativada para todos os perfis.

7. Clique **Concluído**.

Verifique os Filtros de condição do gatilho

Valide o perfil e verifique se os filtros de condição do gatilho configurados estão funcionando conforme o esperado.

Antes de Iniciar
Função necessária: sn_si.admin ou sn_si.analyst

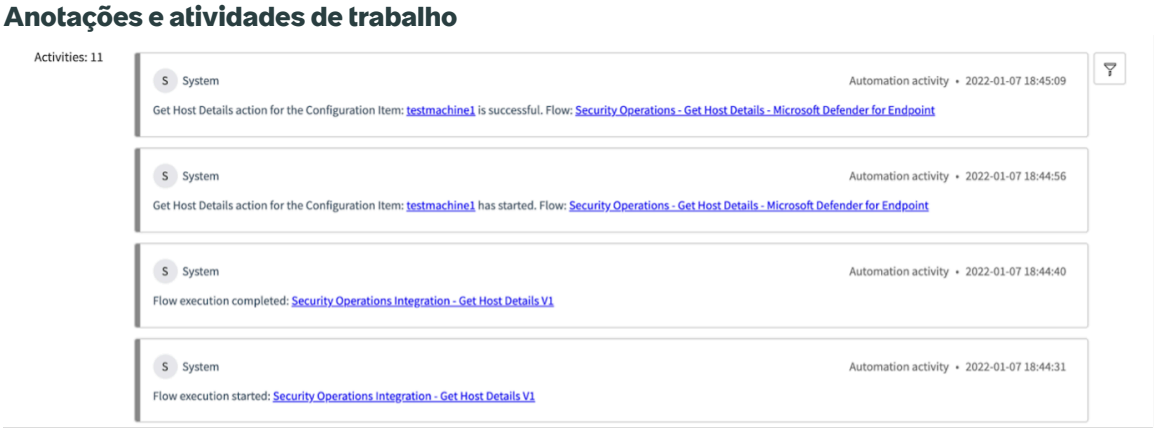
Por Que e Quando Desempenhar Esta Tarefa
Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta no ServiceNow AI Platform® incidentes de segurança.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Para criar um novo incidente de segurança, selecione **Novo(a)**.
3. Para acionar o respectivo perfil, forneça as condições de filtro conforme fornecidas no perfil de capacidade.
4. Clique **Salvar**.
5. Para validar a seção Anotações de trabalho e atividades, exiba e verifique os registros marcados com os marcadores de perfil iniciado, perfil concluído ou perfil com falha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Para validar todos os dados nas listas relacionadas, clique em **Mostrar todas as listas relacionadas** .
7. Clique em Qualquer **Lista relacionada** para validar os detalhes.
   Por exemplo, Detalhes do host.

Acionar o. Microsoft Defender for Endpoint Recursos de links relacionados

Acionar um perfil de capacidade manualmente depois de revisar um incidente de segurança a partir de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Além de executar o perfil para o IC ou o IC alternativo do incidente de segurança, você também pode executar o perfil para valores de IC presentes na lista relacionada Item de configuração selecionando **Incluir IC relacionado** na caixa de diálogo. Também recupera os dados dos valores de IC presentes na lista relacionada. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

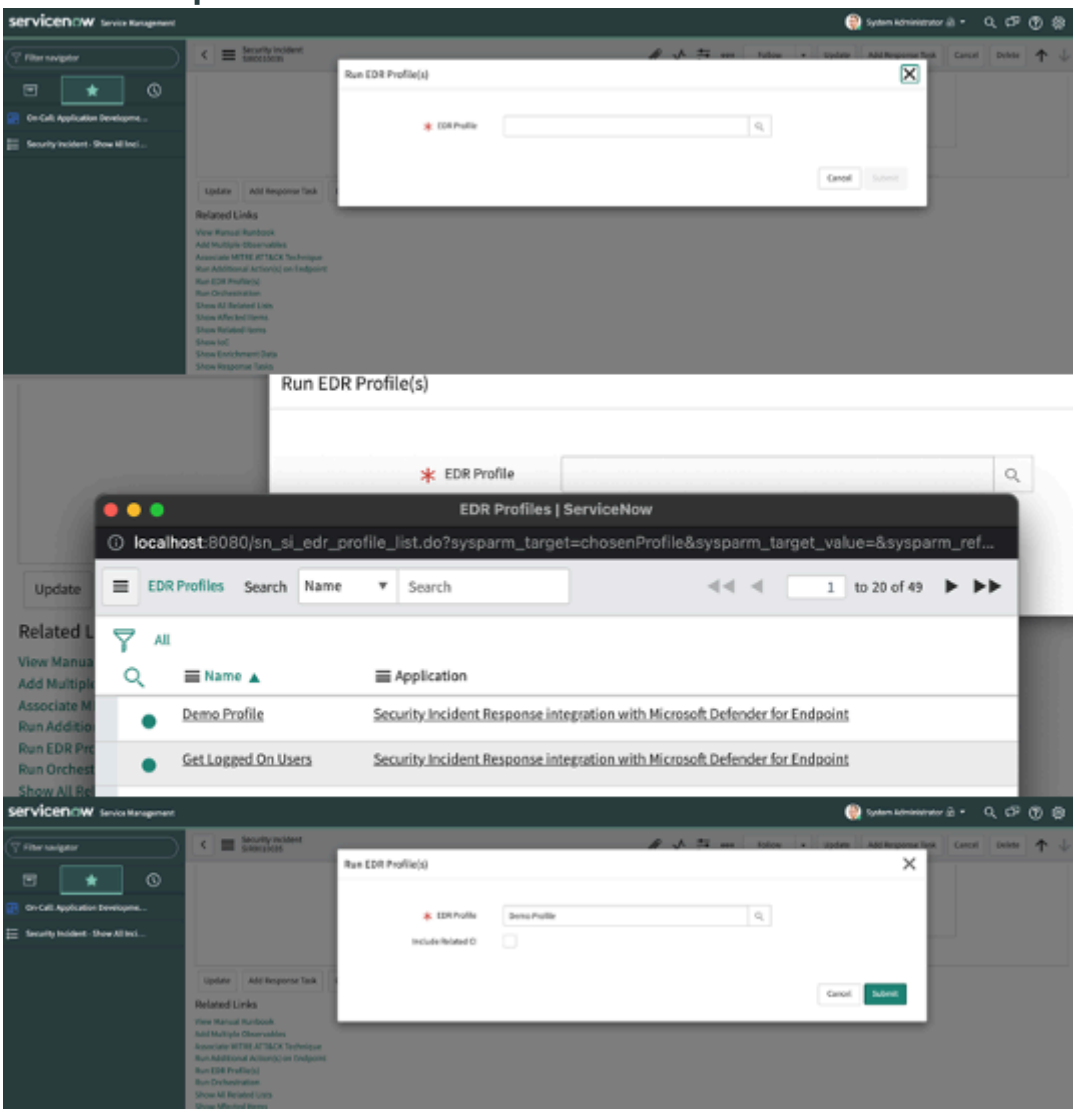
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com Microsoft Defender for Endpoint informações.
3. Na seção Links relacionados, clique em **Executar perfil(s) EDR** .
4. Procure e selecione um perfil na lista de perfis disponíveis e clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecionar um perfil



O perfil selecionado é acionado manualmente.

5. Valide a seção Anotações de trabalho e atividades.
6. Exiba os marcadores e valide os dados nas listas relacionadas.

Acionar o. Microsoft Defender for Endpoint Da lista relacionada Item de configuração

Acionar um perfil de capacidade manualmente na lista relacionada do item de configuração.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com Microsoft Defender for Endpoint informações.
3. Clique **Mostrar todas as listas relacionadas**.
4. Clique na lista relacionada Item de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os itens de configuração adicionados.
6. Em **Ações** nas linhas selecionadas, selecione uma capacidade.
   A capacidade selecionada é acionada manualmente.
7. Valide a seção Anotações de trabalho e atividades.
8. Exiba os marcadores e valide os dados nas listas relacionadas.

Configurações adicionais em Microsoft Defender for Endpoint

. Microsoft Defender for Endpoint a integração oferece suporte à execução de ações adicionais além das ações padrão.

. Microsoft Defender for Endpoint o oferece suporte às seguintes configurações adicionais:

Isolar capacidade de host em Microsoft Defender for Endpoint

Isole o host de acessar a rede no Microsoft Defender for Endpoint com base na gravidade do ataque. Isolar o host da rede permite que você evite outras atividades mal-intencionadas ou possíveis ataques a outros hosts.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para isolar capacidade de host

Capacidade	Necessários	Descrição
Isolar Host	Tipo de isolamento	(Obrigatório) Tipo de isolamento (completo ou seletivo).
	Comentário	(Obrigatório) Comentário a ser associado à ação.

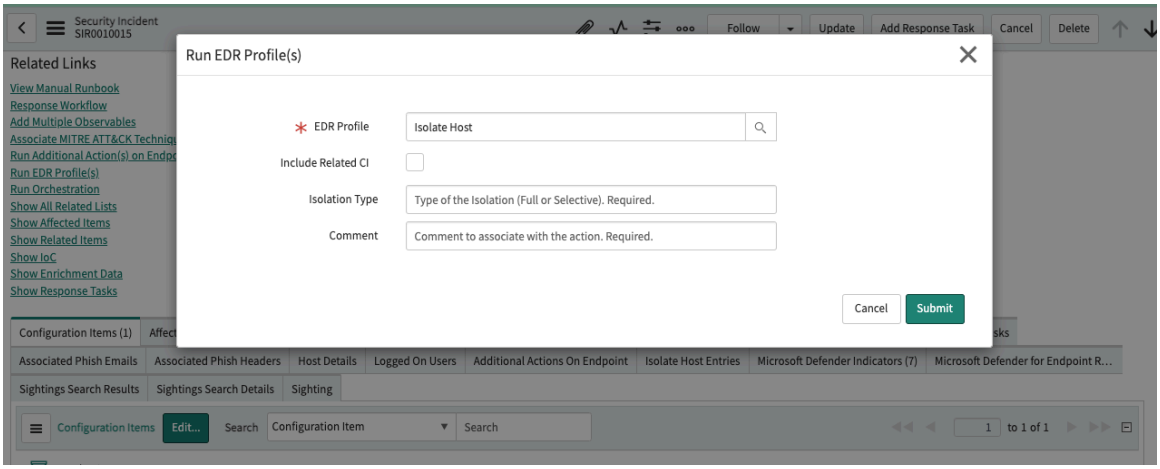
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(s) EDR** .
4. Procure e selecione um perfil com **Isolar capacidade do host** selecionado na lista de perfis disponíveis e clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isolar Host



Como alternativa, você pode executar as seguintes etapas:

a. Na seção Listas relacionadas, clique em **Mostrar todas as listas relacionadas** .

b. Clique em **Item de configuração** lista relacionada.

c. Selecione **Isolar host** e selecione os recursos correspondentes.

5. Valide a atividade de automação e a seção Atividades e certifique-se de que os dados estejam conforme o esperado.
6. Exiba os dados e valide os detalhes do isolar host nas listas relacionadas.

Configurar Remover recurso de isolamento de host em Microsoft Defender for Endpoint

Se necessário, remova o isolamento de um host que foi isolado anteriormente da rede em Microsoft Defender for Endpoint. Você pode impedir outras atividades mal-intencionadas ou possíveis ataques a outros hosts.

Antes de Iniciar

Requisitos para Remover capacidade de isolamento

Capacidade	Entrada necessária	Descrição
Remover isolamento	Comentário	(Obrigatório) Comentário a ser associado à ação.

Função necessária: sn_si.admin ou sn_si.analyst

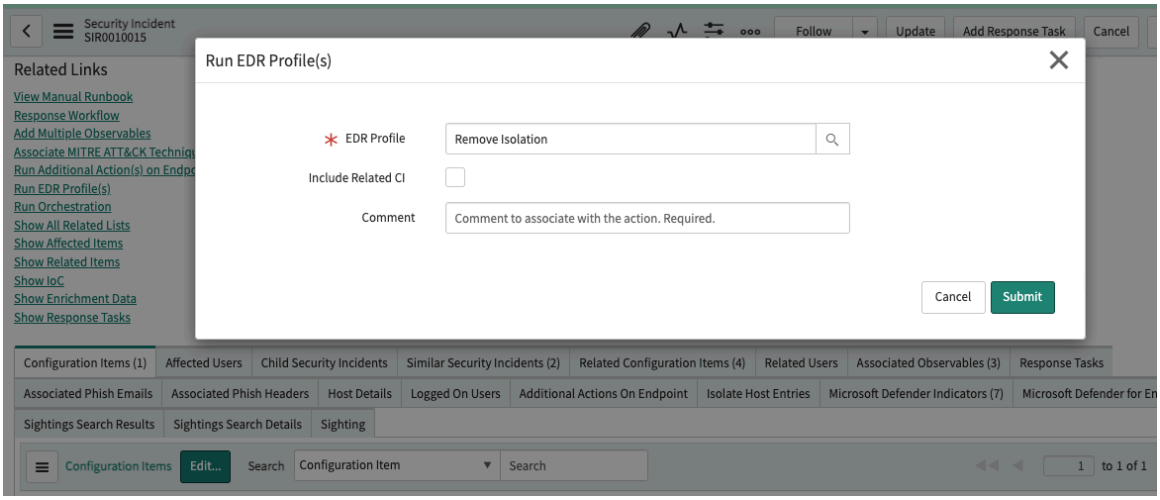
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(s) EDR** .
4. Procure e selecione um perfil com **Remover capacidade de isolamento** selecionado na lista de perfis disponíveis e clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Remover isolamento



Como alternativa, você pode executar as seguintes etapas:

a. Clique em **Mostrar todas as listas relacionadas** na seção listas relacionadas.

b. Clique em **Item de configuração** lista relacionada.

c. Selecione **Remover isolamento** e selecione os recursos correspondentes.

5. Valide a atividade de automação e a seção Atividades.
6. Exiba os dados e valide os detalhes do isolar host nas listas relacionadas.
7. Valide as atividades de automação da execução.

Configurar o recurso Executar verificação antivírus em Microsoft Defender for Endpoint

Inicie remotamente uma verificação antivírus para ajudar a identificar e corrigir malware que possa estar presente em um dispositivo comprometido. Execute a verificação como parte do processo de investigação ou resposta.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para Executar recurso de verificação antivírus

Entrada	Descrição
Tipo de Verificação	(Obrigatório) Tipo de verificação (Completa ou Rápida).
Comentário	(Obrigatório) Comentário a ser associado à ação.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.

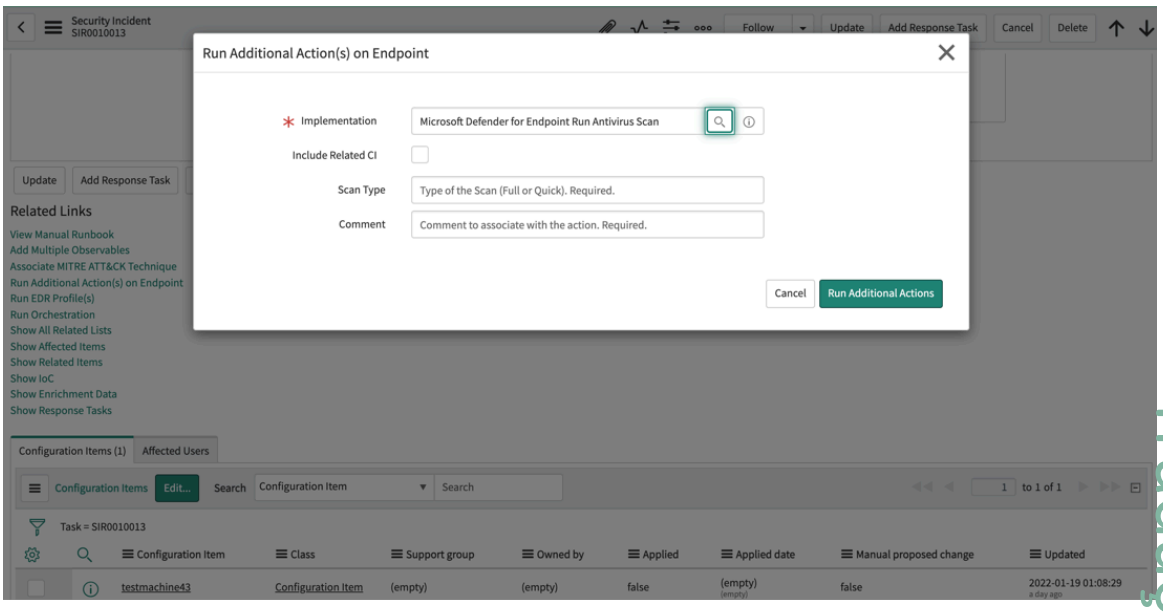
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint**.

b. Procure e selecione a capacidade necessária.
Por exemplo, clique em **Execute a verificação antivírus** capacidade.

Executar a varredura antivírus



Como alternativa, você pode executar as seguintes etapas:

a. Na seção Listas relacionadas, clique em **Mostrar todas as listas relacionadas** .

b. Clique em **Item de configuração** lista relacionada.

c. Selecione os itens de configuração adicionados e, em Ações nas linhas selecionadas, selecione **Executar ações adicionais no endpoint** .

Depois de selecionar **Execute a verificação antivírus** implementação de capacidade, o. **Tipo de verificação adicional** e. **Entrada de comentário** os campos são exibidos.

3. Selecione **Tipo de verificação** Que você deseja executar (Rápido ou Completo) e adicione um comentário antes de executar a verificação.
4. Para iniciar a verificação antivírus, clique em **Executar ação adicional** .
5. Exiba as atividades de automação da execução e valide-as.
6. Valide o status da ação nas listas relacionadas Ações adicionais no endpoint.

Configurar o recurso Restringir execução de apps em Microsoft Defender for Endpoint

Para conter um ataque, restrinja ou bloqueie um dispositivo e impeça a execução de tentativas subsequentes de programas potencialmente mal-intencionados.

Antes de Iniciar

Requisitos para restringir a capacidade de execução do app

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Função necessária: sn_si.admin ou sn_si.analyst

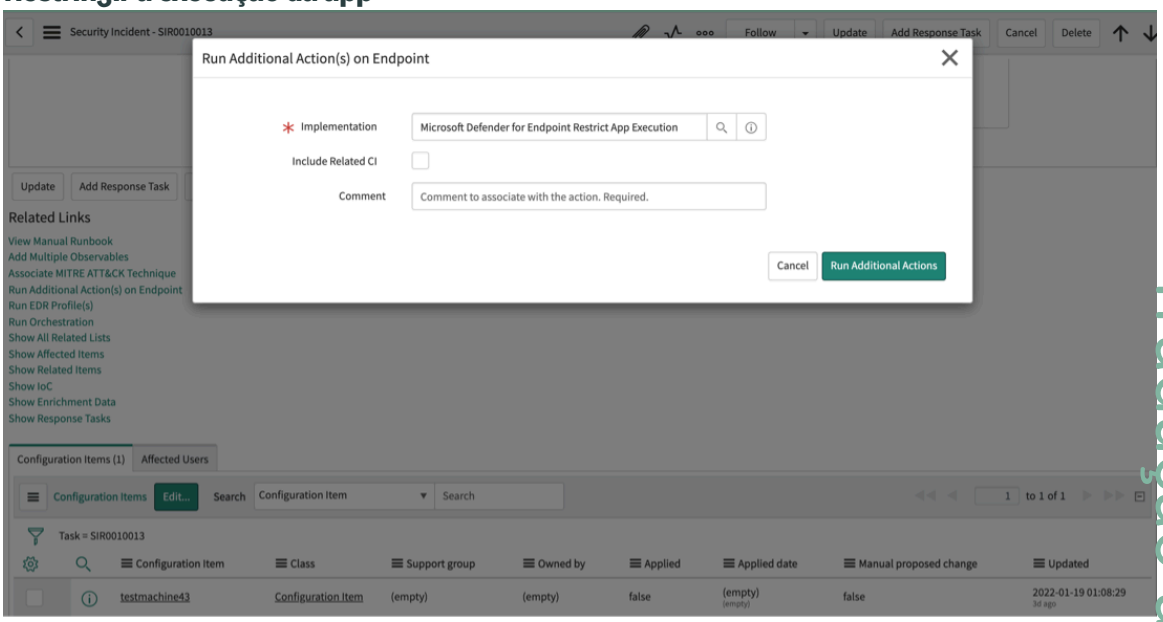
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
   a. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Procure e selecione **Restringir execução da aplicação** capacidade.

Restringir a execução da app



Como alternativa, você pode executar as seguintes etapas:

a. Na seção Listas relacionadas, clique em **Mostrar todas as listas relacionadas** .
b. Clique em **Item de configuração** lista relacionada.
c. Selecione os itens de configuração adicionados.
d. Em Ações nas linhas selecionadas, selecione **Executar ações adicionais no endpoint** .

3. Para habilitar Restringir execução de apps na máquina, clique em **Executar ação adicional** .
4. Exiba as atividades de automação da execução e valide-as.
5. Valide o status da ação nas listas relacionadas Ações adicionais no endpoint.

Configurar o recurso Remover restrição de app em Microsoft Defender for Endpoint

Se necessário, remova as restrições de qualquer aplicação no dispositivo.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para Remover recurso de restrição de app

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

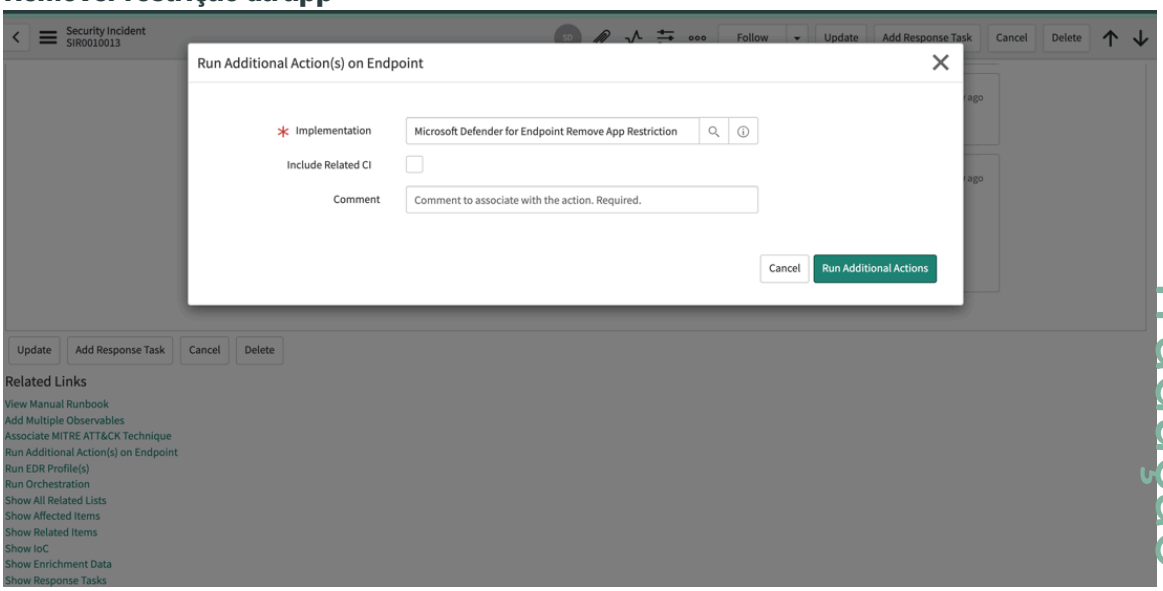
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
   a. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Procure e selecione **Remover restrição do app** capacidade.

Remover restrição da app



Como alternativa, você pode executar as seguintes etapas:

   a. Na seção Listas relacionadas, clique em **Mostrar todas as listas relacionadas** .
   b. Clique em **Item de configuração** lista relacionada.
   c. Selecione os itens de configuração adicionados.
   d. Selecione **Executar ações adicionais no endpoint** .
   O campo de entrada Comentário adicional é exibido.
3. Para remover a restrição do app, clique em **Executar ação adicional** .
4. Exiba as atividades de automação da execução e valide-as.
5. Valide o status da ação nas listas relacionadas Ações adicionais no endpoint.

Configurar Obter máquinas relacionadas do Defender em Microsoft Defender for Endpoint

Obtenha a lista de máquinas relacionadas de observáveis específicos.

Antes de Iniciar

Nota: Os tipos observáveis compatíveis são Nome de domínio, hash SHA1 e Nome de usuário.

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode recuperar a lista de máquinas que acessaram os observáveis específicos. Você pode armazenar a lista na tabela Detalhes de máquinas relacionadas ao Microsoft Defender para endpoint. Você pode acionar o recurso Obter máquinas relacionadas do Defender na lista relacionada de observáveis associados.

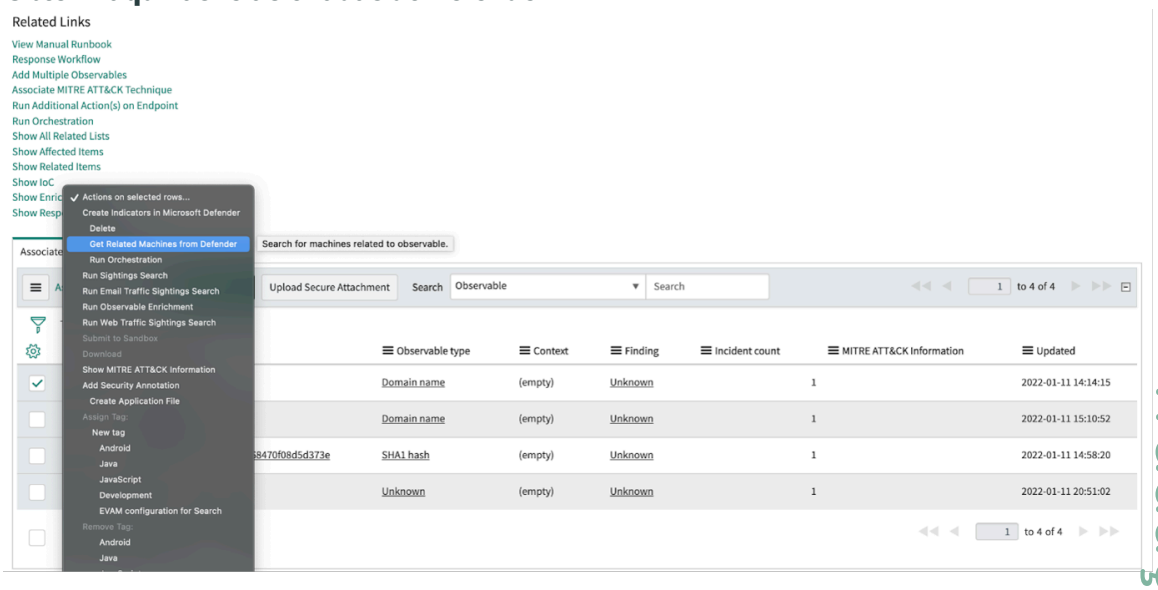
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.

Obter máquinas relacionadas do Defender



3. Na seção Links relacionados, clique em **Mostrar IOC** .
4. Clique na lista relacionada Observáveis associados.
5. Selecione os observáveis associados.
6. Na lista Ações, selecione **Obtenha máquinas relacionadas do Defender** capacidade.
7. Valide a atividade de automação e a seção Atividades.
8. Exiba os dados e valide os detalhes do Microsoft Defender para máquinas relacionadas ao Endpoint nas listas relacionadas.
9. Exiba as atividades de automação da execução e valide-as.

Configure o recurso Parar e Quarentena de arquivos em Microsoft Defender for Endpoint

Interrompa e coloque em quarentena arquivos da plataforma Microsoft Defender.

Antes de Iniciar

Tipos de observáveis compatíveis: Hash SHA1.

Requisitos para a capacidade de Parar e Quarentena de Arquivo

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode executar a ação Parar e colocar arquivo em quarentena somente nos observáveis específicos do tipo SHA1. Armazene os detalhes na tabela Ações adicionais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no endpoint. Você pode acionar o recurso Interromper arquivo e quarentena na lista relacionada de detalhes de máquinas relacionadas ao Microsoft Defender para endpoint.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
3. Na seção Links relacionados, clique em **Mostrar todas as listas relacionadas** .
4. Clique na lista relacionada Detalhes de máquinas relacionadas ao Microsoft Defender para endpoint.
5. Selecione um ou mais registros.
6. Em **Ações** em linhas selecionadas, selecione **Parar e colocar arquivo em quarentena** capacidade.
7. Valide a atividade de automação e a seção Atividades.
8. Exiba os dados e valide os dados nas listas relacionadas.
9. Exiba as atividades de automação da execução e valide-as.

Crie e configure um perfil para pesquisa de vistas com Microsoft Defender for Endpoint integração

Crie e configure o perfil de pesquisa de vistas automaticamente usando Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar o fluxo de trabalho Pesquisa de vistas para executar as pesquisas de vistas. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vistas e executa as pesquisas baseadas no fluxo de trabalho configurado.

. Microsoft Defender for Endpoint fornece um perfil de pesquisa de detecções do sistema de base que permite configurar as pesquisas de detecções automáticas. Com este perfil, você pode acessar as informações de avistamento observável relacionadas de uma organização e também ver as vistas de outras organizações.

Procedimento

1. Navegar até **Integrações** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.
3. No formulário, preencha os campos a seguir.

Formulário Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome do perfil de pesquisa de vistas.
Pesquisa salva	Opção para salvar a configuração de pesquisa. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações de pesquisa salvas adicionais conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem da pesquisa de detecções	A origem configurada para a pesquisa de vistas em Microsoft Defender for Endpoint integração.
Pesquisar	Cadeia de caracteres de pesquisa nativa que forma uma consulta.
Ativo	Opção para habilitar a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de vistas.
Tipo de observável	Tipo de categoria de observável. Por exemplo, endereço IP, valor de hash, URL e nome de domínio.
Observável máximo por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de vistas	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de logs especificado.

4. Clique em **Enviar**.

Execute uma pesquisa de detecção manual em Microsoft Defender for Endpoint

Selecione observáveis individuais ou múltiplos e execute uma pesquisa de vista manual em Microsoft Defender for Endpoint determinar a prevalência de uma ameaça ao longo do tempo.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os tipos de observáveis compatíveis são os seguintes:

- Nome do domínio
- Endereço IP (V4)
- Endereço IP (v6)
- Hash MD5
- Hash SHA1
- Hash SHA256

Procedimento

1. Navegue até **Incidentes de segurança** .
2. Abra um SIR existente ou crie um novo SIR.
3. Em Links relacionados, clique em **Mostrar IOC** .
4. Clique nas listas relacionadas de observáveis associados.
5. Selecione os observáveis.
6. Na lista Ações, clique em **Executar aprimoramento de observável** .
7. Selecione os observáveis em **Ação** nas linhas selecionadas e clique em **Executar Pesquisa de vistas** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A pesquisa de vistas é compatível com Nome de domínio, endereço IP (V4), endereço IP (V6), hash MD5, hash SHA1, e tipos de observáveis de hash SHA256, respectivamente.

8. Especifique o intervalo de tempo para a pesquisa e clique em **Pesquisa** .

Nota: O Microsoft Defender para Endpoint oferece suporte à pesquisa de vistas somente nos últimos 30 dias. Se sua consulta de intervalo for anterior aos últimos 30 dias, a pesquisa de vistas não recuperará dados. Se sua consulta de intervalo se sobrepor aos últimos 30 dias, as vistas dos últimos 30 dias serão recuperadas e, se sua consulta de intervalo estiver nos últimos 30 dias, as vistas da hora de início definida até a hora atual serão recuperadas.

9. Ao concluir a pesquisa, valide os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes da pesquisa de vistas** para exibir os detalhes da pesquisa de vistas.
11. Clique em **Vista** para obter detalhes e. **Resultados da pesquisa de vistas** guia para resultados da pesquisa.

Você pode exibir informações adicionais relacionadas à vista específica em **Resumo** campo.

Execute um aprimoramento de observável automático em Microsoft Defender for Endpoint

Execute um aprimoramento de observável automático em Microsoft Defender for Endpoint enriquecer observáveis com informações adicionais de várias fontes.

Antes de Iniciar

Verifique se você habilitou o. **Resposta a incidentes de segurança** propriedade do sistema. Esta opção aciona a capacidade de aprimoramento de observável no SIR, sempre que um observável é associado a um incidente de segurança.

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar esse recurso durante as investigações de resposta a incidentes para conter uma ameaça identificada. Quando novos observáveis são associados ao incidente de segurança, você pode habilitar o aprimoramento de observável no Microsoft Defender para o recurso Endpoint para ser executado automaticamente.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
3. Valide a atividade de automação depois que os novos observáveis forem associados ao incidente de segurança.
4. Exiba os resultados do aprimoramento na lista relacionada de indicadores do incidente de segurança. Você pode usar a tabela a seguir para obter mais informações sobre o aprimoramento do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade do indicador. Clique em **Aberto** para exibir o registro em detalhes no ServiceNow AI Platform instância
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender a partir da qual os dados são recuperados.
Data de Vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento é criado.

Execute um aprimoramento de observável manual em Microsoft Defender for Endpoint

Selecione observáveis individuais ou múltiplos e execute um aprimoramento de observável manual para enriquecer observáveis com informações adicionais de Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

. Microsoft Defender for Endpoint A integração permite o aprimoramento do observável para todos os tipos de observáveis mapeados no módulo Mapeamento de indicador observável.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para Endpoint.
3. Clique em **Mostrar todas as listas relacionadas** .
4. Clique em **Observáveis associados** guia.
5. Selecione os observáveis.
6. Na lista Ações, clique em **Executar aprimoramento de observável** .
7. Selecione um Microsoft Defender para Endpoint **origem** e mova-o para **Selecionado** coluna para especificar qual implementação você deseja usar para enriquecer os observáveis selecionados.
8. Clique em **Enviar**.
9. Para validar o status da execução, exiba as anotações de trabalho.
10. Para exibir os resultados, clique em **Indicador do Microsoft Defender** guia.
    Você pode usar a tabela a seguir para obter mais informações sobre o aprimoramento do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade do indicador. Clique em **Aberto** para exibir o registro em detalhes no ServiceNow AI Platform instância
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender a partir da qual os dados são recuperados.
Data de Vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento é criado.

Como criar Indicadores em Microsoft Defender for Endpoint

Crie indicadores a partir de observáveis associados do incidente de segurança usando Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

. Microsoft Defender for Endpoint A integração permite o aprimoramento do observável para todos os tipos de observáveis mapeados no módulo de mapeamento Observable-Indicador.

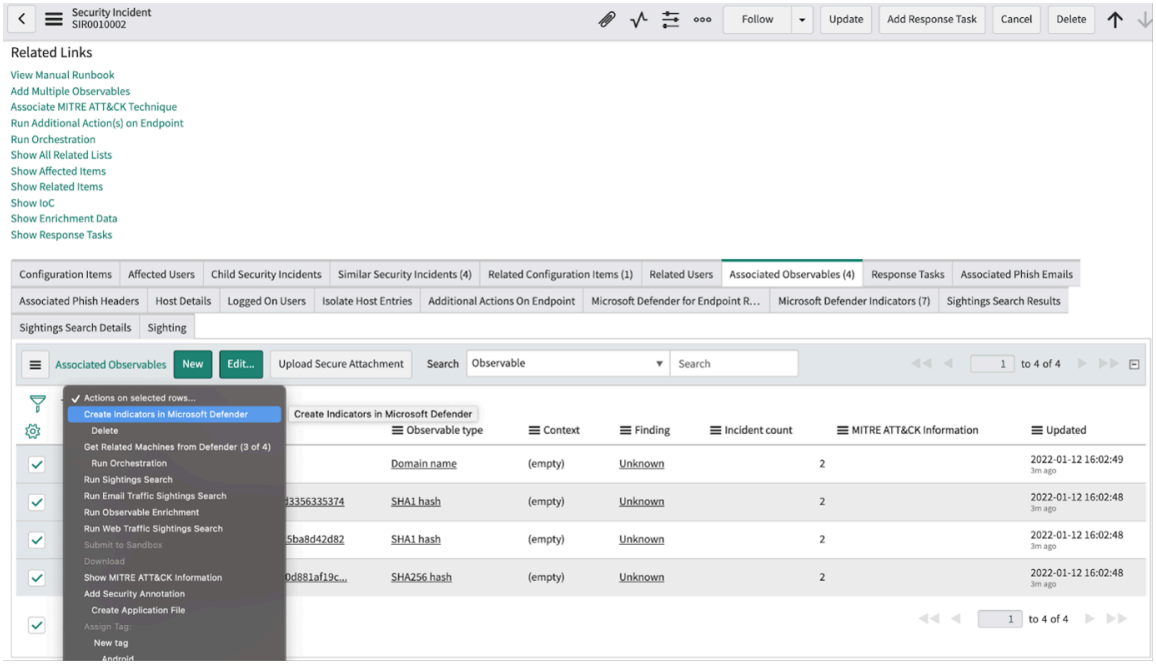
Criar indicadores fornece a capacidade de definir uma lista de indicadores para detecção e para bloquear prevenção e respostas. Você pode criar os indicadores do observável associado do incidente de segurança.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar indicadores no Microsoft Defender para Endpoint.
3. Clique nas listas relacionadas de observáveis associados.
4. Adicione observáveis existentes ou crie novos observáveis.
5. Selecione os observáveis.
6. Em **Ações** nas linhas selecionadas, clique em **Criar indicador no Microsoft Defender** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. No formulário, preencha os campos.

Campo	Descrição
Observáveis selecionados	Observáveis afetados. Esta ação pode ser usada para criar indicadores para vários observáveis. Se você quiser desmarcar um observável, poderá fazer isso desmarcando os observáveis da lista. **Nota:** Se os tipos de observáveis compatíveis não forem mapeados, os indicadores não serão criados no Microsoft Defender para esses observáveis.
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.
Ações recomendadas	Ações recomendadas que devem ser executadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que serão executadas se o Indicador for descoberto na organização. Os valores possíveis são os seguintes: ○ **Aviso** ○ **Bloquear** ○ **Auditoria** ○ **BloqueeCorreção** ○ **Permitido**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	A aplicação Microsoft Defender for Endpoint associada ao indicador. Este campo é aplicável somente a um novo indicador e não pode ser usado para um indicador existente.
Gravidade	Gravidade do Indicador. Os valores possíveis são os seguintes: ○ **Baixo(a)** ○ **Média** ○ **Alto**
Nomes do grupo RBAC	Nomes de grupo RBAC aos quais o indicador seria aplicado. Os nomes estão em uma lista separada por vírgulas.

8. Clique em **Criar indicador**
9. Valide a atividade e as mensagens de IU.
10. Clique em **Indicador do Microsoft Defender** para exibir os resultados.

Atualizar indicadores em Microsoft Defender for Endpoint

Atualize os indicadores existentes em Microsoft Defender for Endpoint No menu de contexto da lista ou na exibição de formulário do Indicador do Microsoft Defender, respectivamente.

Antes de Iniciar
Função necessária: sn_si.admin, sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Clique em **Mostrar todas as listas relacionadas** e, em seguida, clique em **Indicadores do Microsoft Defender** guia.

Nota:

Você deve configurar a lista relacionada para os indicadores do Microsoft Defender, que aparecem nas listas relacionadas de Incidentes de segurança. Para obter mais informações, consulte Ações de IU do formulário .

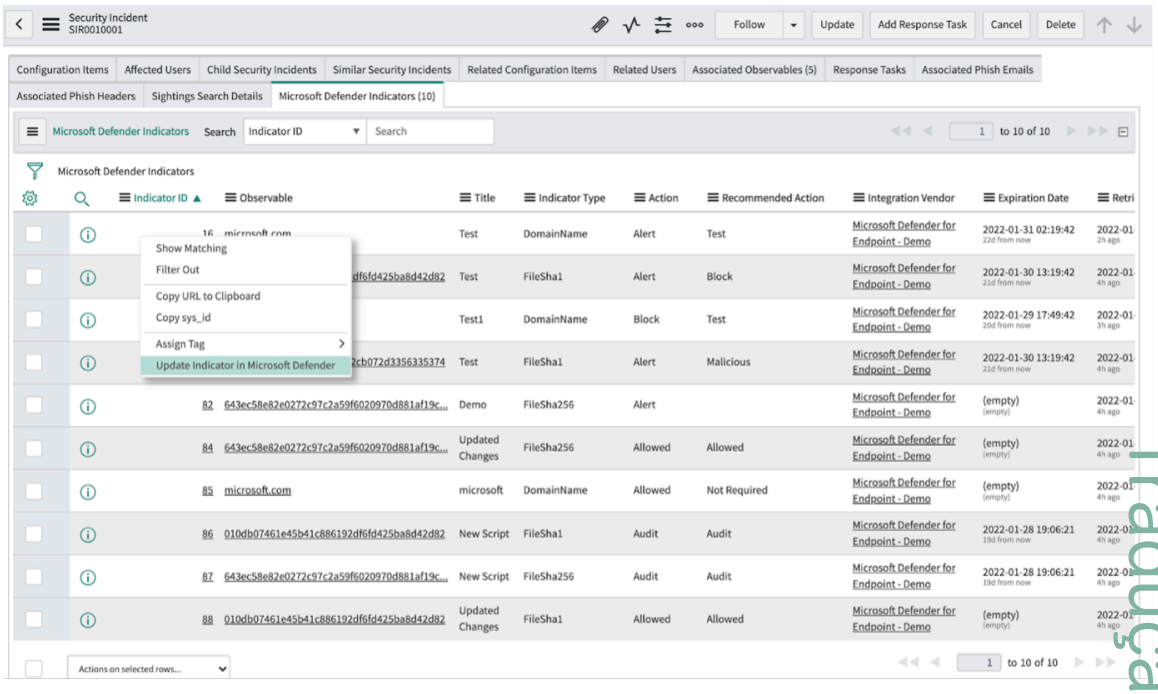
3. Atualize o Microsoft Defender para Indicadores de endpoint de uma das seguintes maneiras:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

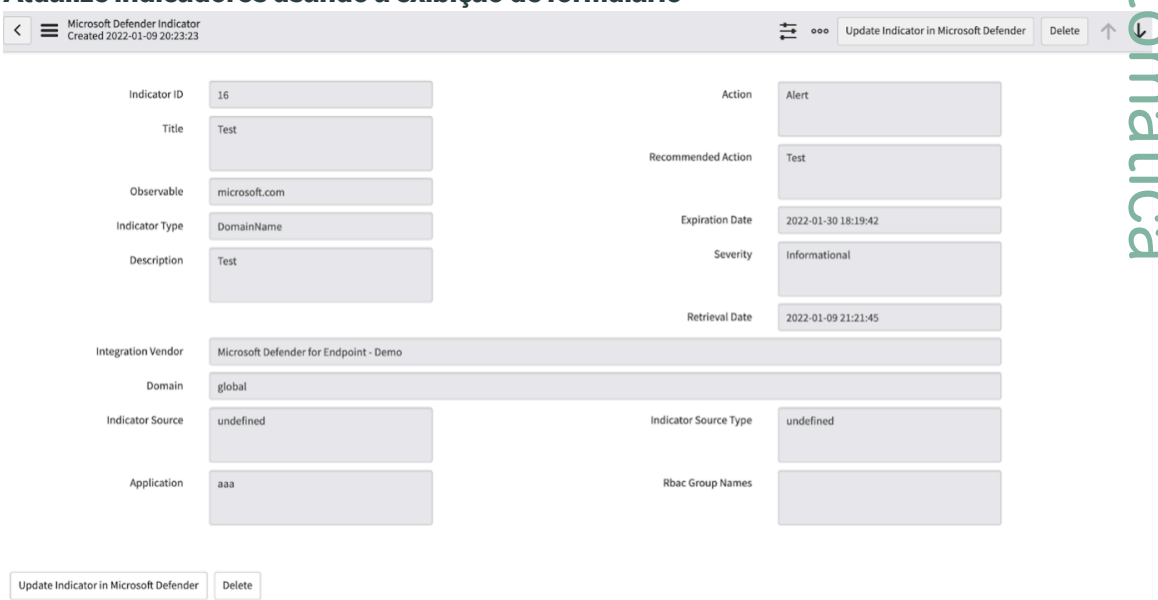
- Para atualizar os indicadores no menu de contexto da lista, selecione a linha do indicador que você deseja atualizar e clique em **Indicador de atualização no Microsoft Defender** opção.

Atualizar indicadores usando o menu de contexto da lista



- Para atualizar os indicadores na exibição do formulário, clique em **Indicador de atualização no Microsoft Defender** na exibição do formulário.

Atualize indicadores usando a exibição de formulário



4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Indicador do Microsoft Defender

Campo	Descrição
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.
Ações recomendadas	Ações recomendadas a serem executadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que serão executadas se o indicador for descoberto na organização. Os valores possíveis são os seguintes: ○ **Aviso** ○ **Bloquear** ○ **Auditoria** ○ **BloqueeCorreção** ○ **Permitido**
Aplicação	A aplicação Microsoft Defender for Endpoint associada ao indicador. Este campo é aplicável somente a um novo indicador e não pode ser usado para um indicador existente.
Gravidade	Gravidade do Indicador. Os valores possíveis são os seguintes: ○ **Baixo(a)** ○ **Média** ○ **Alto**
Nomes do grupo RBAC	Nomes de grupo RBAC aos quais o indicador é aplicado. Os nomes estão em uma lista separada por vírgulas.

5. Clique em **Atualizar indicador** .
6. Valide a atividade e as mensagens de IU.

Domain Separation em Microsoft Defender for Endpoint integração

Domain Separation é compatível com Microsoft Defender for Endpoint integração. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico

Use as seguintes etapas para separação de domínio:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Crie um usuário com sn_si.admin função no respectivo domínio.
2. Execute Microsoft Defender for Endpoint procedimentos de integração no domínio apropriado.

Configuração do limite de taxa em Microsoft Defender for Endpoint integração

Configure o limite de taxa da API e o tempo limite para o limite de taxa para Microsoft Defender for Endpoint integração.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Procedimento

1. No filtro de navegação, insira `sys.properties.list` .
   A lista inteira de propriedades na tabela Propriedades do sistema [sys_properties] é exibida.
2. PESQUISE e modifique as propriedades a seguir de acordo com seus requisitos.

Nome da Propriedade	Descrição
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Se uma solicitação não for executada dentro do intervalo de tempo especificado, a execução será interrompida e uma mensagem de erro apropriada será exibida. Valor padrão: 75.
sn_sec_defender_ep.request_per_hour_limit	Se a chamada de API configurada for feita no mesmo endpoint em uma hora, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 1500.
sn_sec_defender_ep.request_per_minute_limit	Se a chamada de API configurada for feita no mesmo endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Se a chamada de API configurada for feita no endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 30.

Microsoft Exchange Online integração

Para Microsoft Exchange Online aplicação de integração por ServiceNow. ServiceNow AI Platform® Resposta a incidentes de segurança(SIR) o produto está integrado ao Microsoft Exchange Online, um dos serviços baseados em nuvem no Microsoft Pacote de produtos do Office 365. Seu analista do Security Operation Center (SOC) pode pesquisar ameaças relacionadas à segurança no ambiente de e-mail corporativo e remover e corrigir e corrigir e-mails de phishing com recursos de pesquisa e exclusão de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral de Microsoft Exchange Online integração

Como analista de incidentes de segurança, você executa a integração na interface do analista de segurança e o fluxo de trabalho retorna detalhes da mensagem de e-mail que correspondem aos critérios de pesquisa. As pesquisas de e-mail são baseadas em critérios que incluem linhas de assunto, bem como endereços de e-mail do remetente e do destinatário. Após a conclusão da pesquisa de e-mail, você pode excluir e-mails suspeitos do Microsoft Exchange Online e um processo de aprovação opcional pode ser configurado para solicitar aprovação antes de excluir e-mails.

Esta integração de pesquisa e exclusão de e-mail pode ser usada com um fluxo de trabalho ou runbook de incidente de resposta a phishing mais amplo. Depois que um usuário corporativo ou funcionário recebe um e-mail suspeito e o relata à equipe de resposta a phishing da empresa ou à caixa de entrada, o e-mail relatado é encaminhado para ServiceNow AI Platform e categorizado como um incidente de segurança. Depois de verificar que um e-mail é um ataque de phishing, como analista responsável por investigar incidentes de phishing, você pode iniciar uma pesquisa de e-mail para determinar se outros usuários corporativos receberam esse e-mail de phishing. A pesquisa permite localizar e-mails relacionados da mesma campanha de phishing e identificar outras possíveis vítimas que podem ter recebido o e-mail, lido e também clicado em um URL malicioso ou aberto um anexo.

Principais recursos

A integração inclui os seguintes recursos principais:

- Configure critérios de pesquisa para ameaças de phishing na Resposta a incidentes de segurança com base em combinações dos campos remetente, destinatário e assunto em mensagens de e-mail.
- Para pesquisas de e-mail grandes e longas, o analista de incidentes de segurança é notificado por e-mail quando a pesquisa é concluída com sucesso, junto com o número de mensagens correspondentes.
- O status de mensagens individuais informa se os destinatários leram ou excluíram e-mails suspeitos.
- Se configurados, os processos de aprovação opcionais garantem que os e-mails suspeitos não sejam excluídos sem aprovação prévia.
- Uma trilha de auditoria completa para solicitações de exclusão que inclui o número de e-mails excluídos é registrada nas anotações de trabalho de incidentes de segurança.
- Se a marcação estiver configurada, os marcadores de segurança registrarão quando os fluxos de trabalho de pesquisa e exclusão de e-mail forem iniciados e concluídos com sucesso em incidentes de segurança.

Versões da Microsoft Exchange Online compatíveis

Esta integração oferece suporte a Microsoft Exchange Online, que fazem parte do Microsoft Pacote do Office 365. A integração não oferece suporte a hospedado Microsoft Ambientes do Exchange. Microsoft execuções Microsoft Exchange Online Serviços na versão do Exchange 2016.

Pré-requisitos

O plug-in com.snc.si_dep é necessário para qualquer um ServiceNow AI Platform versão. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações.

A seguir Operações de segurança as aplicações devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila:

1. Framework de integração de segurança
2. Security Support Common
3. Orquestração do suporte de segurança
4. Resposta a incidentes de segurança

Configure seu Microsoft Conta do Azure

Conclua as tarefas de configuração a seguir em seu Microsoft Portal do Azure antes de instalar o. ServiceNow aplicação para esta integração. Esta conta permite acesso ao Microsoft Exchange Online locatário para obter detalhes da mensagem de e-mail.

Antes de Iniciar

Função necessária: Microsoft Administrador do portal do Azure

Esta conta é necessária para acessar o. Microsoft Exchange Online locatário para coletar detalhes adicionais da mensagem de e-mail e excluir mensagens de e-mail. Esta conta está configurada no Microsoft Portal do Azure.

As imagens nas tarefas a seguir são privilegiadas e proprietárias e são usadas com permissão de Microsoft. Este conteúdo está sujeito a atualizações por Microsoft. Para verificar se você tem acesso ao conteúdo mais atual, consulte Documento da Microsoft site.

Nas imagens a seguir, ServiceNow Inc É exibido para o nome da conta nos exemplos do portal do Azure. Em sua conta do portal do Azure, o nome da empresa da sua conta no portal do Azure é exibido.

Procedimento

Se você não criou um ID de aplicação para autenticação OAUTH no Microsoft Portal do Azure, siga estas etapas.

a. Faça login no Microsoft Portal do Azure usando suas credenciais de administrador do portal do Azure.

b. Insira **Registros de aplicações** em **Pesquisa** caixa.

c. Selecione **Novo registro** .

d. Preencha o formulário Registrar uma aplicação exibido.

Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, Integração do ServiceNow Exchange Online inserido.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, selecione **Somente contas neste diretório**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	organizacional (nome da sua organização) . Este domínio é usado para pesquisas de e-mail.
URL de redirecionamento (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.

e. Selecione **Registrar**.
Um ID de aplicação é criado. Este ID é semelhante a um nome de usuário. Insira este valor na página de configuração do **ID da aplicação OAUTH** durante a etapa de configuração em ServiceNow AI Platform instância descrita em Configure o. Microsoft Exchange Online integração.

f. Em **Gerenciar** selecione, **Manifesto** .

g. Encontre **RequiredResourceAccess** entrada (na linha 52 ou sobre ela).

h. Modificar **ResourceAppId** , **ID do resourceAccess** e **Tipo de resourceAccess** valores com o seguinte snippet de código:

```
"requiredResourceAccess": [
        {
                "resourceAppId": "00000003-0000-0000-c000-000000000000",
                "resourceAccess": [
                        {
                                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                                "type": "Role"
                        },
                        {
                                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                                "type": "Role"
                        }
                ]
        }
  ],
```

i. Selecione **Save** (Salvar).

j. Em **Gerenciar** selecione, **Permissões de API** .

k. Selecione **Adicione uma permissão** .

l. No painel Solicitar permissões da API exibido, selecione **Microsoft Graph** .

m. No painel Solicitar permissões da API exibido, selecione **Permissões da aplicação** .

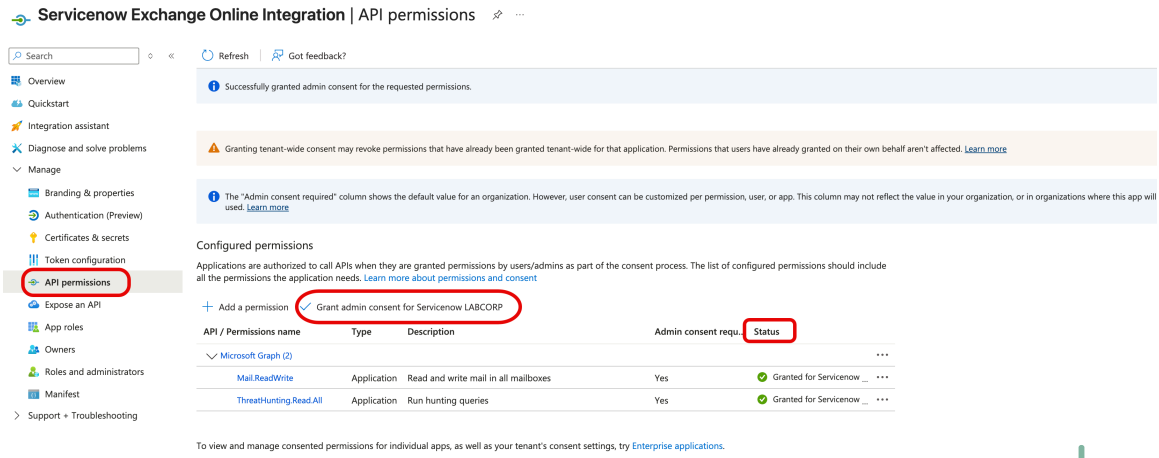
n. No campo Selecionar permissões exibido, insira **Ameaça** e selecione **ThreatHunting.Read.All** caixa de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

o. Selecione **Conceda consentimento do administrador para o <Organization>** .

p. Selecione **Sim**.
. **Status** agora o valor deve ser **Concedido para o**



<Organization>.

O que Fazer Depois

Você está pronto para configurar seu ServiceNow AI Platform® instância da integração.

Instalar Microsoft Exchange Online aplicação

Antes de executar a integração em sua instância, instale o. Microsoft Exchange Online aplicação para a integração do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação do ServiceNow Store em seu ServiceNow AI Platform conclua todas as tarefas listadas nas check-lists de pré-requisitos.

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação do ServiceNow Store, configure-o para se conectar ao seu ServiceNow AI Platform instância.

Configure o. Microsoft Exchange Online integração

Depois de instalar a aplicação do ServiceNow Store, configure-o para se conectar ao seu ServiceNow AI Platform instância. Esta ativação ativa os fluxos de trabalho de pesquisa e exclusão.

Antes de Iniciar

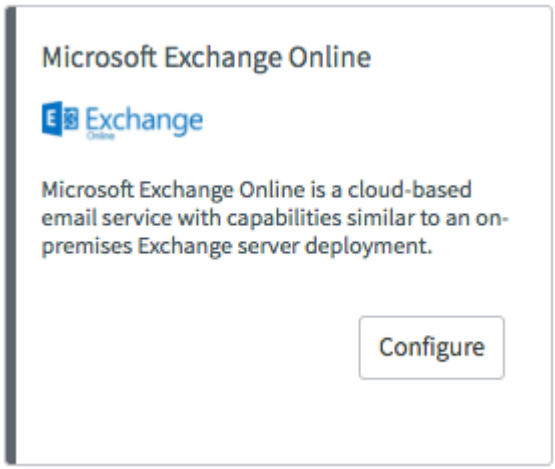
Função necessária: sn_si.admin

Procedimento

1. Em seu ServiceNow AI Platform instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
2. Localize Microsoft Exchange Online lado a lado.
3. Clique em **Configurar**.

Tradução automática

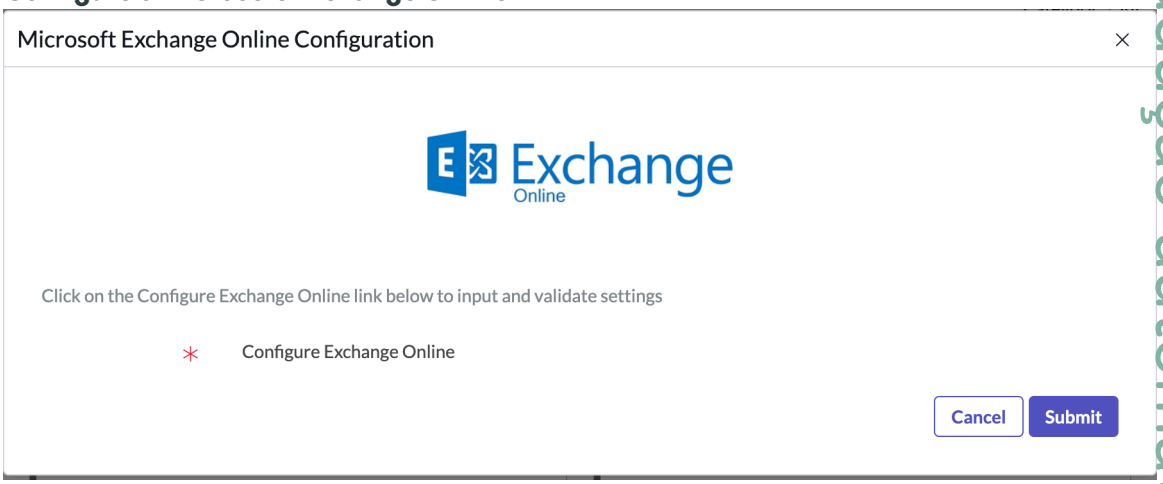
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Em Microsoft Exchange Online Caixa de diálogo de configuração exibida, clique em **Configurar o Exchange Online** .

Um exemplo de um formulário preenchido e validado segue a tabela.

Configure o Microsoft Exchange Online



Opção	Descrição
Guia Configurações de conexão	
Locatário	. Microsoft Exchange Online locatário no qual você deseja executar pesquisas. Este texto é o nome exclusivo que aparece após a para endereços de e-mail da sua organização. Para este exemplo, `snowse–cops.onmicrosoft.com` é o locatário (domínio).
Impressão Digital do Certificado	Uma impressão digital de certificado é um hash de um certificado, calculado sobre todos os dados do certificado e sua assinatura. As impressões digitais são usadas como identificadores exclusivos para certificados, em aplicações ao tomar decisões de confiança, em arquivos de configuração e exibidas em interfaces.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
ID da aplicação OAuth	O ID da aplicação (cliente) que foi gerado para a conta que você criou no Microsoft Portal do Azure. Para obter mais informações, consulte Configure seu Microsoft Conta do Azure.
Segredo do cliente do OAuth	Senha (segredo do cliente) da conta que você criou no Microsoft Portal do Azure. Para obter mais informações, consulte Configure seu Microsoft Conta do Azure.
Guia Configurações adicionais	
Janela de pesquisa de e-mail (dias)	Intervalo do histórico de pesquisa de e-mail em número de dias. A integração pesquisa mensagens de e-mail que foram enviadas ou recebidas no Microsoft Exchange Online servidor para o número de dias corridos que você insere. Você deve inserir um valor entre 1 e 30. 30 dias é o padrão e o número máximo de dias que você pode inserir para uma pesquisa. Inserir um número baixo de dias no intervalo da janela de pesquisa melhora o tempo de resposta, mas você pode não capturar todas as mensagens correspondentes como resultado. Esta configuração global é para todas as pesquisas. Antes de executar a pesquisa de e-mail, não há parâmetros que permitam alterar esse valor para pesquisas individuais.
Duração máxima da pesquisa	Use esta opção para definir o limite de tempo limite de pesquisa. Se o limite de tempo limite for atingido, a pesquisa será encerrada e nenhum resultado será exibido. Você pode especificar um valor padrão de 90 minutos e um valor máximo de 240 minutos. Ao definir esse limite, você pode evitar loops de pesquisa infinitos que podem causar problemas de desempenho no Microsoft Exchange Online locatário e ServiceNow instância.
Marcação	Marcador de segurança. O padrão é selecionado. Quando habilitados, os marcadores de segurança são aplicados automaticamente aos incidentes de segurança relacionados quando os recursos de pesquisa e exclusão são iniciados e concluídos com sucesso. Os nomes de marcador padrão são exibidos, mas os nomes e as cores dos marcadores podem ser editados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Para obter mais informações, consulte Edite marcadores de segurança para Microsoft Exchange Online integração.
Recuperar e-mails excluídos	O padrão é selecionado. Este item se aplica somente a e-mails que você excluiu usando esta integração. Se você não quiser que os usuários em sua organização tenham acesso aos e-mails que você excluiu, verifique se esta caixa de seleção está desmarcada. Se a caixa de seleção estiver desmarcada, os e-mails que você excluir usando o fluxo de trabalho desta integração serão excluídos permanentemente e colocados na pasta Limpas. Esta pasta é uma subpasta dentro da pasta Itens recuperáveis em Microsoft Exchange Online que um usuário normalmente não pode acessar. Se você quiser que os usuários recuperem os e-mails excluídos, marque esta caixa de seleção. Se esta caixa de seleção estiver marcada, dependendo de como a conta do usuário está configurada em Microsoft Exchange Online, Os e-mails que você exclui usando o fluxo de trabalho desta integração são colocados na pasta Itens excluídos na caixa de correio do usuário. Se uma conta estiver configurada para que o usuário possa exibir a pasta Itens excluídos em sua caixa de correio, ele poderá recuperar os e-mails excluídos da conta do Microsoft Exchange Online. Para obter mais informações, consulte Recupere itens excluídos ou e-mail no Outlook Web App .
Pesquisar notificações de conclusão	Selecione esta opção para habilitar notificações quando a pesquisa for concluída. . **Habilitar** se a caixa de seleção estiver marcada, você receberá notificações se algum e-mail correspondente for encontrado. Se a caixa de seleção estiver desmarcada, as notificações de conclusão de pesquisa não serão enviadas.
Aprovações	Solicitar aprovação para excluir e-mails. O padrão é limpo.

Tradução automática

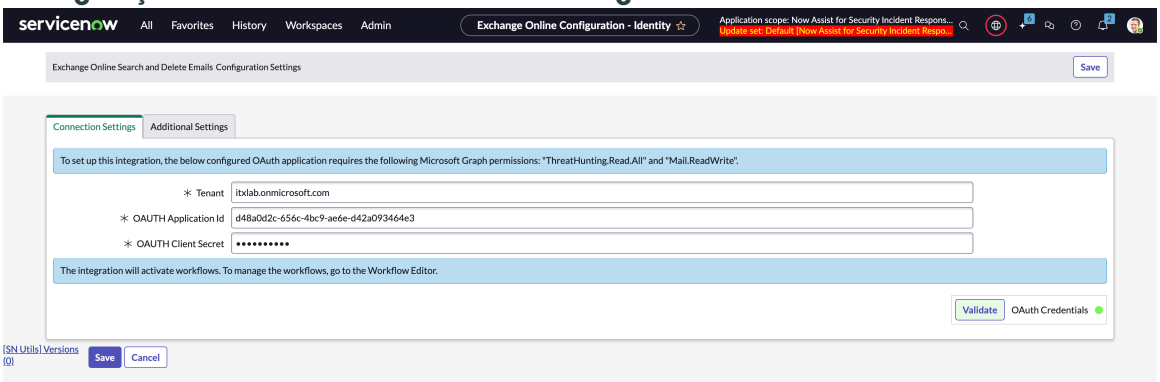
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Quando a caixa de seleção está desmarcada, o processo de aprovação opcional para solicitar permissão prévia antes de excluir e-mails do Microsoft Exchange Online o serviço está desabilitado. Verifique se esta caixa de seleção está desmarcada se quiser conceder ao analista de incidentes de segurança permissão para excluir e-mails sem solicitar permissão prévia. Se habilitada, uma solicitação será enviada por e-mail para cada membro de um grupo de aprovação. Na lista, selecione um grupo de aprovação na lista. Depois que uma solicitação é enviada para um grupo de aprovação, somente uma aprovação é necessária do grupo para concluir a solicitação. Qualquer membro do grupo de aprovação tem autoridade de aprovação. Ter um grupo com mais de uma pessoa com permissão de aprovação garante que essas solicitações sejam processadas em tempo hábil.
Notificações de falha	Marque a caixa de seleção para habilitar notificações de falha quando a ação de pesquisa ou exclusão falhar devido a credenciais inválidas do OAuth. Se habilitado, as notificações de falha serão enviadas por e-mail para cada membro do grupo de notificações de falha quando as credenciais do OAuth forem inválidas. Se a caixa de seleção estiver desmarcada, nenhuma notificação de falha será enviada.
Limite de resultado de e-mail	A partir da versão 10,3 ou posterior, você pode especificar um limite de exclusão de e-mail para aprovações. Se o número de e-mails que estão sendo excluídos for maior ou igual ao valor especificado aqui, a solicitação Excluir deverá ser aprovada antes que a ação Excluir seja invocada. Se o valor limite estiver definido como 1, cada solicitação de exclusão deverá ser aprovada.

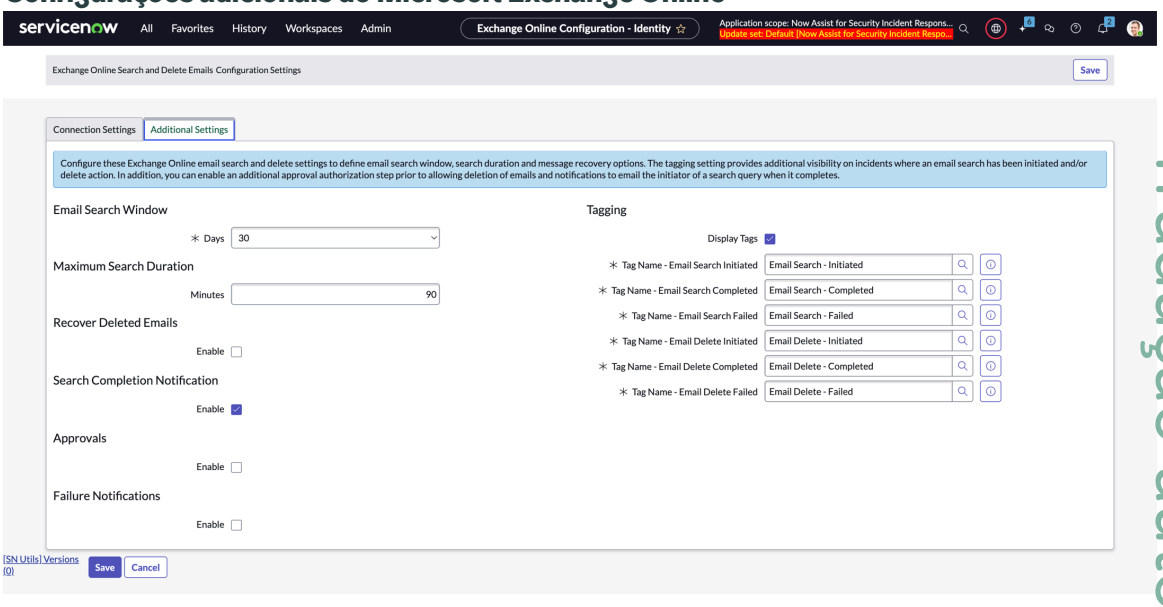
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de conexão do Microsoft Exchange Online



Configurações adicionais do Microsoft Exchange Online



5. Escolha um para continuar.

Opção	Descrição
Salvar	Salve suas edições. Esta ação não verifica sua conexão.
Na guia Configurações de conexão, clique em Validar.	Esta ação valida sua autenticação de certificado, sua conexão do MID Server e credenciais OAuth. Se suas credenciais forem válidas, o **Validar** e ambos os indicadores estão verdes.

Trouble?
Se uma mensagem de erro for exibida ou um ou mais indicadores à direita do botão Validar estiverem vermelhos, verifique se as credenciais da conta de usuário inseridas são válidas. Insira suas credenciais e clique em **Salvar** novamente.

Validação malsucedida

Consulte a tabela a seguir para obter mais informações sobre **Validar** e os ícones coloridos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado do botão Validar e indicadores	Descrição
O botão Validar está verde e todos os indicadores coloridos pequenos estão verdes.	Indica que a conexão do MID Server e as credenciais são válidas.
O botão Validar é vermelho claro com uma borda azul e um ou todos os pequenos indicadores coloridos são laranja.	A validação está em andamento. A validação pode levar mais alguns minutos para ser concluída.
O botão Validar está vermelho claro e um ou todos os indicadores coloridos pequenos estão vermelhos.	• Autenticação baseada em certificado do Exchange Online ou o botão Credenciais OAuth está vermelho: Indica que as credenciais do Exchange Online são inválidas. • Autenticação baseada em certificado do Exchange Online e os botões Pronto do MID Server estão vermelhos: Indica que o MID Server não está acessível e, portanto, a autenticação baseada em certificado do Exchange Online por meio do MID Server falhou. • O indicador de autenticação baseada em certificado do Exchange Online está vermelho, mas o botão Pronto do MID Server está verde: Indica que o MID Server está ativo e configurado corretamente, mas a autenticação baseada em certificado do Exchange Online está incorreta.

Defina critérios de pesquisa de e-mail e solicite uma pesquisa no Microsoft Exchange Online serviço

Como um usuário com a função sn_si.analyst, defina critérios de pesquisa e envie uma solicitação de pesquisa por e-mail com base nos detalhes do incidente em um registro de incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

As figuras neste procedimento são mostradas com **Formulários com guias** Selecionado em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção intitulada Exibir formulários com guias em Configurar o layout de formulário no Site de documentação do produto da ServiceNow .

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O status de mensagens individuais que correspondem à consulta de pesquisa e os resultados da pesquisa são relatados no registro de incidente de segurança. Se as notificações por e-mail estiverem habilitadas, você poderá exibir os resultados da pesquisa de uma mensagem de e-mail.

Os critérios de pesquisa podem incluir endereços do remetente da mensagem, endereços do destinatário ou nomes de assunto. As seguintes combinações de parâmetros de pesquisa Assunto da mensagem, Remetente e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Destinatário são frequentemente usadas para encontrar mensagens de e-mail relacionadas a phishing que podem fazer parte de uma única campanha de phishing:

- Encontrar todos os e-mails originais enviados por uma conta de phishing: Pesquisar por remetente.
- Encontre todos os e-mails originais para uma única campanha de phishing: PESQUISE por assunto e remetente.
- Encontrar todos os e-mails recebidos para uma única campanha de phishing (original e encaminhado, qualquer remetente): Pesquisar por assunto.
- Encontre todos os e-mails encaminhados para um único e-mail de phishing de um único usuário: PESQUISE por destinatário e assunto.
- Encontre todos os e-mails relacionados a phishing enviados a um único usuário: PESQUISE por remetente e destinatário.

Nota: As pesquisas são realizadas em e-mails enviados ou recebidos nos últimos 30 dias corridos, a menos que uma janela de pesquisa mais curta seja configurada durante a configuração inicial. Uma pesquisa de e-mail bem-sucedida é necessária antes que você possa excluir e-mails.

O exemplo a seguir mostra como iniciar uma pesquisa de um ServiceNow AI Platform incidente de segurança. Um incidente de segurança é criado com base no e-mail original de um ataque de phishing suspeito no Microsoft Exchange Online servidor da sua organização. Para este exemplo, os critérios de pesquisa são Remetente (De) mais Assunto, em que De . phisher@cbazyx.com e Assunto . faça login na sua conta .

Os resultados das pesquisas sobre assuntos são retornados quando a pesquisa encontra cadeias de caracteres de texto que contêm palavras-chave que correspondem aos critérios de pesquisa inseridos. Neste exemplo, o assunto é faça login na sua conta . Use **E.** Operador para separar as condições de pesquisa De e Assunto para retornar resultados de todas as mensagens de e-mail que contêm esses critérios de pesquisa fornecidos. As etapas a seguir descrevem como configurar uma pesquisa que encontra somente e-mails que contêm texto de linha de assunto enviado por uma conta de phishing específica.

Procedimento

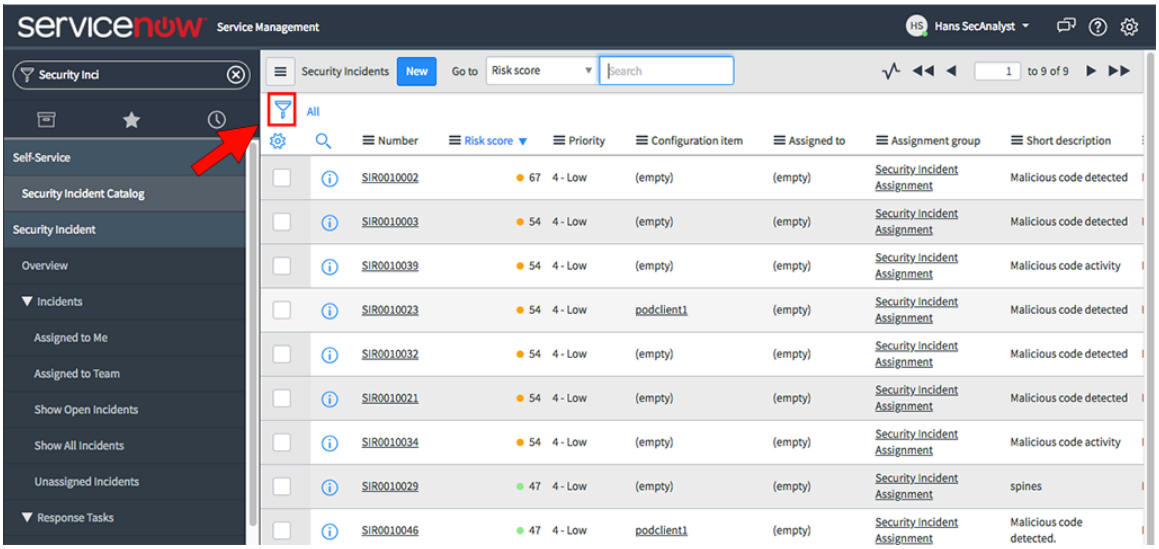
1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando.
2. Como alternativa, siga estas etapas para definir e executar um filtro para que somente os incidentes de segurança criados por eventos de phishing sejam exibidos.

   a. Navegar até **Incidente de segurança** > **Mostrar todos os incidentes** Para abrir a lista Incidentes de segurança.

   b. No canto superior esquerdo da lista exibida, clique no ícone de filtro.

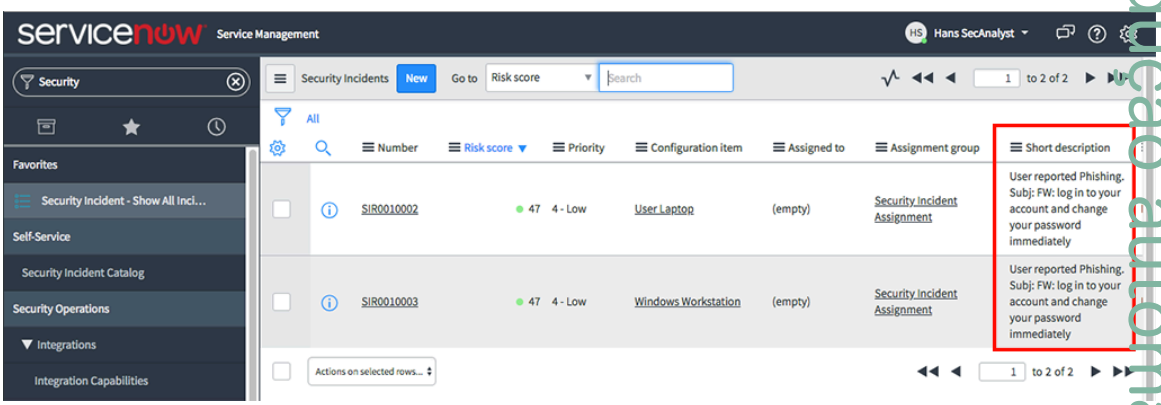
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Nos campos exibidos, selecione **Descrição resumida** > **contém** nas listas de seleção, insira **phishing relatado pelo usuário** e clique em **Executar** .

Os incidentes de segurança relacionados a phishing são exibidos.



d. Use o texto na coluna Descrição resumida para ajudá-lo a localizar o incidente de segurança com o qual você está trabalhando.

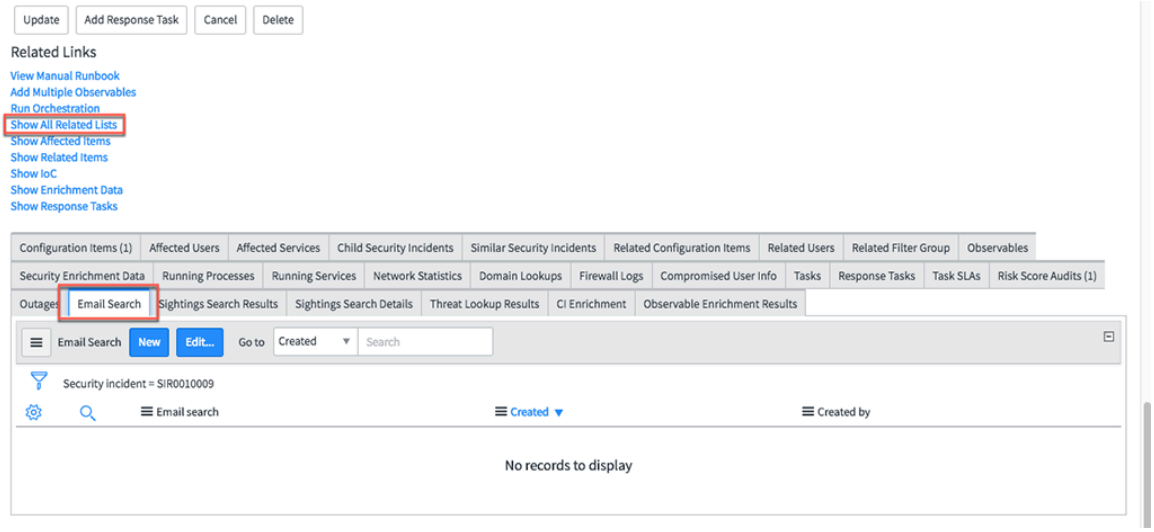
e. Na coluna Número, clique em um incidente de segurança para abrir um registro.

3. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

Se a lista relacionada Pesquisa de e-mail não for exibida, clique em **Mostrar todas as listas relacionadas** link relacionado para exibir esta lista relacionada.

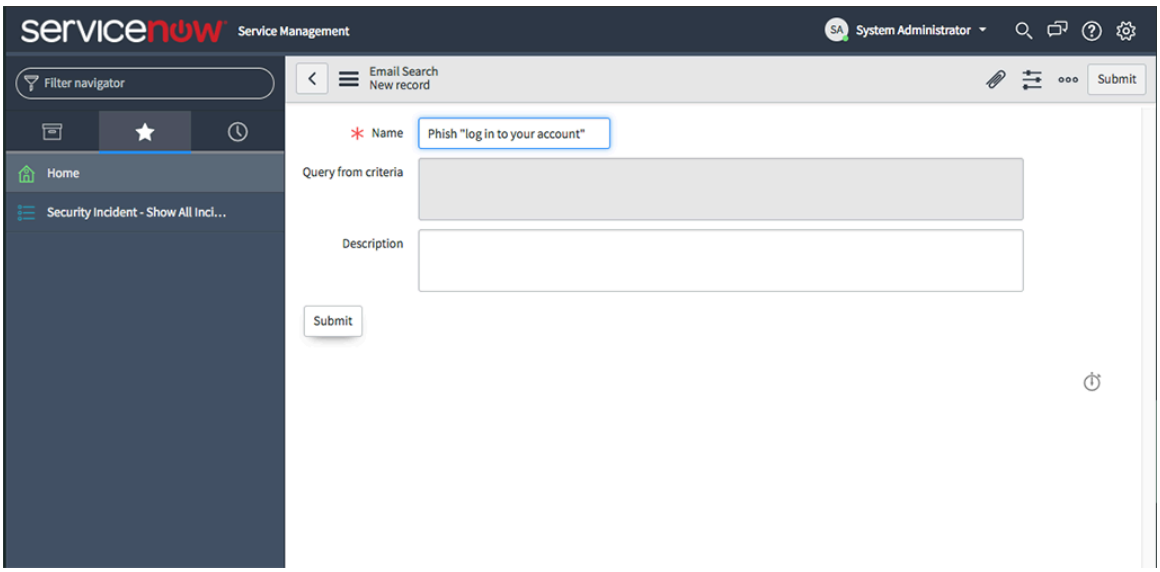
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na lista relacionada Pesquisa de e-mail, clique em **Novo** para criar um novo registro de pesquisa de e-mail. O formulário Pesquisa de e-mail é exibido. Se você determinar que deseja executar novamente esta consulta de pesquisa para o mesmo incidente relacionado a phishing com pequenas modificações, poderá usar este registro de consulta de pesquisa novamente. No entanto, é improvável que você use essa pesquisa para um incidente relacionado a phishing diferente, porque as campanhas de phishing são dinâmicas e os campos de remetente e mensagem mudam com frequência.
5. **Opcional:** Para editar um registro de consulta de pesquisa existente, clique em **Editar** .
6. No formulário Pesquisa de e-mail, preencha os campos.

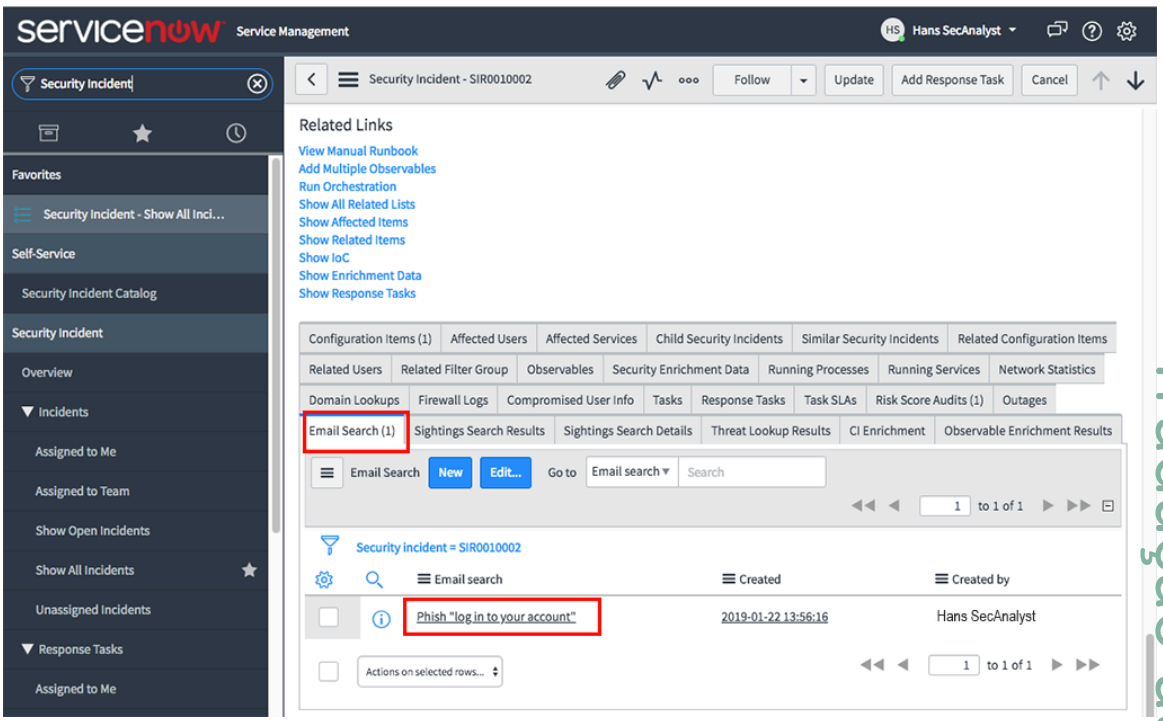
Campo	Descrição
Nome	Informações para descrever o tipo de pesquisa. Para este exemplo, um nome para uma pesquisa De e assunto é Phish "faça login na sua conta" .
Descrição	Informações sobre a pesquisa no servidor de e-mail. Um exemplo para esta pesquisa é Mais de phisher@cbazyx.com assunto: Faça login na sua conta .



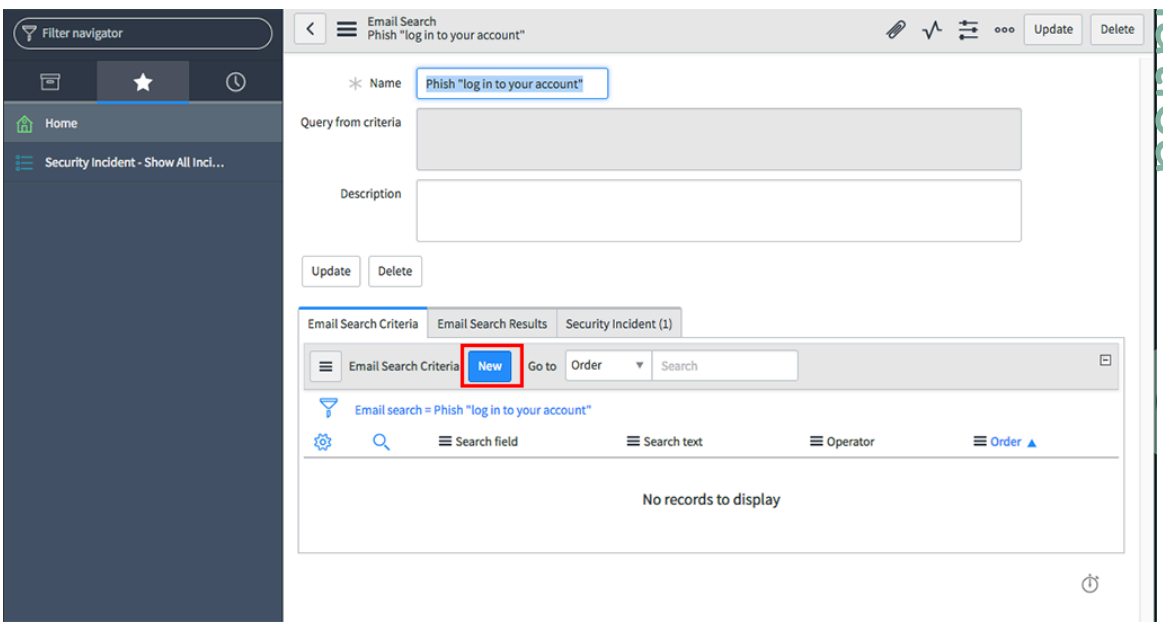
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.
   O incidente de segurança é exibido e o nome da pesquisa de e-mail é exibido na coluna Pesquisa de e-mail na lista relacionada Pesquisa de e-mail. Para que você possa usar esta nova consulta de pesquisa, os critérios de pesquisa devem ser definidos para o registro de pesquisa.
8. Para definir critérios de pesquisa, com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique em **Phish "faça login na sua conta"** .



9. No registro de pesquisa de e-mail exibido, clique na lista relacionada Critérios de pesquisa de e-mail e clique em **Novo** .



10. No formulário Critérios de pesquisa de e-mail, preencha os campos.

    Um exemplo de um formulário preenchido segue a tabela.

Tradução automática

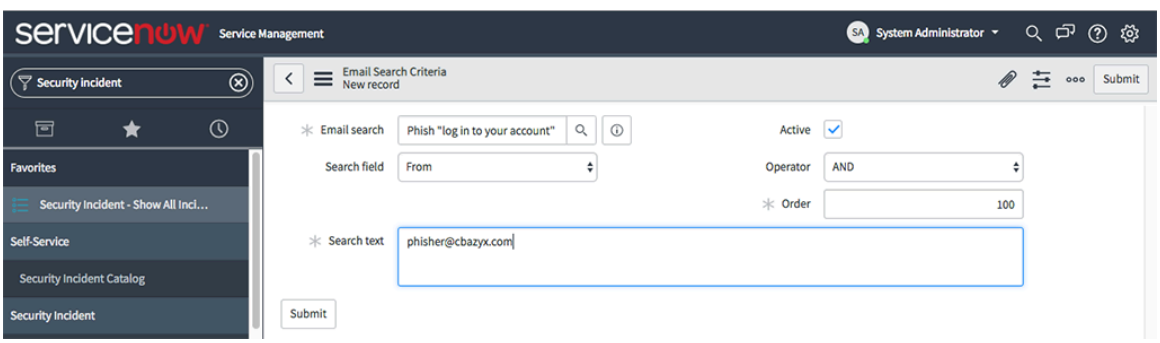
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisa de e-mail	O campo é preenchido automaticamente com o nome que você inseriu para o registro de Pesquisa de e-mail.
Ícone de pesquisa	Pesquisa usando lista. Uma lista de pesquisas salvas. Clique no ícone para abrir uma lista de pesquisas de e-mail salvas. Clique em um item nesta lista para remover a pesquisa atual e selecionar uma pesquisa de e-mail salva anteriormente.
Ícone de informações	Ícone usado para exibir o registro de Pesquisa de e-mail. Clique no ícone para exibir o registro de pesquisa de e-mail.
Campo de pesquisa	Critério de pesquisa (**Assunto** , **De** ou **Destinatário**). Selecione o critério de pesquisa na lista de seleção e defina um valor que você deseja pesquisar no campo de texto. Para este exemplo, comece com de `phisher@cbazyx.com` (o endereço de e-mail do remetente do e-mail de phishing).
Ativo	Opção para ativar a pesquisa. A pesquisa é ativada por padrão. Se você desmarcar esta opção, este registro não será incluído em uma pesquisa.
Operador	Operadores (**E.** , **OU**) para definir ainda mais sua pesquisa. **E.** : O sistema pesquisa as condições separadas por **E.** e retornará resultados somente se todas as condições forem atendidas. Para a pesquisa de remetente mais assunto, use **E.** para que ambas as condições de pesquisa sejam atendidas durante a pesquisa de e-mail. Para este exemplo, use **E.** Para que a consulta seja de (remetente) `phisher@cbazyx.com` **E.** Assunto `faça login na sua conta` . **OU** : O sistema pesquisa e retorna resultados se qualquer uma das condições for separada por **OU** atendidos. Um exemplo é De (remetente) `phisher@cbazyx.com` **OU** De (remetente) `phisher-2@cbazyx.com` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Se você inserir mais de duas condições de pesquisa, use a ordem para priorizar as condições. 100 é o padrão. Insira um valor entre 1 e 100 para cada condição, por exemplo, 100, 95, 90, 80. A condição com o menor número atribuído tem a prioridade de pesquisa mais alta em um grupo de condições.
Pesquisar texto	Os valores de texto (palavras-chave) da pesquisa (endereços de e-mail ou linhas de assunto). O campo de pesquisa contém o texto usado na pesquisa, por exemplo, phisher@cbazyx.com . Para que a pesquisa retorne resultados com precisão para pesquisas de remetente (de) e destinatário, as cadeias de caracteres de pesquisa devem corresponder exatamente. Para pesquisas de assunto, a cadeia de caracteres de pesquisa pode conter palavras-chave que fazem parte de uma cadeia de caracteres maior. Por exemplo, um assunto pode conter a cadeia de caracteres de pesquisa exata que corresponde a um cabeçalho de mensagem encaminhada ou de resposta, como FW: Faça login em sua conta e mude sua senha imediatamente . Por exemplo, Faça login na sua conta são palavras-chave exatas na cadeia de caracteres faça login em sua conta e mude sua senha imediatamente . Nenhuma designação curinga (*) é necessária para oferecer suporte a *contém* tipo de pesquisa. Atualmente, não existe nenhum método de filtragem para corresponder a uma cadeia de caracteres de pesquisa exata que não faz parte de uma cadeia de caracteres de texto maior.

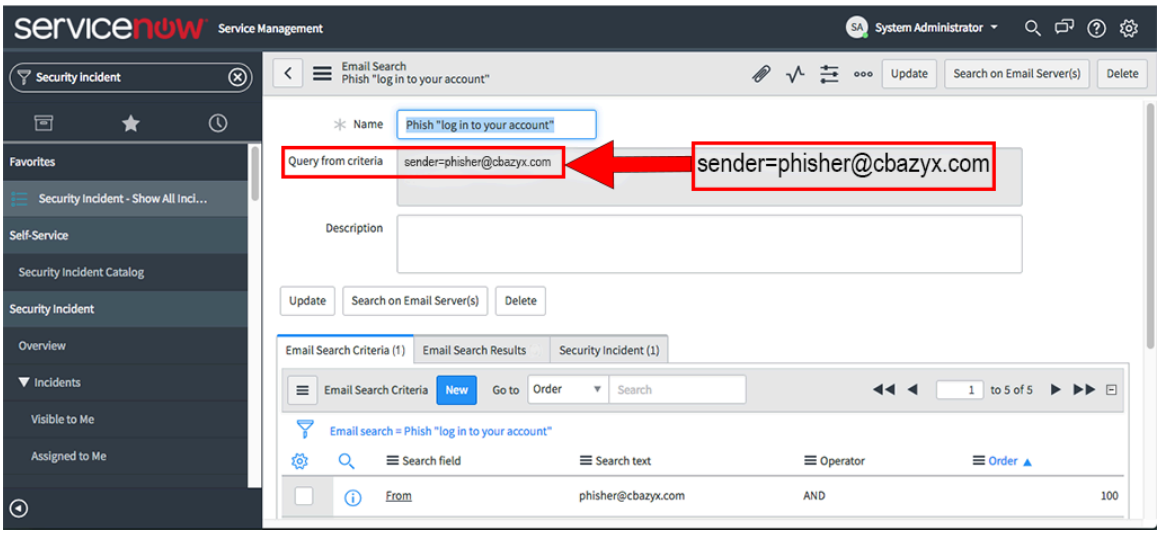


11. Clique em **Enviar**.

Tradução automática

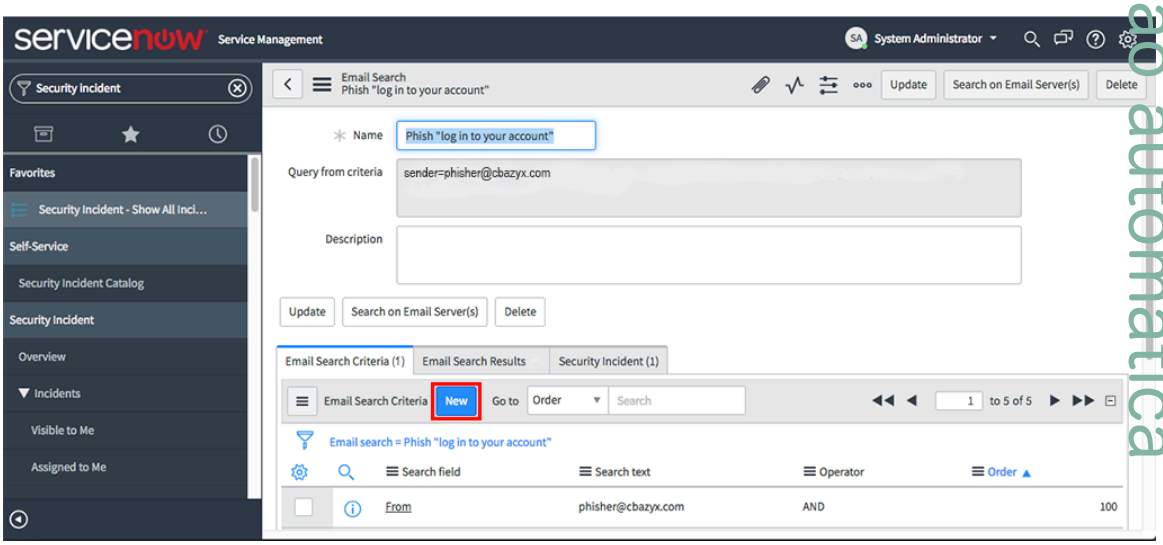
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro de Pesquisa de e-mail é exibido. Em **Consulta a partir dos critérios** Os critérios de pesquisa adicionados para o remetente (de) são exibidos.



12. Para atualizar esses critérios de pesquisa de e-mail com mais informações para que a consulta inclua a condição assunto mais remetente desejada, siga as etapas para adicionar outra condição de pesquisa.

a. Na lista relacionada Critérios de pesquisa de e-mail, clique em **Novo** .



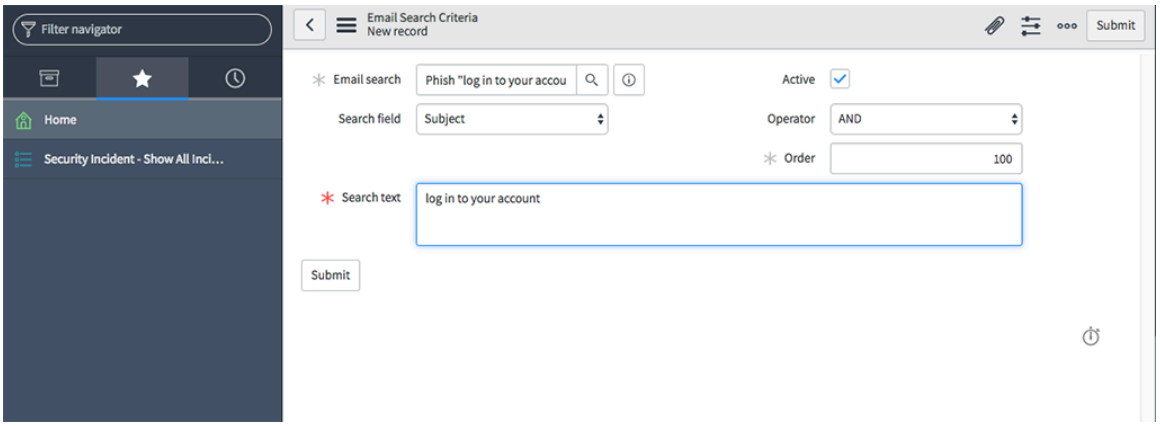
b. Em **Campo de pesquisa** No registro Critérios de pesquisa de e-mail exibido, selecione **Assunto** .

c. Na lista Operador, selecione **E.** ou **OU** .
Se você selecionar **OU** , a pesquisa retornará resultados se as palavras-chave na cadeia de caracteres de texto da linha de assunto forem correspondidas ou se a condição do endereço de e-mail for correspondida. **E.** está selecionado para este exemplo para que a pesquisa retorne resultados somente para e-mails que contenham as palavras-chave da cadeia de caracteres de texto do assunto e que correspondam ao endereço de e-mail do remetente.

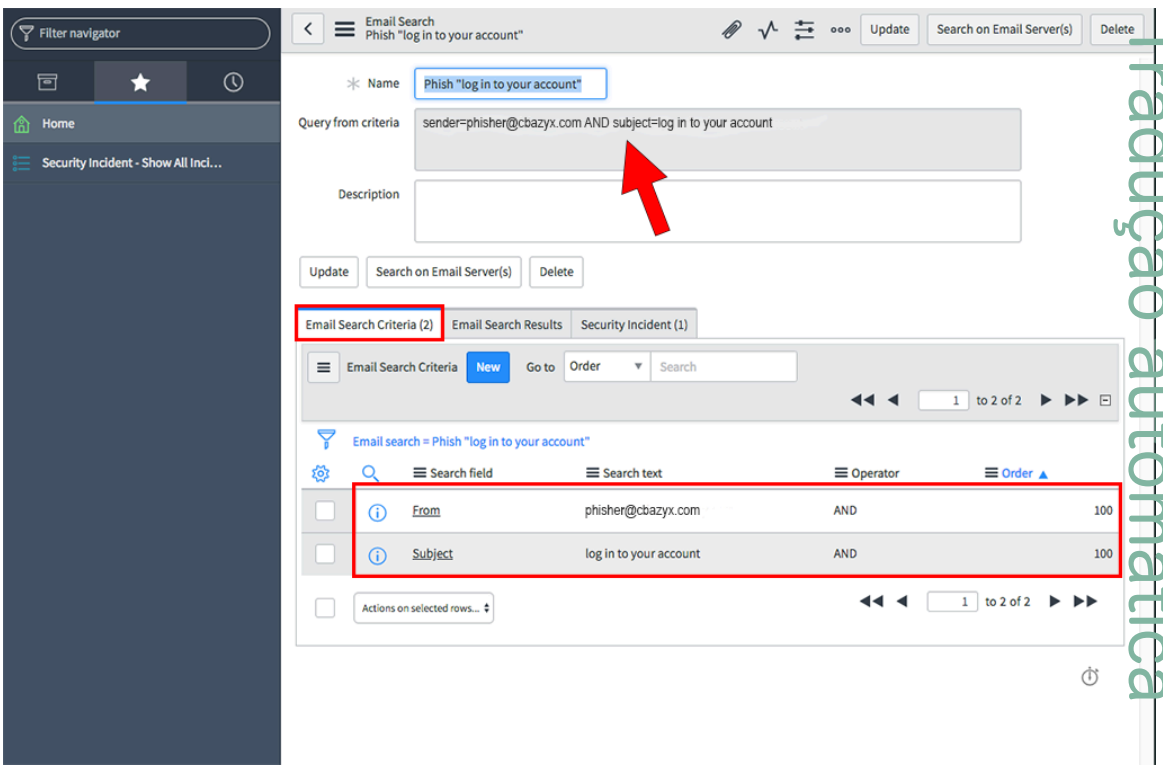
d. Em **Texto de pesquisa** , insira o valor do texto da linha de assunto, `faça login na sua conta` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Clique em **Enviar**.
A nova condição é exibida na lista relacionada Critérios de pesquisa de e-mail e ambas as condições são exibidas no **Consulta a partir dos critérios** campo separado por **E.** operador.



Tradução automática

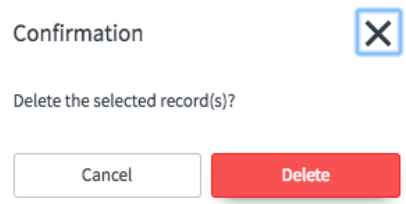
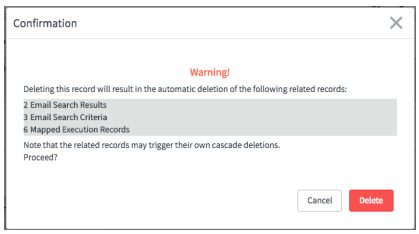
f. Opcional: Se você tiver mais de duas condições de pesquisa e selecionar **E.** para separar cada condição, defina o valor do pedido para priorizá-las.

g. Continue a adicionar, modificar ou remover critérios de pesquisa conforme desejado e clique em **Atualização** para salvar suas mudanças no registro.

13. Escolha uma opção para continuar.

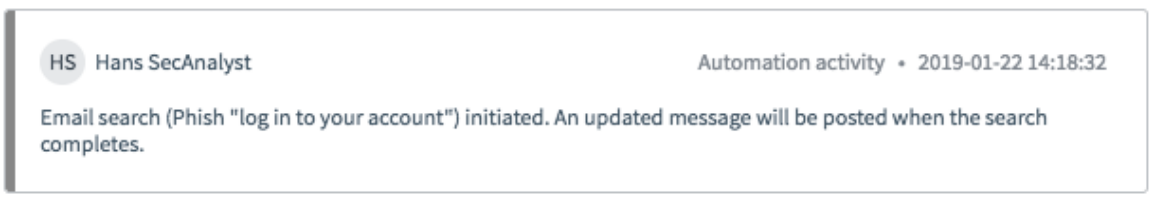
Opção	Descrição
Atualizar	Atualize e salve suas mudanças no registro.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Pesquisar em Servidor(es) de E-mail	Inicie uma pesquisa nos servidores com os critérios salvos no registro Critérios de pesquisa de e-mail.
Excluir	Exclua este registro de Pesquisa de e-mail do seu ServiceNow AI Platform instância. Esta ação não exclui as mensagens de e-mail reais. Exclui somente o registro de pesquisa usado para encontrar mensagens. Uma caixa de diálogo é exibida. Se você clicar em **Excluir**, os resultados da pesquisa de e-mail e os critérios de pesquisa de e-mail para este registro de pesquisa são excluídos.  Se um registro tiver resultados de pesquisa, o aviso a seguir será exibido. 

14. Para iniciar uma pesquisa de e-mail, no registro de pesquisa de e-mail, clique em **Pesquisar em servidores de e-mail**.
É exibida uma mensagem indicando que a solicitação de pesquisa foi enviada.

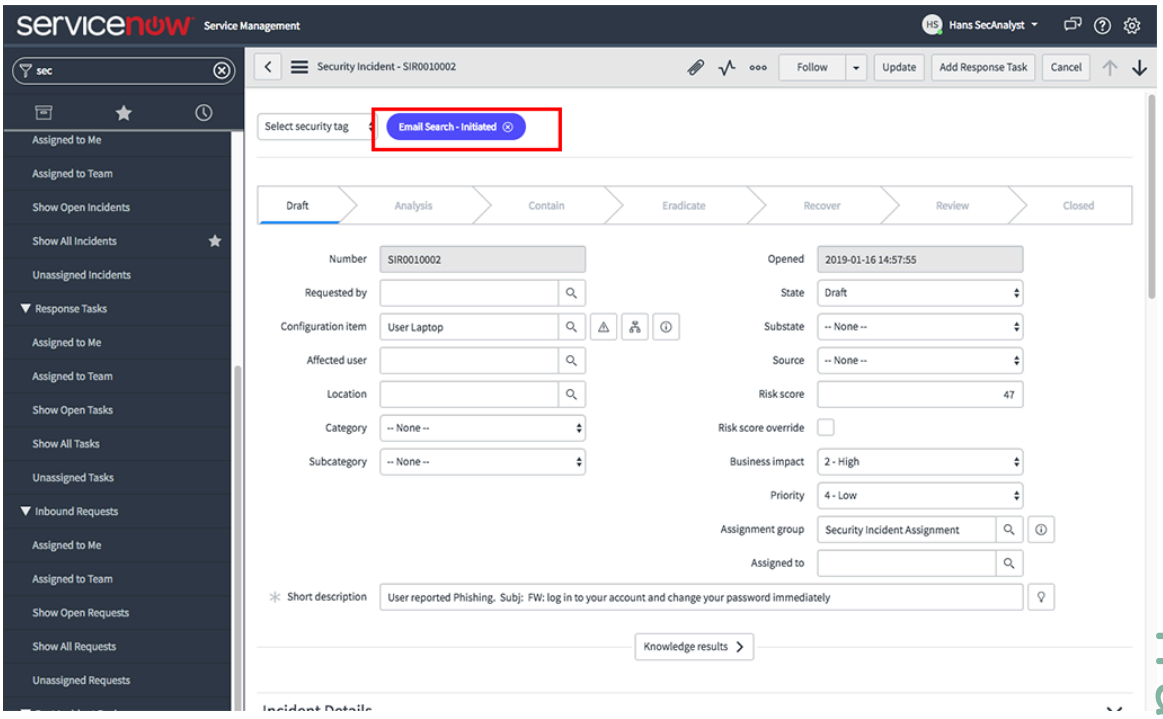
No registro de Incidente de segurança, uma anotação de trabalho é exibida indicando que uma pesquisa foi iniciada.



Se a marcação estiver habilitada, na parte superior do registro de Incidente de segurança, o. Pesquisa de e-mail - Iniciada o marcador de segurança é exibido.

Tradução automática

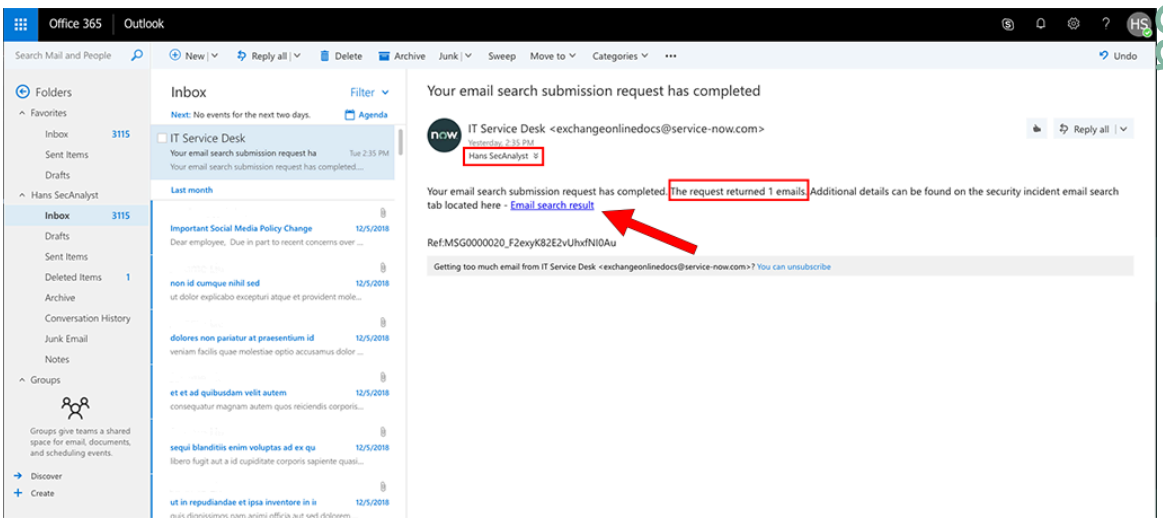
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se a pesquisa for concluída com sucesso, se as notificações por e-mail estiverem habilitadas, um e-mail será enviado para o endereço de e-mail do indivíduo que iniciou a pesquisa.

Neste exemplo, o usuário com a função sn_si.analyst, Hans SecAnalyst esta pesquisa foi enviada. A imagem a seguir mostra que esta notificação é enviada para uma conta em Microsoft Exchange Online. No entanto, essas notificações podem ser enviadas para um serviço de e-mail diferente, conforme necessário.

Esta notificação permite exibir todos os resultados correspondentes que exigem acompanhamento e exclusão. O exemplo a seguir mostra que há um e-mail que correspondeu aos critérios de pesquisa. Um link do resultado da pesquisa por e-mail para o registro do resultado da pesquisa por e-mail em seu ServiceNow AI Platform a instância também é fornecida. Se você quiser exibir o registro de pesquisa, clique neste link.



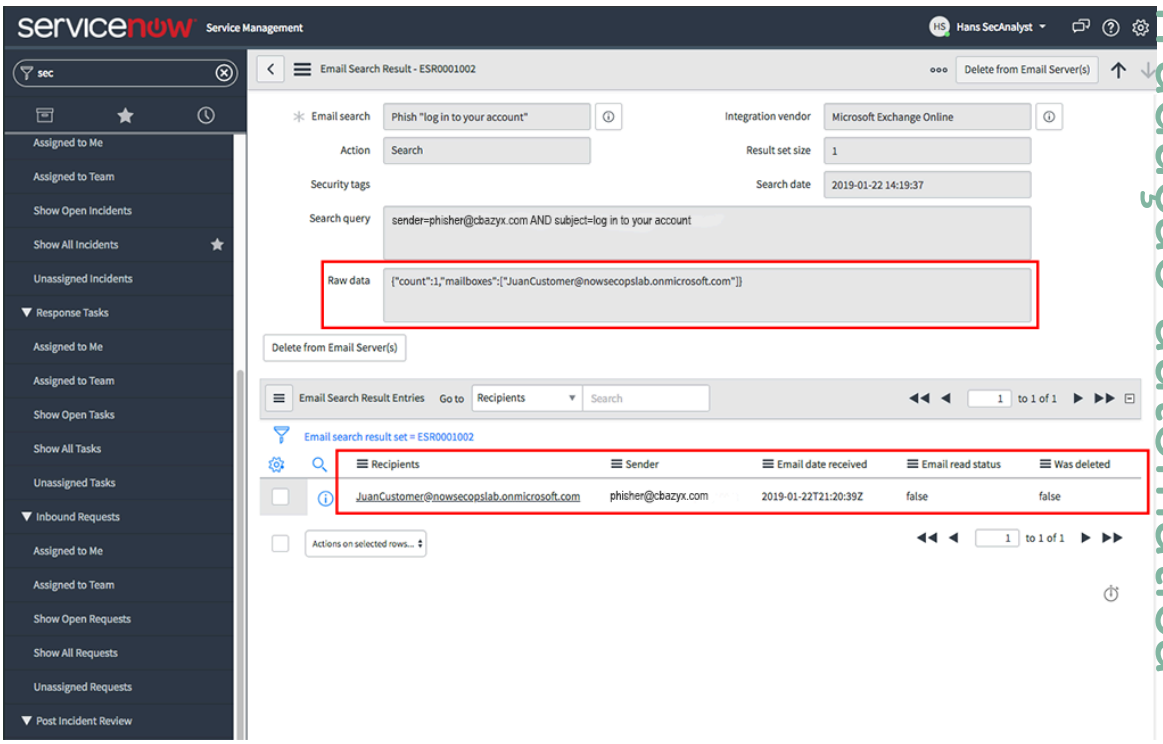
15. Neste e-mail, para exibir os resultados da pesquisa, clique em **Resultado da pesquisa de e-mail** link.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro do resultado da pesquisa de e-mail é exibido. Neste registro, você pode verificar e revisar os dados a seguir.

- Em **Dados brutos** campo, a contagem de e-mails referente ao número de e-mails que corresponderam aos critérios de pesquisa "contagem": 1 e os endereços de caixa de correio em que os e-mails foram encontrados são exibidos ["JuanCustomer@nowsecopslab.onmicrosoft.com"] .
- Na coluna Destinatários, o destinatário é (JuanCustomer@nowsecopslab.onmicrosoft.com).
- Em Remetente , a origem do e-mail é exibida.
- Em Data de recebimento do e-mail a data e a hora em que o e-mail foi recebido são exibidas para ajudar você a rastrear os cronogramas da campanha de phishing.
- Em Status de leitura de e-mail , o e-mail neste exemplo não foi lido (falso). Se um e-mail tiver sido lido, verdadeiro é exibido.
- Em Excluído , o e-mail neste exemplo não foi excluído. Se um e-mail tiver sido excluído, verdadeiro é exibido.

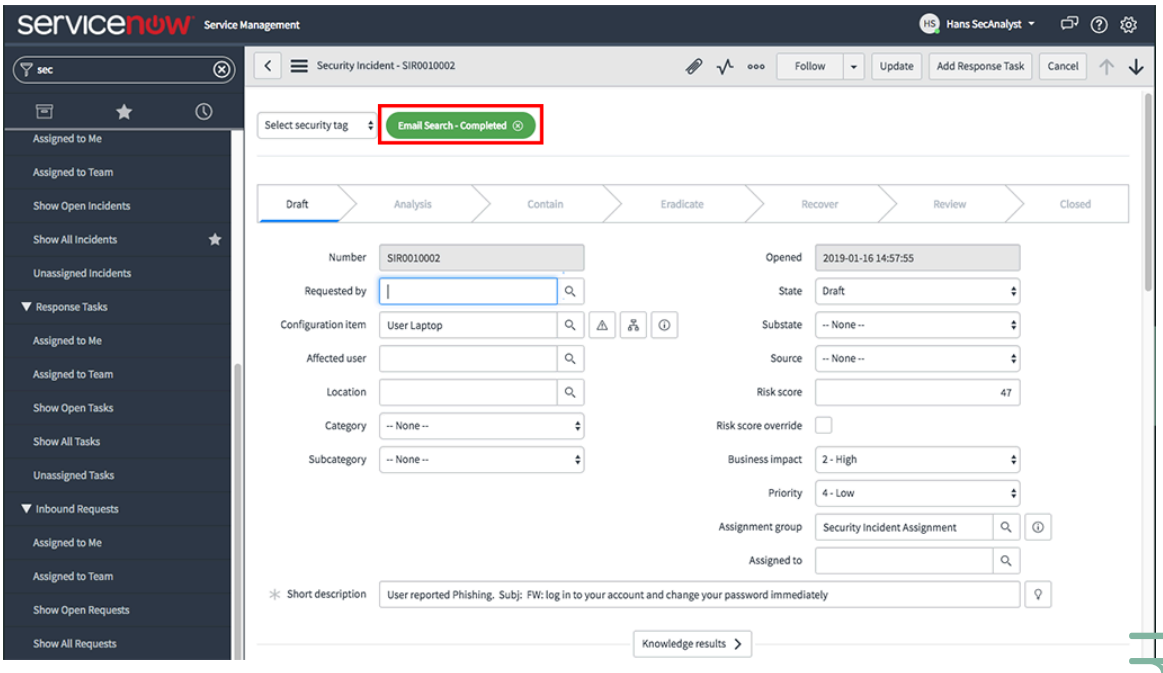


Tradução automática

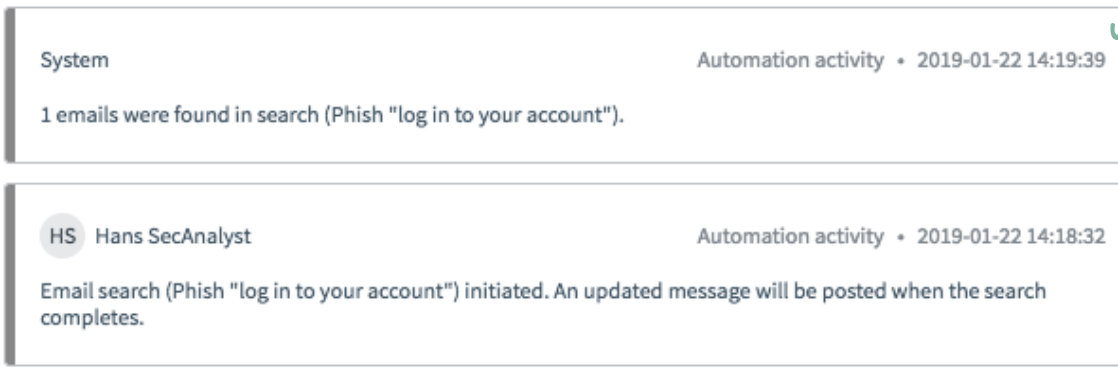
16. Como alternativa, para exibir os resultados da pesquisa do incidente de segurança, siga estas etapas.

a. Navegar até **Incidente de segurança** > **incidentes** e abra o incidente de segurança com o qual você está trabalhando.
Na parte superior do registro, quando a pesquisa é concluída com sucesso, o. Pesquisa de e-mail - Concluída o marcador de segurança substitui o. Pesquisa de e-mail - Iniciada marcador de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As anotações de trabalho são exibidas informando que a pesquisa foi concluída com sucesso e que um e-mail correspondente foi encontrado.

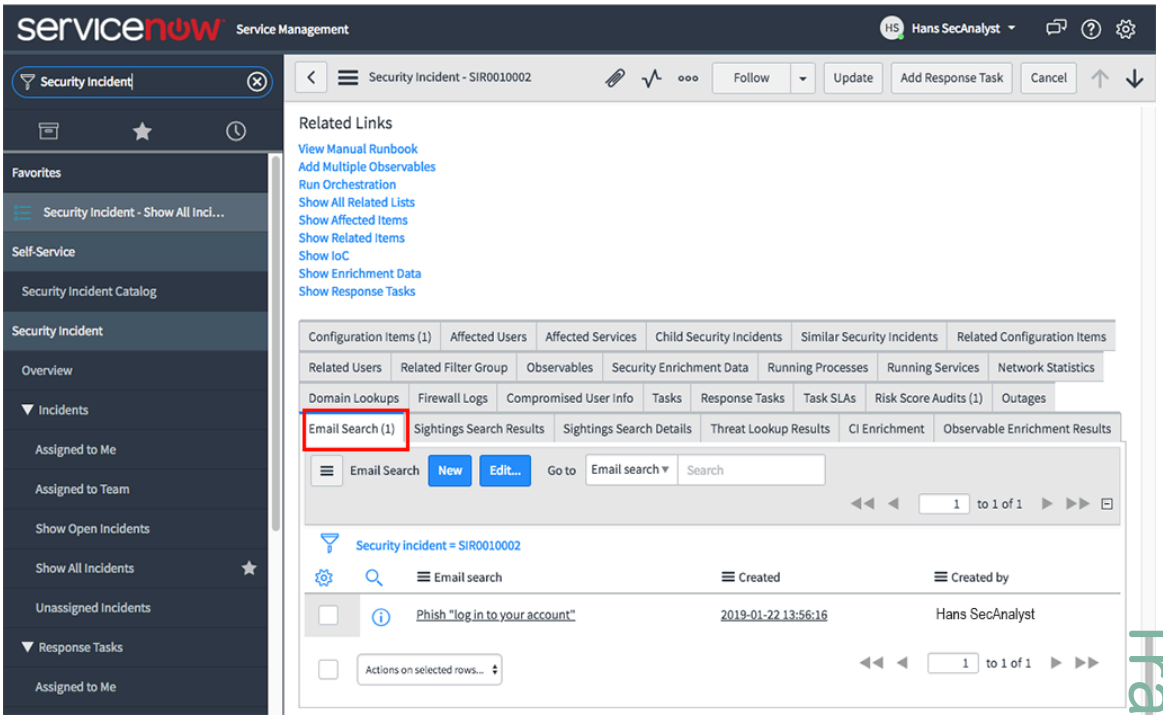


b. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

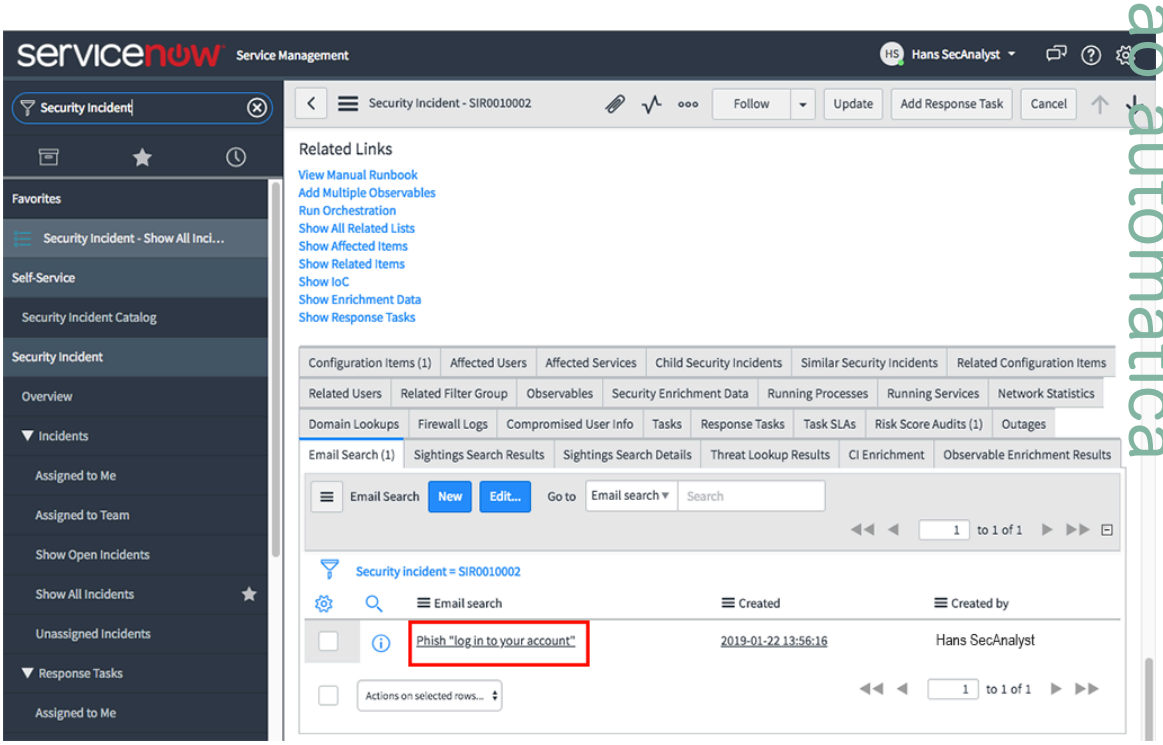
Se a lista relacionada Pesquisa de e-mail não for exibida, clique em **Mostrar todas as listas relacionadas** link relacionado para exibir esta lista relacionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da pesquisa.



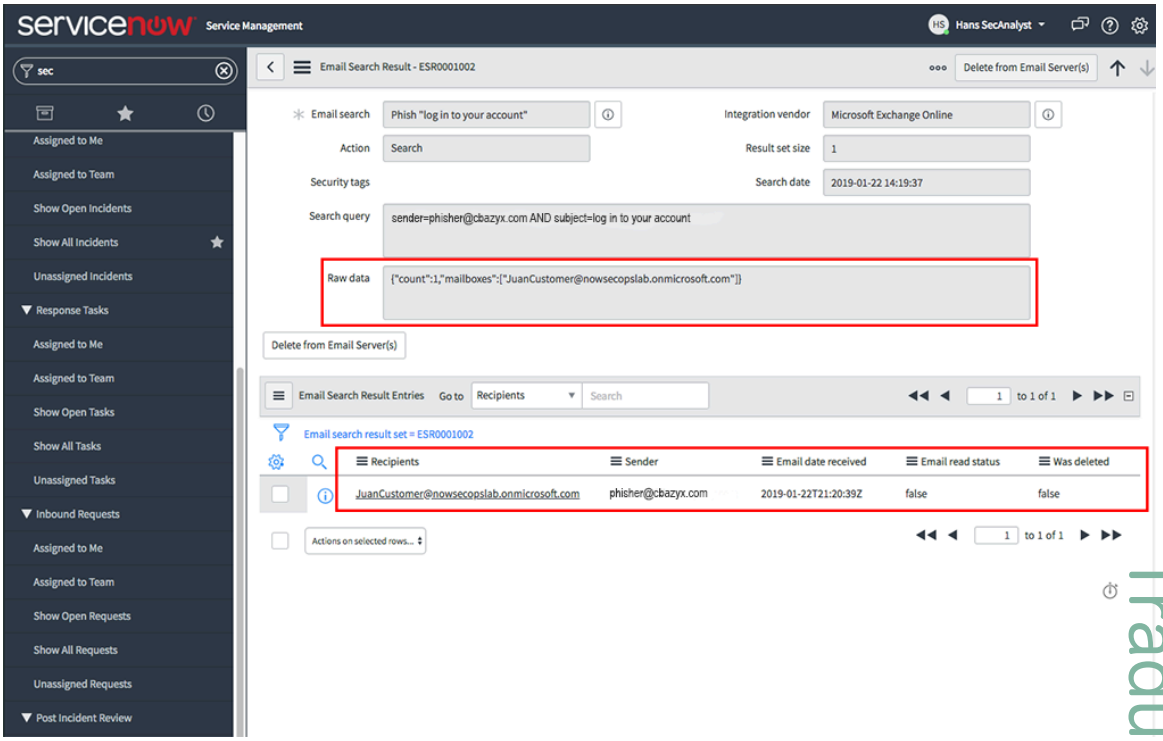
d. No registro de Pesquisa de e-mail, clique na lista relacionada Resultados da pesquisa de e-mail.

e. Na coluna Data da pesquisa, clique na data da pesquisa para exibir os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro do resultado da pesquisa de e-mail é exibido.



Depois que uma pesquisa de e-mail for concluída com sucesso, avalie os resultados. Se você determinar que os e-mails exigem correção, agora você está pronto para excluir e-mails ou solicitar aprovação de exclusão.

Solicitar aprovação de exclusão para e-mails no serviço online do Microsoft Exchange

Depois que uma pesquisa de e-mail for concluída com sucesso e as mensagens correspondentes forem identificadas, você poderá excluir permanentemente todos os e-mails suspeitos do serviço online do Microsoft Exchange relacionados ao incidente de segurança e à campanha de phishing.

Antes de Iniciar

Função necessária: sn_si.analyst

O sistema executa exclusões nos resultados de pesquisa bem-sucedidos mais recentes.

Por Que e Quando Desempenhar Esta Tarefa

Se as aprovações e as notificações por e-mail estiverem habilitadas, envie uma solicitação para excluir e-mails para um grupo de aprovação antes da remoção do e-mail.

Os resultados da pesquisa por e-mail são exibidos com todas as mensagens recebidas. Para garantir que os e-mails de phishing sejam excluídos com sucesso, os resultados da exclusão são publicados nas anotações de trabalho do incidente de segurança associado. Se a marcação estiver habilitada, um marcador de segurança também será exibido no incidente de segurança relacionado. Se o e-mail não for excluído com sucesso, você também será notificado nas anotações de trabalho.

Dependendo das políticas organizacionais, pode ser necessário solicitar aprovação antes de excluir e-mails de phishing. O processo de aprovação de exclusão requer informações sobre o número de e-mails a serem excluídos e, potencialmente, acesso a outros detalhes da mensagem. Para processar a solicitação de exclusão, em uma notificação por e-mail, um aprovador recebe a contagem de mensagens de e-mail correspondente, o link do incidente de segurança para acessar os detalhes completos da mensagem e aprovar ou rejeitar links. Os links neste e-mail permitem que um aprovador aceite ou rejeite a solicitação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exclusão da notificação por e-mail. Uma trilha de auditoria completa com carimbo de data/hora também está disponível para rastrear quando o status de aprovação foi alterado nas anotações de trabalho. Se um grupo de aprovação for atribuído, um usuário no grupo poderá processar a solicitação para todo o grupo. Cada membro do grupo de aprovação recebe uma notificação por e-mail para a solicitação.

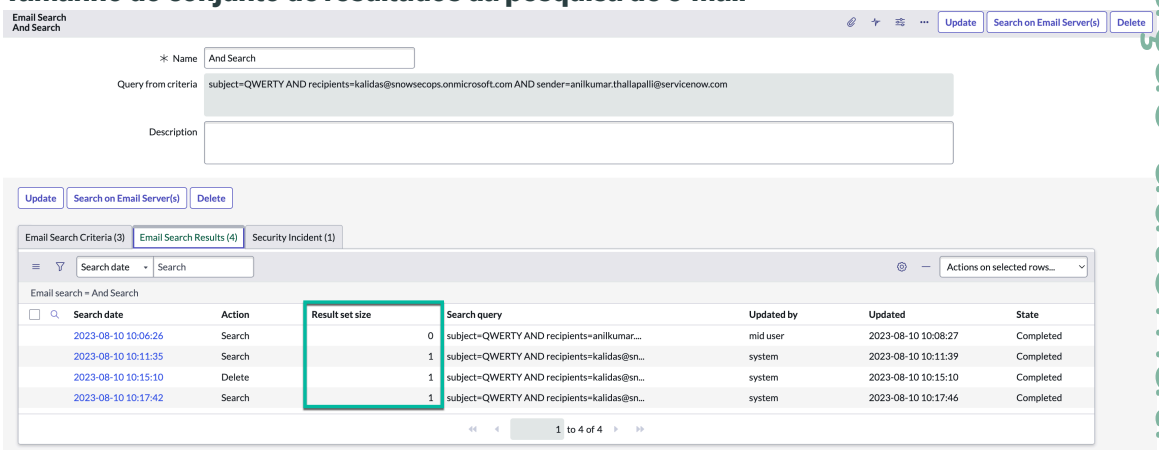
Como um usuário com a função sn_si.analyst, se você determinar que os e-mails precisam de correção, siga as etapas necessárias para excluir e-mails. Se as aprovações estiverem habilitadas, solicite aprovação para excluir e-mails do Microsoft Exchange Online serviço.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança > Mostrar todos os incidentes**.
2. Clique em **Pesquisa de e-mail** lista relacionada.
3. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da pesquisa.
   Os resultados da pesquisa são exibidos na lista relacionada Resultados da pesquisa de e-mail.

   Para este exemplo, esta pesquisa encontrou e-mails que correspondem aos seus critérios de pesquisa. Há duas ações de pesquisa listadas no registro. Uma pesquisa não tem correspondências (0) e a outra pesquisa tem um e-mail correspondente (1).

Tamanho do conjunto de resultados da pesquisa de e-mail

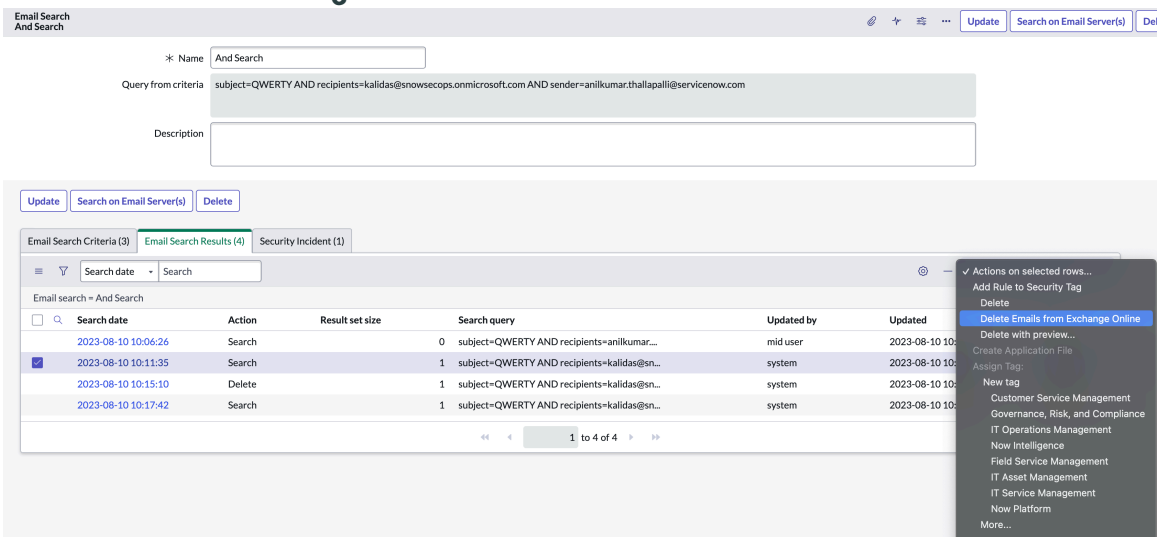


4. Para excluir itens de e-mail associados a uma pesquisa, à esquerda da coluna Data de pesquisa, marque a caixa de seleção de um conjunto de resultados de pesquisa.
   Você pode selecionar um único conjunto de resultados ou vários conjuntos de resultados na lista.
5. Selecione os conjuntos de resultados que você deseja excluir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Excluir e-mails do Exchange Online

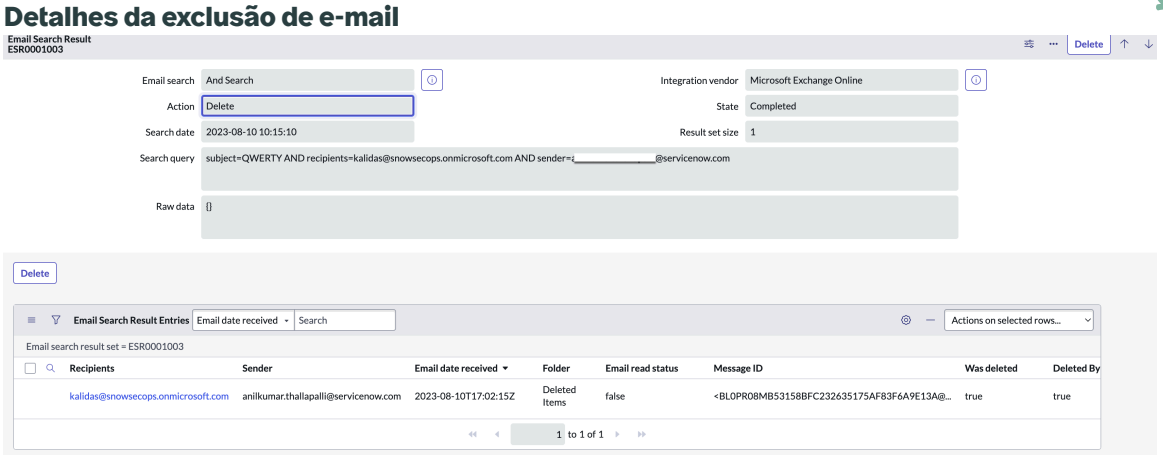


6. Na parte inferior da lista relacionada Resultados da pesquisa de e-mail, na lista Ações nas linhas selecionadas, selecione **Exclua e-mails do Exchange Online** Para excluir todos os itens de e-mail associados a um ou mais conjuntos de resultados do servidor do Exchange Online.
Se um conjunto de resultados contiver mais de um e-mail, você não precisará abrir o registro Resultado da Pesquisa de e-mail e selecionar e-mails individuais para excluí-los. Todos os itens de e-mail com status falso Na coluna Foi excluído no registro Resultado da pesquisa de e-mail são excluídos depois que você seleciona **Exclua e-mails do Exchange Online** .

   Se um item de e-mail em um conjunto de resultados já tiver sido excluído, o status na coluna Foi excluído no registro Resultado da pesquisa de e-mail será verdadeiro . Esses itens não são excluídos novamente.

   Se a opção Aprovação estiver desabilitada durante a etapa de configuração, depois de selecionar **Exclua e-mails do Exchange Online** , os e-mails associados ao conjunto de resultados são excluídos. O conjunto de resultados em si não é excluído. No entanto, o status de todos os itens de e-mail excluídos do conjunto de resultados é atualizado para verdadeiro Na coluna Foi excluído do registro Resultado da pesquisa de e-mail. Para obter mais informações sobre o recurso de aprovação, consulte Configure o. Microsoft Exchange Online integração.

Detalhes da exclusão de e-mail

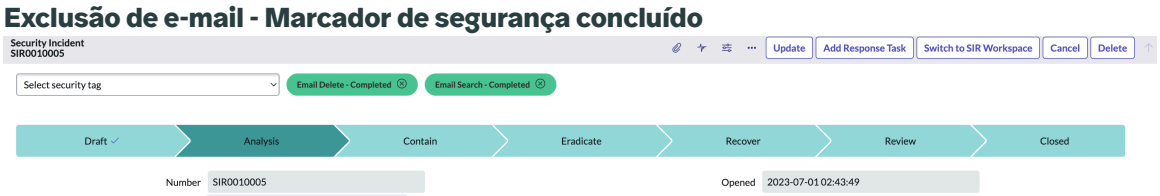


   Esses e-mails são excluídos do Microsoft Exchange Online locatário no qual você realizou as pesquisas. Uma anotação de trabalho será exibida se os e-mails forem excluídos com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No registro de incidente de segurança, o. Exclusão de e-mail - Concluída o marcador de segurança é exibido.

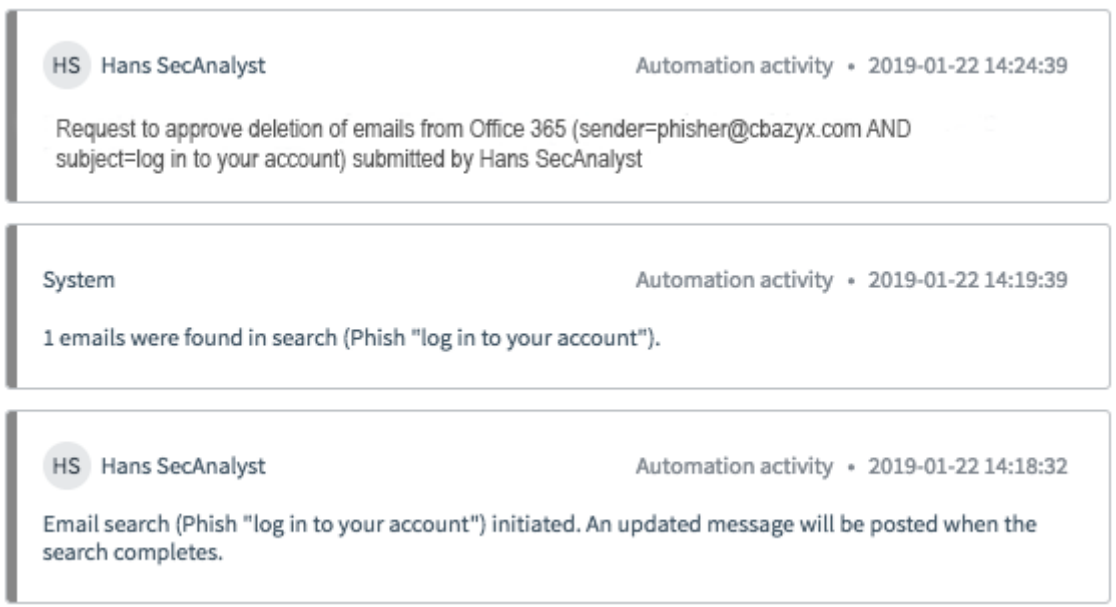


Se as aprovações estiverem desabilitadas para solicitações de exclusão, você excluirá e-mails com sucesso do Microsoft Exchange Online locatário.

Se as aprovações estiverem habilitadas para solicitações de exclusão durante a etapa de configuração, depois de selecionar **Exclua e-mails do Exchange Online** uma notificação por e-mail é enviada para cada membro do grupo de aprovação selecionado durante a etapa de configuração.

Se a marcação estiver habilitada durante a etapa de configuração, o. Exclusão de e-mail - Iniciada o marcador de segurança é exibido no registro de incidente de segurança relacionado. Para obter mais informações sobre marcação, consulte Configure o. Microsoft Exchange Online integração.

As anotações de trabalho são exibidas informando que uma solicitação para excluir e-mails é enviada pelo usuário com a função sn_si.analyst (Hans SecAnalyst).



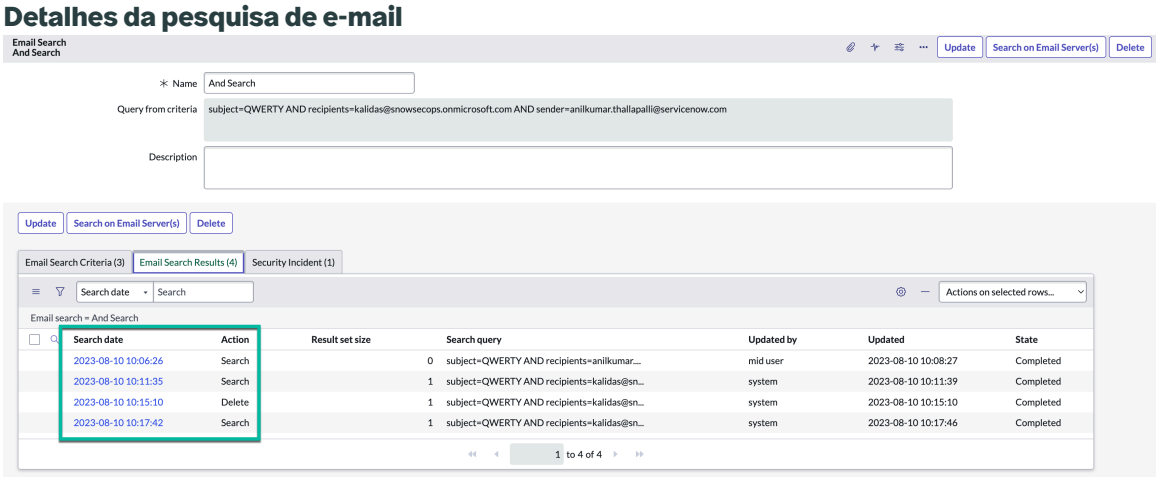
Se as aprovações estiverem habilitadas, a próxima etapa será processar a solicitação de exclusão.

7. Se você quiser exibir os detalhes e itens de e-mail individuais de um registro de pesquisa antes de excluí-lo ou enviar uma solicitação de exclusão, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Com a lista relacionada Resultados da pesquisa de e-mail selecionada, na coluna Data da pesquisa, clique na data de uma pesquisa que você deseja revisar.



As seguintes informações sobre os e-mails são exibidas:

- Destinatários
- Remetente
- Data de recebimento do e-mail
- Status de leitura de e-mail (verdadeiro ou falso)
- Foi excluído (verdadeiro ou falso)
- Excluído pela integração (verdadeiro ou falso)

Nota:

O valor é definido como verdadeiro quando o e-mail é excluído quando o analista inicia a exclusão do(s) servidor(es) de e-mail.

As anotações de trabalho são atualizadas com o número total de registros excluídos, o que inclui os registros excluídos pela integração e pelo usuário.

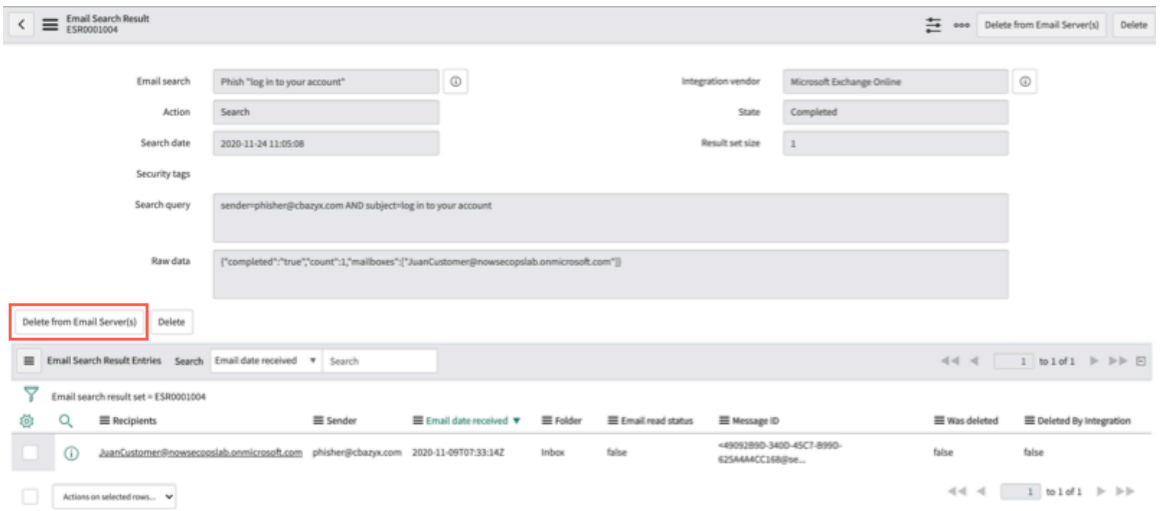
b. Depois de revisar os dados, para excluir todos os e-mails ou enviar uma solicitação para excluir todos os e-mails, clique em **Excluir do(s) servidor(es) de e-mail** .

Conforme descrito no exemplo anterior, se houver mais de um e-mail listado no registro de resultado da pesquisa, você não precisará selecionar os e-mails individuais para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

removê-los. A solicitação de exclusão remove todos os e-mails associados à pesquisa quando falso É exibido na coluna Foi excluído dos resultados da pesquisa mais recentes.



Se as aprovações estiverem habilitadas, você enviou com sucesso uma solicitação para excluir e-mails. Os marcadores de segurança e as anotações de trabalho são exibidos no registro de incidente de segurança relacionado, conforme descrito no exemplo anterior. Como aprovador, a próxima etapa é processar a solicitação de exclusão.

Aprovar solicitações de exclusão de e-mail para Microsoft Exchange Online integração

Se a opção Aprovação estiver habilitada em seu ServiceNow AI Platform solicitações para excluir e-mails são enviadas para cada membro do grupo de aprovação por e-mail. Você seleciona o grupo de aprovação durante a etapa de configuração. As aprovações fornecem à sua organização um nível adicional de controle sobre a exclusão de e-mails.

Antes de Iniciar

Verifique se você tem **Aprovações** Opção selecionada na guia Configurações adicionais do formulário Configurações de configuração de pesquisa e exclusão de e-mails do Exchange Online.

Verifique se você habilitou o e-mail **Envio de e-mail habilitado** e. **Recebimento de e-mail habilitado** opções em seu ServiceNow AI Platform instância para solicitações de aprovação.

Por padrão, quando o usuário com a função sn_si.analyst envia solicitações de exclusão por e-mail, essas solicitações são enviadas por e-mail para sn_si.admin. Se você criou um grupo de aprovação, cada membro do grupo receberá uma notificação. Os aprovadores podem processar solicitações de exclusão por e-mail diretamente da notificação por e-mail. Como alternativa, as solicitações podem ser processadas a partir dos registros de resultados de pesquisa de e-mail em ServiceNow AI Platform instâncias. Este tópico mostra os dois métodos de aprovação.

As seguintes informações descrevem a solicitação na notificação por e-mail:

Número do registro do resultado da pesquisa de e-mail

Número exclusivo atribuído ao registro de pesquisa pelo ServiceNow AI Platform como parte da trilha de auditoria.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do analista que enviou a solicitação

Nome da pessoa que enviou a solicitação como parte da trilha de auditoria.

Link para o incidente de segurança

Um link para o incidente de segurança relacionado ao evento de phishing. Exiba o incidente de segurança com as anotações de trabalho, pesquisas de e-mail e resultados de pesquisa de e-mail diretamente do e-mail.

Aprovar ou rejeitar links

Links para aprovar ou rejeitar a solicitação da notificação por e-mail. Depois que você clica em um link, o sistema inicia automaticamente o fluxo de trabalho relacionado e uma anotação de trabalho é publicada no registro de incidente de segurança.

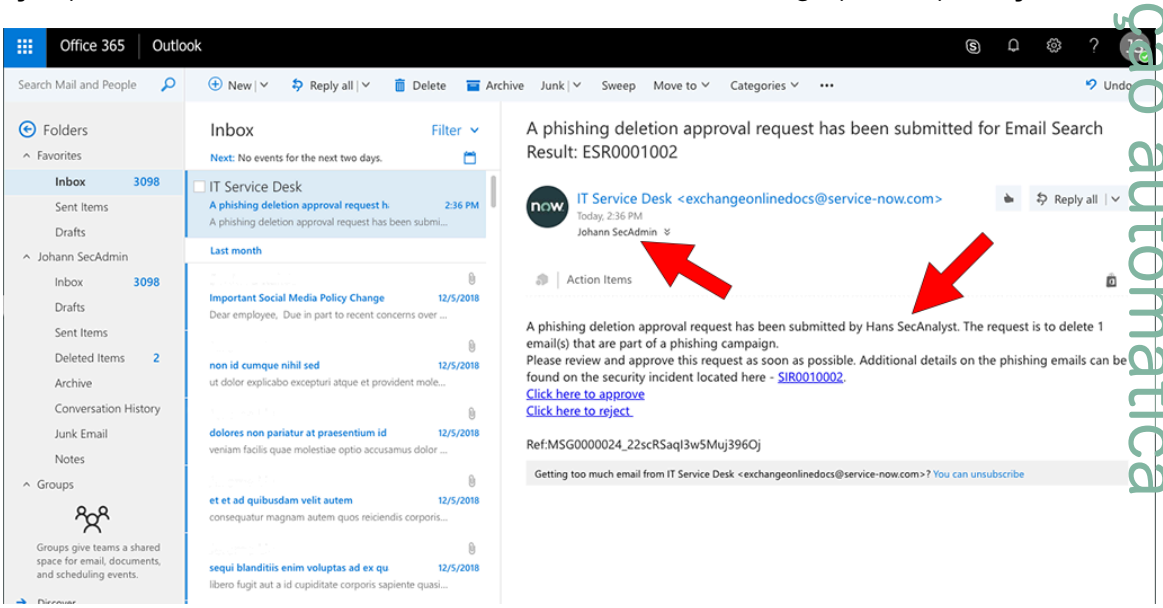
Função necessária: sn_si.admin ou todos os membros de um grupo de aprovação atribuído.

Procedimento

1. Para processar a solicitação de exclusão da notificação por e-mail, siga estas etapas.

   a. Como aprovador, localize o e-mail de notificação na conta de e-mail que você configurou em ServiceNow AI Platform conta de usuário.

   Neste exemplo, o usuário com a função sn_si.analyst (Hans SecAnalyst) envia uma solicitação para excluir um e-mail. Johann SecAdmin é membro do grupo de aprovação.



   b. Na notificação por e-mail, escolha uma opção para continuar.

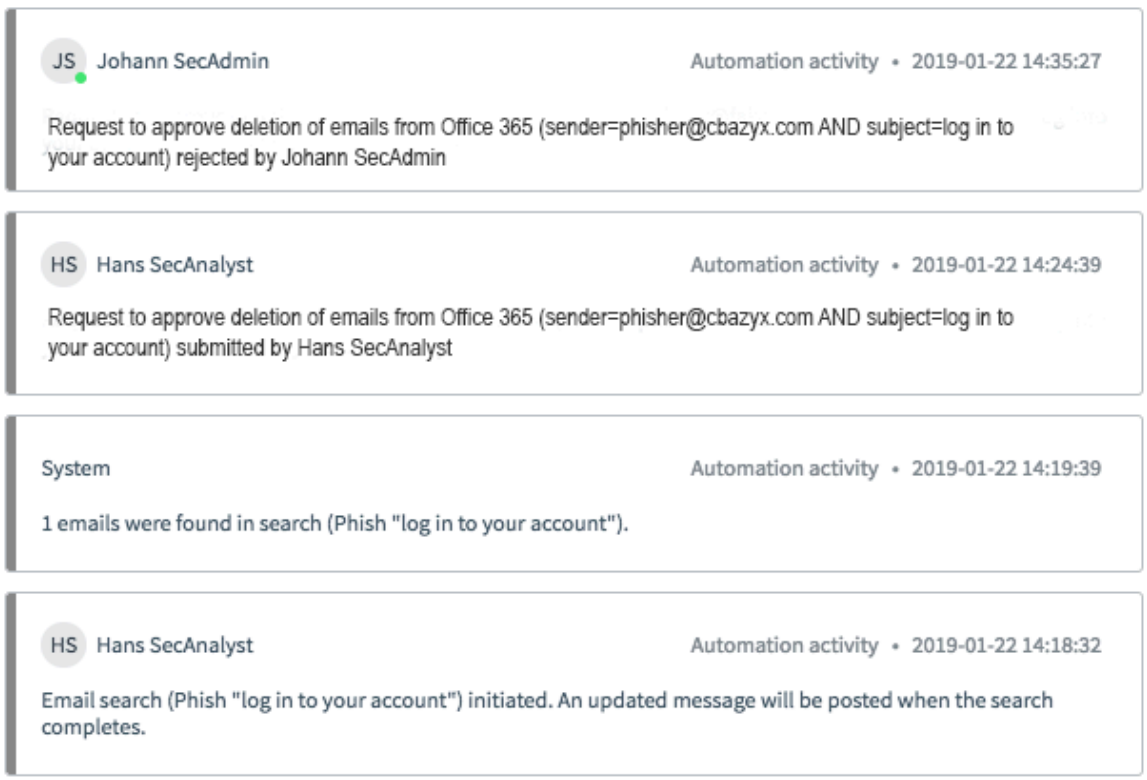
Opção	Descrição
Clique no link Clique aqui para aprovar a aprovação	Aprovar a solicitação de exclusão. Todos os itens de e-mail com status falso Na coluna Foi excluído que estão associados ao registro do resultado da pesquisa são excluídos automaticamente do Microsoft Exchange Online locatário. O status de todos os itens de e-mail do conjunto de resultados é atualizado para verdadeiro Na coluna Foi excluído do registro de resultado da pesquisa de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Uma anotação de trabalho é publicada no registro de incidente de segurança com o número de e-mails excluídos com sucesso. Se a marcação estiver habilitada, o. Exclusão de e-mail - Concluída o marcador substitui Exclusão de e-mail - Iniciada marcador.
Clique no link Clique aqui para rejeitar	Rejeitar a solicitação de exclusão. Uma anotação de trabalho é publicada com o nome da pessoa que rejeitou a solicitação. Depois que uma solicitação é rejeitada, como o usuário com a função sn_si.analyst, você deverá enviar uma nova solicitação de exclusão se determinar que os e-mails devem ser excluídos.
Clique no link para o registro de incidente de segurança (SIR0010002)	Revise o incidente de segurança relacionado e todos os dados de pesquisa relacionados antes de processar a solicitação.

A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado para este exemplo. Quando a solicitação é rejeitada da notificação por e-mail por um aprovador, uma anotação de trabalho é publicada com a pessoa que rejeitou a solicitação. Johann SecAdmin rejeita esta solicitação.



Em ServiceNow AI Platform Instância da pessoa que rejeitou a solicitação (Johann SecAdmin), em **Autoatendimento > Minhas aprovações**, Rejeitado É exibido na coluna Estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

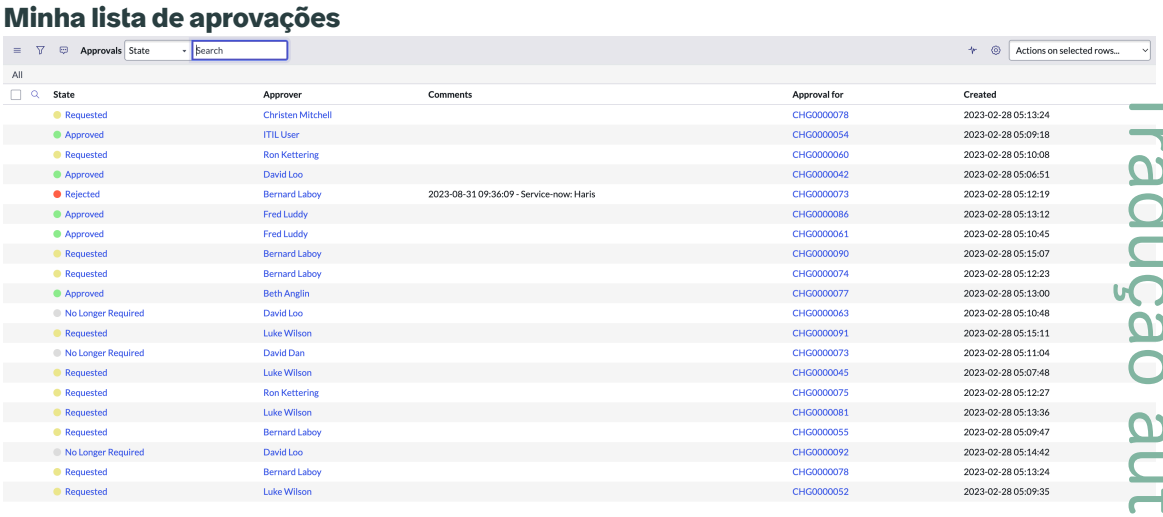
Depois que uma solicitação é rejeitada por qualquer membro do grupo de aprovação, como o usuário com a função sn_si.analyst, você deverá enviar uma nova solicitação para excluir esses e-mails se determinar que eles devem ser excluídos.

Para este exemplo, depois que a solicitação é rejeitada, o usuário com a função sn_si.analyst envia uma nova solicitação.

Outro membro do grupo de aprovação, John Approver, recebe um e-mail semelhante ao mostrado no exemplo anterior. John Aprovador também pode processar esta solicitação.

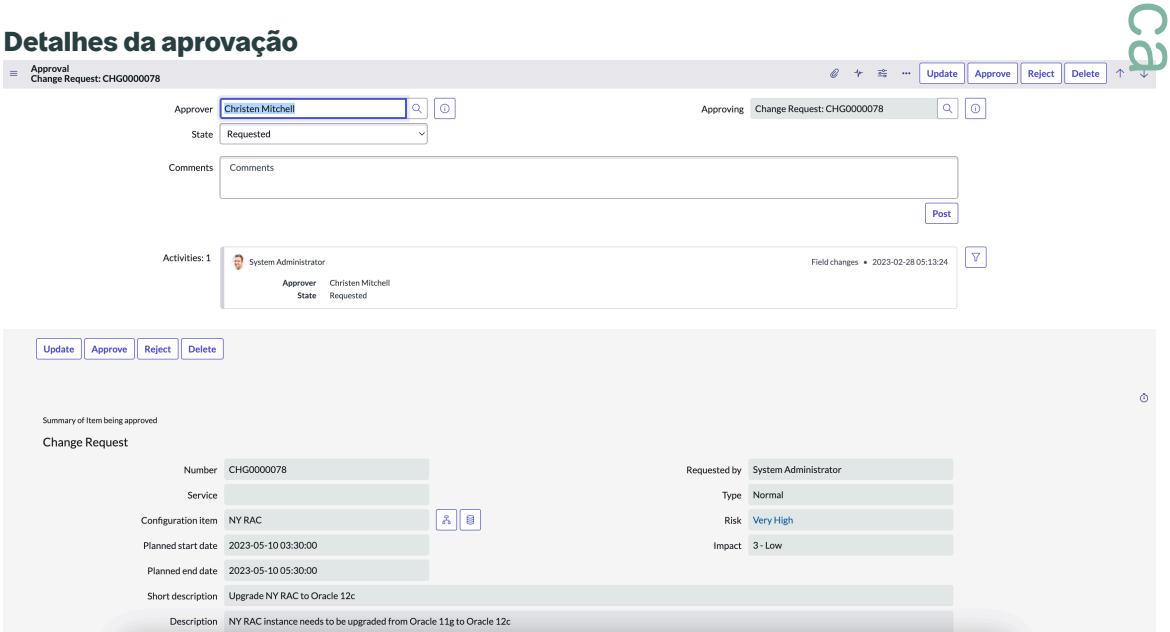
2. Como alternativa, os aprovadores podem navegar até **Autoatendimento > Minhas aprovações** em ServiceNow AI Platform instâncias para exibir e processar solicitações de exclusão.
Para processar uma solicitação de **Minhas aprovações** , siga estas etapas.

   a. Navegar até **Autoatendimento > Minhas aprovações**.



   b. Na coluna Estado, clique no item solicitado.

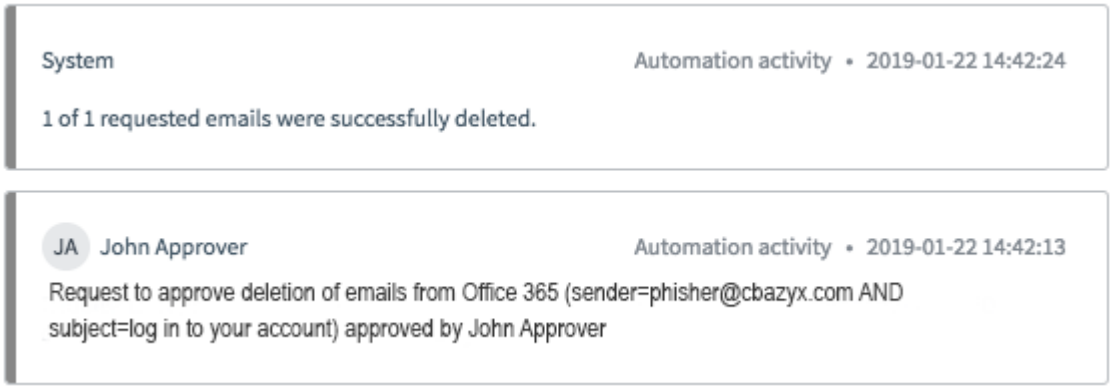
   No registro de aprovação exibido, os dados sobre a pesquisa, a solicitação de pesquisa e os resultados da pesquisa são listados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Neste registro, clique em **Aprovar** para aprovar a solicitação.
Depois que a solicitação é aprovada, o sistema inicia o fluxo de trabalho de exclusão para remover os e-mails. A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado para este exemplo. Esta solicitação de exclusão é enviada novamente, ela é aprovada. Independentemente do método usado para aprovar uma solicitação, o número de e-mails excluídos com sucesso é publicado em uma anotação de trabalho.



Depois que os e-mails forem excluídos com sucesso, no registro de incidente de segurança relacionado, se a marcação estiver habilitada, o. Exclusão de e-mail - Concluída o marcador substitui Exclusão de e-mail - Iniciada marcador.

Recebido(a) **Autoatendimento > Minhas aprovações** Para o aprovador (John Approver), o estado muda de Solicitado . Aprovado .

Recebido(a) **Autoatendimento > Minhas aprovações** Para outros membros do grupo de aprovação, por exemplo, Johann SecAdmin, o estado muda para Não é mais necessário depois que a solicitação é aprovada.

3. Como alternativa, para confirmar que os e-mails foram excluídos no registro Resultado da pesquisa de e-mail no registro de incidente de segurança relacionado, siga estas etapas.

a. Navegar até **Incidentes de segurança > Mostrar todos os incidentes** e localizar o incidente de segurança relacionado a phishing.
Na parte inferior do registro, as listas relacionadas são exibidas.

b. Clique em **Pesquisa de e-mail** lista relacionada.

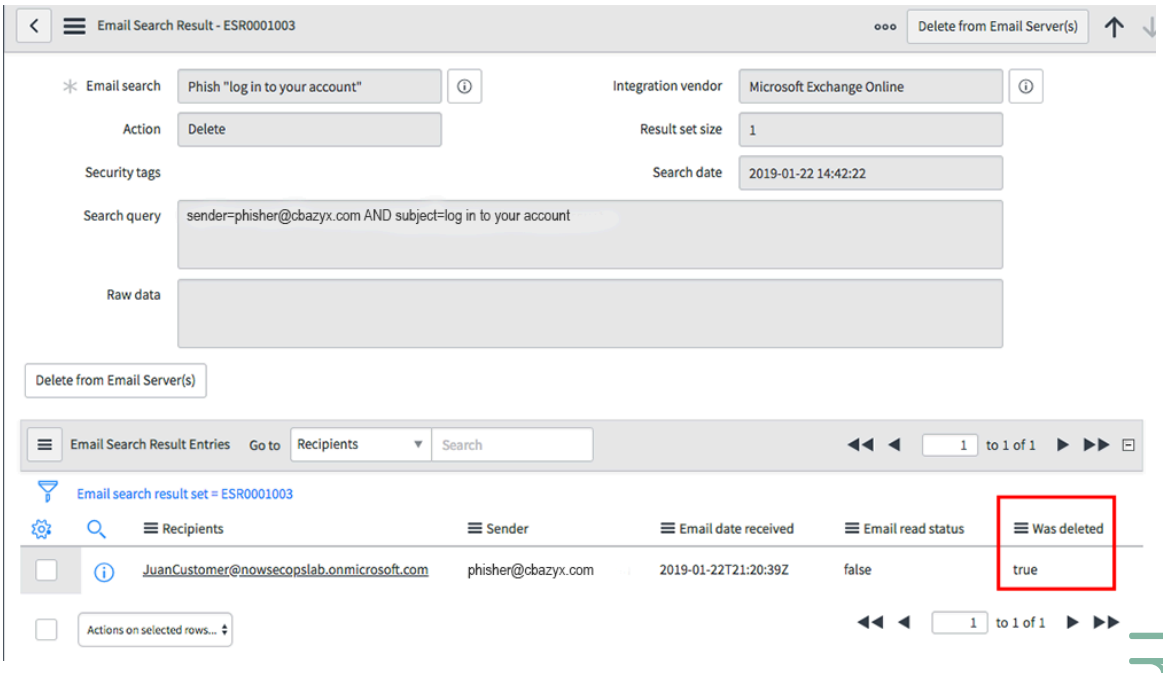
c. Clique no nome da pesquisa na coluna Pesquisa de e-mail (Phish "faça login na sua conta").
O registro de Pesquisa de e-mail é exibido. Se a lista relacionada Pesquisa de e-mail não estiver visível, clique em **Mostrar todas as listas relacionadas** link.

d. Clique em **Resultados da pesquisa de e-mail** lista relacionada.
Na coluna Data de pesquisa, as ações de pesquisa e exclusão de e-mail são exibidas com as datas correspondentes.

e. Na coluna Data de pesquisa, clique no item que corresponde à ação de exclusão.
No registro Resultado da pesquisa de e-mail exibido, o status da coluna Foi excluído mostra que o e-mail foi excluído (verdadeiro).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você aprovou solicitações de exclusão de e-mail de uma notificação por e-mail e um registro de aprovação e confirmou que os e-mails foram excluídos. Para obter mais informações sobre como localizar o registro de resultado da Pesquisa de e-mail, consulte Defina critérios de pesquisa de e-mail e solicite uma pesquisa no Microsoft Exchange Online serviço.

Recupere e-mails excluídos no Microsoft Exchange Online serviço

(Opcional) Como administrador do Microsoft Exchange, você pode recuperar e-mails excluídos se a correção do incidente exigir que você recupere os e-mails excluídos pelo fluxo de trabalho desta integração.

Antes de Iniciar

Para obter mais informações sobre como esta integração exclui e-mails, consulte Configure o. Microsoft Exchange Online integração.

Para obter mais informações sobre a função administrativa no Microsoft Produto do Office 365, incluindo informações sobre como recuperar itens excluídos em uma caixa de correio do usuário, consulte Sobre a função de administrador do Exchange Online .

Função necessária: administrador, Administrador do Microsoft Exchange

Por Que e Quando Desempenhar Esta Tarefa

Se você selecionar **Recuperar e-mails excluídos** Na guia Configurações adicionais Durante a etapa de configuração, você habilita a recuperação de e-mails excluídos em Microsoft Exchange Online locatário. Os e-mails excluídos usando o fluxo de trabalho de exclusão desta integração são colocados na subpasta Itens excluídos da pasta Itens recuperáveis na caixa de correio do usuário no Microsoft Exchange Online serviço. Se a conta do usuário estiver configurada em Microsoft Exchange Online Locatário Para que o usuário possa exibir a pasta Itens excluídos, ele pode recuperar esses e-mails usando Microsoft Serviço do Outlook na Web. Como alternativa, o Microsoft Exchange Online O administrador pode recuperar e-mails excluídos de uma pasta Itens excluídos de um usuário. Consulte Recupere itens excluídos ou e-mail no Outlook Web App para obter mais informações.

Função necessária: Microsoft Exchange Online administrador ou Microsoft Administrador global para recuperar e-mails excluídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si.admin em ServiceNow AI Platform Para habilitar a opção Recuperar e-mails excluídos.

Função necessária: sn_si.analyst em ServiceNow AI Platform para concluir uma pesquisa bem-sucedida de e-mails e verificar se os e-mails foram excluídos com sucesso antes da recuperação.

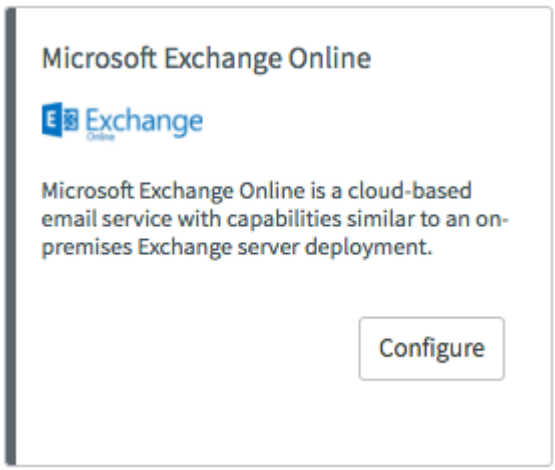
Procedimento

Para habilitar a opção de recuperação de e-mail, siga estas etapas.

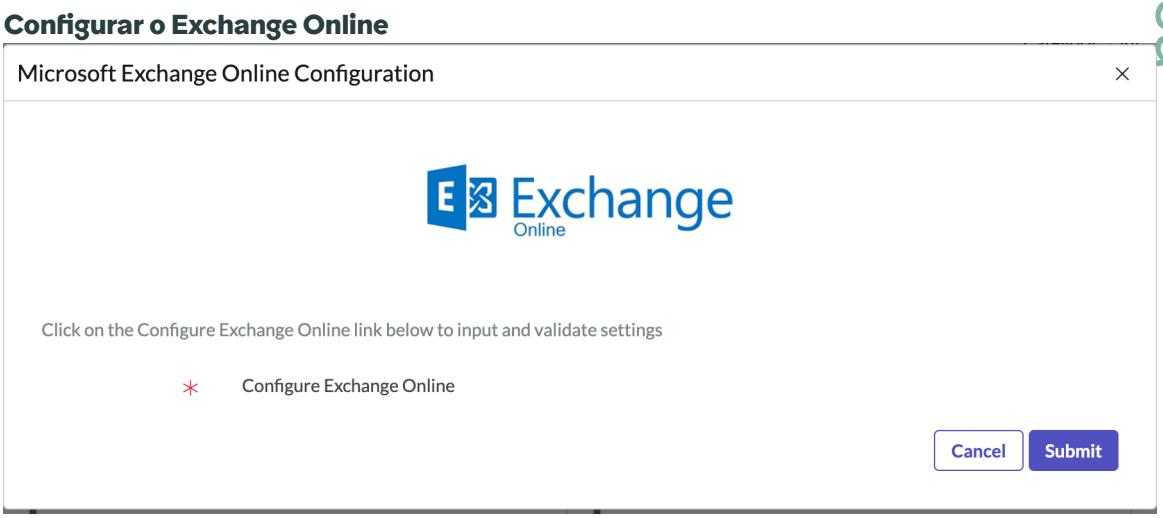
a. Navegar até **Operações de segurança** > **Integrações** > **Configurações**.

b. Localize Microsoft Exchange Online lado a lado.

c. Clique em **Configurar**.



d. Em Microsoft Exchange Online Caixa de diálogo Configuração exibida, clique em **Configurar o Exchange Online** .

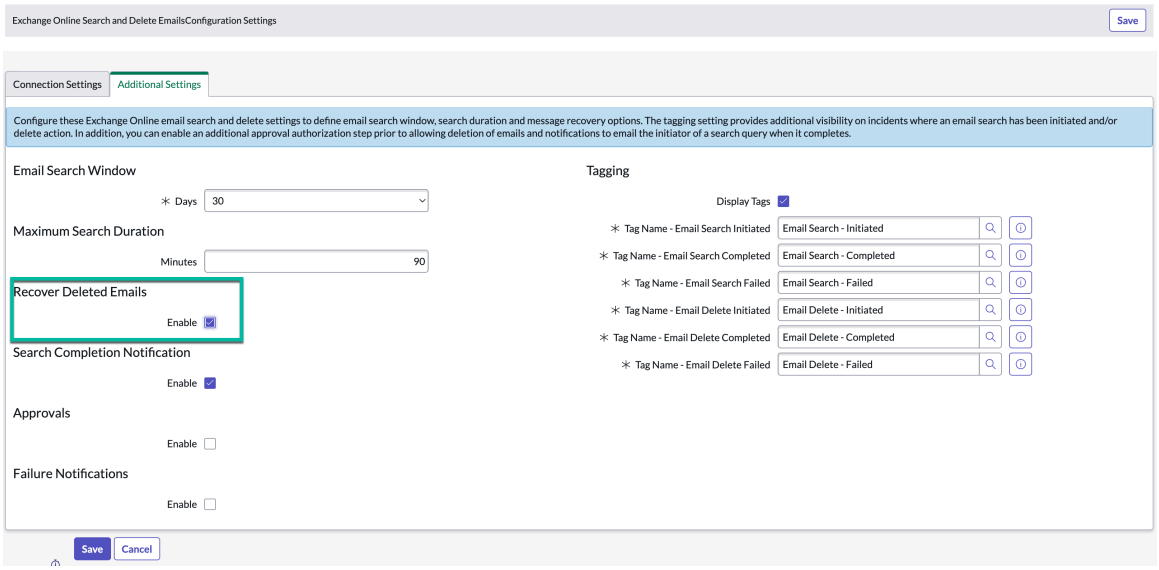


e. Em Configurações adicionais em Recuperar e-mails excluídos . selecione **Habilitar** caixa de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recuperar e-mails excluídos



f. Verifique quaisquer outras configurações e clique em **Enviar** .

g. Para verificar se uma pesquisa e exclusão de mensagens de e-mail foram concluídas com sucesso para as mensagens de e-mail que você deseja recuperar, navegue até o incidente de segurança que registrou os fluxos de trabalho de pesquisa de e-mail e exclusão.

h. Localize as anotações de trabalho e verifique se o sistema excluiu as mensagens com êxito.



i. . Microsoft Exchange Online Administrador ou Administrador global, faça login em Microsoft Conta do Office 365.

j. Siga as etapas descritas em Recupere itens excluídos ou e-mail no Outlook Web App em Microsoft site de documentação.

Edite marcadores de segurança para Microsoft Exchange Online integração

Você pode editar os nomes e as cores das etiquetas de segurança em seu ServiceNow AI Platform® instância do Microsoft Exchange Online integração. Esses marcadores de segurança ajudam a identificar rapidamente quando a pesquisa de e-mail é concluída ou falha. Eles também identificam quando as solicitações para excluir e-mails são iniciadas e quando os itens de e-mail são excluídos com sucesso.

Antes de Iniciar

Por padrão, os marcadores de segurança estão habilitados em seu ServiceNow AI Platform® se você selecionar **Marcadores de exibição** durante a etapa de configuração. Você pode editar cores e nomes de marcador e atribuir marcadores a grupos de marcadores de segurança para ajudá-lo a organizá-los em seu ServiceNow AI Platform® instância. Por exemplo, você pode mudar as cores dos marcadores para que o marcador de início de um recurso seja uma cor e o marcador de conclusão seja outra cor para corresponder aos outros marcadores de segurança habilitados em seu ServiceNow AI Platform® instância. Essas

Tradução automática

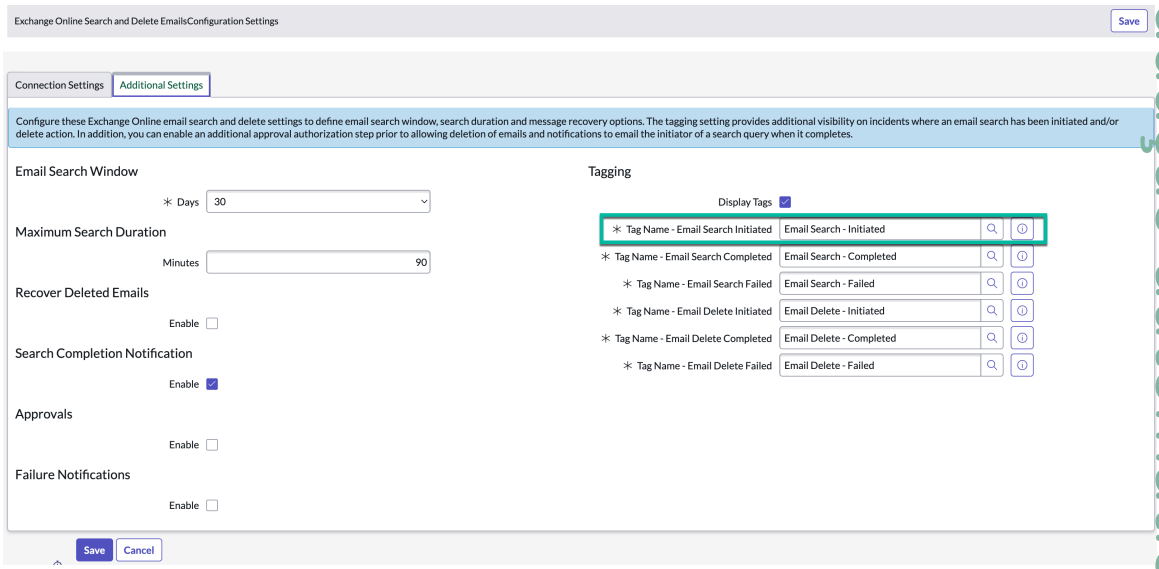
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

cores diferentes podem ajudar você a identificar rapidamente quando os fluxos de trabalho começam e são concluídos com sucesso. Se você decidir que não precisa de um marcador específico, sem desabilitar a marcação para a integração, também poderá desabilitar um único marcador no registro de marcador. Se desabilitado, este marcador não será mais exibido nos incidentes de segurança relacionados. Para obter mais informações sobre como configurar grupos de marcadores de segurança e marcadores, consulte Configurar grupos de marcadores de segurança e marcadores no Site de documentação do produto ServiceNow .

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Configurações do Exchange Online**.
2. Clique em **Configurações adicionais** para selecioná-lo.
3. Na guia exibida, se **Marcadores de exibição** se a opção estiver desmarcada, selecione-a para exibir os nomes dos marcadores.
4. Com os nomes de marcador exibidos, à direita de um marcador, clique no ícone de informações.



5. Na caixa de diálogo Marcador de segurança exibida, clique em **Registro em aberto** .
6. No registro exibido, edite os campos.

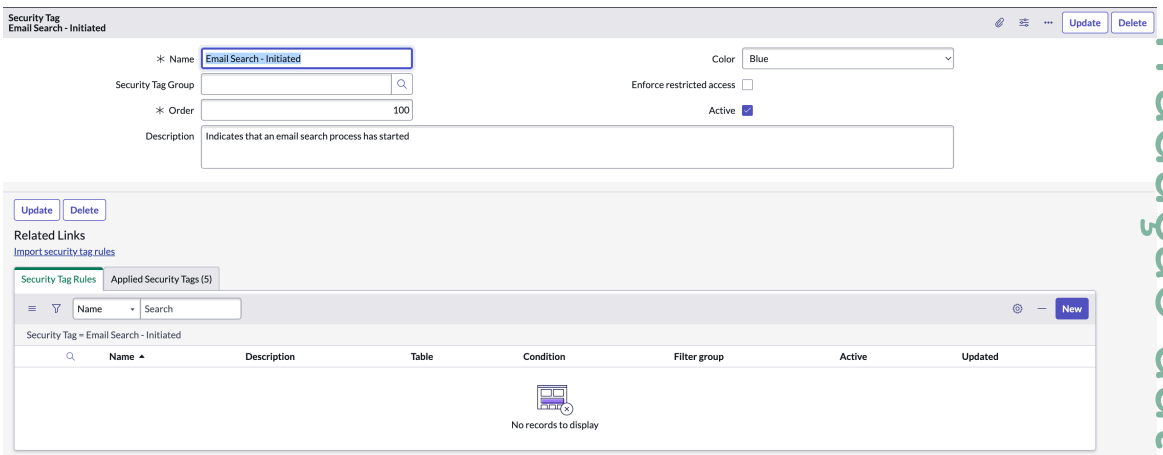
Opção	Descrição
Nome	Nome exclusivo da etiqueta de segurança.
Cor	Cor do marcador de segurança. Selecione uma cor na lista de seleção.
Grupo de marcadores de segurança	Nome do grupo de marcadores de segurança. Clique no ícone de informações para exibir os grupos disponíveis. O padrão é Grupo Metatag.
Impor acesso restrito	Selecione esta opção para atribuir funções de leitura e gravação necessárias para que os usuários leiam ou gravem em registros que tenham este marcador de segurança. O padrão é limpo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista. O padrão é 100. Para definir a ordem na lista, insira um valor. Por exemplo, 100, 200, 300, 400. O marcador com o menor número é exibido primeiro na lista. O perfil com o número mais alto é exibido por último.
Ativo	Ative ou desative este marcador. O padrão é selecionado (ativo)
Descrição	Descrição do marcador.

7. Clique em **Atualizar** para salvar suas mudanças.



Você editou com sucesso o registro de marcador de um marcador de segurança.

Integração do Microsoft Exchange no Local

. Microsoft Exchange A integração no local fornece ferramentas para que os analistas de segurança contenham e eliminem ameaças de e-mail de phishing e spear phishing em instâncias no local.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

Comece a usar a integração do Microsoft Exchange no local

Usar

PESQUISE e exclua e-mails de phishing

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Comece a usar a integração do Microsoft Exchange no local

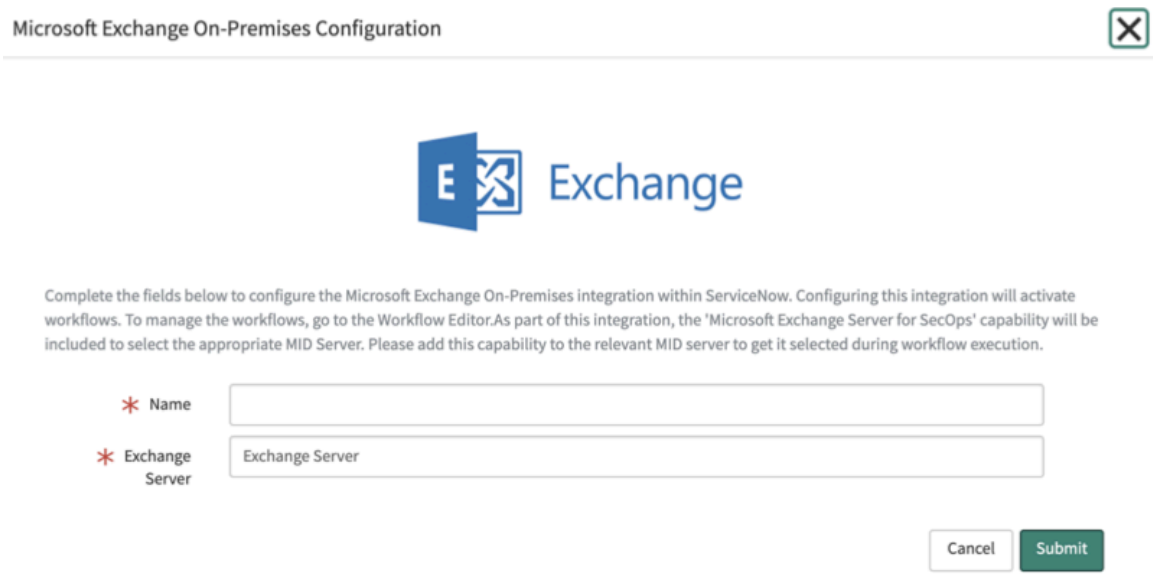
. Microsoft Exchange A integração no local fornece ferramentas para que os analistas de segurança contenham e corrijam ameaças de e-mail de phishing e spear phishing em instâncias no local. Antes de poder usar Microsoft Exchange Integração no local, você deve baixá-la do ServiceNow Store E identificar os Exchange e MID Servers apropriados.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação do SO for concluída, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. Em Microsoft Exchange Cartão no local, clique em **Novo** .



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Exchange Server	Especifique o servidor Exchange a ser usado.

Nota: Configurar esta integração ativa fluxos. Para gerenciar os fluxos, navegue até **Workflow Studio/Flow Designer.** .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.
8. Navegar até **Orquestração** > **MID Servers**.
9. Abra o registro e verifique o status do MID Server que pode ser acessado pelo Exchange Server e seus **Status** a opção está definida como **Para cima** e. **Validado** opção como **Sim** .
10. Adicione a capacidade do MID Server:
    - Selecione o respectivo MID Server para adicionar a capacidade.
    - Clique em **.** lista relacionada e clique em **Editar** .

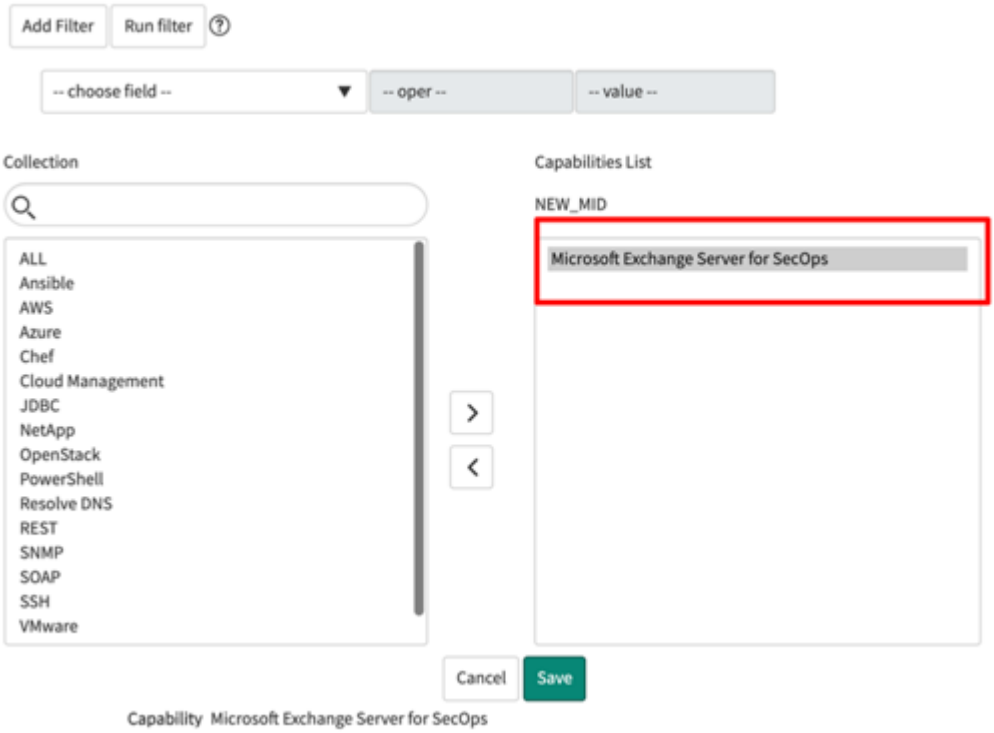
Capacidade do MID Server



    - Remover **Todos** e adicionar **Microsoft Exchange Server para SecOps** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Selecione **Intervalos de IPs** em **Listas relacionadas** e defina o valor como **TODOS** ou qualquer valor desejado.
- Selecione **Aplicações compatíveis** em **Listas relacionadas** E defina o valor como TODOS ou Orquestração.
- **Salvar** o registro.

11. Valide as conexões e credenciais.
12. Depois que as credenciais são validadas, a configuração na instância da ServiceNow está concluída e está pronta para executar operações de pesquisa e exclusão de e-mail usando esta integração.

Microsoft Exchange - Realizar fluxo de pesquisa e exclusão de e-mail

. **Microsoft Exchange - Executar pesquisa e exclusão de e-mail** O fluxo é executado, ele pesquisa o servidor do Exchange usando a consulta de pesquisa fornecida e retorna os detalhes para a instância no local.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

. **Microsoft Exchange - Executar pesquisa e exclusão de e-mail** o fluxo é executado quando as pesquisas de e-mail são configuradas e o **Excluir do(s) servidor(es) de e-mail** ou **Pesquisar em servidor(es) de e-mail** pressionados.

As ações específicas desta integração são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As ações de fluxo incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Criar ação de pesquisa de conformidade
- Ação Verificar status da pesquisa de conformidade

Criar ação de visualização da pesquisa de conformidade

A ação Criar visualização de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo visualização no Exchange Server para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Concluídas	Quando a ação de pesquisa de conformidade é criada com sucesso.
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na ação de fluxo.

Verificar Status da ação de visualização

O Status da ação de visualização verifica o status da ação de pesquisa de conformidade do tipo visualização e retorna as informações de visualização dos e-mails encontrados, como destinatário, remetente, assunto e data de recebimento do e-mail.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e as informações de visualização do e-mail encontrado como parte da pesquisa de conformidade.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Visualização em andamento	Quando o status da ação de pesquisa de conformidade é Em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é Concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Visualização concluída	Quando o status da ação de pesquisa de conformidade é concluído e os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Criar ação de exclusão da pesquisa de conformidade

Criar ação de exclusão de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo limpeza no Exchange Server para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Concluídas	Quando a ação de pesquisa de conformidade é criada com sucesso.
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na ação de fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar Status da ação de exclusão

Verificar status da ação de exclusão verifica o status da ação de pesquisa de conformidade do tipo limpeza e executa a operação de exclusão flexível no servidor de troca para os e-mails encontrados como parte da pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e a contagem de e-mails excluídos, que foram encontrados como parte da pesquisa de conformidade.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Exclusão em Andamento	Quando o status da ação de pesquisa de conformidade é Em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é Concluído e nenhum e-mail é excluído como parte da pesquisa de conformidade.
Exclusão concluída	Quando o status da ação de pesquisa de conformidade é concluído e os e-mails são excluídos como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na ação de fluxo.

Remover ação de pesquisa de conformidade

A ação Remover pesquisa de conformidade remove a pesquisa de conformidade criada do Exchange Server.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Integração de ingestão de alerta da API de segurança do Microsoft Graph

Use API de segurança do Microsoft Graph Integração para ingerir alertas de provedores de segurança do Microsoft Graph e criar incidentes de segurança automaticamente.

Visão geral

. API de segurança do Microsoft GraphÉ um serviço intermediário (ou agente) que fornece uma interface programática única para conectar vários provedores de segurança (nativo da Microsoft e dos parceiros da ServiceNow).

. API de segurança do Microsoft Graph a integração resolve esses problemas usando API de segurança do Microsoft Graph Para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Microsoft Defender Advanced Threat Protection e Azure Advanced Threat Protection. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente no Resposta a incidentes de segurança.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Descoberta de API de segurança do Microsoft Graph alertas que são candidatos a incidentes de segurança e automatizam a criação de incidentes de segurança.
- Mapeamento de campos de alerta para campos de incidente de segurança.
- Agregação de alertas semelhantes a incidentes de segurança em aberto existentes em vez de criar incidentes de segurança duplicados.
- Visualize valores de campos de alerta e valide seus mapeamentos no incidente de segurança.
- Atualização automática de status de alerta para criação e fechamento de incidentes de segurança.
- Configure a ingestão programada de alertas para criar incidentes de segurança periodicamente.

Configure sua instância da Now Platform para a integração da API de segurança do Microsoft Graph

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform® e. Resposta a incidentes de segurança funções.	As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform® instância. • Um usuário com ServiceNow AI Platform® a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no ServiceNow AI Platform®: ◦ Cria e edita perfis de alerta. ◦ Seleciona e mapeia campos de dados de alerta da API de segurança do Microsoft Graph para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração. ◦ Agenda a ingestão de alertas em andamento. ◦ Habilita atualizações de alerta quando um Resposta a incidentes de segurança o incidente foi criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no Site de documentação do produto ServiceNow .
Registre sua aplicação no Microsoft Azure portal.	Antes de ingerir alertas, você deve configurar sua aplicação no Microsoft Azure portal. Consulte Configure o portal do Microsoft Azure para obter detalhes.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. 1. Resposta a incidentes de segurança 2. Ingestão de evento e alerta para operações de segurança: Esta aplicação requer:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	○ Tempo de execução do IntegrationHub da ServiceNow com.glide.hub.integration.runtime ○ Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in de ingestão de evento e alerta. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Configure o portal do Microsoft Azure

Para recuperar alertas de segurança para uma aplicação disponível no locatário do Microsoft Azure usando API de segurança do Microsoft Graph, você deve registrar a aplicação no Microsoft Azure e conceder acesso de leitura e gravação ao evento de segurança à aplicação.

Antes de Iniciar

Função necessária:

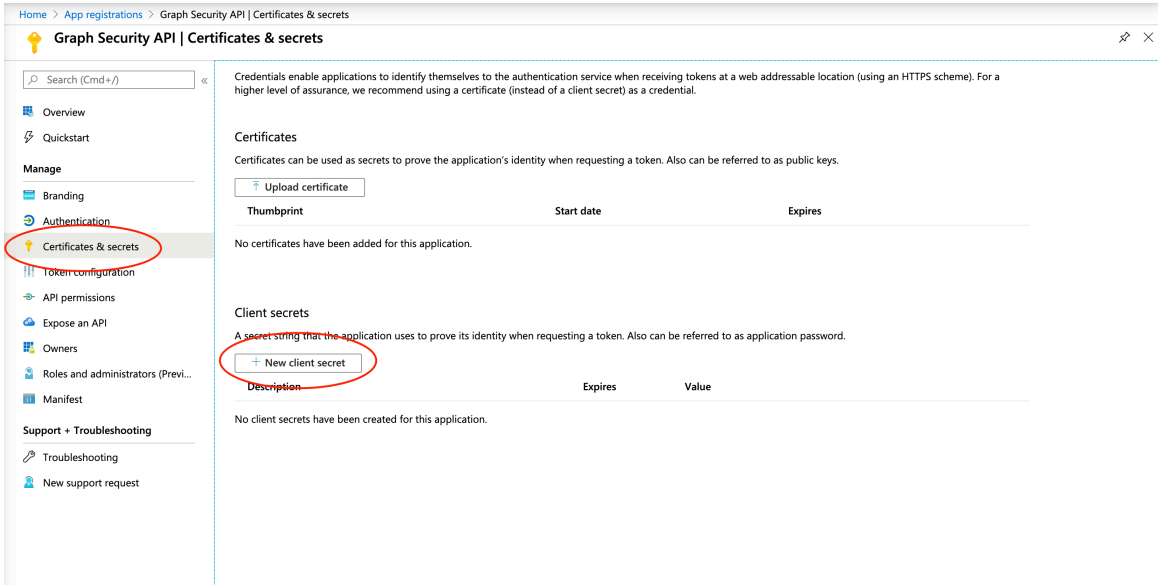
- Desenvolvedor de aplicações: Necessário para registrar a aplicação.
- Administrador de locatário: O. Microsoft Azure o administrador locatário deve conceder permissões à aplicação fazendo uma chamada para o endpoint de consentimento do administrador.

Procedimento

1. Faça login no Microsoft Azure portal.
2. Insira **Registros de aplicações** em **Pesquisa** caixa.
3. Clique em **Novo registro** .
4. Insira um nome para sua aplicação e o URI de redirecionamento, por exemplo, http://localhost e clique em **Registre-se** .
   O URI de redirecionamento é usado ao fornecer consentimento do administrador para a aplicação.
5. Na página Registros de aplicações, selecione a aplicação que você registrou, por exemplo, Demonstração de segurança do Graph.
6. Em **Gerenciar** , selecione **Certificados e segredos** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

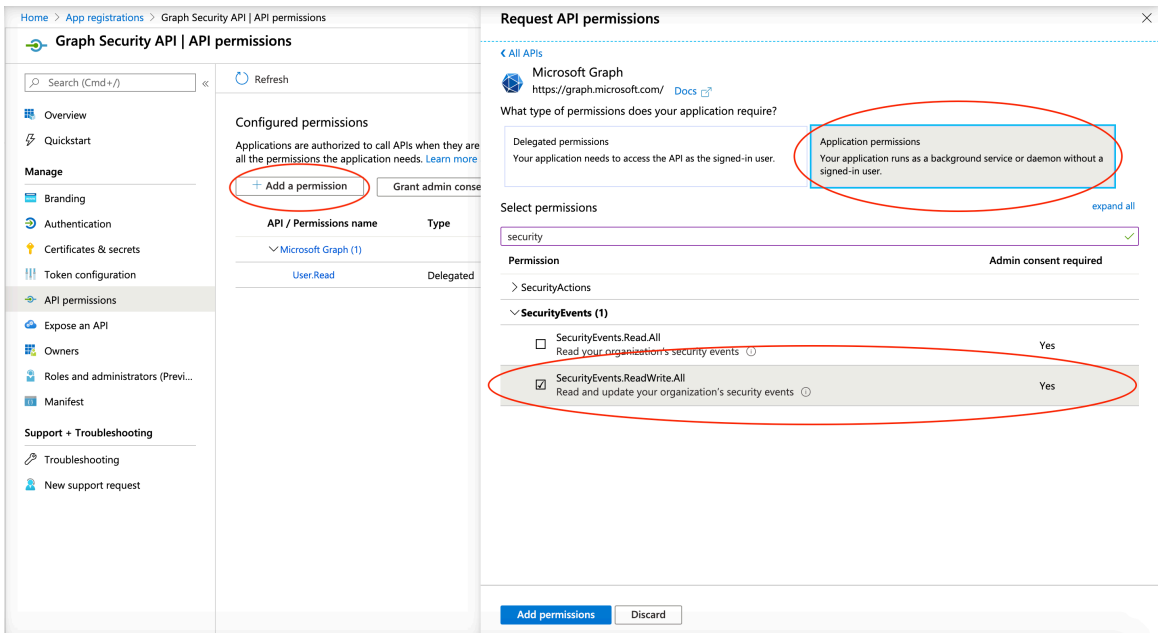


7. Selecione **Novo segredo do cliente** para criar um segredo do cliente.
   Copie o segredo do cliente e salve-o, pois ele não ficará visível mais tarde. Caso você tenha esquecido o segredo do cliente, poderá gerar um novo segredo do cliente.

   Nota: Se você esquecer o segredo do cliente, poderá gerar um novo segredo seguindo as instruções nas etapas 4 e 5.

8. Clique em **Exibir permissões de API** Na página Visão geral.

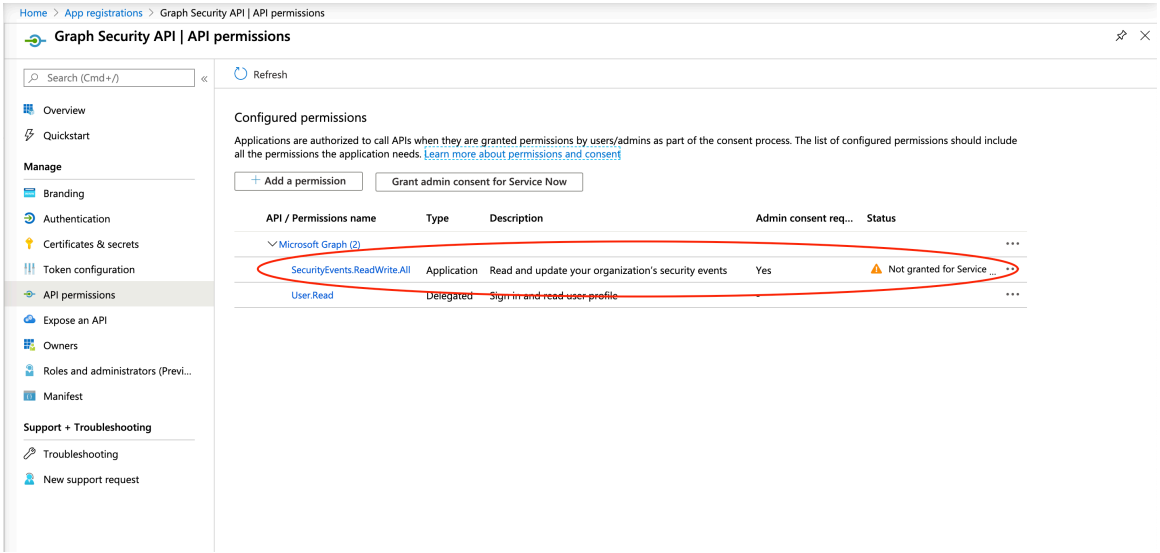
9. Adicione novas permissões de API no nível da aplicação para eventos de segurança SecurityEvents.ReadWrite.All.



10. Conceda consentimento do administrador para as permissões de API recém-adicionadas.
    Para obter mais informações, consulte Referência de permissões do Microsoft Graph Modelo de permissão do Microsoft Graph.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Faça login como administrador de locatário e forneça consentimento para a aplicação.
As etapas são fornecidas abaixo:

    a. Navegue até o seguinte URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    Insira o APPLICATION_ID da aplicação que você registrou.

12. Clique em **Aceitar** para aceitar permissões solicitadas pela aplicação criada acima.
Você pode usar a aplicação para ler eventos de segurança. Consulte Autorização de segurança do Microsoft Graph documentação para obter mais detalhes.

Instale e configure a aplicação ServiceNow para integração de ingestão de alertas da API Microsoft Graph Security

Antes de executar a integração no seu ServiceNow AI Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform instância.

Antes de Iniciar

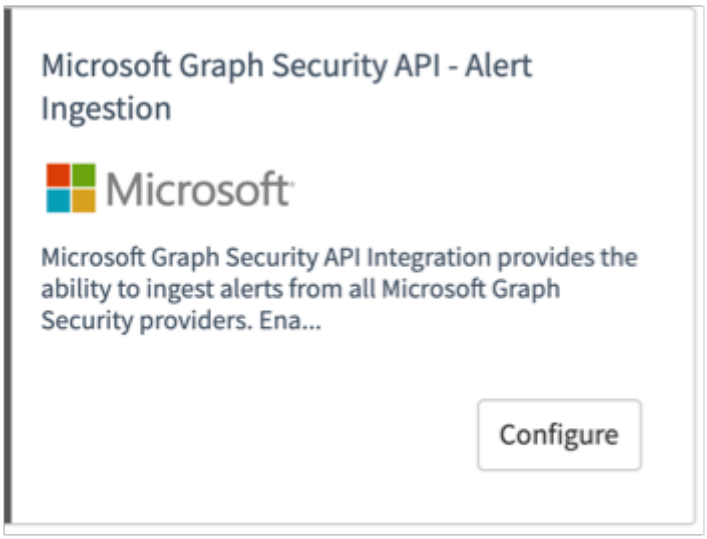
Função necessária: sn_si.admin

Procedimento

1. Se você não instalou o. API de segurança do Microsoft Graph aplicação do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações**
E localize o bloco API de segurança do Microsoft Graph - Ingestão de alertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para configurar a aplicação, clique em **Configurar** .
4. Na caixa de diálogo Configuração de ingestões de alerta exibida, preencha os campos.

Campo	Descrição
Nome	Nome do Microsoft Azure Instância de nuvem. Somente valores alfanuméricos e hifens (-) podem ser inseridos neste campo.
ID de locatário	. Microsoft Azure ID do locatário. Esta é a instância da qual todos os alertas no Microsoft Azure os portais são recuperados.
ID de cliente	O ID do cliente da aplicação que você registrou no Microsoft Azure portal. Consulte Configure o portal do Microsoft Azure para obter detalhes.
Segredo do cliente	A senha da sua aplicação registrada.

5. Clique em **Enviar**.
   Depois que ela é validada e enviada com sucesso, cada configuração do servidor de ingestões de alerta é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim** .

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de alerta.

Crie um perfil para a integração de ingestão de alertas da API de segurança do Microsoft Graph

Como um usuário com a função sn_si.admin, você cria um perfil de alerta em seu ServiceNow AI Platform e determinar quais alertas criam incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de alertas ingeridos, os valores de campo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

dos alertas são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será exibido.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A integração permite ingerir diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo. Esses alertas são ingeridos com base nos perfis que você configura no Operações de segurança ambiente da sua instância. Inicialmente, todos os alertas são ingeridos para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados ainda mais para especificar quais alertas criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para alertas identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de alertas ingeridos, os valores de campos individuais nos alertas filtrados são mapeados para os campos correspondentes em um layout de incidente de segurança para uma visualização. Todos os alertas que atendem aos critérios de seleção em seu Microsoft Azure locatário e estão disponíveis sobre API de segurança do Microsoft Graph inicialmente são ingeridos em seu ServiceNow AI Platform instância.

Identifique a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um alerta em seu ServiceNow AI Platform instância, navegue até **Integração da API de segurança do Microsoft Graph** > **Perfil da API de segurança do Microsoft Graph**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

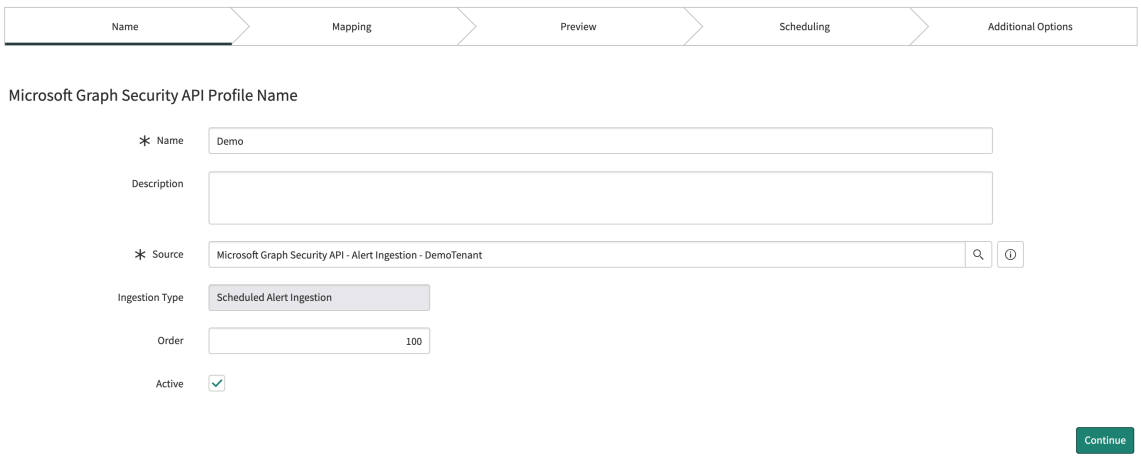
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e os nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.
Ativo	A caixa de seleção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo. **Nota:** Você deve concluir todas as seções no perfil antes de ativá-lo.
Origem	. Microsoft Azure locatário que você configurou para ingerir alertas. Se você tiver vários locatários

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	configurados, selecione o locatário apropriado para os tipos de alerta que você planeja ingerir para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. Menor o valor do pedido, maior a prioridade.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é mapear os campos de alerta.

Mapeamento de campos de alerta para integração de ingestão de alertas da API de segurança do Microsoft Graph

Depois de identificar as origens da ingestão de alertas programada, a próxima etapa é mapear campos de alerta individuais para os campos em um ServiceNow AI Platform SIR incidente de segurança.

Para a etapa de mapeamento, você deve primeiro ingerir alertas de amostra do Microsoft Azure locatário. Em seguida, você deve garantir que todos os dados do campo de alerta relevantes sejam mapeados para o local apropriado no SIR formulário de incidente e visualize o. SIR incidente na seção de visualização.

O mapeamento dos campos de alerta de amostra envolve o seguinte:

- Ingerir alertas da API de segurança do Microsoft Graph
- Mapeamento de alertas para campos de resposta a incidentes de segurança

Ingerir alertas da API de segurança do Microsoft Graph

Ingerir alertas de amostra do seu Microsoft Azure locatário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

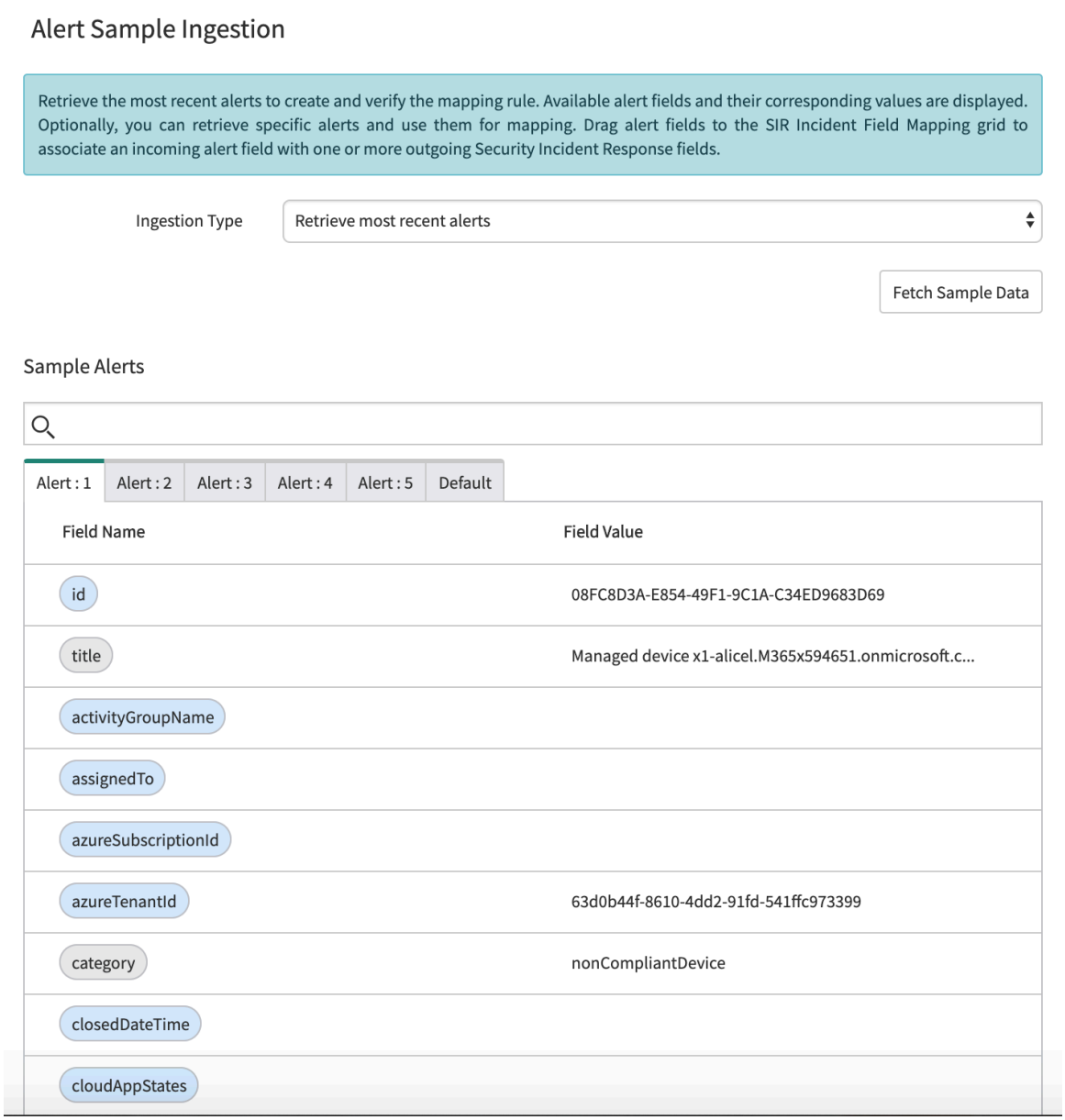
1. Você pode extrair os 5 alertas de amostra mais recentes ou fornecer os IDs de alerta exclusivos para os alertas específicos que você deseja usar para sua experiência de mapeamento.
   Em **Preferência de ingestão** lista de seleção, selecione uma das seguintes opções:
   - Recuperar alertas mais recentes: Os 5 alertas mais recentes são recuperados.
   - Selecionar alertas com base no ID de alertas: Especifique o ID de alerta para que os alertas sejam recuperados. Você pode especificar um máximo de 5 ids de alerta separados por vírgulas.
2. Clique em **Buscar dados de amostra** para extrair os dados de alerta de amostra mais recentes do Microsoft Azure locatário.
   A extração de alertas de amostra pode levar alguns minutos.

   Os valores do campo de alerta de amostra são preenchidos no lado esquerdo do formulário quando os alertas de amostra são ingeridos pelo perfil. Estes são os alertas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que você mapeia para SIR campos de incidente de segurança. Os campos de alerta e os resultados de valores são exibidos como guias individuais.



O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança.

Mapeamento de alertas para campos de resposta a incidentes de segurança

Mapeie campos de alerta individuais de alertas acionados para campos em um ServiceNow AI Platform incidente de segurança.

Mapeamento de campo de alerta

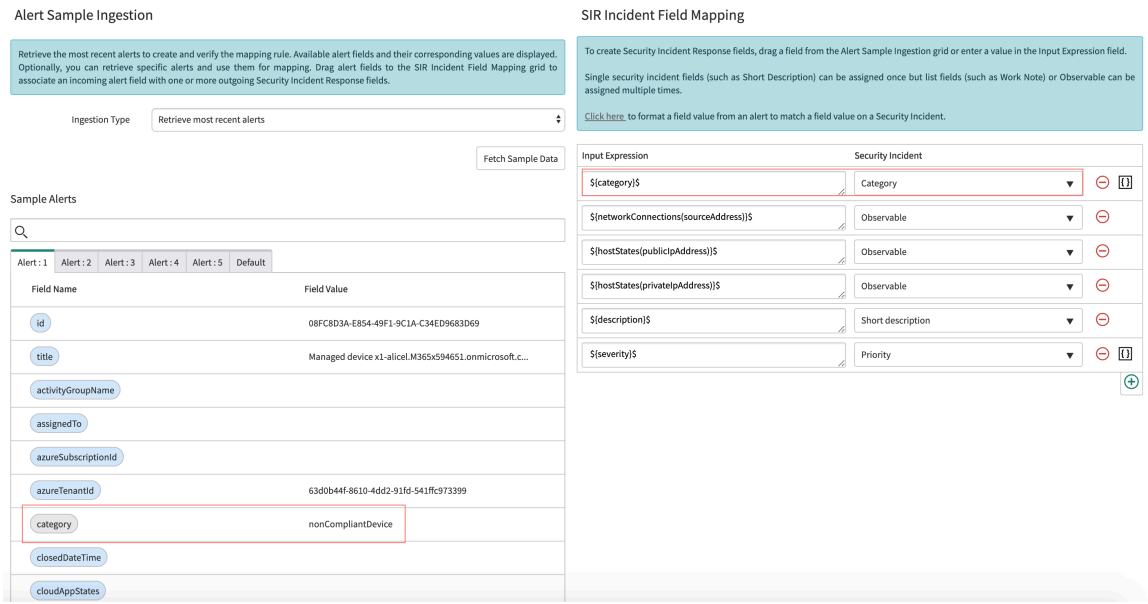
Como um usuário com a função sn_si.admin, use os campos da seção Alertas de amostra à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR no painel direito. Edite a configuração de mapeamento arrastando os campos de alerta do lado esquerdo e soltando-os no SIR seção de mapeamento de incidentes à direita. O mapeamento à direita associa o campo Alerta de entrada a um campo de incidente de segurança de saída.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Depois de obter os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, categoria E solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, categoria está mapeado para Categoria campo no incidente de segurança.



No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar você a garantir que nenhum campo de alerta seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de alerta ajuda a acompanhar os valores de alerta que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de alerta importante restante permanece não mapeada.

Campos azuis claros à esquerda indicam que um campo de alerta ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Esta codificação por cores ajuda você a rastrear o mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

a. Para inserir manualmente um valor no campo Expressão de entrada, insira-o no formato "fieldname". O campo de alerta será mapeado para o campo de incidente de segurança.

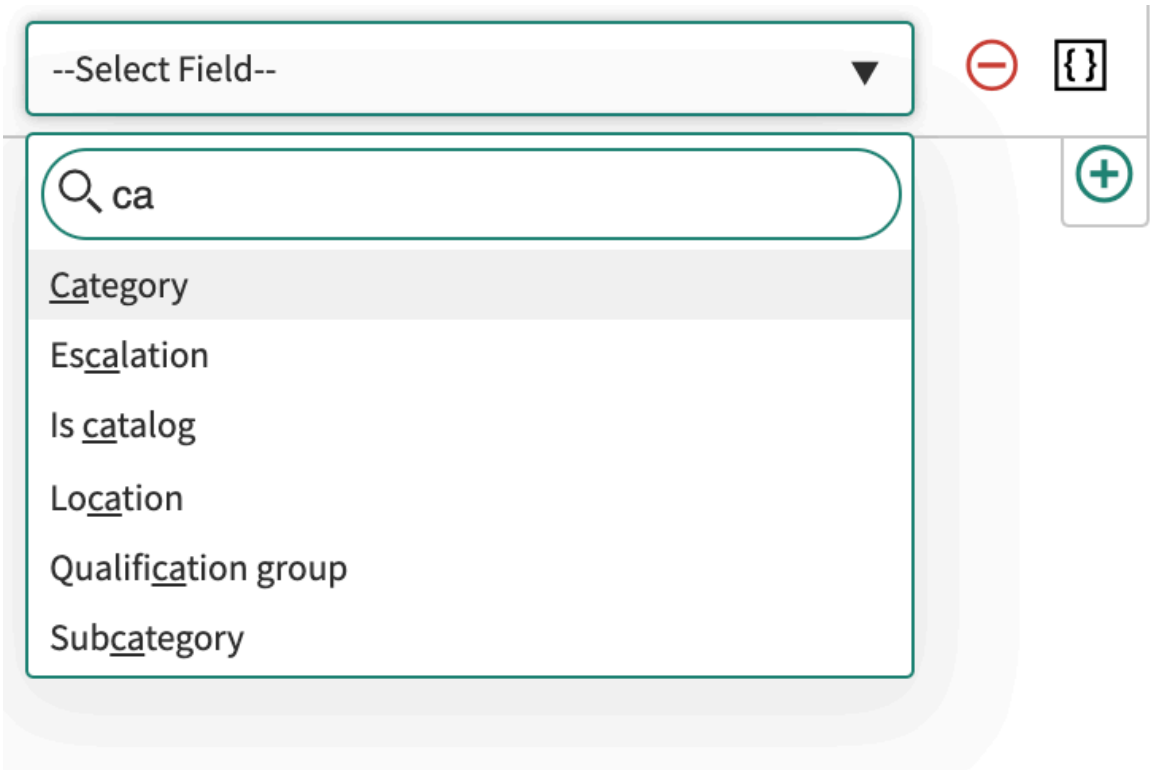
b. Não é possível mapear alertas ingeridos para MITRE-ATT&CK Campos da estrutura na seção Mapeamento de incidentes de segurança. Se você ainda mapear os campos, as informações não estarão disponíveis como parte do MITRE-ATT&CK cartão no MITRE-ATT&CK seção estrutura no formulário de incidente de segurança. Para associar o. MITRE-ATT&CK Técnicas, use Recurso de extração automática disponível como parte do MITRE-ATT&CK Estrutura no Inteligência contra ameaças Módulo.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário em SIR Na seção Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição. Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

Na lista de seleção expandida do novo campo, alguns campos são sombreados. Na figura a seguir, Categoria tem um fundo cinza, porque foi mapeada no incidente de segurança. Semelhante à codificação por cores dos campos de alerta no lado esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear os já mapeados SIR campos de incidente.



© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID do alerta desejado no campo Expressão de entrada. Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

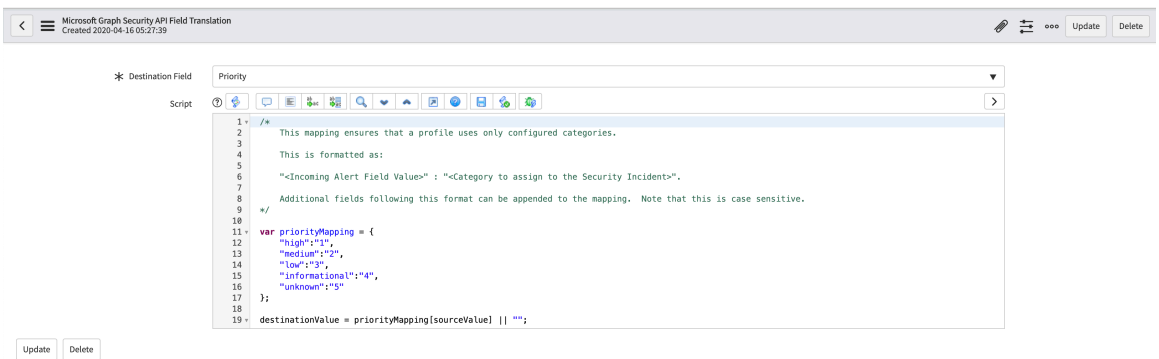
4. Continue o mapeamento adicionando ou removendo valores de campo ao mapeamento.

5. Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um alerta de entrada deve atender para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

Formatar tradução de campo

Em determinados casos, os valores do campo de alerta em API de segurança do Microsoft Graph Não pode ser traduzido diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria Alerta de malware e infecção por vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser traduzidos em uma Atividade de código mal-intencionado comum no campo Categoria no incidente de segurança SIR usando a funcionalidade Tradução de campo de formatação.

Para usar o editor de scripts, clique no ícone . O editor de script é exibido.



Condições de geração de incidentes

Quando a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais alertas devem criar incidentes de segurança versus quais alertas devem ser filtrados, por exemplo, alertas de baixa prioridade. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um alerta de entrada deve atender para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

Tradução automática

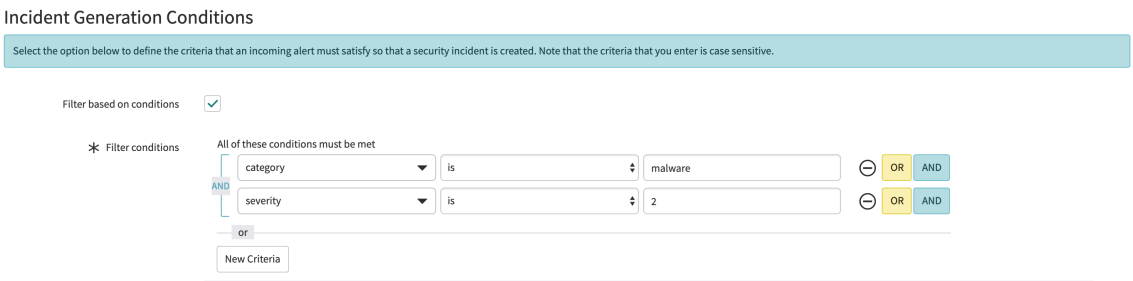
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Role até a seção Condições de geração de incidentes no formulário e selecione a opção Filtrar com base em condições. O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de alerta para o alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo do alerta que você ingere. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores do alerta. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao locatário do Microsoft Azure e revisar os alertas para as palavras-chave.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
   - Se **E.** selecionado, todas as condições devem ser correspondidas.
   - Se **OU** está selecionado, qualquer condição pode ser correspondida.
4. Na segunda linha, defina uma segunda condição de filtro

   A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



   Você definiu as condições de acionamento para que os incidentes de segurança sejam criados somente quando as duas condições de filtragem inseridas forem correspondidas.

   Esse tipo de filtragem ajuda a isolar alertas de segurança e limita o número de incidentes de segurança que você cria. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem precisar mudar a consulta ou a configuração de alerta acionada.

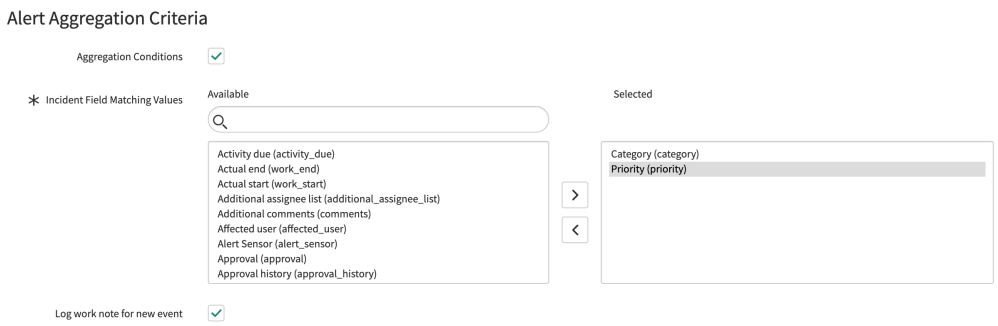
Critérios de agregação de alertas para lidar com alertas semelhantes e evitar incidentes duplicados

Defina critérios de agregação de alertas adicionais que agregue um alerta de entrada a um existente SIR incidente de segurança em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, esse recurso de agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de alerta relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Role até a seção Critérios de agregação de alertas no formulário e selecione a opção Condições de agregação. As colunas Valores de correspondência do campo do incidente são exibidas. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.
2. Na lista Disponível, selecione os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform E mova-os para a lista Selecionado. Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de alerta mapeados para eles. Todos os valores devem corresponder. Se somente um subconjunto dos valores for correspondido, as condições de agregação de alertas não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para obter o mapeamento de campos de vários valores.



Se um novo alerta corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos na lista relacionada Alertas agregados do Microsoft Graph. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam você a entender por que os alertas são adicionados a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique em **Mostrar todas as listas relacionadas** link.

3. (Opcional) Para registrar em log uma anotação de trabalho para um novo alerta que foi adicionado recentemente no incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra em log que um novo alerta foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Valores mapeados de um alerta para campos em um foram mapeados com sucesso SIR incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos ao existente SIR incidentes de segurança.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualize o incidente de segurança da integração da API de segurança do Microsoft Graph

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um ServiceNow AI Platform SIR incidente de segurança. Esta etapa de visualização permite que

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

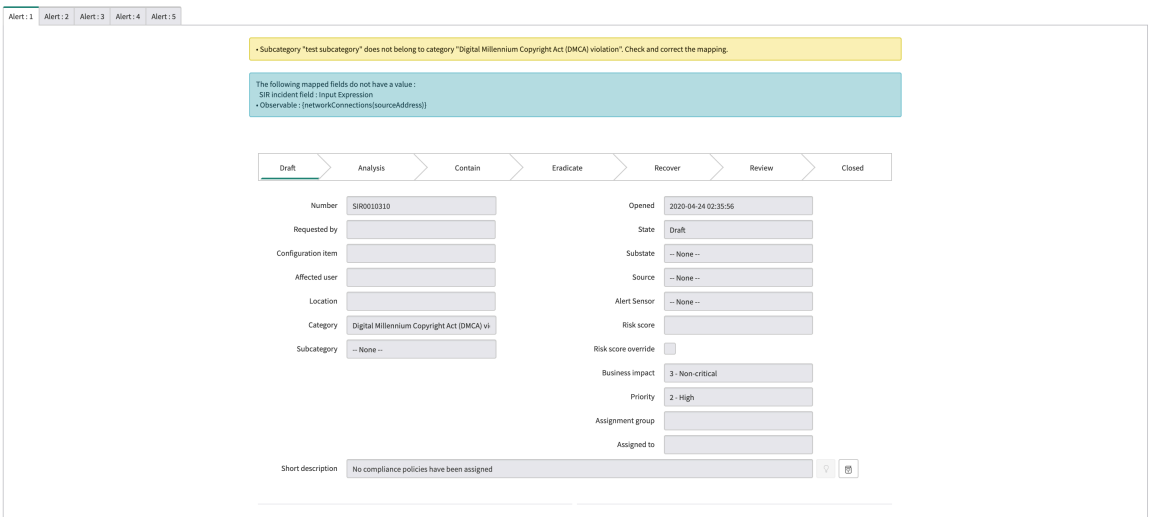
você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. Visualizações de SIR os incidentes de segurança não são salvos como incidentes reais no Resposta a incidentes de segurança produto.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
   Todos os alertas ingeridos e os mapeamentos de campo definidos na página Mapeamento são exibidos.
2. Clique em um ID de alerta para ver uma visualização do incidente de segurança.
   Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será definir a programação.

Definir programação para integração da API de segurança do Microsoft Graph

Verifique as configurações padrão para recuperação de alertas ou modifique a programação conforme necessário. Esta etapa permite filtrar sua recuperação de alertas com base em um intervalo de datas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também escolhe a frequência com que pesquisará alertas futuros que correspondam à configuração do perfil de alerta. Para perfis de ingestão de alertas automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação de alertas. Esta etapa é necessária para perfis de alerta programados.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho do API de segurança do Microsoft Graph a integração de ingestão de alertas é afetada pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Procedimento
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando os alertas são extraídos do Microsoft Azure locatário.

Opção	Descrição
Ingestão de alerta contínua selecionada	Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do Microsoft Azure locatário para novos alertas a cada cinco minutos. Os incidentes de segurança serão criados se alertas acionados forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a ingestão de alertas em relação à carga do servidor e extrair os dados mais atuais, cinco minutos é a configuração que você pode preferir. No entanto, este valor pode ser modificado conforme necessário.
○ Ingestão de alerta contínua selecionada ○ Definir tempo de ingestão do alerta inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas: ○ Selecione os campos Ingestão de alerta em andamento e Definir tempo de ingestão de alerta inicial. ○ Especifique a hora no campo Tempo de ingestão do alerta inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida no campo Incremento de pesquisa (minutos). Como exemplo de programação, se você tiver um trabalho de alerta diário executado uma vez por dia às 4 hora local, poderá configurar o perfil de alerta correspondente em seu ServiceNow AI Platform Instância a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ser executada às 4:05 hora local para capturar o alerta imediatamente e criar um incidente de segurança. Insira 04 05 00 no campo Ingestão de alerta inicial. No campo Incremento (minutos), insira 1440 (24 horas) para programar a próxima ingestão de alerta para 24 horas a partir da ingestão de alerta inicial. A hora de ingestão do alerta inicial e a hora da próxima ingestão do alerta são exibidas nos campos. Para definir as configurações neste exemplo, siga estas etapas: ○ Selecione **Ingestão de alerta contínua** opção. ○ No campo Incremento de pesquisa (minutos), insira 1440 (24 horas). ○ Clique em **Defina o tempo de ingestão do alerta inicial** Opção para habilitar a edição dos campos Hora de ingestão de alerta inicial e Hora da próxima ingestão de alerta (estimada). ○ No campo Tempo de ingestão do alerta inicial, insira 04 05 00. No campo Tempo da próxima ingestão de alerta (estimada), a hora da próxima ingestão de alerta é exibida.
Campo Recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única ingere alertas históricos. Quando esta configuração é definida, um perfil é usado uma vez para recuperar alertas de eventos históricos baseados em um intervalo de datas. À direita do campo Desde data, clique no ícone de calendário. No calendário exibido, selecione a data em que você deseja começar a extrair alertas. A partir do valor da data Desde, os alertas são recuperados até a data atual. Observe que você pode extrair até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de alertas históricos, mas sim uma quantidade mínima de alertas em trânsito que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os alertas forem extraídos, esta configuração não recuperará mais alertas para este perfil a partir da data atual. Esta configuração preenche o in-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cidente de segurança com todos os alertas encontrados para o intervalo inserido.

3. Clique em **Continuar** Para navegar até a página Opções adicionais.

Automatize atualizações de alerta e fechamento com base no status do incidente SIR

. API de segurança do Microsoft Graph A integração de ingestão de alertas tem uma interface bidirecional que permite que ambos os alertas criem incidentes de segurança, bem como a capacidade de atualizar os alertas depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como SIR número do incidente, grupo de atribuição, SIR URL do incidente e assim por diante. T

Antes de Iniciar

Função necessária: sn_si.admin

Nota: Os status de alerta inicial e de fechamento serão atualizados somente se esta funcionalidade for compatível com o provedor de serviços. Para obter detalhes, consulte API de segurança do Microsoft Graph e a documentação do provedor de segurança.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais** .
2. Siga as instruções abaixo para concluir a configuração para atualizar alertas quando o incidente de segurança for criado.

Opção ou Campo	Descrição
Atualizar alertas após a criação do incidente SIR	Selecione esta opção se quiser atualizar o status do alerta e adicionar comentários adicionais quando um incidente de segurança for criado a partir do alerta. Isso pode ocorrer para os alertas de gatilho iniciais que criam o incidente de segurança, bem como alertas agregados.
Atualização do status do alerta inicial	Selecione um status de alerta inicial na lista. Este status será definido para todos os alertas quando um incidente de segurança for criado para um alerta ingerido. Isso inclui alertas que criam novos incidentes e alertas que são ingeridos e agregados a um incidente em aberto existente. **Nota:** Com base no status de alerta selecionado aqui, o status de alerta usado pelos provedores de segurança será atualizado correspondentemente.
Comentários iniciais retornados ao Alerta	Com base na fase selecionada, os comentários padrão são exibidos. Você pode modificar o texto padrão e usar o formato "nome do campo" para adicionar ou modificar todos os campos disponíveis no formulário de incidente de segurança.
Fechar alertas após o fechamento do incidente SIR	Selecione esta opção se quiser usar a opção de fechamento de alerta automatizado. Isso pode ocorrer para os alertas de gatilho iniciais que criam o inciden-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou Campo	Descrição
	te de segurança, bem como alertas agregados. O status do alerta será atualizado no provedor de segurança com o status e os comentários de fechamento após SIR o incidente está encerrado em ServiceNow AI Platform.
Atualização do status do alerta de fechamento	Selecione um status de alerta na lista. Selecione o valor de status a ser definido para todos os alertas quando um incidente de segurança for encerrado para um alerta ingerido.
Comentários de fechamento retornados para o alerta	Os comentários de fechamento padrão são exibidos aqui. Você pode editar o texto padrão e usar o formato "nome do campo" para adicionar ou modificar todos os campos disponíveis no formulário de incidente de segurança.

3. Clique em **Concluir** para concluir a configuração e mover o perfil para **Aguardando** estado.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair alertas do Microsoft Azure locatário com base em sua programação. Máximo de 1000 incidentes de segurança podem ser criados em um período de 24 horas.

Definições de configuração de integração da API de segurança do Microsoft Graph

Use esta opção para modificar API de segurança do Microsoft Graph propriedades do sistema padrão da integração de ingestão.

Antes de Iniciar
Função necessária: sn_si.admin

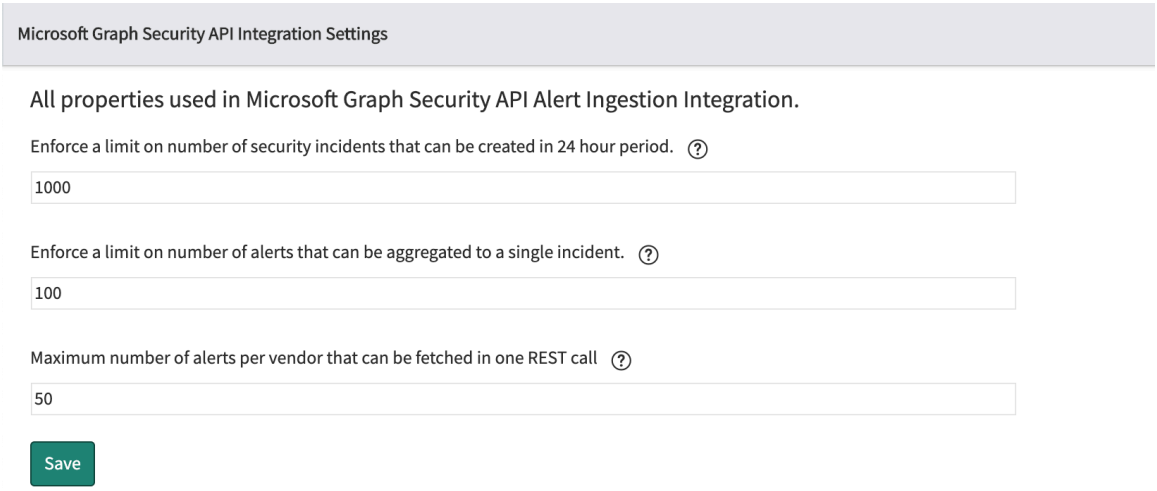
Por Que e Quando Desempenhar Esta Tarefa
Modifique as propriedades de configuração padrão para limitar o número de incidentes de segurança que podem ser criados durante um período de 24 horas ou o número de alertas que podem ser agregados em um incidente de segurança.

Para modificar as propriedades do sistema, faça login como um usuário com *sn_si.admin* e navegue até **Integração da API de segurança do Microsoft Graph** > **Configuração de integração da API de segurança do Microsoft Graph**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



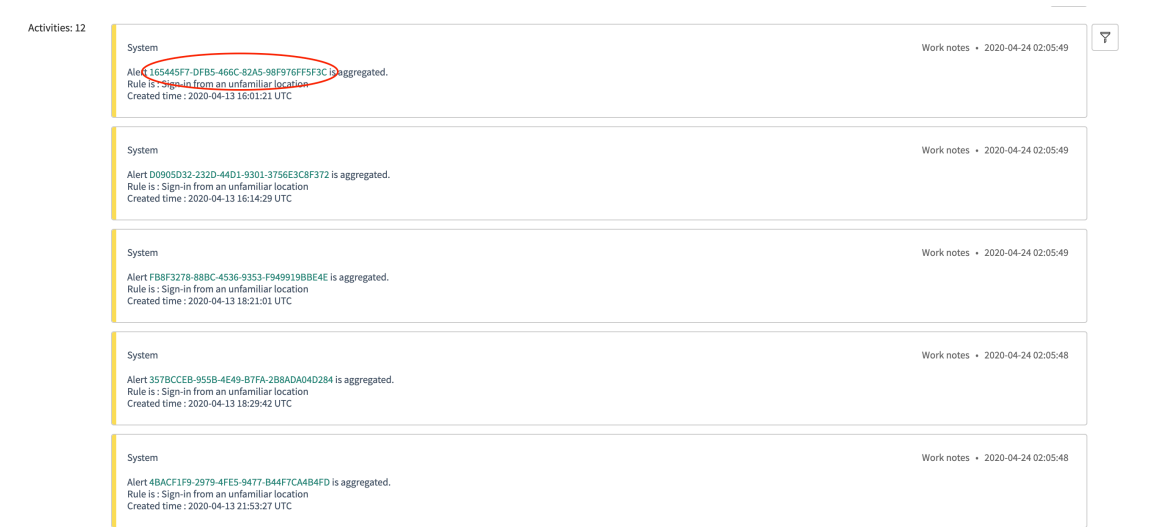
Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Formulário de resposta a incidentes de segurança após a ingestão de alertas

Depois de um API de segurança do Microsoft Graph um alerta foi ingerido, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro de incidente de segurança.

Anotações de trabalho

Se você tiver selecionado **Anotação de trabalho em log para o novo alerta** Opção nos critérios de agregação de alertas conforme descrito em Mapeamento de alertas para campos de resposta a incidentes de segurança uma anotação de trabalho é publicada quando o alerta é agregado.



Clique no link de alerta para navegar até o registro de importação de alerta interno que contém dados brutos de alerta.

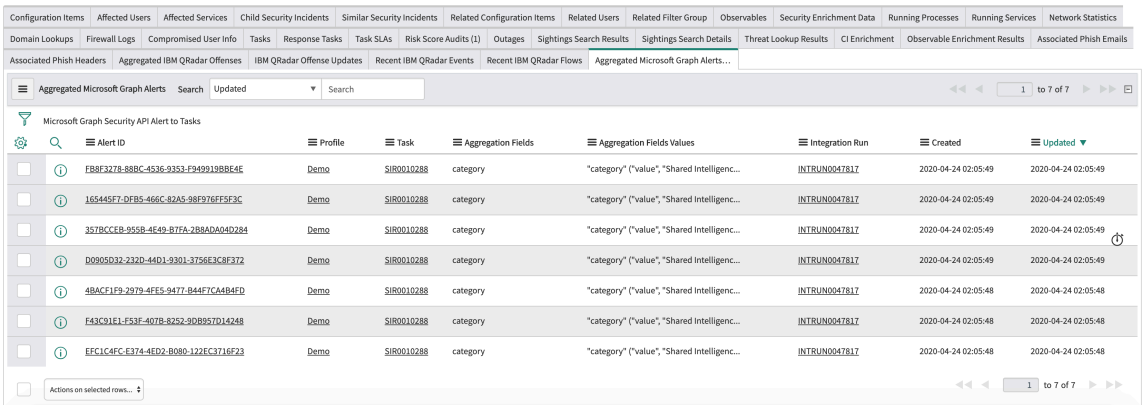
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Alertas agregados

Clique **Listas relacionadas** > **Alertas agregados de segurança do Microsoft Graph** para exibir os alertas agregados ao incidente de segurança.



- **Criar incidente de segurança** : Selecione um alerta na lista e clique em **Ações** e clique em **Criar incidente de segurança** . Esta opção cria um novo incidente de segurança para o alerta e este alerta é desagregado do incidente de segurança primário.
- **Excluir registro de alerta** : Selecione um alerta na lista e clique em **Ações** e clique em **Excluir** . Esta opção exclui o registro de alerta.

Opcional: Copie um perfil da API de segurança do Microsoft Graph

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração da API de segurança do Microsoft Graph** > **Perfil da API de segurança do Microsoft Graph**.
2. Em API de segurança do Microsoft Graph Lista de perfis exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Cópia** .
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que **Ativo** o status da coluna é definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Domain Separation e. API de segurança do Microsoft Graph ingestão de alertas

Domain Separation é compatível com esta aplicação. . API de segurança do Microsoft Graph A integração ingere alertas dos provedores de segurança do Microsoft Graph e cria incidentes de segurança automaticamente. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

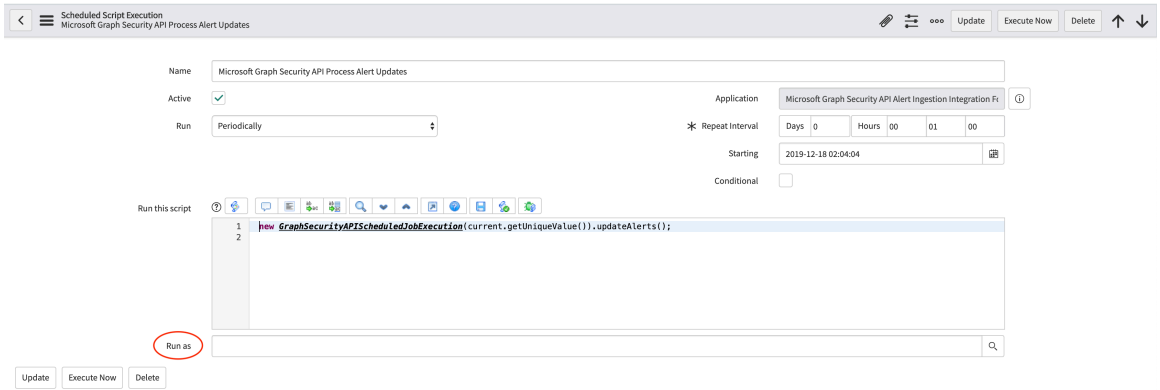
Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

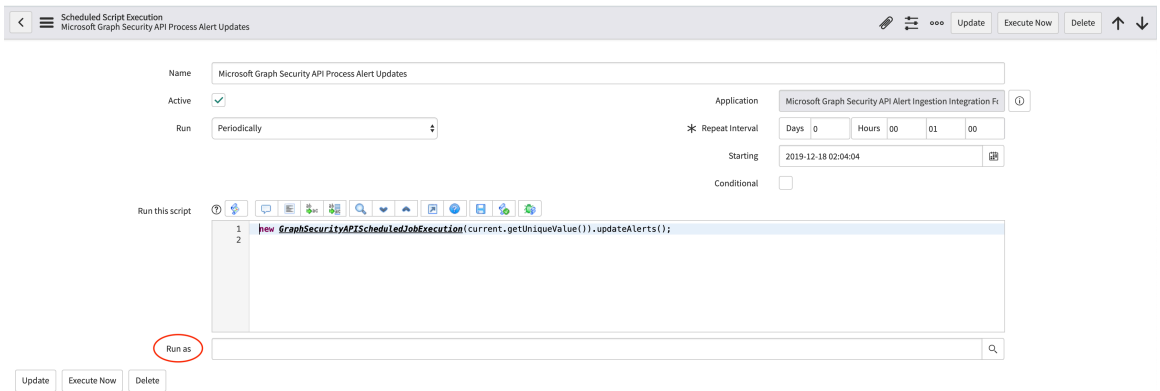
Como o Domain Separation funciona no API de segurança do Microsoft Graph

Para obter a separação de domínio, replique o. API de segurança do Microsoft Graph Processo de perfil e. SIR Processar alertas atualiza trabalhos agendados e muda o. **Executar como** usuários. Por padrão, os usuários do sistema executam esses trabalhos agendados. Mude **Executar como** para um usuário com a função sn_si.admin no respectivo domínio e execute o trabalho agendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tópicos relacionados

Domain Separation para provedores de serviço

Flow Designer e uso do Integration Hub na integração da API de segurança do Microsoft Graph

Usando a funcionalidade Flow Designer e Hub de integração, vários subfluxos e ações foram criados como parte do API de segurança do Microsoft Graph integração.

Os seguintes subfluxos estão disponíveis:

- API de segurança do Microsoft Graph Validação da configuração: Isso é usado no bloco de configuração para validar as credenciais na configuração inicial.
- Chamada REST para API de segurança do Microsoft Graph: Isso é usado para todas as interações com a API de segurança do Microsoft Graph usando chamadas REST.
- Recuperar alertas de amostra: Isso é usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.

Solução de problemas de integração da API de segurança do Microsoft Graph

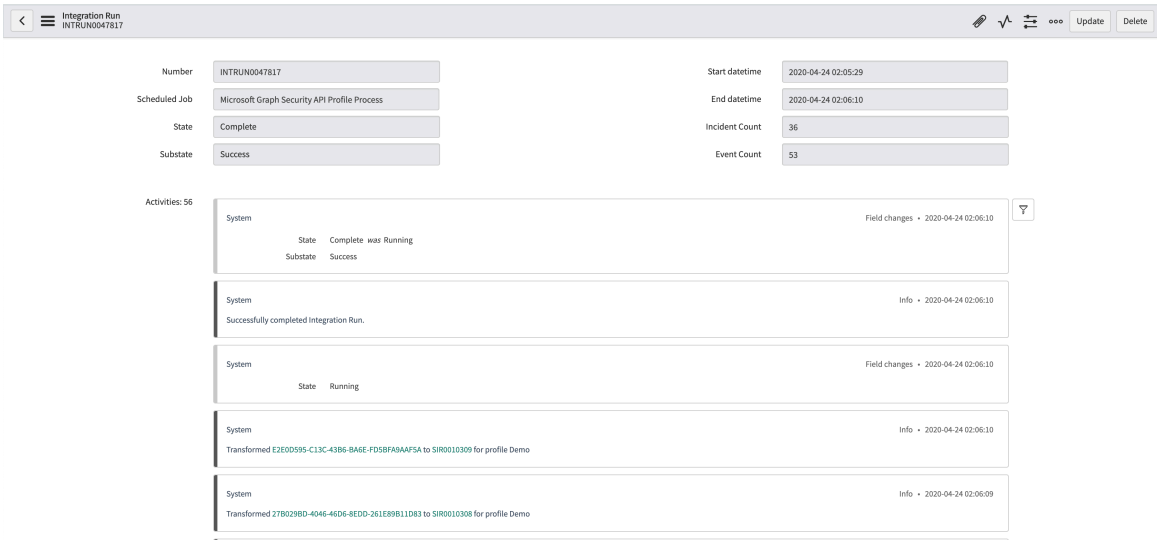
Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas ao API de segurança do Microsoft Graph integração de ingestão de alertas.

- **Execução de integração** : Quando um trabalho agendado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de alertas extraídos e o número de incidentes criados em uma execução de trabalho programada também são exibidos. Usuários com `sn_si.analista` a função pode ver se houve falha na extração de erros/perfis durante a execução da integração. Usuários com `sn_si.analista` a função pode verificar `sn_event_ingestion_integration_run` tabela para todos os erros que ocorreram. Para solucionar quaisquer problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de trabalho nos registros de execução de integração para cada execução de trabalho programada.



- **Perfil incompleto** : Ao configurar o perfil, nas Opções adicionais (Automatize atualizações de alerta e fechamento com base no status do incidente SIR), você deve clicar em **Concluir** Botão para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando ingestão.
- **Validar perfil** : Para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de alertas e os registros da tabela de alerta para tarefas.
- **Problemas de SSL** : Ao se conectar por meio do API de segurança do Microsoft Graph Certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte KB0778285 para obter detalhes.

Palo Alto Networks - AutoFocus integração

. Palo Alto Networks - AutoFocus o sistema de base de integração inclui um fluxo de trabalho e uma série de atividades de fluxo de trabalho que você pode usar para integrar Palo Alto Networks - AutoFocus com sua instância.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

Ativar e configurar Palo Alto Networks - AutoFocus integração

---

Usar

- Operações de segurança Palo Alto Networks - Verificar e bloquear fluxo de trabalho de valor
- Fluxo de aprimoramento de informações da sessão de foco automático

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Ativar e configurar Palo Alto Networks - AutoFocus integração

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - AutoFocus. Antes de poder usar Palo Alto Networks - AutoFocus, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixar uma aplicação do ServiceNow Store pela primeira vez.
2. Quando a instalação estiver concluída, acesse o site de suporte da Palo Alto Networks e obtenha a chave de API.
3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**.
4. No cartão de foco automático da Palo Alto Networks, clique em **Configurar** .
5. Insira (ou cole) o. **Chave de API** Você adquiriu no site de suporte da Palo Alto Networks.
6. Clique em **Enviar**.

Fluxo de aprimoramento de informações da sessão de foco automático

. **Operações de segurança Palo Alto Networks- Obtenha aprimoramento de informações da sessão de foco automático** O fluxo é executado, ele fila uma consulta de pesquisa com foco automático para coletar informações sobre um IP de origem especificado. Se o foco automático tiver conhecimento sobre sessões anteriores originadas desse endereço IP, um relatório no formato JSON será retornado.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

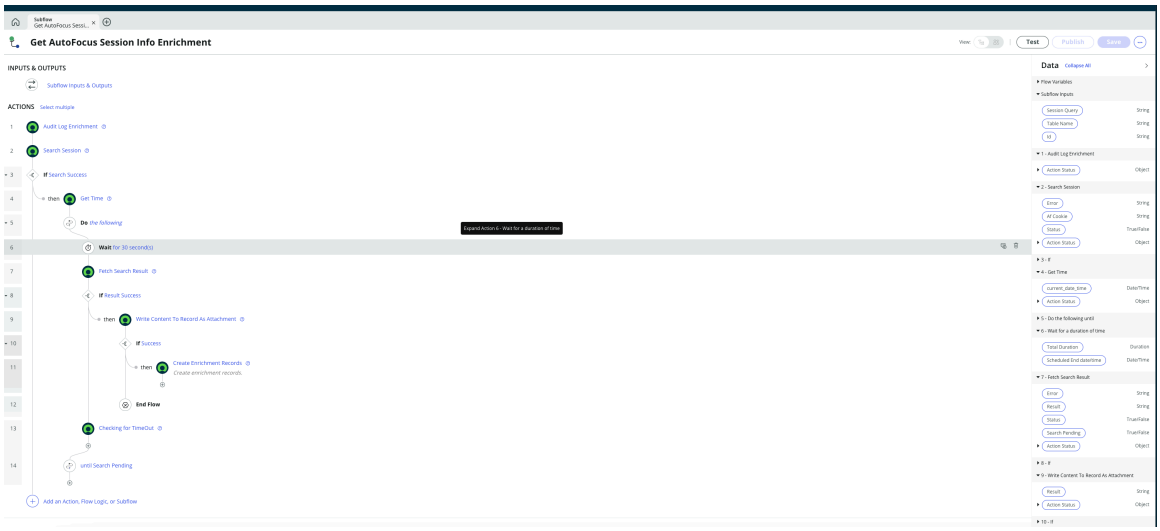
. **Operações de segurança Palo Alto Networks- Obtenha aprimoramento de informações da sessão de foco automático** o fluxo é executado quando **IP de origem** o campo em um incidente de segurança é modificado e o registro é atualizado. O fluxo busca o endereço IP e envia uma solicitação de consulta para foco automático. Se o foco automático tiver

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

identificado sessões originadas do endereço IP anteriormente, um relatório no formato JSON será retornado.

Palo Alto Networks de operações de segurança - Obter fluxo de aprimoramento de dados do Wildfire



Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Clique em **Indicadores de compromisso** e preencha **IP de origem** campo.
3. Clique em **Atualizar**.
   O foco automático verifica as informações do endereço IP e um arquivo de texto no formato JSON é anexado ao incidente de segurança.

   As ações específicas desta integração são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Ação da sessão de pesquisa de foco automático

. **Sessão de pesquisa de foco automático** A ação de fluxo carrega informações de um endereço IP atribuído a um incidente de segurança para foco automático e as coloca na fila para uma consulta de pesquisa.

Variáveis de entrada

Nota:

Quando a ação é executada, ela fila uma consulta de pesquisa com foco automático para coletar informações para um IP de origem especificado. Se o foco automático tiver identificado sessões originadas desse endereço IP anteriormente, um relatório no formato JSON será retornado.

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
SearchSessionQuery [cadeia de caracteres]	A consulta de pesquisa de informações da sessão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação Buscar resultados da pesquisa

. **Buscar resultados da pesquisa** a ação de fluxo busca resultados de pesquisa identificados por um cookie para a consulta de pesquisa iniciada pelo **Sessão de pesquisa de foco automático** ação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
afcookie [cadeia de caracteres]	O cookie de foco automático para a solicitação de pesquisa gerada pelo Ação da sessão de pesquisa de foco automático.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
Pesquisa pendente [booliano]	Verdadeiro se a solicitação de pesquisa ainda estiver sendo processada no foco automático.
resultado [cadeia de caracteres]	Os dados dos resultados da pesquisa.
Status [booliano]	Verdadeiro se a pesquisa for concluída e os resultados tiverem sido gerados com sucesso.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na ação.

Palo Alto Networks - Firewall integração

Para executar Palo Alto Networks - Firewall integração, certifique-se de que você tenha um MID Server Configure com credenciais SSH. Se um firewall ainda não estiver configurado, adicione um.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

- Ativar e configurar a Integração de firewall da Palo Alto Networks
- Configure credenciais SSH para o MID Server

Usar

Palo Alto Networks Fluxo de trabalho do Inicializador de firewall

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configure credenciais SSH para o MID Server

O Firewall da Palo Alto Networks envia chamadas de API para o MID Server. Dessa forma, certifique-se de que as credenciais SSH tenham sido criadas para o MID Server.

Antes de Iniciar

- O plug-in Orquestração deve ser ativado.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Orquestração** > **Credenciais e Conexões** > **Credenciais**.
2. Clique em **Nova**.
3. Na tela Interceptador, clique em **Credenciais SSH** .
4. Preencha os campos, conforme necessário.

Credenciais SSH

Campo	Descrição
Nome	Insira um nome para a credencial.
Ativo	Marque esta caixa de seleção para ativar esta credencial.
Aplica-se a	Selecione **Todos os MID Servers** ou **MID Servers específicos** .
MID Servers	Se você selecionou **MID Servers específicos** , Clique no ícone de cadeado e selecione os MID Servers aos quais você deseja aplicar essas credenciais.
Ordem	Selecione a ordem na qual as credenciais são testadas pelo servidor. Números menores são testados primeiro.
Nome de usuário	Insira o nome de usuário do usuário associado a essas credenciais, se houver.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Senha	Se você inseriu um **Nome de usuário** insira a senha do usuário.
Marcador	Insira um marcador a ser usado para critérios de pesquisa. . **Marcador** o campo deve conter o mesmo valor que **Nome** .

Ativar e configurar a Integração de firewall da Palo Alto Networks

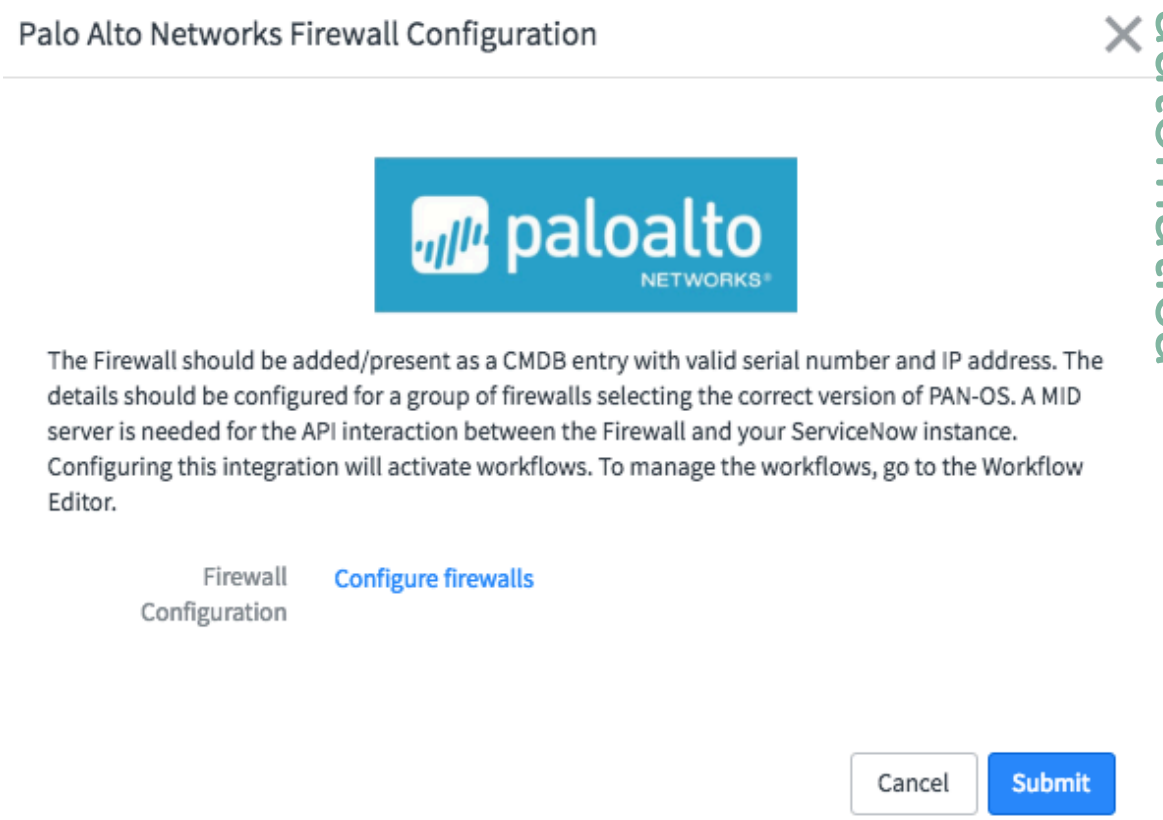
O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - Firewall. Antes de poder usar Palo Alto Networks - Firewall, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Antes de ativar e configurar a integração, acesse o painel Firewall da Palo Alto Networks.
   Anote os nomes da Lista dinâmica de IPs, Lista dinâmica de URL ou Lista dinâmica de domínio que você está usando para bloqueio de firewall.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Firewall da Palo Alto Networks, clique em **Configurar** .



5. Clique em **Configurar firewalls** .
6. Na tela Configurações do firewall, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Firewalls	Clique no ícone de cadeado e selecione o firewall a ser configurado.
Versão do firewall	Selecione a versão do Firewall da Palo Alto Networks.**PAN-OS-7,1** é a versão recomendada. Selecionar versões anteriores pode retornar resultados inconsistentes.
Nome do usuário	Insira o nome de usuário a ser usado ao se conectar ao firewall por endpoints REST.
Senha	Insira a senha do usuário conectado.
Lista dinâmica de IPs	Insira o nome da Lista dinâmica externa ou da Lista de bloqueios dinâmicos que você usa para endereços IP.
Lista dinâmica de URL	Insira o nome da Lista dinâmica externa ou da Lista de bloqueios dinâmicos que você usa para URLs.
Lista dinâmica de domínio	Insira o nome da Lista dinâmica externa ou da Lista de bloqueios dinâmicos que você usa para domínios.

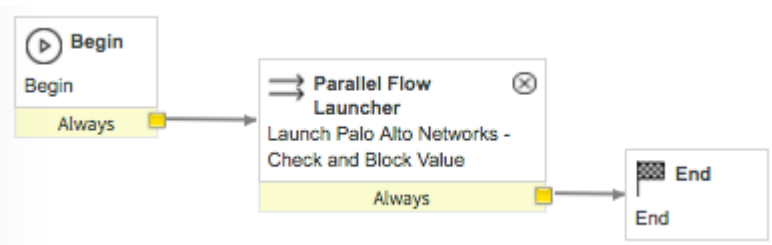
8. Clique em **Enviar**.

Palo Alto Networks Fluxo de trabalho do Inicializador de firewall

Inicializador de firewall da Palo Alto Networks para integração de operações de segurança
O fluxo de trabalho é a implementação do firewall da Palo Alto Networks iniciada pelo **Integração de operações de segurança - Solicitação de bloqueio** fluxo de trabalho de capacidade.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
as atividades do processo de fluxo de trabalho incluem: Operações de segurança Palo Alto Networks - Verificar e bloquear fluxo de trabalho de valor.



Operações de segurança Palo Alto Networks - Verificar e bloquear fluxo de trabalho de valor

Como os incidentes de segurança são criados e triados para identificar possíveis ameaças, você pode usar **Operações de segurança Palo Alto Networks - Verificar e bloquear valor** Fluxo de trabalho para verificar e atualizar automaticamente endereços IP, URLs e domínios usando listas dinâmicas externas definidas em Palo Alto Networks - Firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

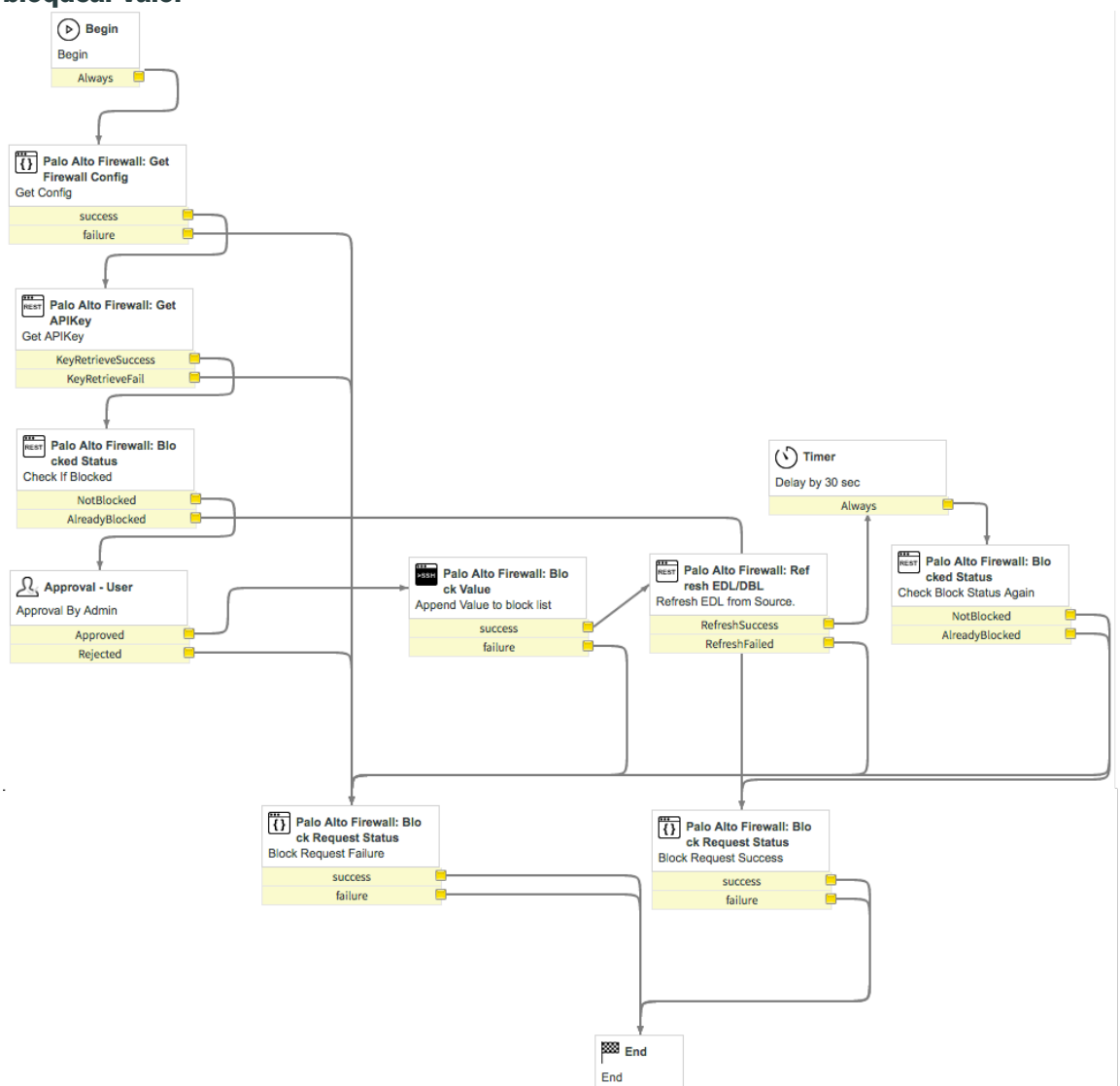
Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
. **Operações de segurança Palo Alto Networks - Verificar e bloquear valor** O fluxo de trabalho é executado quando as solicitações de bloqueio de firewall são enviadas. A solicitação de bloqueio especifica o firewall a ser usado, o tipo de observável a ser verificado e bloqueado (se necessário) e o valor do bloco. Ou seja, o endereço IP, URL ou domínio em questão.

Durante a execução do fluxo de trabalho, comandos definidos em **Palo Alto Networks Integration** > **Firewall** > **Comandos** são executados. Os comandos do tipo Mostrar (por exemplo, Show-ip-ExternalDynamicList) determinam se o valor existe no firewall. Os comandos do tipo Refresh (por exemplo, Refresh-IP-ExternalDynamicList) adicionam um valor que não existe no firewall à lista de bloqueios.

Após Status bloqueado a atividade é executada, a aprovação de um administrador do sistema é necessária antes que o fluxo de trabalho possa prosseguir.

Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Palo Alto Networks Integration** > **Firewall** > **Solicitações de bloqueio**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Firewall	Selecione o firewall a ser usado.
Tipos de bloco	Selecione o tipo de valor a ser verificado: ○ IP ○ URL ○ DOMÍNIO
Valor do bloco	Insira o valor do tipo selecionado a ser verificado no firewall.

4. Clique em **Enviar**.

Firewall de Palo Alto - Atividade Bloquear status da solicitação

Esta atividade é chamada por outras atividades para definir o status da solicitação de bloqueio de firewall como Sucesso ou Falha.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
FirewallBlockRequestSysid [cadeia de caracteres]	O ID do sistema da solicitação de bloqueio de firewall. Esta variável de entrada é obrigatória.
status [cadeia de caracteres]	Indica se o trabalho de atualização foi executado: Sucesso ou falha.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se o sucesso ou a falha do trabalho de atualização.

Firewall de Palo Alto - Atividade Bloquear valor

Depois que o fluxo de trabalho identifica um valor que não está no firewall, o registro é roteado para aprovação. Após a aprovação, esta atividade se conecta ao MID Server por meio de suas credenciais SSH e invoca um script que adiciona o valor à Lista de bloqueios externos do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Nota: Você deve inserir manualmente as variáveis de entrada para esta atividade e, em seguida publique o fluxo de trabalho . Se o fluxo de trabalho não for publicado, as variáveis de entrada não serão salvas para usuários não administradores.

Variáveis de entrada

Variável	Descrição
BeBlockedValue [cadeia de caracteres]	O valor a ser adicionado ao EDL se ainda não estiver presente. Esta variável de entrada é obrigatória.
TypeToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado: IP, URL ou Domínio. Esta variável de entrada é obrigatória.
TargetHost [cadeia de caracteres]	MID Server no qual o script é executado.
SSHCredentialTag [cadeia de caracteres]	. Marcador de credencial SSH definido no MID Server .
ScriptCommand [cadeia de caracteres]	O script AppendValueToList.sh usado para adicionar o valor ao EDL. Requer o caminho completo para o MID Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	O resultado passou para o EDL.

Firewall de Palo Alto - Atividade Status bloqueado

Esta atividade verifica se o valor (IP, URL ou domínio) está incluído em sua respectiva Lista dinâmica externa/Lista de bloqueios dinâmicos (EDL/DBL) no firewall. Os detalhes de EDL/DBL são obtidos do firewall usando um comando operacional e uma rotina é realizada para verificar se o valor está bloqueado no firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
ValorToBeCheck [cadeia de caracteres]	O valor na solicitação de bloco.
ShowEDLDetalhsCommand [cadeia de caracteres]	O comando Lista dinâmica externa que está sendo usado para determinar se o valor existe no firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall usado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente usando a mensagem da API Comando operacional do Firewall Palo Alto.

Variáveis de saída

Variável	Descrição
CommandResult [cadeia de caracteres]	Os resultados do firewall para o comando Mostrar detalhes do EDL.
BlockedStatus [boolian]	Verdadeiro indica bloqueado. Falso indica não bloqueado.
CommandResponse [cadeia de caracteres]	O status da resposta obtido do firewall para o comando show EDL Details.

Palo Alto Firewall: Obter ação de chave de API

Esta ação recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
Nome de usuário [cadeia de caracteres]	O nome de usuário do administrador do firewall.
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Palo Alto Firewall: Obter ação de configuração do firewall

. **Palo Alto Firewall: Obter configuração de firewall** a ação de fluxo obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela ação subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
FirewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
TypeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou Domínio.
FirewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
IpEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
UrlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.
DomainEDLName [cadeia de caracteres]	O nome da Lista dinâmica externa para domínios.
FirewallVersionSysId [cadeia de caracteres]	O ID do sistema da versão do firewall.
RefreshEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar o EDL da origem.
ShowEDLDetalhsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes do EDL.
Status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na ação.
Endpoint [criptografado]	O endpoint criptografado do banco de dados.

Firewall de Palo Alto- Atualize a atividade EDL/DBL

Esta atividade executa um comando operacional no firewall para atualizar a Lista dinâmica externa da origem configurada no firewall. A saída desta atividade indica se o trabalho de atualização foi enfileirado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall que está sendo atualizado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall atualizada.
FirewallCommand [cadeia de caracteres]	O comando operacional a ser executado para enfileirar o trabalho de atualização.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
Resultado.Saída.Atividade [cadeia de caracteres]	Uma cadeia de caracteres de texto para indicar se o trabalho de atualização foi enfileirado para execução: Sucesso ou falha.

Obter fluxo de dados de log

Se Resposta a incidentes de segurança, Inteligência contra ameaças e Palo Alto Networks - Firewall estão ativados, o. **Operações de segurança Palo Alto Networks - Obter dados de log** O fluxo é executado automaticamente quando o IP de origem dos observáveis em um incidente de segurança é alterado.

Antes de Iniciar

Função necessária: sn_si.analyst

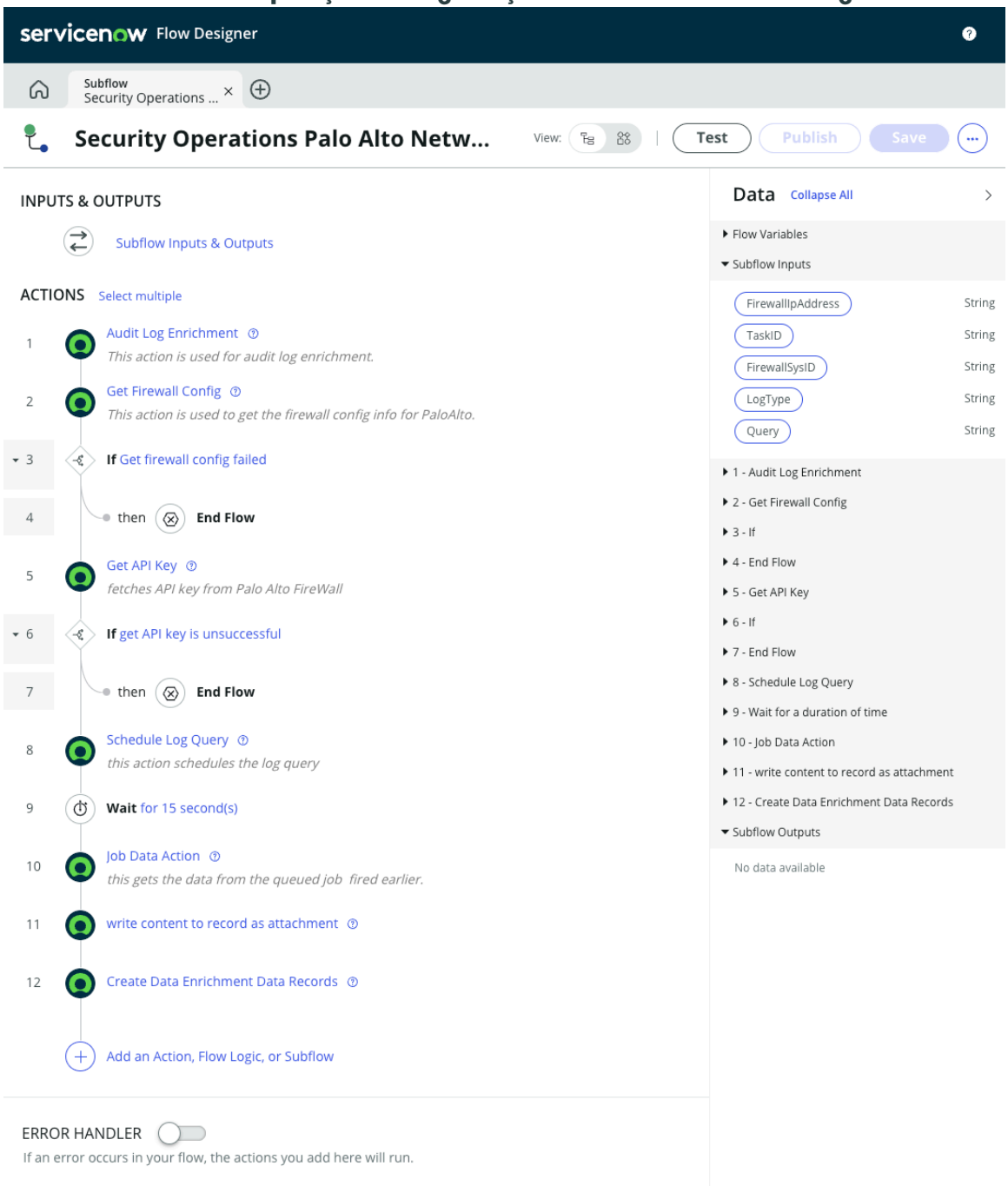
Por Que e Quando Desempenhar Esta Tarefa

Durante a execução do fluxo, as informações de configuração do firewall são recuperadas do banco de dados e a chave de API é recuperada do firewall. A ação Obter log enfila uma consulta de pesquisa no firewall. Quando a consulta é executada, ela retorna um ID de trabalho que é usado para recuperar dados de logs de ameaças do firewall. Anexa os dados de log como um arquivo XML ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Palo Alto Networks de operações de segurança - Obter fluxo de dados de log



Tradução automática

Procedimento

1. Navegue até um incidente de segurança que contém observáveis.
2. Clique em **Observáveis de incidentes de segurança** guia.
3. Em **IP de origem** , Adicione ou modifique o endereço IP.
4. Clique em **Atualizar**.
   . **Operações de segurança Palo Alto Networks - Obter dados de log** o fluxo é executado e os dados de log de ameaças aprimorados são anexados ao incidente de segurança. As informações também são analisadas e exibidas no **Logs do firewall** seção em **Dados de aprimoramento** guia.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Palo Alto Firewall: Obter ação de chave de API

Esta ação recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
Nome de usuário [cadeia de caracteres]	O nome de usuário do administrador do firewall.
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Palo Alto Firewall: Obter ação de configuração do firewall

. **Palo Alto Firewall: Obter configuração de firewall** a ação de fluxo obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela ação subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
FirewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
TypeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou Domínio.
FirewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
IpEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
UrlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.
DomainEDLName [cadeia de caracteres]	O nome da Lista dinâmica externa para domínios.
FirewallVersionSysId [cadeia de caracteres]	O ID do sistema da versão do firewall.
RefreshEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar o EDL da origem.
ShowEDLDetalhsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes do EDL.
Status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na ação.
Endpoint [criptografado]	O endpoint criptografado do banco de dados.

Palo Alto Firewall- Obter ação de log

. **Palo Alto Firewall: Obter log** A ação de fluxo agenda uma consulta no firewall para recuperar logs e retorna um JOBID usado para recuperar os dados do log.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall. Esta variável de entrada é obrigatória.
FirewallApiKey [cadeia de caracteres]	A chave de acesso à API do firewall. Esta variável de entrada é obrigatória.
FirewallLogType [cadeia de caracteres]	O tipo de dados de log a serem recuperados (definido como Ameaça). Esta variável de entrada é obrigatória.
FirewallLogFilterQuery [cadeia de caracteres]	A consulta a ser executada para pesquisar logs no firewall. Esta variável de entrada é obrigatória.
LogDirection [cadeia de caracteres]	Especifica se os logs são mostrados mais antigos primeiro (para trás) ou mais recentes primeiro (para frente).
LogNumber [cadeia de caracteres]	Especifica o número de logs a serem recuperados.
LogSkipCount [cadeia de caracteres]	Especifica o número de logs a serem ignorados ao fazer uma recuperação de log.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
QueuedJOBID [cadeia de caracteres]	O ID do trabalho retornado do firewall.
JobScheduled [cadeia de caracteres]	Especifica (sucesso ou falha) se o trabalho foi enviado para o firewall.
erro [cadeia de caracteres]	Todos os erros retornados.

Palo Alto Firewall- Ação de dados de trabalho

Após **Palo Alto Firewall: Obter log** a ação fila a consulta de pesquisa para o firewall e o trabalho é executado, o. **Palo Alto Firewall: Ação de dados de trabalho** a ação recupera os dados do log de ameaças do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação. Todos os campos de entrada são obrigatórios.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.
FirewallApiKey [cadeia de caracteres]	A chave de acesso à API do firewall.
JOBID [cadeia de caracteres]	O ID do trabalho enfileirado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
CommandStatus [cadeia de caracteres]	Especifica (sucesso ou falha) se os dados foram recuperados do firewall.
JobData [cadeia de caracteres]	Os dados coletados do firewall.
erro [cadeia de caracteres]	Todos os erros retornados.

Palo Alto Networks - WildFire integração

Palo Alto Networks - WildFire é uma aplicação baseada em nuvem que interage com o firewall do sistema.

Tradução automática

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

Ativar Palo Alto Networks - WildFire

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar	Desenvolver
Obter fluxo de aprimoramento de dados do Wildfire	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Ativar Palo Alto Networks - WildFire

Antes de usar a integração Security Operations Palo Alto Networks - Wildfire, você deve baixar a integração do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

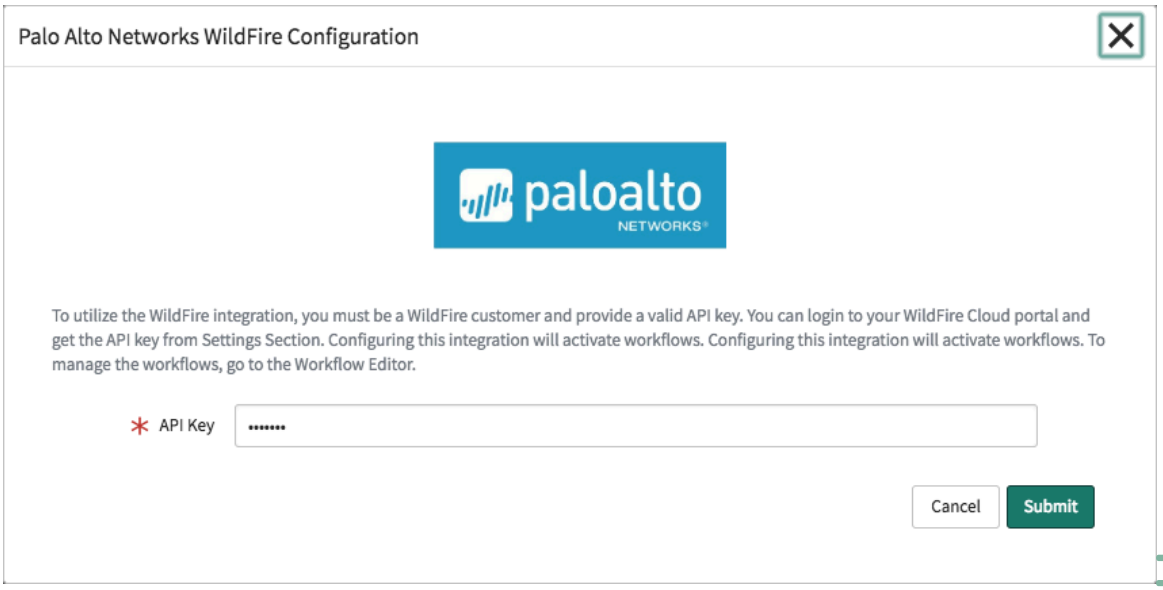
1. Baixe a integração do ServiceNow Store.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em Carbon Black cartão, clique em **Configurar** .



4. Insira a chave de API e clique em **Enviar** .
   O cartão de configuração de integração é exibido.
5. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Obter fluxo de aprimoramento de dados do Wildfire

. **Palo Alto Networks de operações de segurança - Obtenha aprimoramento de dados selvagens** O fluxo é executado, um arquivo de hash é carregado no Wildfire. Os dados são aprimorados e os relatórios são baixados para a instância para ajudar no processamento de possíveis ataques de malware.

Antes de Iniciar

Função necessária: sn_si.analyst

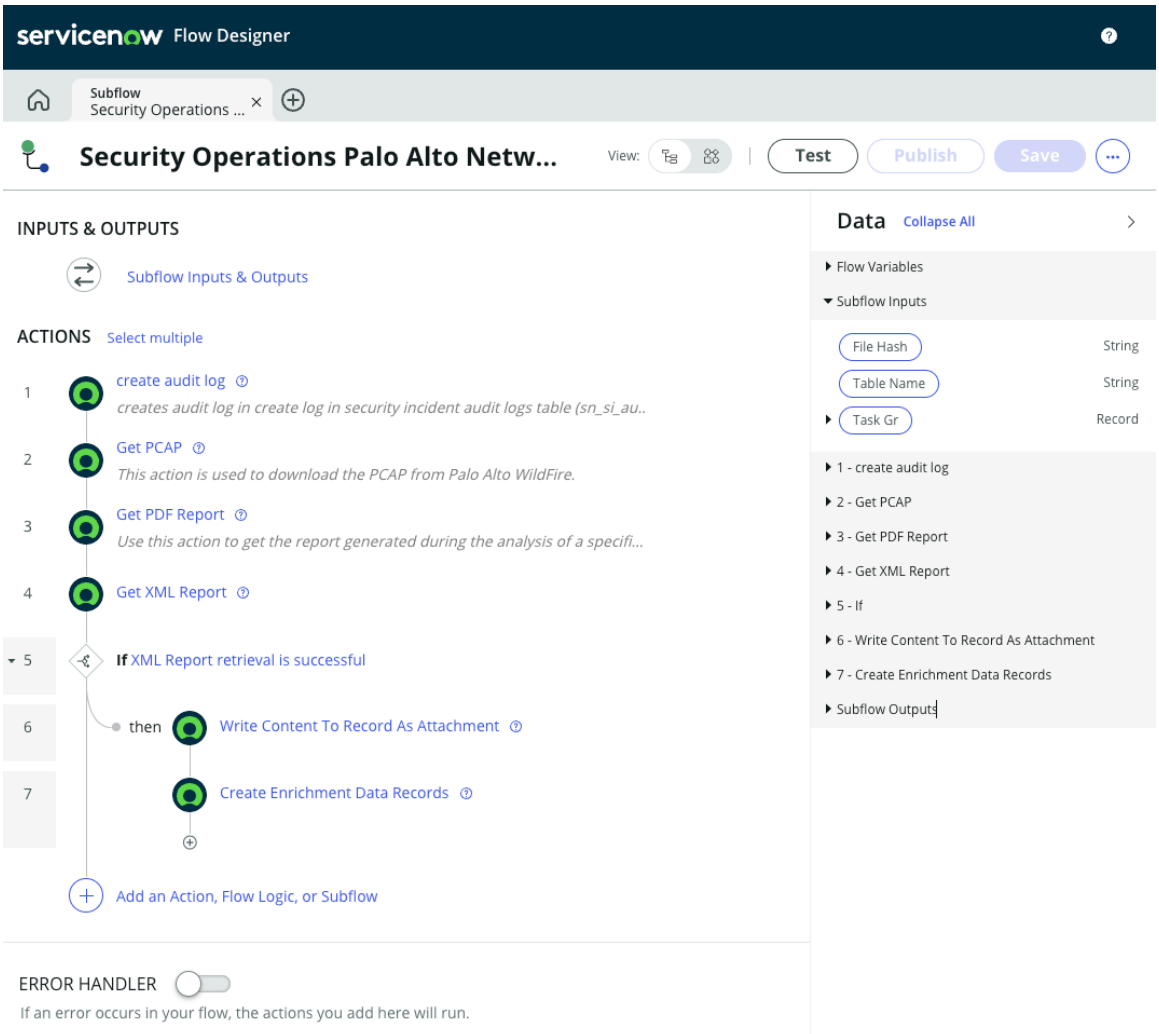
Por Que e Quando Desempenhar Esta Tarefa

. **Palo Alto Networks de operações de segurança - Obtenha aprimoramento de dados selvagens** O fluxo é executado quando um incidente de segurança é criado a partir de um alerta recebido da aplicação Firewall de rede Palo Alto. Um hash de malware da notificação por e-mail recebida do firewall é inserido no **IOC** do incidente de segurança e o registro é atualizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Palo Alto Networks de operações de segurança - Obter fluxo de aprimoramento de dados do Wildfire



Procedimento

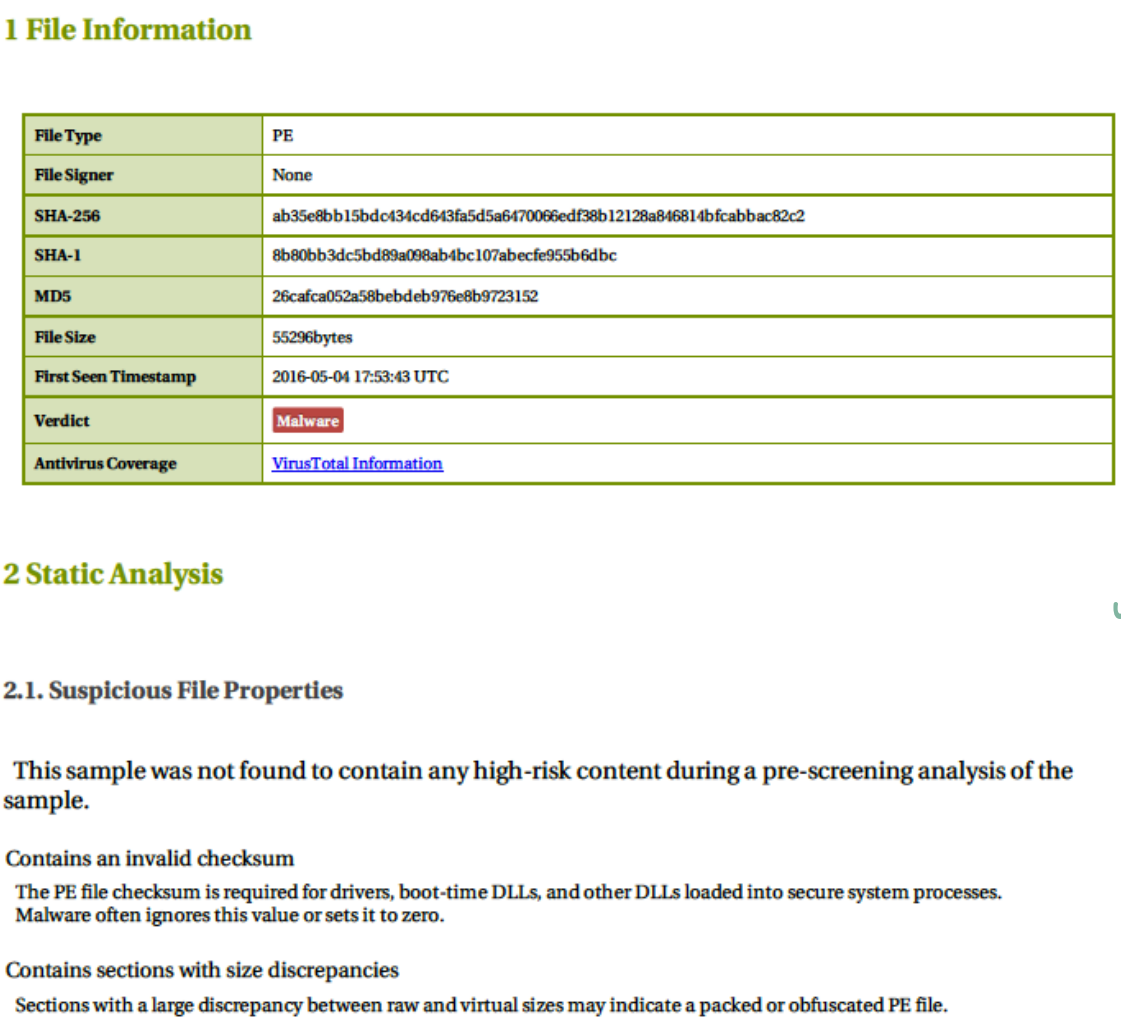
1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Com base na notificação por e-mail recebida do Firewall, localize e abra o incidente de segurança que foi criado.
3. Clique em **Indicadores de compromisso** e preencha **Hash de malware** com o hash que você recebeu no alerta.
4. Clique em **Atualizar**.
   O fluxo faz com que o arquivo de hash seja carregado no Wildfire, onde os dados são aprimorados. Os relatórios nos formatos PDF e XML são anexados ao registro (incidente de segurança ou IOC) em sua instância para ajudar no processamento de possíveis ataques de malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se os dados aprimorados incluírem informações de captura de pacote, as informações do PCAP também serão baixadas. Os dados do PCAP capturam quais ações o arquivo estava executando. Por exemplo, ele pode relatar quais servidores o arquivo estava contatando. Para exibir arquivos pCAP, você precisa de um analisador de pacotes, como Wireshark .

PDF de amostra gerado pelo Wildfire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Tradução automática

Wildfire- Obter ação PCAP

. **Wildfire: Obter pCAP** A ação de fluxo obtém as informações de captura de pacote (PCAP) geradas durante a análise de um hash de arquivo especificado no wildfire. O resultado desta ação é anexado a um registro específico, conforme identificado por **Tablename** e. **RecordId** .

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Firewall de rede Palo Alto.
Tablename [cadeia de caracteres]	A tabela afetada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
RecordId [cadeia de caracteres]	O incidente de segurança ou IOC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
CommandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na ação.

Wildfire- Obter ação de relatório em PDF

. **Wildfire: Obter relatório em PDF** A ação de fluxo obtém o relatório gerado durante a análise de um hash de arquivo especificado no Wildfire no formato PDF. O resultado desta ação é anexado a um registro específico, conforme identificado por **Tablename** e. **RecordId** .

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variáveis de entrada

Variável	Descrição
Tablename [cadeia de caracteres]	A tabela afetada.
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Firewall de rede Palo Alto.
RecordId [cadeia de caracteres]	O incidente de segurança ou IOC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
CommandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na ação.

Wildfire- Obter ação de relatório XML

. **Wildfire: Obter relatório XML** A ação de fluxo obtém o relatório gerado durante a análise de um hash de arquivo especificado no Wildfire no formato XML. O resultado desta ação é anexado a um registro específico, conforme identificado por **Tablename** e. **RecordId** .

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
Tablename [cadeia de caracteres]	A tabela afetada.
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Firewall de rede Palo Alto.
RecordId [cadeia de caracteres]	O incidente de segurança ou IOC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
CommandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na ação.

Palo Alto Networks Next-Generation Firewall integração

Uma vez instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP mal-intencionados, URLs e domínios usando recursos de Lista dinâmica externa (EDL) com o. ServiceNow Resposta a incidentes de segurança(SIR) produtos. O analista de incidentes de segurança cria entradas para um EDL a partir de observáveis determinados como mal-intencionados em ServiceNow SIR incidentes de segurança.

Um EDL é um arquivo de texto hospedado em um servidor web externo. Para esta integração, este servidor web é seu ServiceNow AI Platform instância, que permite Palo Alto Networks Next-Generation Firewall Para importar objetos incluídos na lista, endereços IP, URLs e domínios e impor a política.

Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política. À medida que as entradas de EDL são modificadas, o firewall importa dinamicamente a lista no intervalo configurado e impõe a política sem uma mudança de configuração ou confirmação no firewall. Para esta integração, ServiceNow AI Platform Criou uma tabela que contém entradas de EDL que são recuperadas por autorizadas Palo Alto Networks Next-Generation Firewall nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

- Flexibilidade para criar vários EDLs que se aplicam a diferentes políticas de negação ou permissão de firewall.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e permitir sites listados).
- Marcação de ServiceNow AI Platform Incidentes de segurança com entradas EDL por tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração do EDL para manter o tamanho da lista do EDL expirando ou removendo entradas mais antigas automaticamente.
- Pesquisar, excluir ou migrar entradas de EDL entre listas de EDL.
- Vincular entradas de EDL a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A integração requer que os plug-ins (com.snc.security_incident) e (com.snc.secops.orchestration) do Resposta a incidentes de segurança os produtos estão ativados.

Esta integração oferece suporte somente a Palo Alto Networks(PAN-OS 8.x). Versões anteriores não são compatíveis.

Esta integração é compatível com as versões Kingston, Londres, Madrid e Nova York do ServiceNow AI Platform®.

Nota: Os tópicos a seguir são numerados. Para uma instalação, configuração e verificação suaves dos resultados esperados, siga os tópicos na ordem em que são apresentados.

Crie um perfil de certificado para Palo Alto Networks Next-Generation Firewall

A integração requer um perfil de certificado para validar e autenticar a conexão segura entre o. ServiceNow AI Platform® e Palo Alto Networks Next-Generation Firewall servidor.

Função necessária: Palo Alto Networks Next-Generation Firewall Administrador.

. Palo Alto Networks Next-Generation Firewall autentica em um ServiceNow AI Platform® Recupera entradas de EDL da tabela do banco de dados e incorpora as entradas nas regras de política de firewall correspondentes. Esta recuperação requer a função de conta de usuário da API no ServiceNow AI Platform®, que é usada pelo administrador do firewall PAN para acessar o. ServiceNow AI Platform® API.

Siga as etapas abaixo sobre como baixar DigiCertificates e configurar o perfil de certificado.

1. Baixe o certificado DigiCert ou Entrust CA Gateway com base no caso de uso. Para obter mais informações, consulte KB1702083 artigo no Now Support Base de conhecimento.
2. Configure o perfil de certificado. Para obter mais informações, consulte Documentação da Palo Alto Networks .

Tópicos relacionados

"Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10,0

Configurar e instalar Palo Alto Networks Next-Generation Firewall

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação tranquila.

Antes de Iniciar

Função necessária: (administrador)

Configuração de tarefa	Descrição
Verifique se você tem o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções atribuídas.	As seguintes funções são necessárias: • O Administrador do sistema (admin) instala o app e atribui a função de Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e cria, ativa e remove EDLs. Esta função também atribui a função sn_si.analyst.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	• O (administrador) atribui o. ServiceNow AI Platform® Função da conta de API (sn_sec_panfw.api_account_access), que é usada exclusivamente para inserir credenciais necessárias para autenticação em Palo Alto Networks Portanto, os firewalls podem recuperar EDLs do ServiceNow AI Platform®. • (sn_si.analyst), ou analista do Centro de operações de segurança (SOC), cria entradas de EDL e trabalha com incidentes de segurança.
Verifique se você está usando Palo Alto Networks Next-Generation Firewall Versão-OS 9.x e 10.x.	Esta integração oferece suporte somente a Palo Alto Networks Next-Generation Firewall SO 9,0 e posterior.
Configure todos os perfis EDL, regras de política de segurança e perfis de certificado em Palo Alto Networks conforme recomendado em Palo Alto Networks documentação.	Consulte Palo Alto Networks documentação geral e requisitos em: Site de documentação da Paloalto Networks .
Verifique se você baixou e configurou o Certificado de autoridade raiz DigiCert.	A integração requer este certificado para validar e autenticar a conexão segura entre o. ServiceNow AI Platform e Palo Alto Networks Next-Generation Firewall servidor. Para obter mais informações sobre como configurar o certificado, consulte "Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10,0 . Para o download, consulte Crie um perfil de certificado para Palo Alto Networks Next-Generation Firewall e. Certificados de autoridade raiz confiável da DigiCert .
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Madrid e versões posteriores Para a versão Madrid e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	1. Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.
Se sua organização tiver ServiceNow AI Platform® gestão de mudanças e processos de aprovação para exclusão de e-mail, verifique se a capacidade de envio/recebimento de e-mail está habilitada.	Para verificar se a capacidade de envio/recebimento de e-mail está habilitada em seu ServiceNow AI Platform® instância, navegue até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**. Em Configuração de e-mail de saída, verifique **Envio de e-mail** e. **Recebimento de e-mail** selecionados.

Procedimento

Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.

Crie a função de conta de API para Palo Alto Networks Next-Generation Firewall

Uma função de conta de API é necessária em seu ServiceNow AI Platform® instância desta integração. O nome de usuário e a senha associados a esta conta são criados no ServiceNow AI Platform® e inseridos em Palo Alto Networks. Palo Alto Networks Next-Generation Firewall autentica com ServiceNow AI Platform® Ao recuperar entradas de EDL.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

. ServiceNow AI Platform® o administrador cria uma função de conta de API (sn_sec_panfw.api_account_access). Esta conta é usada exclusivamente para inserir credenciais necessárias para autenticação em Palo Alto Networks Portanto, os firewalls podem recuperar EDLs do ServiceNow AI Platform®. Esta conta é uma conta de usuário de API separada e exclusiva no ServiceNow AI Platform® e atribuídos a Palo Alto Networks Next-Generation Firewall administrador.

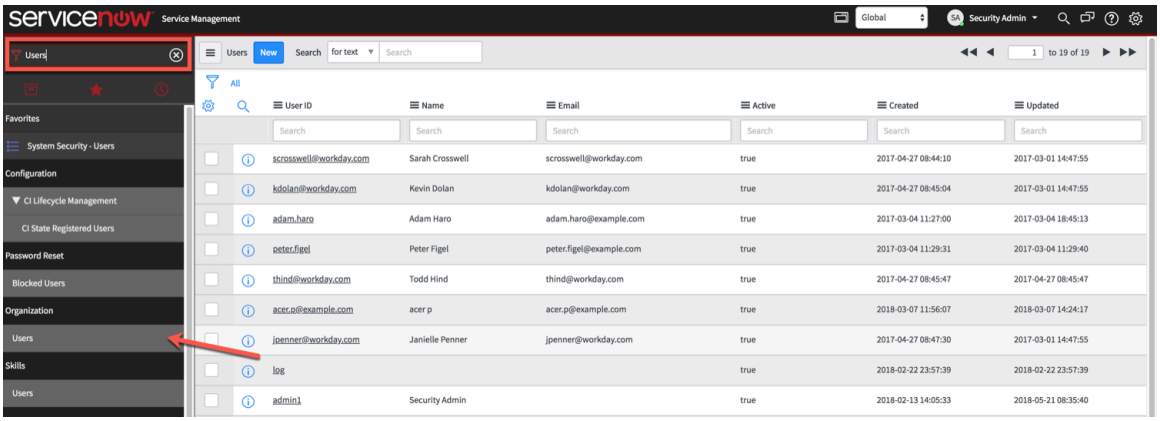
Procedimento

1. Navegar até **Tudo** > **Organização** > **Usuários**.

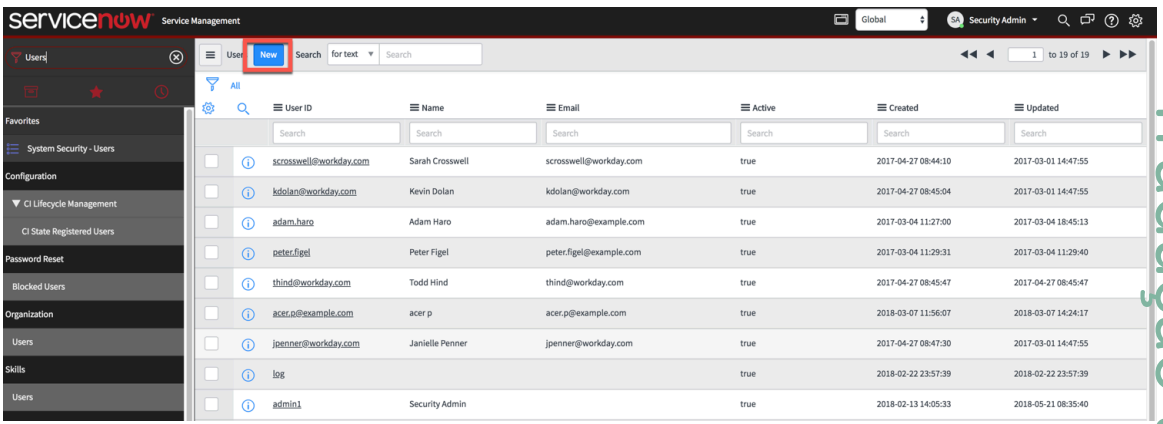
2. Clique em **Usuários** módulo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na lista Usuários exibida, clique em **Novo** .



Um novo formulário de usuário é exibido.

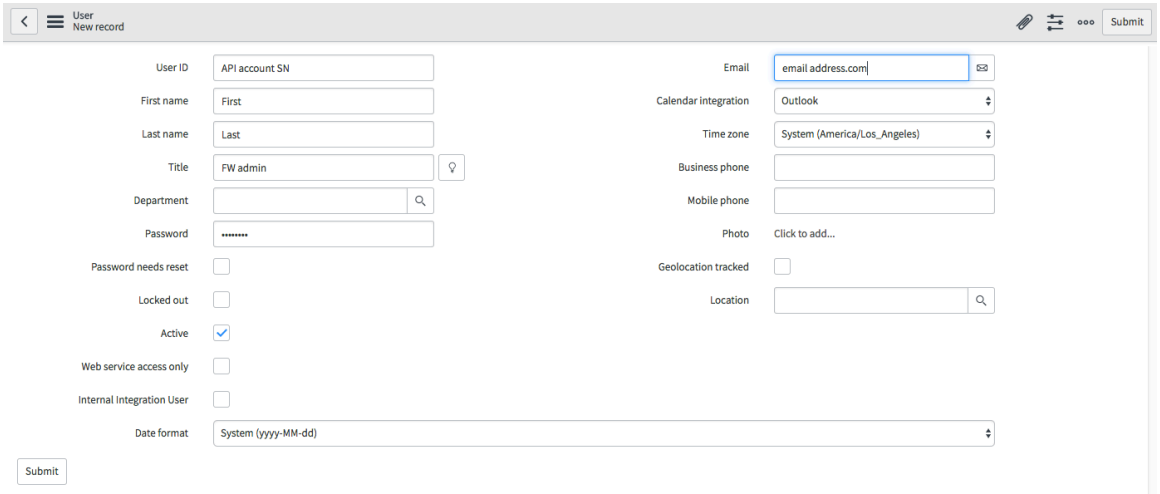
4. Preencha o formulário.

Nota: Os valores do título do ID do usuário e do endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

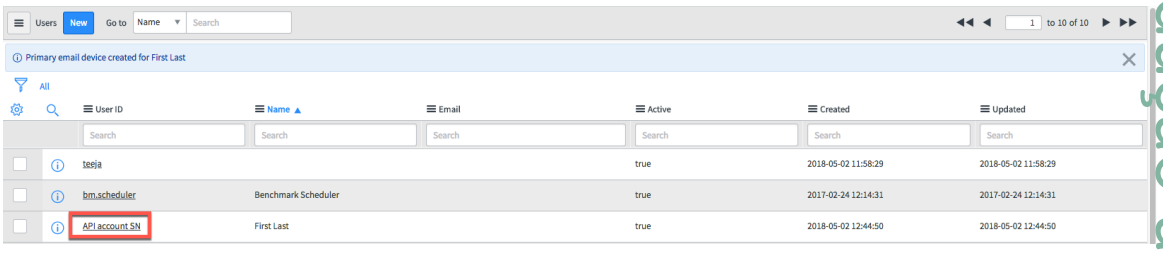
Campo	Descrição
ID do usuário	ID de usuário exclusivo para a função em seu ServiceNow AI Platform® instância. Este ID de usuário é inserido em **Nome de usuário** . **Autenticação de cliente** Da caixa de diálogo Listas dinâmicas externas no Palo Alto Networks site. Um exemplo é `SN da conta da API` .
Nome	Pessoa que você está atribuindo.
Sobrenome	Pessoa que você está atribuindo.
Título	Cargo, por exemplo, `Administrador de FW` .
Senha	Senha exclusiva criada para esta função. Esta senha é inserida em **Senha** . **Autenticação de cliente** Da caixa de diálogo Listas dinâmicas externas no Palo Alto Networks site.
E-mail	Endereço de e-mail exclusivo.

Tradução automática

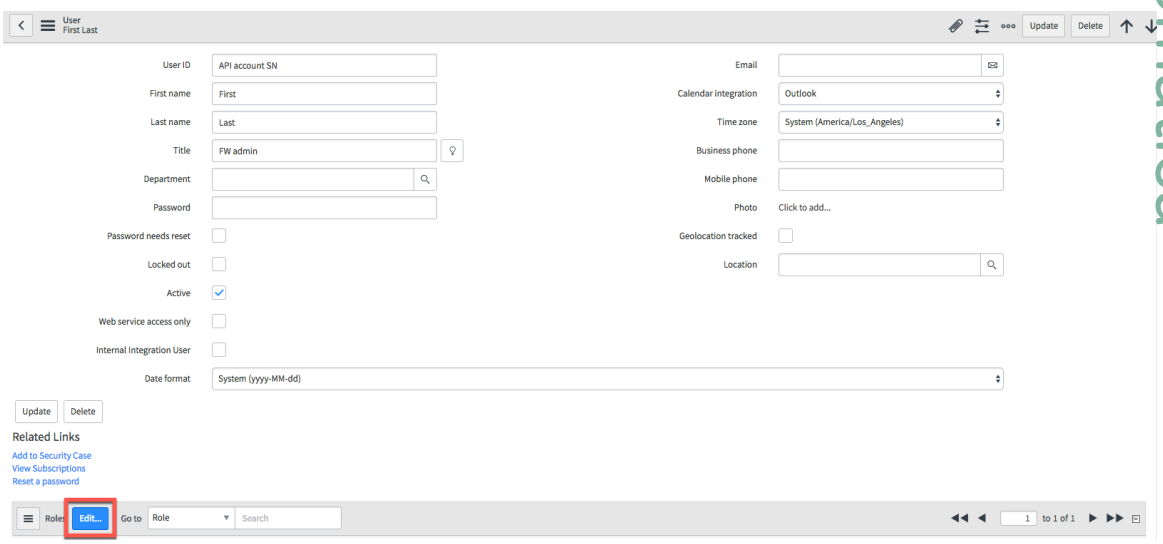
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Uma vez enviado, você pode atribuir a função.
6. Na lista Usuários em **ID do usuário** , clique no nome do ID de usuário inserido, SN da conta da API , por exemplo.



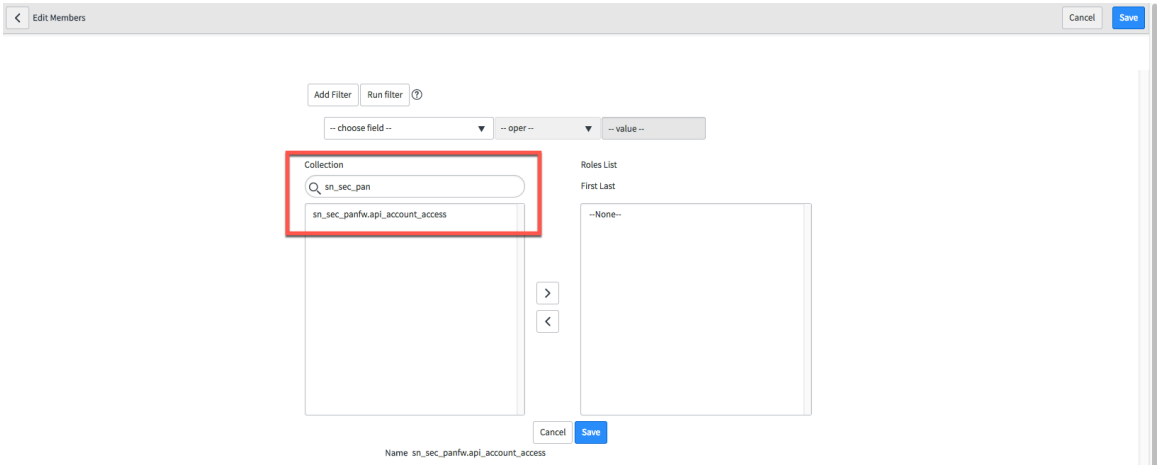
7. No registro Abrir na seção Funções, clique em **Editar** .



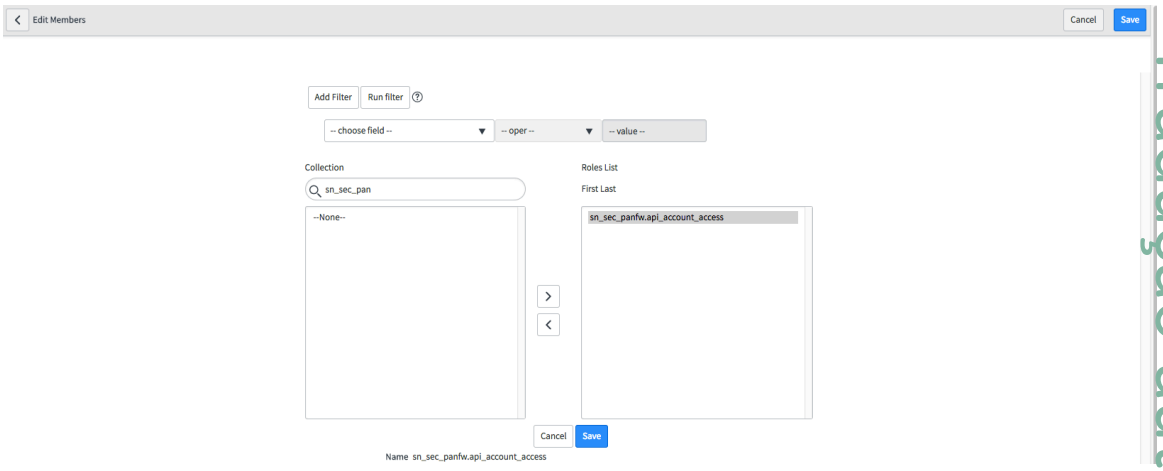
8. Em **Editar membros** formulário exibido, insira `sn_sec_panfw.api_account_access` em **Coleção** campo.
   Abaixo de **Coleção** , a função é exibida na coluna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



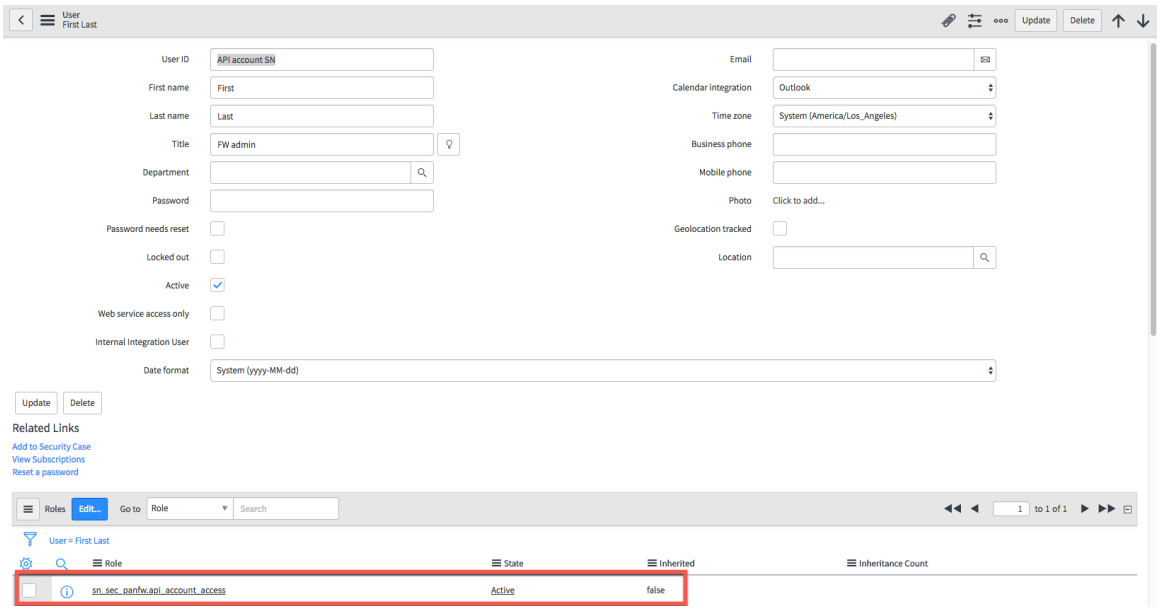
9. Em **Coleção** , selecione e mover `sn_sec_panfw.api_account_access` para **Lista de funções** .



10. Clique em **Salvar**.
11. Navegue até **Usuários** e em **Usuário** Na lista, clique no nome do ID que você criou para a função (SN da conta da API).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída. . **Estado** está ativo e a função não é herdada.

Listas dinâmicas externas compatíveis para Palo Alto Networks Next-Generation Firewall

. ServiceNow Palo Alto Networks Next-Generation Firewall A integração oferece suporte a Listas dinâmicas externas (EDLs) que aceitam observáveis de IP, URL e domínio.

EDLs e observáveis compatíveis

Um *Lista dinâmica externa* é um arquivo de texto hospedado em um externo *servidor web* , que para esta integração é ServiceNow AI Platform instância. . Palo Alto Networks Next-Generation Firewall Pode importar objetos (endereços IP, URLs, domínios) incluídos na lista e impor a política. Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política.

Esta integração oferece suporte a três tipos de EDLs:

- IP (isso inclui um único endereço IP, bem como blocos CIDR (intervalos) de endereços).
- URL
- Domínio

A tabela a seguir lista descrições dos observáveis compatíveis com esta integração e formatos de exemplo para cada tipo.

Observáveis compatíveis e formatos de exemplo

Observável	Formatos de exemplo	Descrição
Endereço IP	• 95.153.103.54 (IPv4) • (IPV6): 2001:00B8:130F:FE03:0000:0960:0830F:150B	Representa um endereço de interface único e distinto. A integração oferece suporte aos formatos IPv4, IPv6 e CIDR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observáveis compatíveis e formatos de exemplo

Observável	Formatos de exemplo	Descrição
		O suporte a observáveis de endereço IP inclui intervalos CIDR (Classless Inter-Domain Routing), por exemplo, 95.153.100.0/22. Observação: Uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a um EDL que você já bloqueou como parte de um intervalo de CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Curingas são compatíveis. . ServiceNow AI Platform Reformata as entradas de URL para conformidade com Palo Alto Networks Requisitos de formato EDL.
Domínio	• www.example.com • example.com • mail.example.com	Curingas não são compatíveis.

Para obter mais informações sobre diretrizes de formatação e EDLs, consulte "Diretrizes de formatação para uma lista dinâmica externa" no Guia do administrador do PAN-OS 10,0 em Palo Alto Networks site.

Crie um EDL para o firewall de última geração da Palo Alto Networks

Crie uma Lista dinâmica externa (EDL) em seu ServiceNow AI Platform instância. Uma vez aprovado e ativado, você pode criar entradas para EDLs a partir de observáveis determinados como mal-intencionados em ServiceNow AI Platform Resposta a incidentes de segurança(SIR) incidentes e solicitar aprovação para bloqueá-los.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Crie o EDL em seu ServiceNow AI Platform Instância para que o firewall possa importar objetos (endereços IP, URLs, domínios) incluídos na lista e impor a política. Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política.

As figuras na seção a seguir são mostradas com **Formulários com guias** Limpo em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

formulários com guias, consulte a seção "Exibir formulários com guias" em Configuração do layout do formulário .

Procedimento

1. Após a conclusão da instalação da aplicação, navegue até **Integrações** > **Configurações de Integração**.
2. Localize Palo Alto Networks Next-Generation Firewall lado a lado e clique **Configurar** .



3. Clique em **Criar nova Lista de EDL** .



4. No formulário, preencha os campos.

Palo Alto Networks Formulário Lista dinâmica externa do firewall

Campo	Descrição
Nome	Palo Alto Networks Nome da lista dinâmica do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Inclua o tipo de observável (URL, IP, domínio) neste campo para que o analista de segurança possa reconhecer facilmente a intenção do EDL pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos EDL estão mapeados. Alguns exemplos de nomes de EDL são IP de Malware de Saída ou URL de Phishing de Saída.
Ativo	Esta caixa de seleção é desmarcada por padrão para indicar que o EDL está inativo. Quando inativo, o EDL não pode receber entradas adicionais. Quando a caixa de seleção é marcada, o EDL é ativado e fica disponível para entradas de EDL.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado em um EDL. Quando selecionado, o tipo de marcador e o marcador EDL para os campos Observáveis ficam disponíveis no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido em **Nome** campo com um *EDL* - Prefixo, por exemplo, IP de saída EDL-Malware. Você pode mudar o nome e a cor do marcador. Consulte: (Opcional) Edite o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall. O nome do marcador é exibido no campo Marcador EDL para observáveis depois que o EDL é salvo. Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o Tipo de marcador e o marcador EDL para os campos Observáveis não estão disponíveis no formulário.
Tipo de observável	Selecione um tipo de observável que este EDL aceita na lista de seleção: IP (incluindo CIDR), URL ou domínio.
Tipo de marcador	Marcadores que estão disponíveis na lista de seleção. Uma lista de bloqueios é uma lista de observáveis que você deseja Palo Alto Networks Next-Generation Firewall para bloquear.

Tradução automática

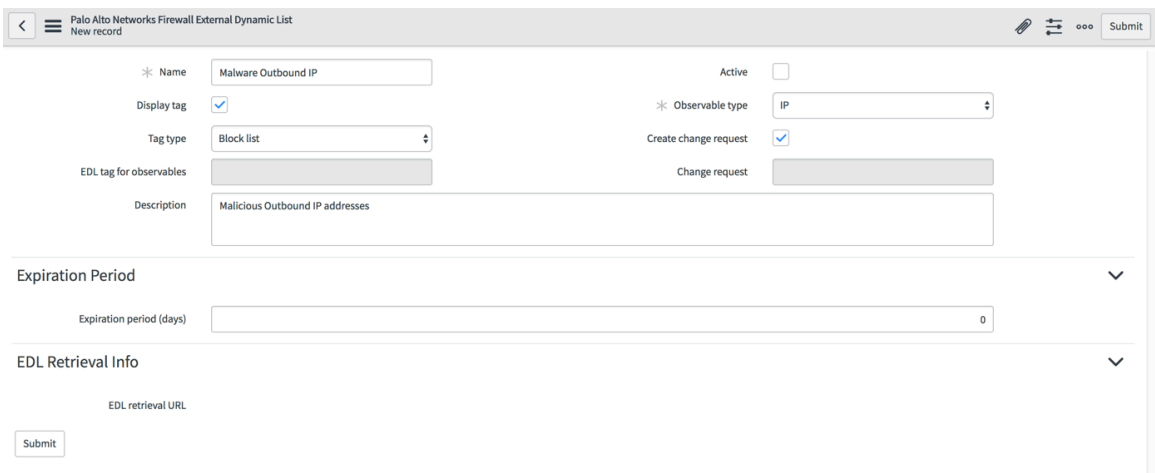
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Uma lista de permissões é uma lista de observáveis que você deseja Palo Alto Networks Next-Generation Firewall para permitir. Por padrão, a cor do marcador da lista de bloqueios é preta e a cor do marcador da lista de permissões é cinza. Você pode mudar a cor. Consulte: (Opcional) Edite o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em seu ServiceNow AI Platform Que estão anexadas ao registro EDL. A solicitação de mudança é usada para configurar o URL de recuperação da lista EDL no Palo Alto Networks Next-Generation Firewall servidor. Esta opção é recomendada se o administrador do firewall também estiver usando o. ServiceNow AI Platform para mudanças de regra ou política de firewall. Se você criar uma solicitação, depois que ela for fechada, a lista EDL será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente o EDL depois de receber um aviso por e-mail do administrador do firewall em que a configuração foi ativada Palo Alto Networks concluído. Quando a caixa de seleção Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Marcador EDL de observáveis	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que o EDL é salvo com um valor padrão do campo Nome. Para obter mais informações sobre como alterar o nome e a cor do marcador padrão, consulte (Opcional) Edite o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall
Solicitação de mudança	Quando a caixa de seleção Criar solicitação de mudança é marcada, o número da solicitação de mudança é exibido no ServiceNow AI Platform Uma vez que o EDL é salvo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

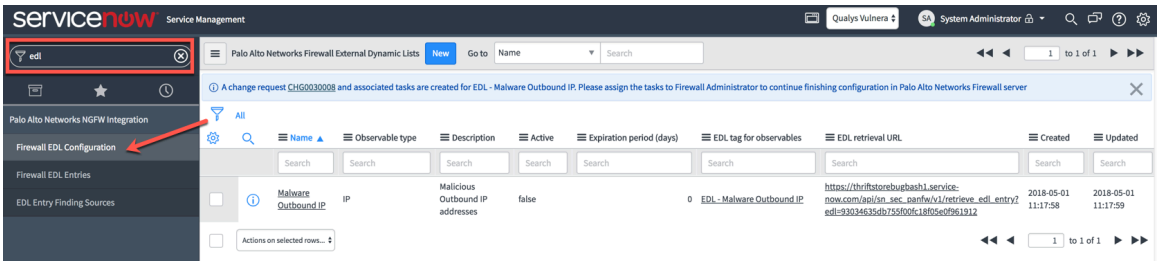
Campo	Descrição
	Quando a caixa de seleção Criar solicitação de mudança está desmarcada, este campo não é exibido.
Descrição	Lista dinâmica de firewall da Palo Alto Networks. Geralmente, o nome contém os tipos de locais e observáveis que você esperaria estar neste EDL, e você pode usar este campo para obter mais detalhes.
Período de expiração (dias)	Período de expiração do EDL. 0 (o padrão) indica que a entrada EDL nunca expira. Se você mudar este valor, esta entrada ficará ativa para o número de dias que você inserir. Você pode inserir um valor mínimo de 1 e não há valor máximo. Por exemplo, se você inserir `30` Às 2:01 do dia 1 de maio, o EDL expirará às 2:01 do dia 31 de maio. Em seguida, todas as entradas neste EDL herdam este valor por padrão, a menos que você substitua o valor na base de entrada individual.



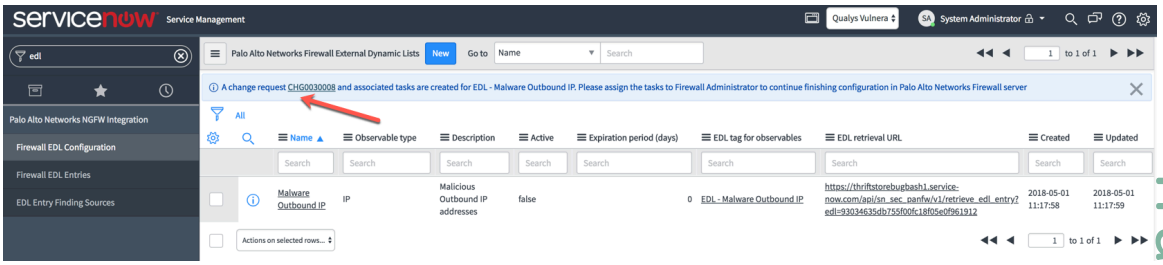
5. Clique em **Enviar**.
6. Se a lista Listas dinâmicas externas do Firewall da Palo Alto Networks não for exibida, navegue até **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall** e clique em **Configuração de EDL do firewall** .

Tradução automática

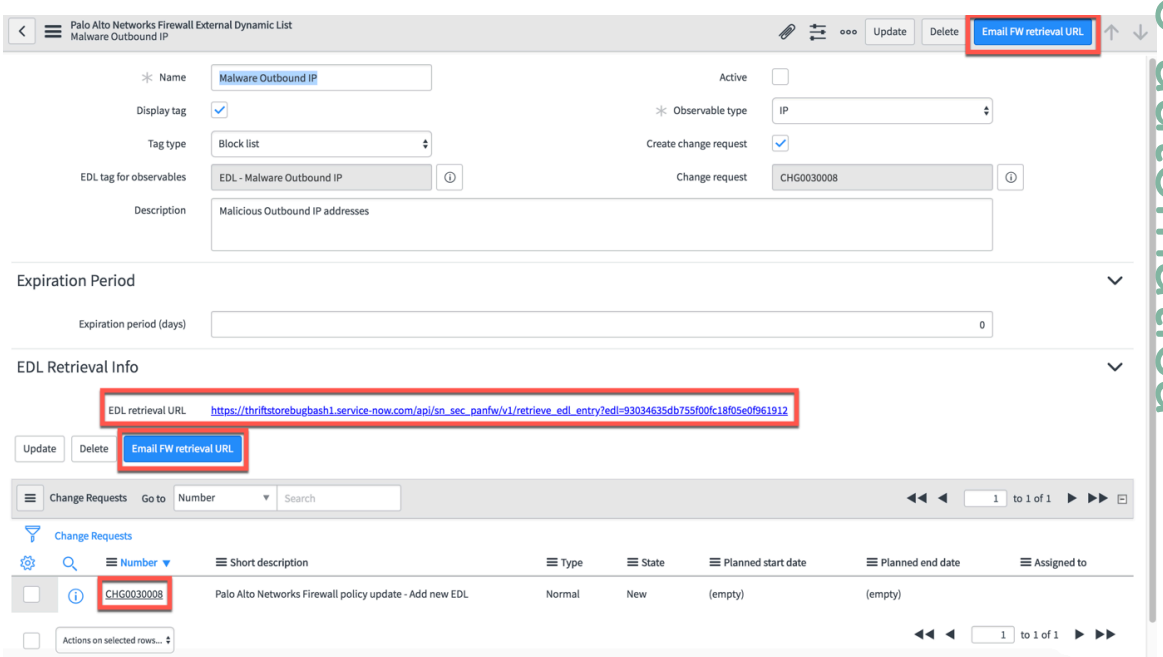
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A nova EDL é exibida. O status do EDL ainda está inativo (`false`), o que significa que o EDL não está disponível para aceitar entradas. Se **Criar solicitação de mudança** foi configurado, uma mensagem é exibida indicando que uma solicitação de mudança e tarefas foram criadas em seu ServiceNow AI Platform instância.



7. Em **Nome** , clique em um item para abrir o registro.
   O registro EDL é exibido. Este exemplo mostra um EDL de IP de saída de malware. Os seguintes campos, opções e links são exibidos no novo registro após o envio e descritos na tabela a seguir.



URL de recuperação e links de solicitação de mudança no registro EDL

Opção	Descrição
URL de recuperação do firmware do e-mail	E-mail com um aviso de que o link EDL está disponível para configuração para Palo Alto Networks administrador de firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
URL de recuperação do EDL	Este URL é colocado em **Origem** Campo na caixa de diálogo Autenticação de listas dinâmicas externas em **Criar lista** no Palo Alto Networks site. O URL vincula o. Palo Alto Networks o administrador do firewall usa para configuração no Palo Alto Networks o firewall é gerado e exibido automaticamente. **Nota:** Se você tiver as Configurações do sistema definidas como **Formulários com guias** , este link é exibido no **Informações de recuperação de EDL** na parte inferior do registro.
ServiceNow AI Platform solicitação de mudança	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Excluir	Exclua o registro.

8. Crie e adicione mais EDLs conforme necessário.
   Os EDLs são exibidos no Palo Alto Networks Lista Listas dinâmicas externas.

O que Fazer Depois

Ative um EDL manualmente ou com um ServiceNow AI Platform solicitação de mudança.

Ativar um EDL

Depois que a Lista dinâmica externa (EDL) tiver sido criada em seu ServiceNow AI Platform® E o URL está disponível, o. Palo Alto Networks O administrador do firewall configura o EDL no Palo Alto Networks Next-Generation Firewall. O URL de recuperação é usado pelo Palo Alto Networks Administrador do firewall para configurar o EDL no Palo Alto Networks Next-Generation Firewall servidor. Antes de aceitar entradas de EDL, a EDL deve ser configurada em Palo Alto Networks e ativados em ServiceNow AI Platform®.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

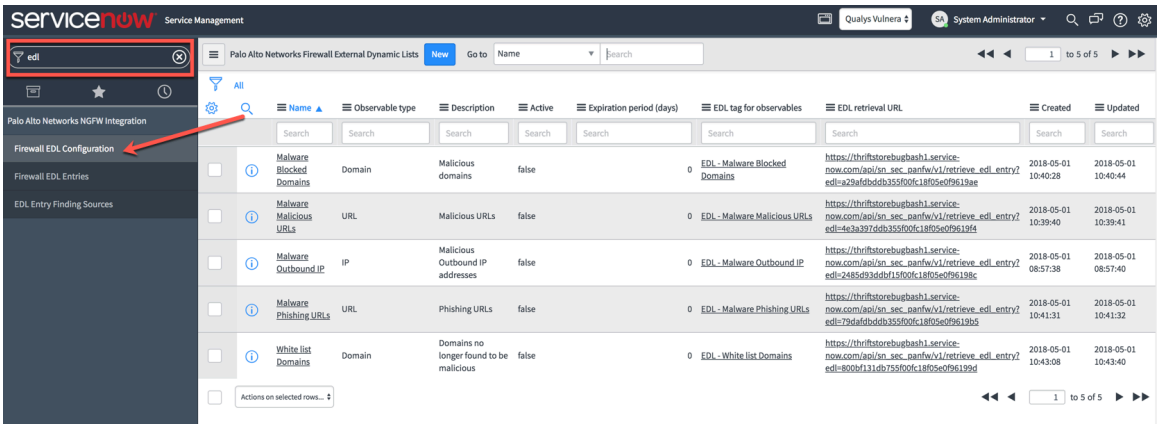
Depois que o EDL é configurado, como administrador de incidentes de segurança, você pode ativar o EDL manualmente ou o EDL é ativado automaticamente após a conclusão de um ServiceNow AI Platform® Solicitação de mudança. O EDL deve ser aprovado e movido do estado inativo para o estado ativo antes de aceitar entradas de EDL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

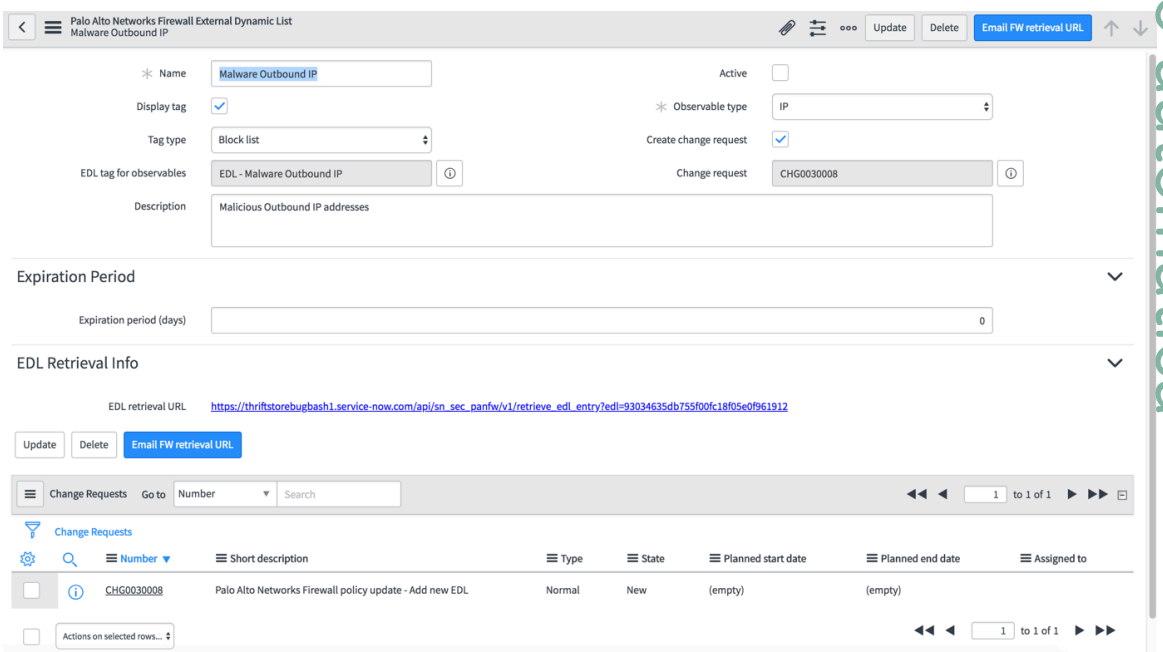
Procedimento

1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall** e selecione **Configuração de EDL do firewall** módulo.



2. Na lista Listas dinâmicas de firewall da Palo Alto Networks exibida, selecione seu novo EDL na coluna Nome.

3. No registro exibido, observe **URL de recuperação de FW de e-mail** , o link de URL de recuperação de EDL ativo e, se configurado, o. ServiceNow AI Platform® Solicitação de mudança na seção Solicitações de mudança.
   Certifique-se de que **Ativo** a caixa de seleção está desmarcada.

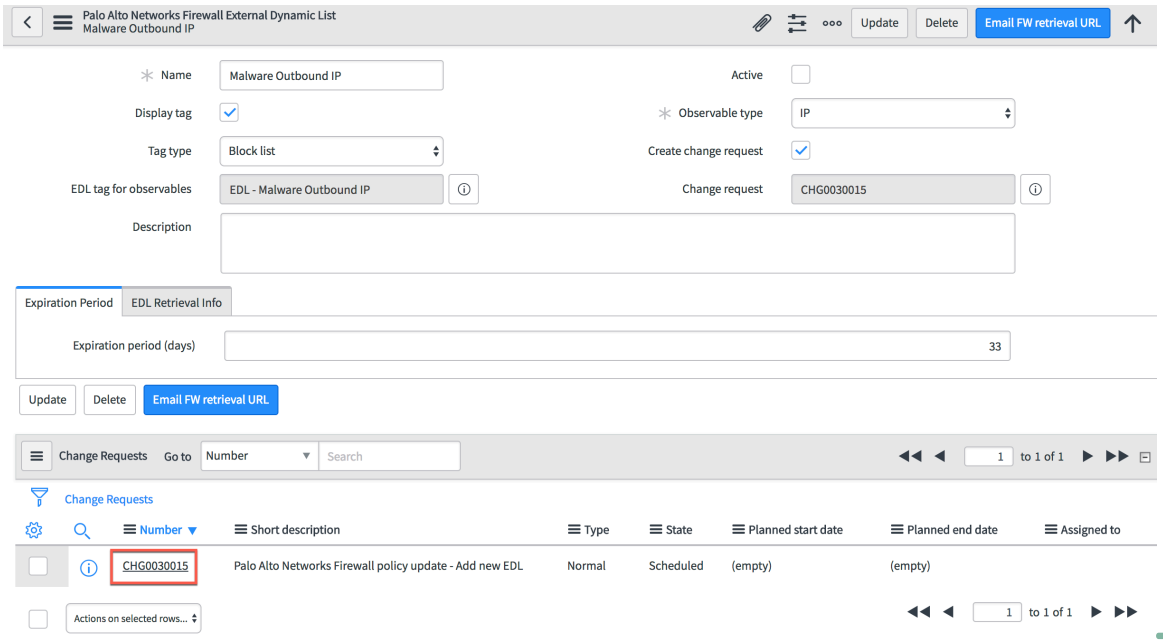


Nota: Com **Formulários com guias** Limpo nas configurações do sistema, o URL de recuperação do EDL aparece em **Informações de recuperação de EDL** conforme mostrado na figura anterior.

A figura a seguir mostra o. **Informações de recuperação de EDL** exibido como uma guia com **Formulários com guias** selecionado nas configurações do sistema. Clique em **Informações de recuperação de EDL** Para exibir o URL de recuperação. O link para a solicitação de mudança (**CH0030015**) também é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para concluir a configuração e mover o EDL de inativo para ativo, você deve escolher uma das seguintes opções para notificar o administrador do firewall de que o URL de recuperação está disponível.

Opção	Descrição
Clique em URL de recuperação de FW de e-mail .	URL de recuperação de EDL por e-mail diretamente para o administrador do firewall. Esta opção permite que o administrador do firewall conclua a configuração no Palo Alto Networks plataforma. Escolha esta opção se o administrador do firewall não estiver usando o. ServiceNow AI Platform® . **Nota:** O administrador de incidentes de segurança ativa manualmente o EDL no ServiceNow AI Platform®após receber o aviso de que Palo Alto Networks Next-Generation Firewall a configuração foi concluída. Consulte: Ative um EDL manualmente.
Conclua ServiceNow AI Platform® solicitação de mudança e atribua as tarefas de configuração ao administrador do firewall.	Esta opção estará disponível somente se o administrador do firewall for Palo Alto Networks também está usando ServiceNow AI Platform® e ServiceNow AI Platform® a gestão de mudanças e os processos de aprovação estão configurados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Usuários com a função sn_si.admin podem aprovar o. ServiceNow AI Platform® solicitação de mudança. Quando as tarefas de configuração são concluídas e a solicitação de mudança é fechada, o EDL é ativado automaticamente. Consulte: Ative um EDL para Palo Alto Networks Next-Generation Firewall com uma solicitação de mudança.

Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e confirmar que o EDL foi configurado em Palo Alto Networks, Como administrador de incidentes de segurança, sua próxima etapa é ativar o EDL. Você ativa o EDL manualmente ou, se configurado, usa o. ServiceNow AI Platform Formulário de solicitação de mudança para ativar o EDL.

Tópicos relacionados

Configurar um EDL

Ative um EDL manualmente

Se o administrador do firewall da Palo Alto Networks não estiver usando o. ServiceNow AI Platform e você será notificado diretamente de que Palo Alto Networks Next-Generation Firewall Estiver configurado, você pode ativar a Lista dinâmica externa (EDL) manualmente.

Antes de Iniciar

Em Palo Alto Networks Atribua um objeto, uma política e o URL de origem do EDL ao EDL que você criou. Para obter mais informações sobre como configurar o EDL para Palo Alto Networks Next-Generation Firewall em Palo Alto Networks, consulte Configurar um EDL.

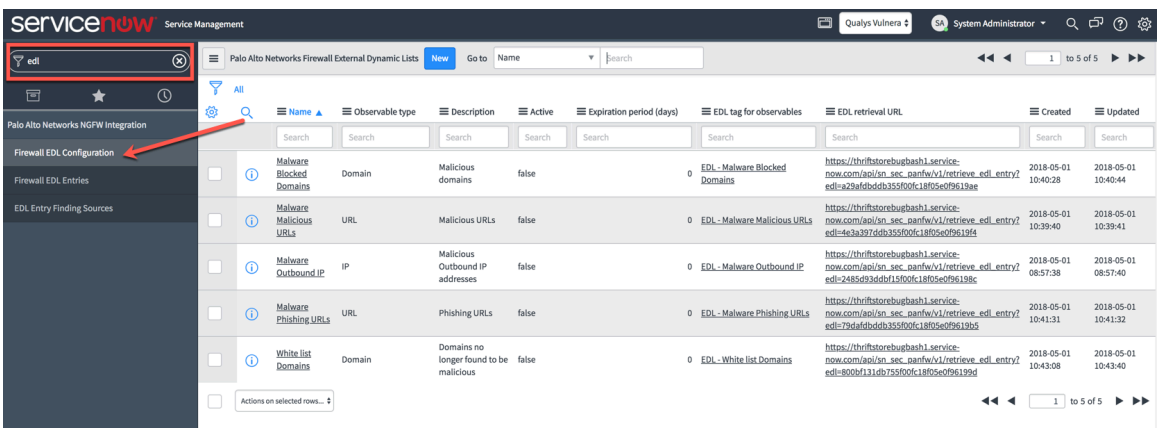
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

. ServiceNow AI Platform administrador de incidentes de segurança, você será notificado pelo Palo Alto Networks Administrador do firewall quando a configuração do EDL é concluída no Palo Alto Networks Next-Generation Firewall.

Procedimento

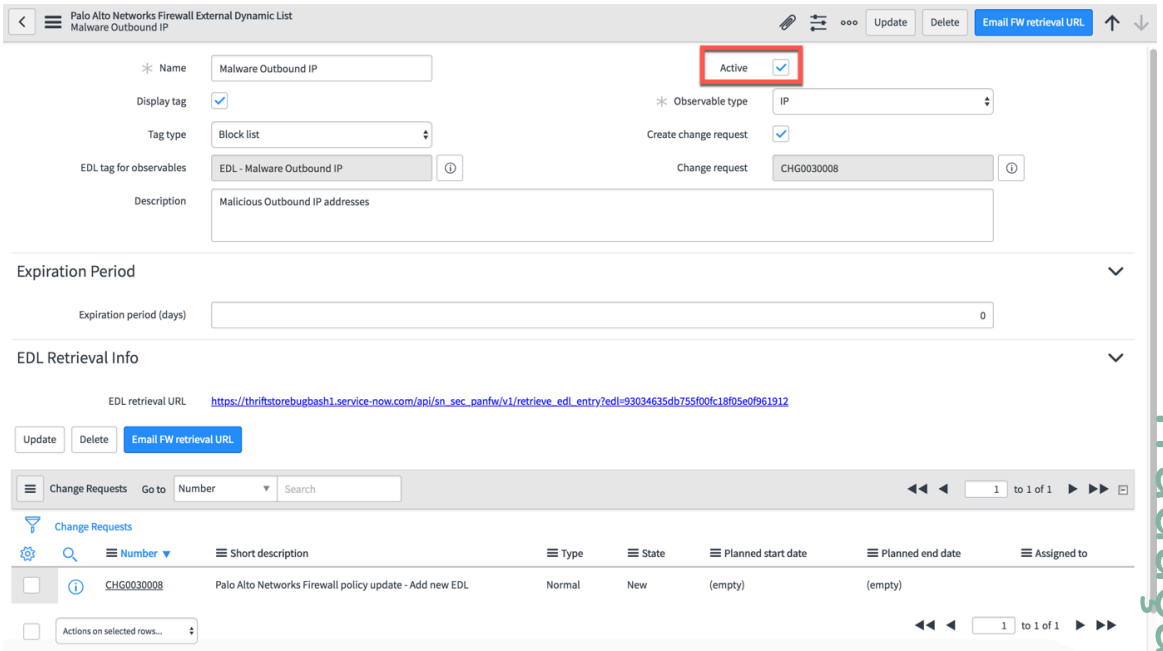
1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall**.



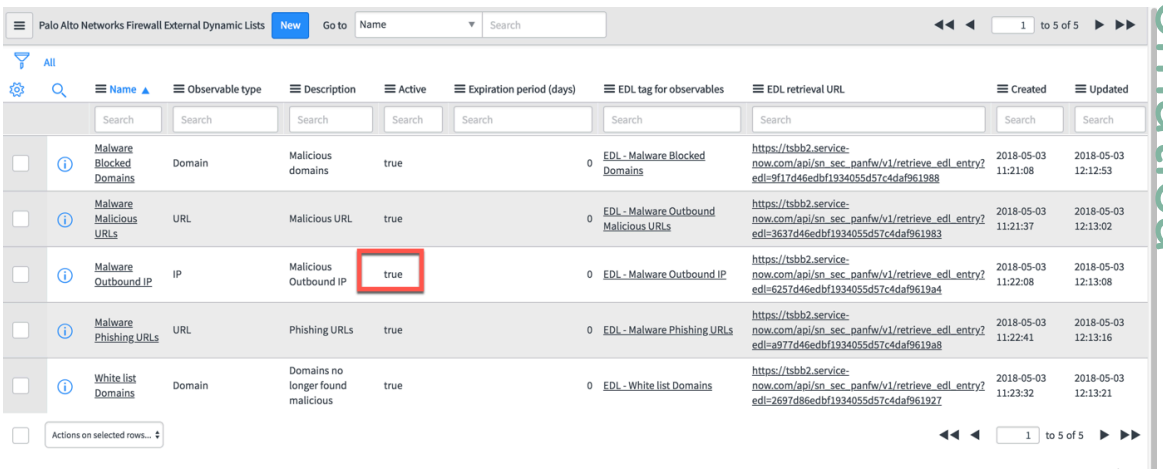
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Selecione **Configuração de EDL do firewall** módulo.
3. Na lista Listas dinâmicas externas do Firewall da Palo Alto Networks, clique em um item em **Nome** coluna para abri-la.
4. No registro que é aberto, selecione **Ativo** caixa de seleção.



5. Clique em **Atualizar**.
   Em **Ativo** Lista Listas dinâmicas externas do Firewall da Palo Alto Networks, verdadeiro É exibido para o estado do EDL.



Resultado

O EDL está ativado e pronto para receber entradas de EDL

O que Fazer Depois

Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Configurar um EDL

. Palo Alto Networks O administrador do firewall configura um EDL para Palo Alto Networks Next-Generation Firewall Uma vez notificado, o URL de recuperação fica disponível no ServiceNow AI

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Platform. EDL pode aceitar entradas de EDL, ele deve ser configurado em Palo Alto Networks e ativados no ServiceNow AI Platform®.

Antes de Iniciar

Função necessária: Palo Alto Networks administrador de firewall

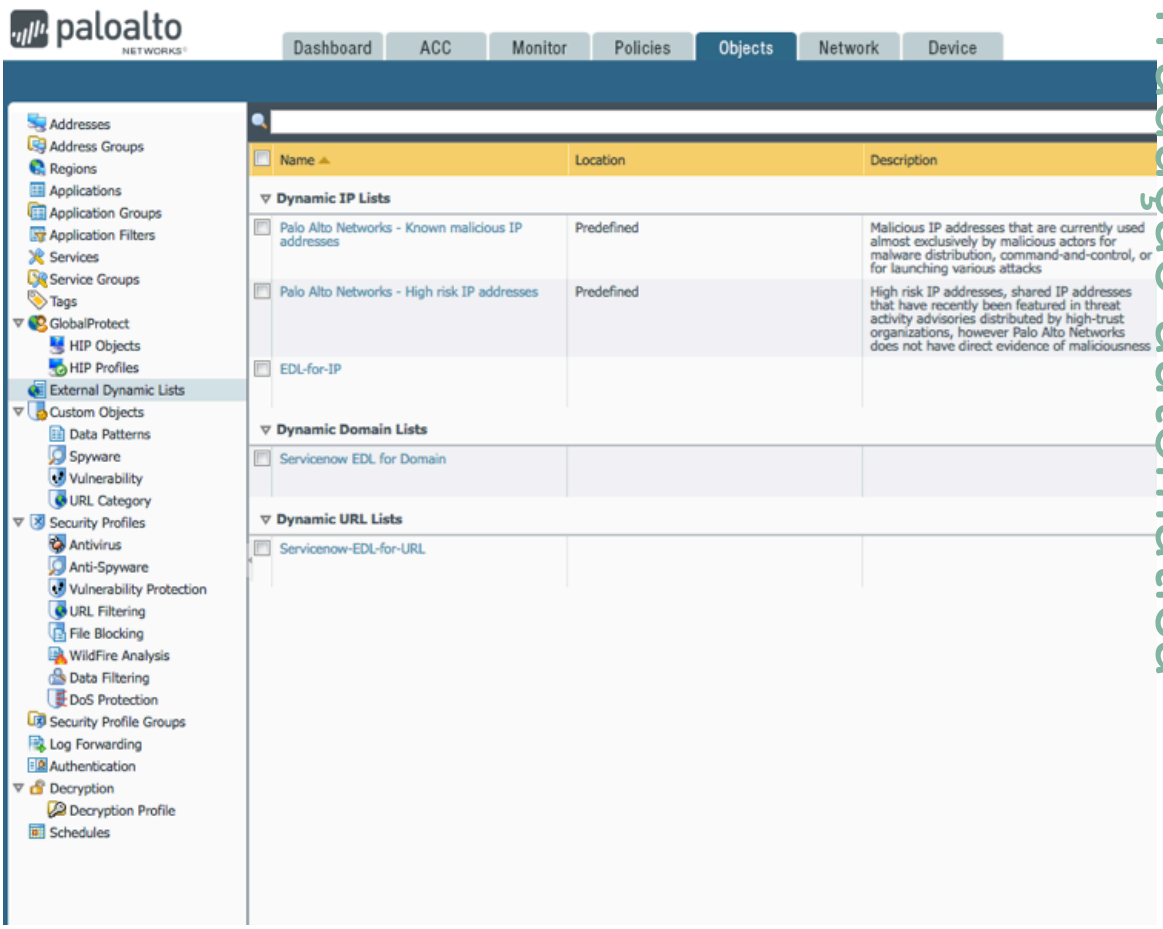
Por Que e Quando Desempenhar Esta Tarefa

. Palo Alto Networks Next-Generation Firewall O administrador cria um objeto EDL e atribui a URL e a política de origem (recuperação) ao EDL. Essas tarefas são executadas em Palo Alto Networks Antes que o EDL seja ativado no ServiceNow AI Platform.

As imagens na seção a seguir são usadas com permissão e são PRIVILEGIADAS e PROPRIETÁRIAS.

Procedimento

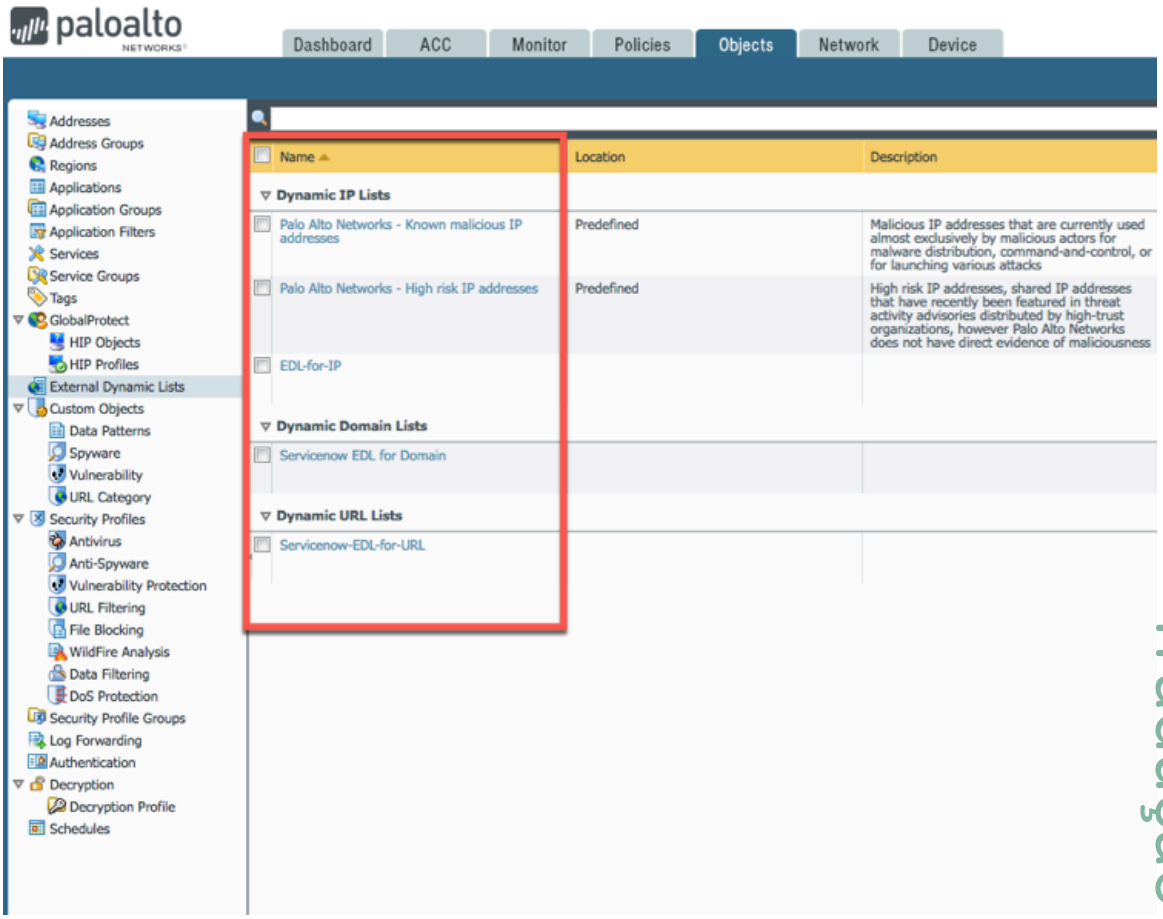
1. Se você não configurou o EDL para o firewall, navegue até **Listas dinâmicas externas** > **Objetos** in Palo Alto Networks.



2. Em **Nome** , selecione ServiceNow EDL que você deseja configurar na lista, por exemplo, **ServiceNow EDL para URL** .

Tradução automática

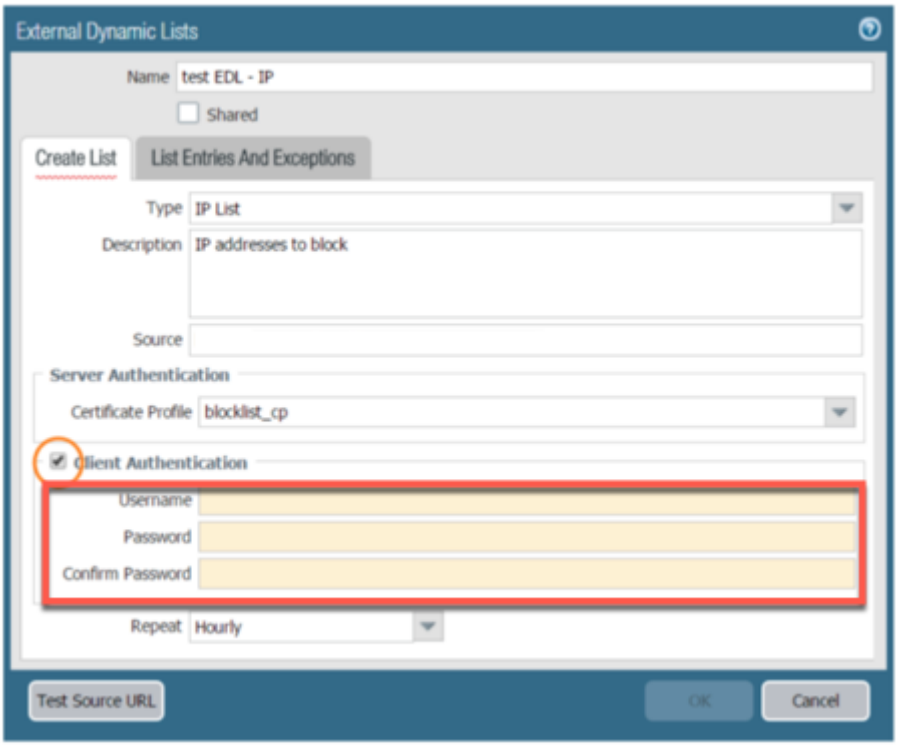
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



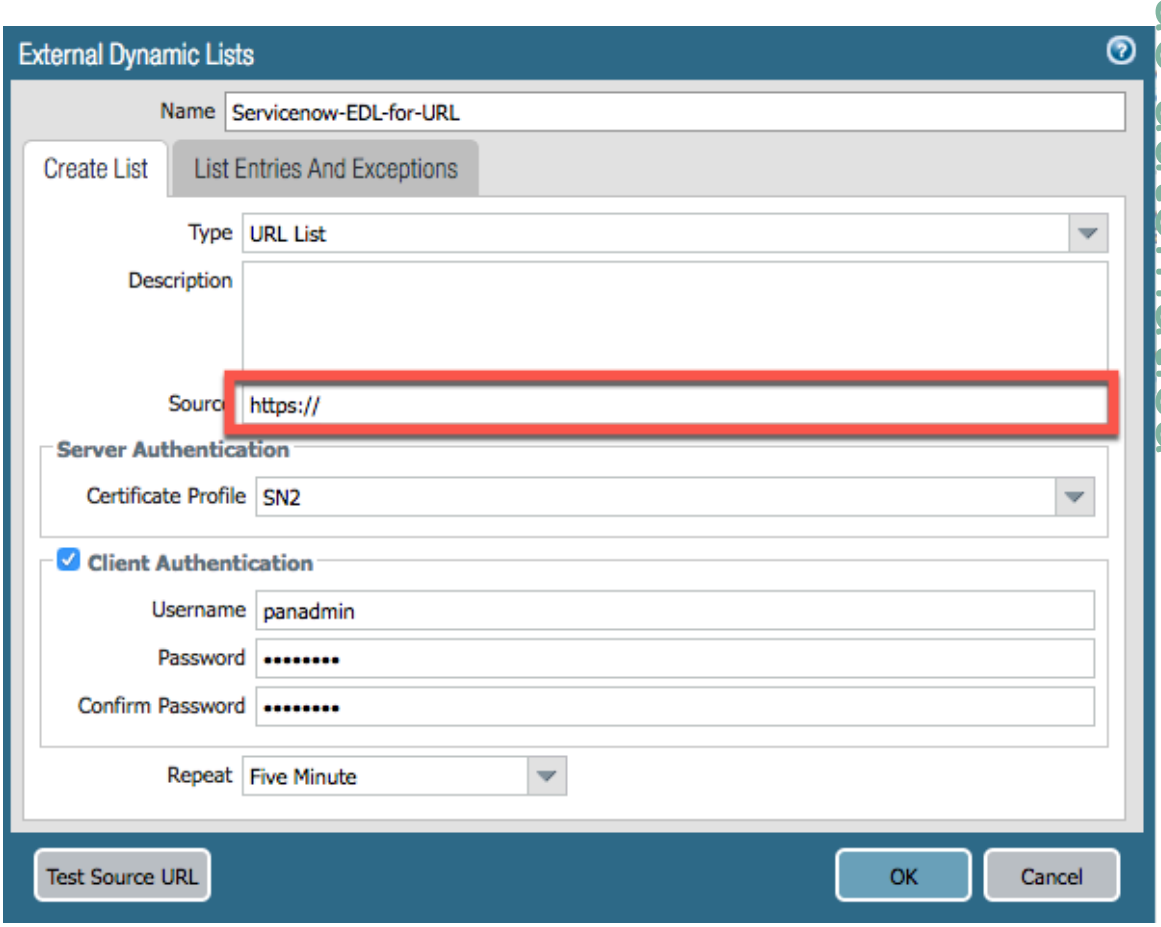
3. Na caixa de diálogo Listas dinâmicas externas, insira o Nome de usuário e a Senha para autenticar com ServiceNow AI Platform®.
Essas credenciais são o nome de usuário e a senha que você criou para a função de conta da API (sn_sec_panfw.api_account_access) em seu ServiceNow instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No campo Origem, insira o URL que foi gerado na lista EDL em seu ServiceNow instância.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione um Perfil de certificado na lista de seleção, SN2 , por exemplo.
6. Clique em OK.

Ative um EDL para Palo Alto Networks Next-Generation Firewall com uma solicitação de mudança

. ServiceNow O formulário Solicitação de mudança é usado para ativar a Lista dinâmica externa (EDL). Esta opção é recomendada se o administrador do firewall também estiver usando o. ServiceNow AI Platform para mudanças de regra ou política de firewall. O EDL é ativado automaticamente e pronto para receber entradas de EDL após o fechamento do ServiceNow AI Platform solicitação de mudança.

Antes de Iniciar

Nota: As figuras na seção a seguir são mostradas com **Formulários com guias** Selecionado em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção Exibir formulários com guias em Configurar o layout de formulário no Site de documentação do produto da ServiceNow .

Função necessária: sn_si.admin para aprovar a solicitação de mudança e as tarefas de mudança

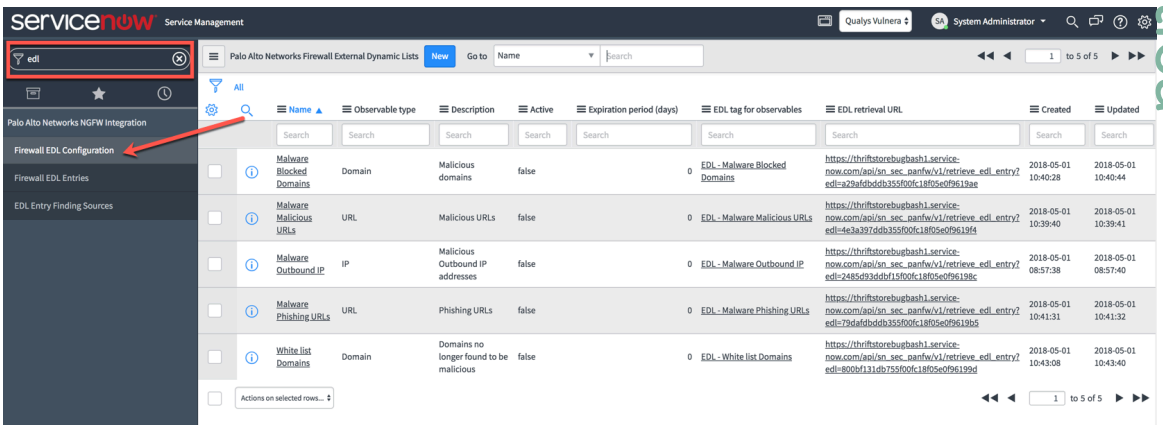
Palo Alto Networks administrador de firewall para concluir tarefas de configuração em Palo Alto Networks

Por Que e Quando Desempenhar Esta Tarefa

Se configurado, monitore seu ServiceNow AI Platform solicite mudança e atribua todas as tarefas necessárias para configurar o. Palo Alto Networks Next-Generation Firewall. Após a conclusão dessas tarefas, feche o. ServiceNow AI Platform Solicitação de mudança para ativar o EDL automaticamente.

Procedimento

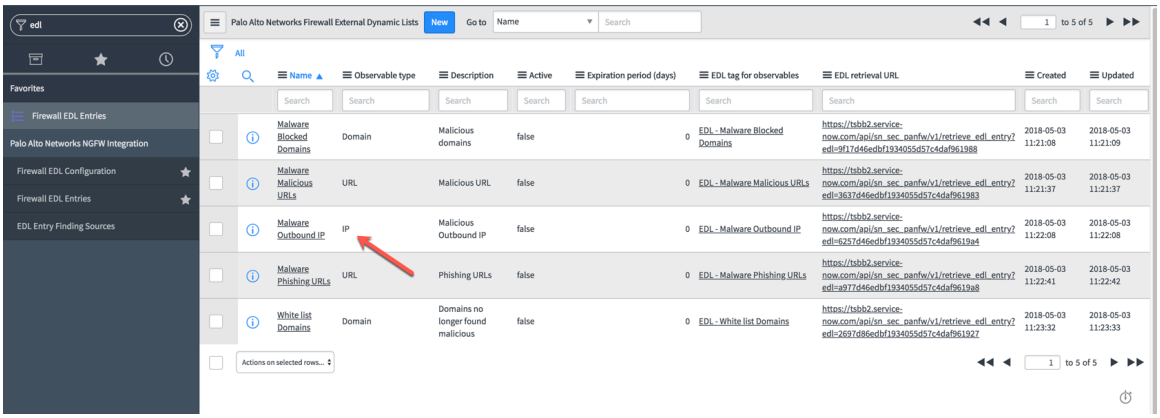
1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall**.



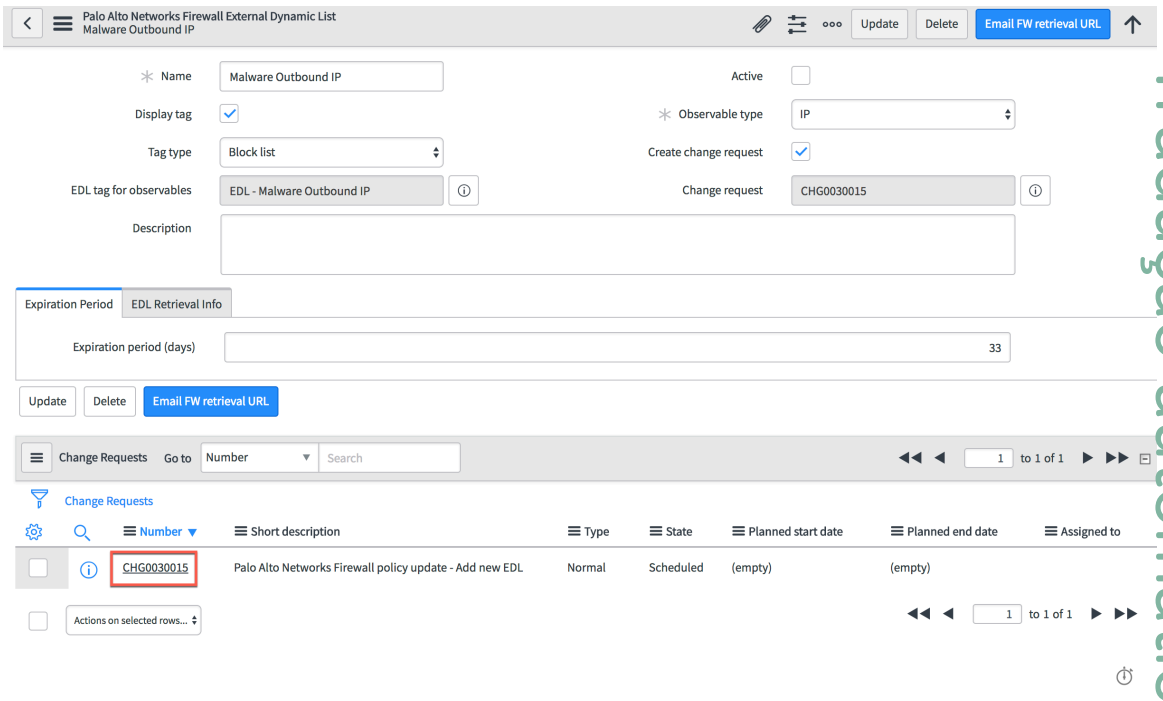
2. Selecione o módulo EDL e clique em um EDL no **Nome** coluna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



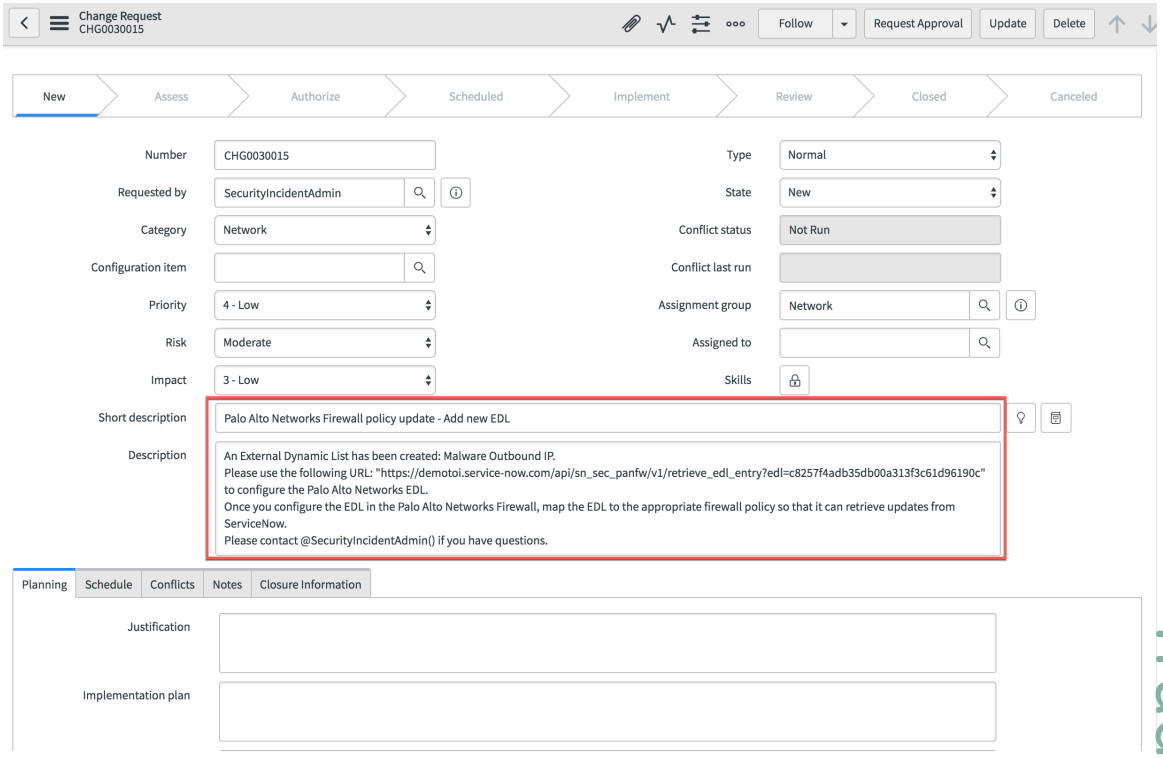
3. No registro EDL aberto, clique no número da solicitação de mudança na lista relacionada Solicitações de mudança.



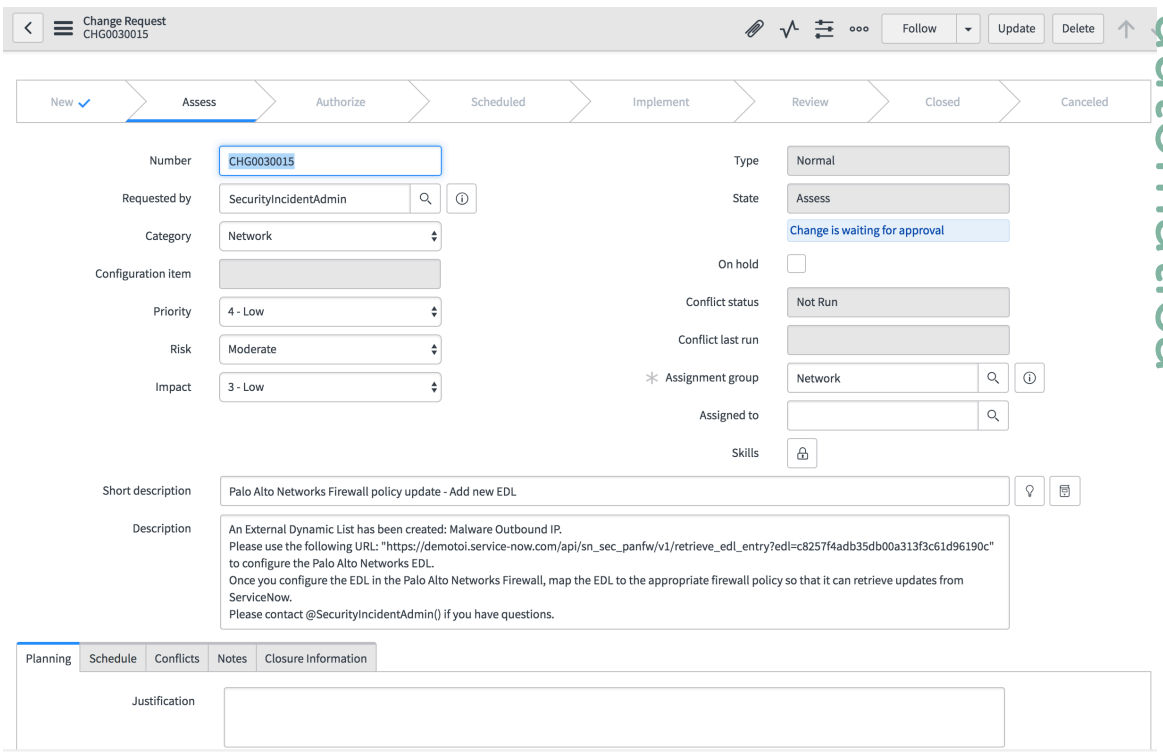
O registro de solicitação de mudança é exibido. . **Descrição** O campo lista o URL de recuperação usado para configurar o. Palo Alto Networks EDL. Detalhes sobre como mapear o EDL para o apropriado Palo Alto Networks Next-Generation Firewall as políticas também estão incluídas. Em **Descrição resumida** Um comentário indica que há uma solicitação para adicionar um novo EDL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No canto superior direito do registro, clique em **Aprovação da solicitação** .
O Estado muda para Avaliar e uma mensagem é exibida informando que a solicitação de mudança está aguardando aprovação.

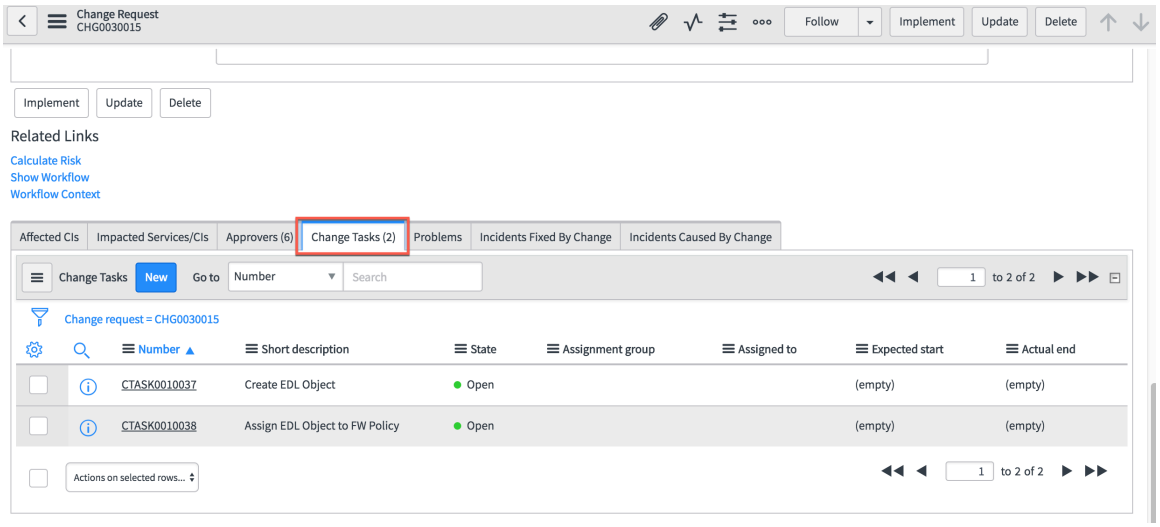


5. Para concluir a solicitação de mudança e ativar o EDL, siga as etapas para atribuir as tarefas e fechar a solicitação de mudança.

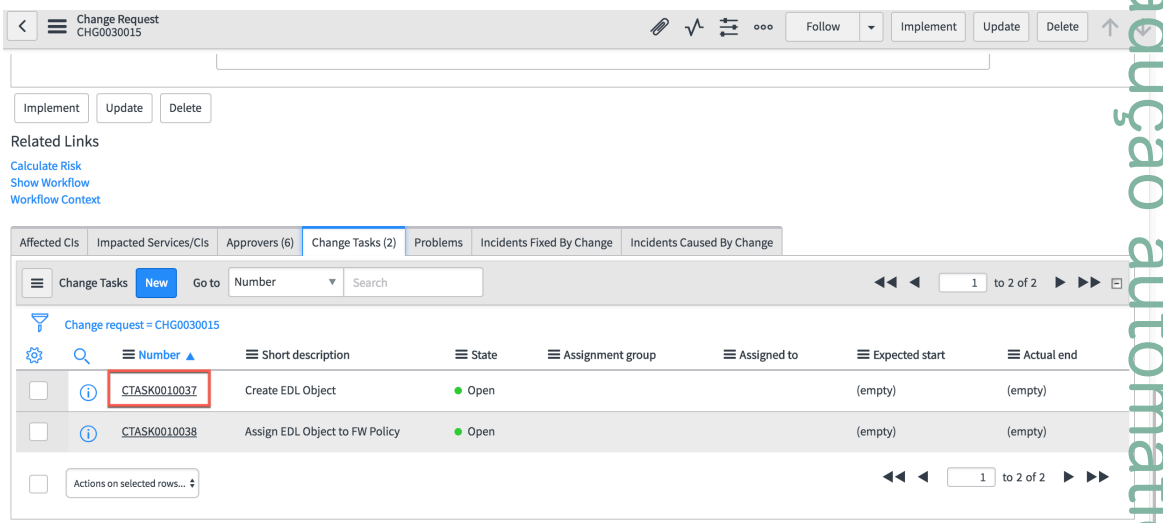
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Se não for exibido, abra a solicitação de mudança e selecione **Tarefas de mudança** guia.



b. Clique na tarefa associada à criação do objeto EDL para abri-la.

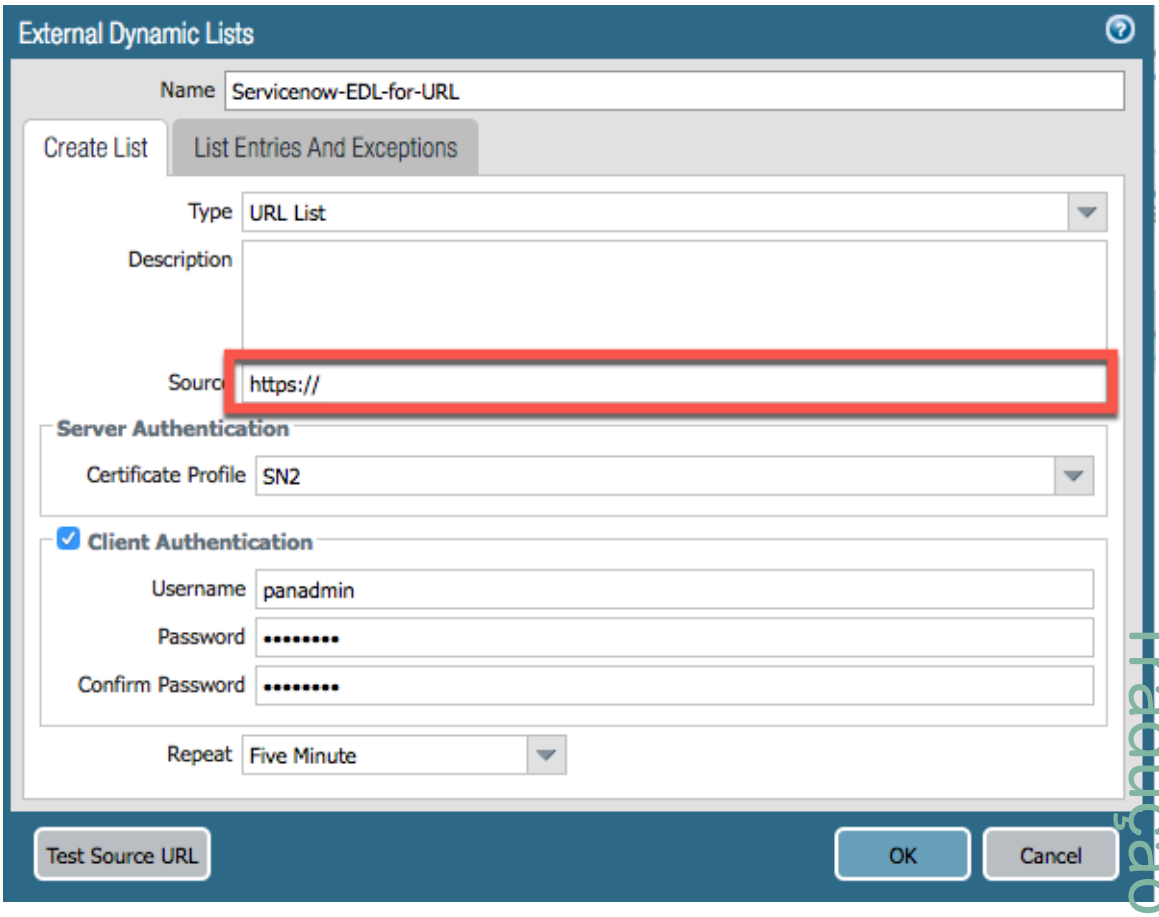


c. No registro exibido, atribua a tarefa ao Palo Alto Networks administrador do firewall e clique em **Atualização** .
O administrador do firewall é notificado e cria o objeto EDL no Palo Alto Networks Next-Generation Firewall.

Para criar o objeto EDL, o. ServiceNow AI Platform O URL de recuperação é copiado em Palo Alto Networks em **Listas dinâmicas externas** > **Criar listas** > **Origem**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

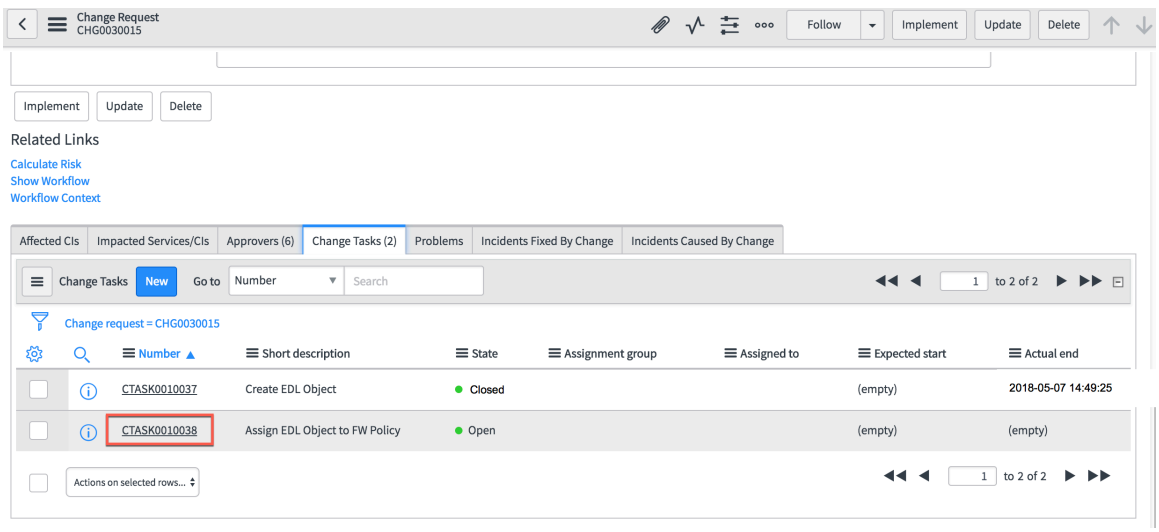


A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

d. Depois de verificar se o objeto EDL foi criado em Palo Alto Networks. em ServiceNow AI Platform, Navegue até a Solicitação de mudança associada à criação do objeto EDL e clique em **Fechar tarefa** .

No registro de tarefa para este exemplo, CTASK0010037 foi encerrado para esta tarefa.

e. Navegue até a guia Tarefas de mudança e clique na tarefa para atribuir uma política de firewall ao objeto EDL.



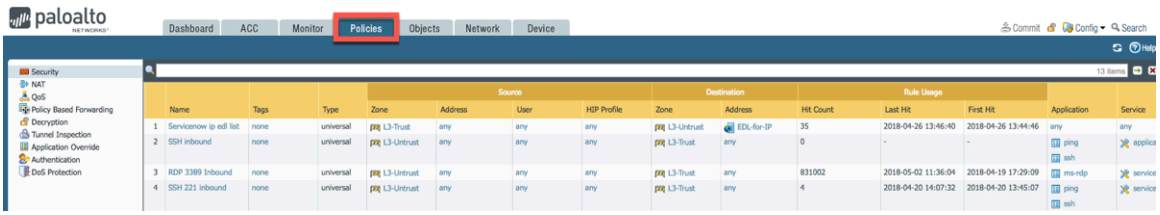
O status de CTASK0010037 . Encerrado .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

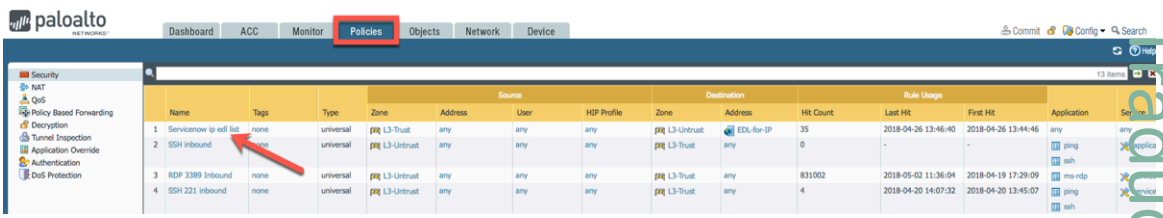
f. Abra o registro e atribua a próxima tarefa.

Depois que a tarefa foi atribuída, em Palo Alto Networks, o administrador do firewall navega até **Políticas** para atribuir a política.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

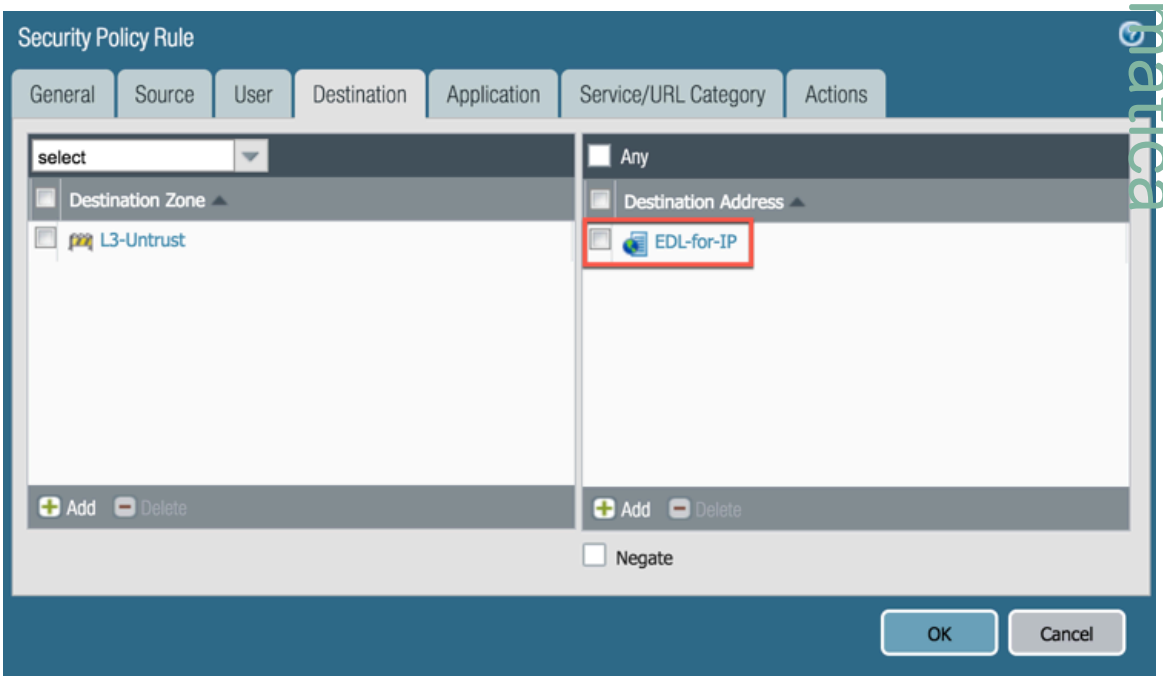
g. Em **Nome** , localize e clique na regra de política de segurança à qual você deseja adicionar o EDL, por exemplo, **Lista de edl de ip da ServiceNow** .



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

h. Na caixa de diálogo Regra de política de segurança, selecione **Destino** Para adicionar um EDL no **Endereço de destino** campo.

i. Para exibir todos os EDLs disponíveis, clique em **Adicionar** ícone.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

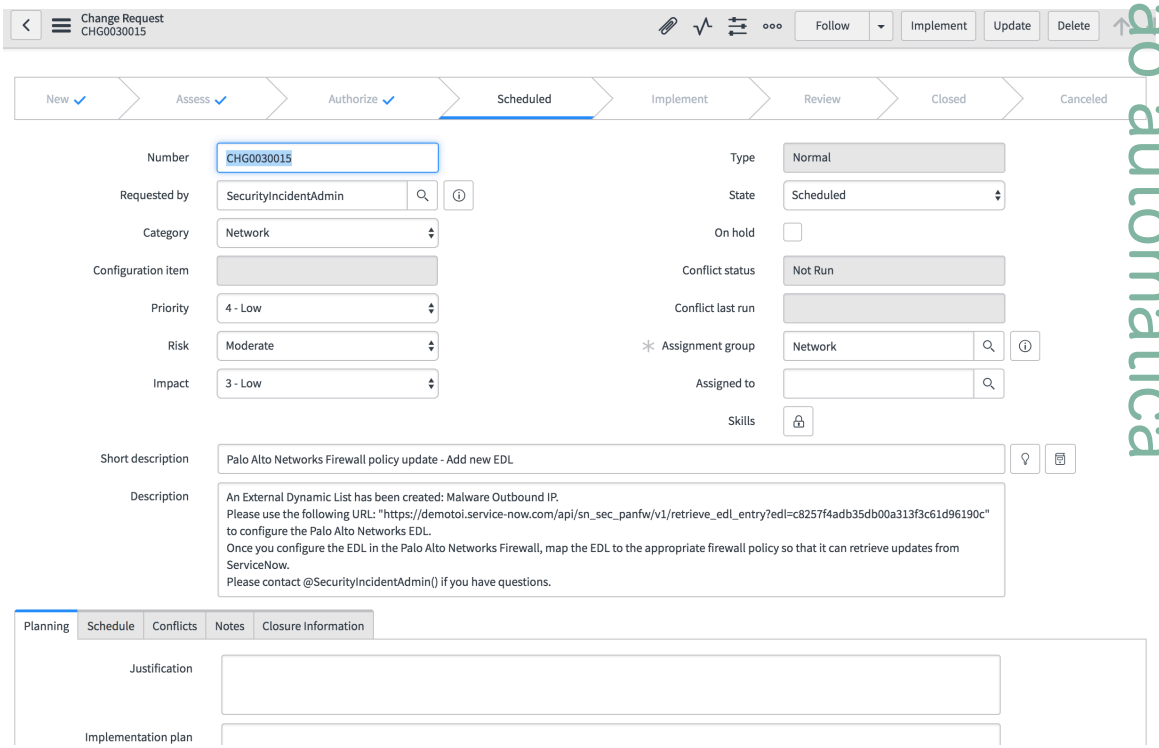
j. Clique em **OK**.

k. Depois de verificar se o objeto EDL foi atribuído a uma política de segurança, em ServiceNow AI Platform, Navegue até a solicitação de mudança, abra a tarefa associada à atribuição do objeto EDL e clique em **Fechar tarefa** .
Depois que ambas as tarefas são encerradas, a solicitação de mudança está pronta para aprovação.

l. No registro de solicitação de mudança, clique em **Aprovadores** e selecione um item no **Estado** Coluna para abrir a solicitação usada para criar o EDL.



m. No formulário Solicitação de aprovação em aberto, clique em **Aprovar** .
O estado da Solicitação de mudança é movido para Programado.



n. Clique em **Implementar**.

o. Clique em **Informações de fechamento** guia relacionada e insira anotações para fechar a solicitação.

Uma entrada neste campo é necessária para fechar a solicitação de mudança.

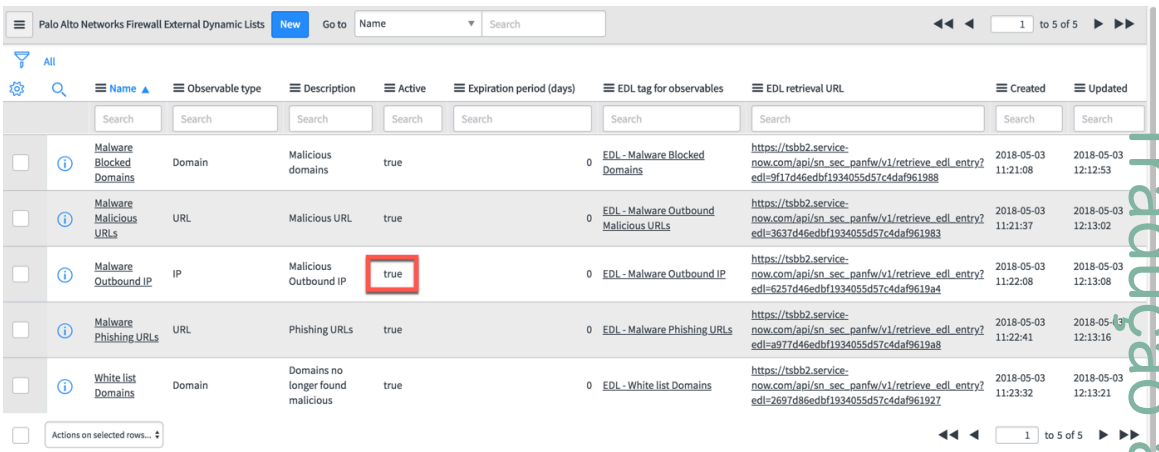
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

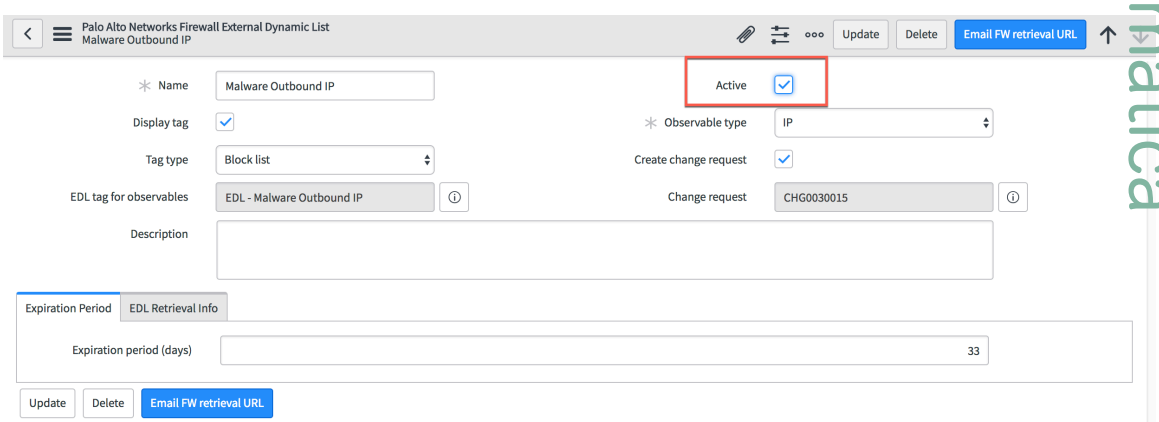


Depois que a solicitação de mudança é fechada, o EDL é ativado automaticamente. Se você não verificou que o EDL está ativado, navegue até **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall**.

Na coluna Ativo da lista, observe que o status do EDL é (verdadeiro).



Na coluna Nome, clique no nome do EDL e, no registro Abrir, observe que **Ativo** a caixa de seleção também está marcada.



O EDL agora está pronto para aceitar entradas de EDL.

O que Fazer Depois

Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Envie entradas de EDL de um registro de incidente de segurança para Palo Alto Networks Next-Generation Firewall

Observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas de Lista dinâmica externa (EDL) para EDLs. Um processo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aprovação para entradas de EDL faz parte do fluxo de trabalho pré-configurado. O firewall importa entradas de EDL (endereços IP, URLs, domínios) que estão incluídas nas listas de EDL e impõe a política.

Antes de Iniciar

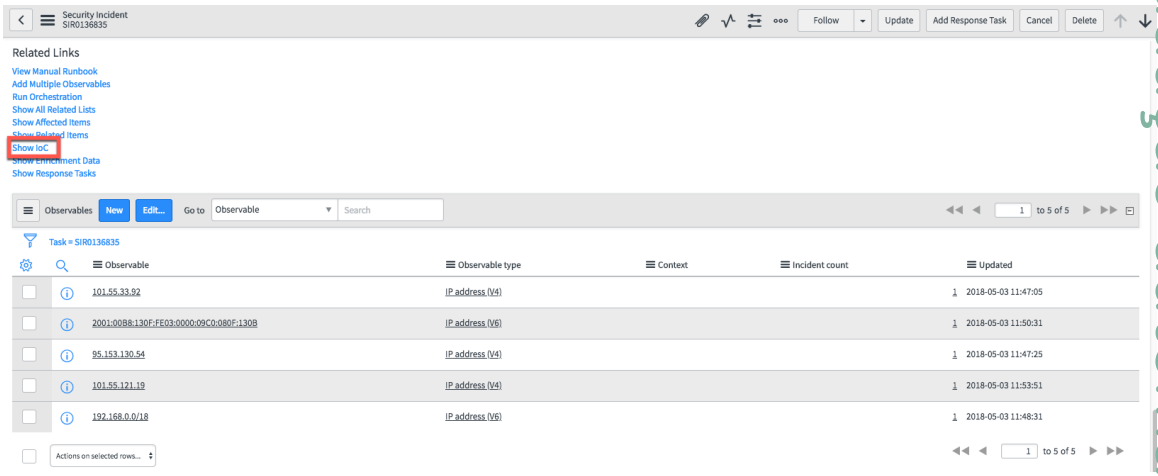
Função necessária: sn_si.analyst para enviar entradas de EDL. Para aprovar entradas de EDL: A aprovação é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização.

Por Que e Quando Desempenhar Esta Tarefa

Usuários com a função sn_si.analyst enviam entradas de EDL solicitando um bloco em observáveis anexados a um registro de incidente de segurança. Uma vez enviada, uma entrada de EDL com status Pendente é gerada e enviada para aprovação. O exemplo a seguir mostra uma solicitação de bloco para um observável de URL.

Procedimento

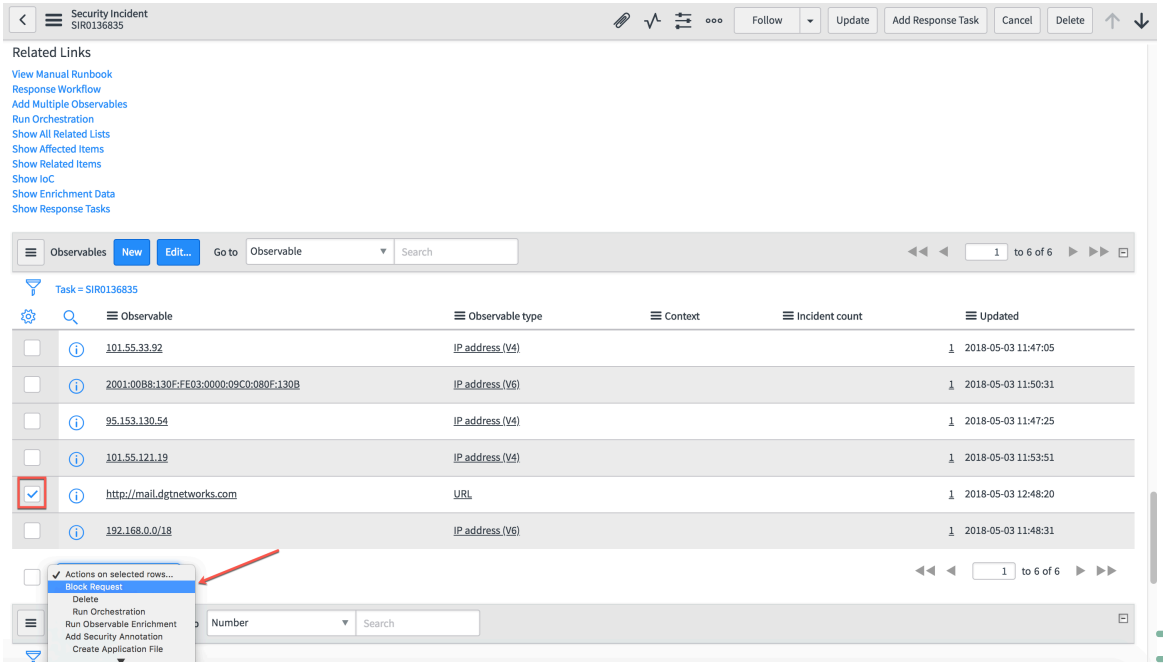
1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique em **Mostrar IOC** link relacionado.



3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e no **Ações nas linhas selecionadas** , selecione **Solicitação de bloqueio** .

Tradução automática

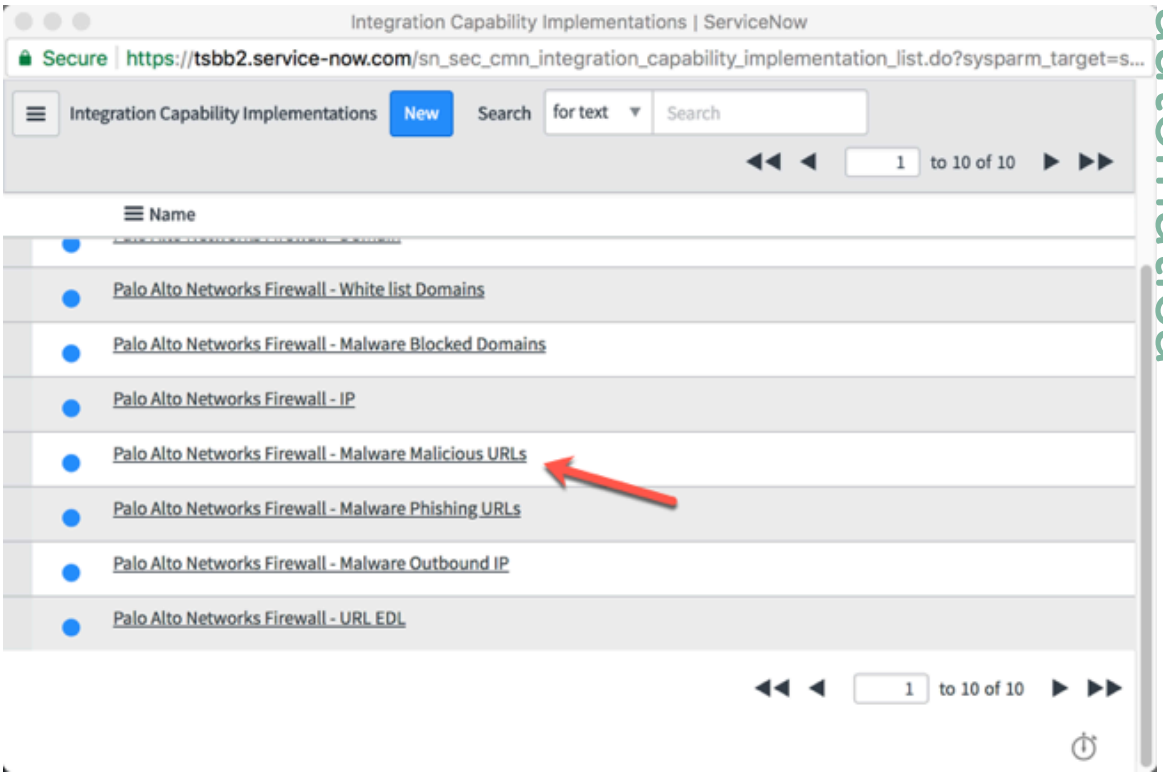
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo exibida, clique no ícone de pesquisa ( ).

5. Na lista exibida, selecione o EDL ao qual você deseja anexar esta entrada.

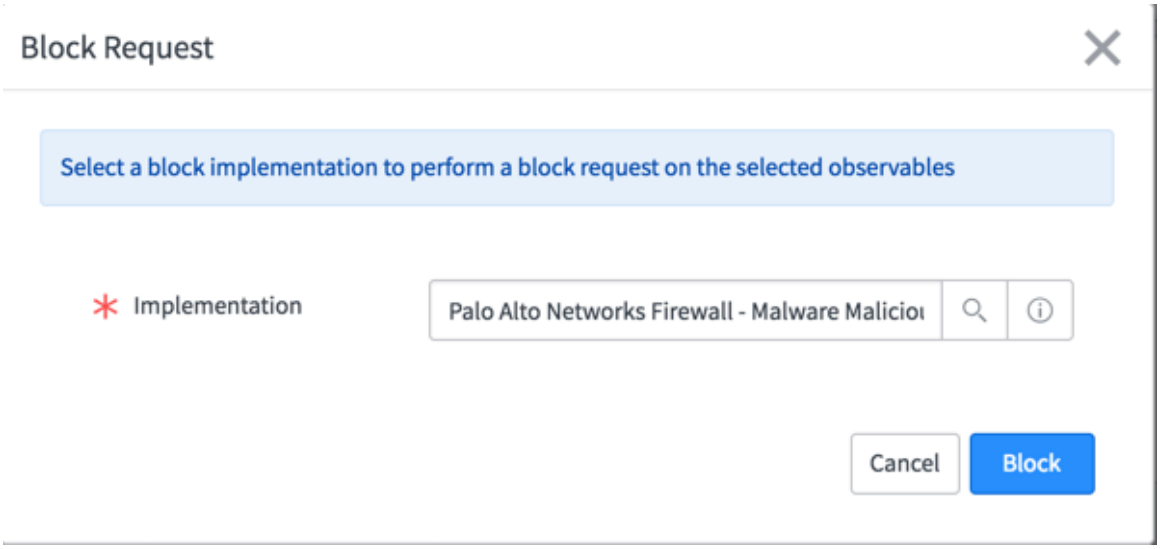
Nota: Para este exemplo, o tipo de observável de entrada (URL) deve corresponder ao tipo de observável EDL (URL).



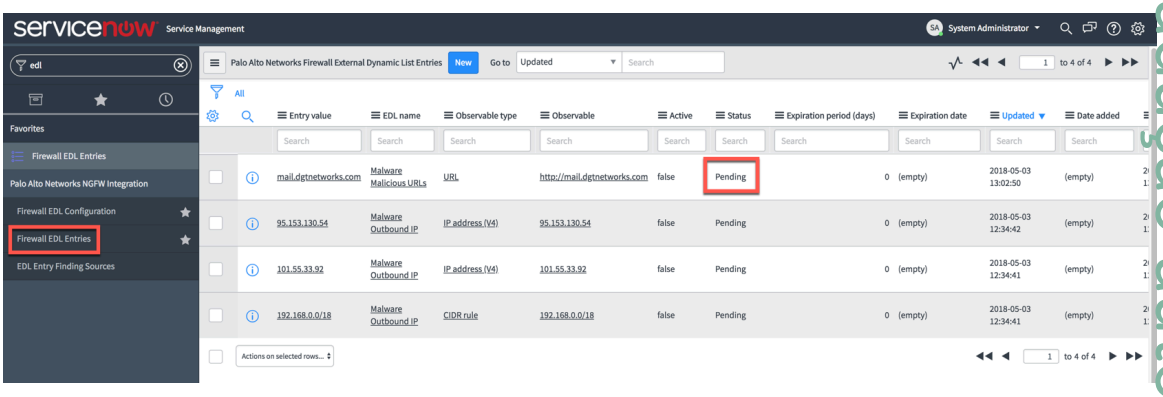
6. Na caixa de diálogo Solicitação de bloqueio com o nome do EDL exibido em **Implementação** clique em **Bloco** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

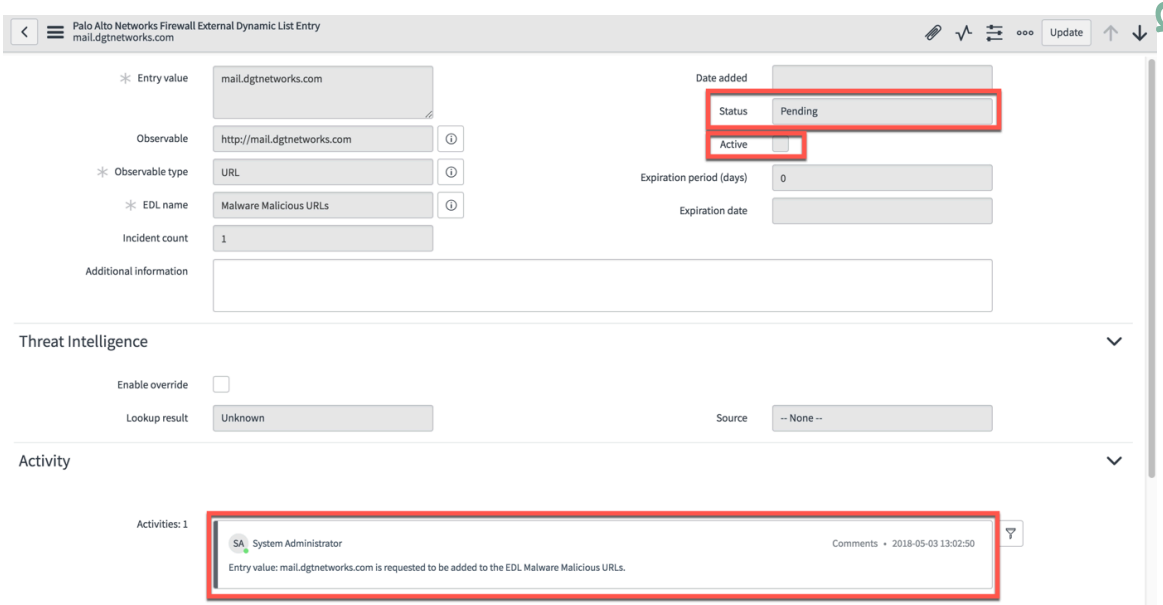


7. Navegar até **Integração do NGFW da Palo Alto Networks** > **Entradas de EDL de firewall** e clique em **Entradas de EDL do firewall** .



8. Na lista Entradas da lista dinâmica externa do firewall da Palo Alto Networks, clique no observável em **Valor de entrada** coluna para abrir o registro.

   Para este exemplo, o registro para **mail.dgtnetworks.com** é exibido.

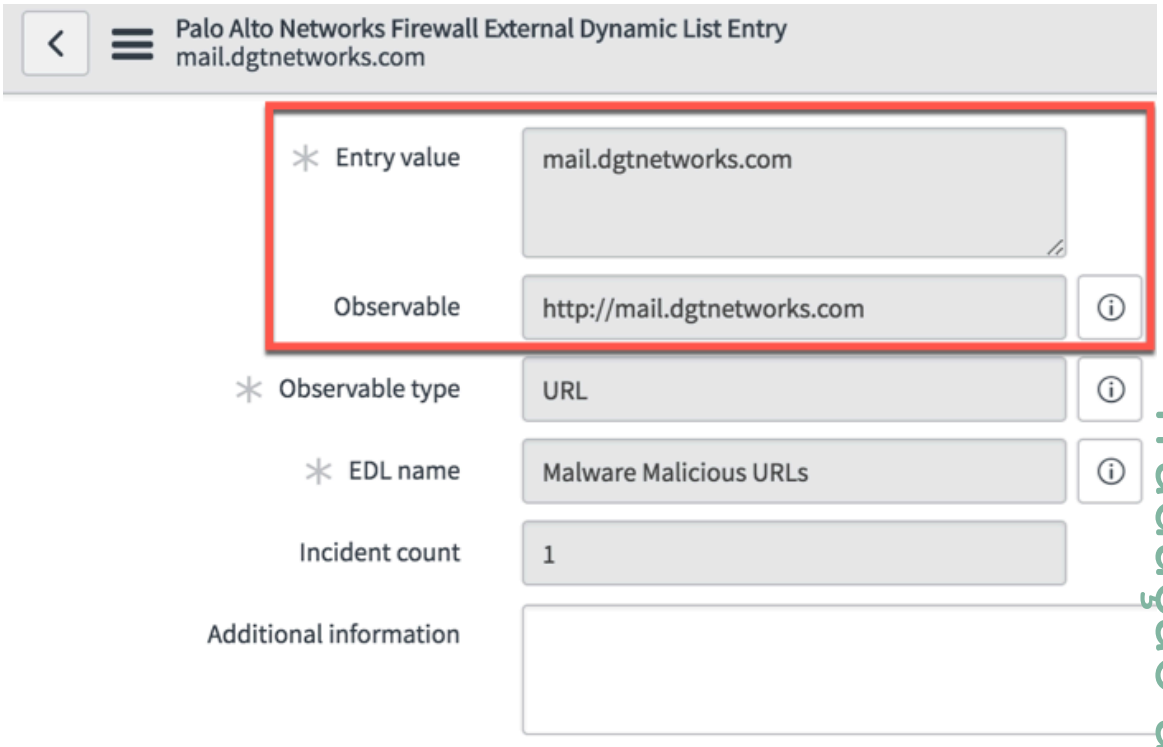


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de entrada de EDL está pronta para aprovação.

Os campos Valor de entrada e Observável mostram formatos diferentes para o observável de URL.



O ícone ao lado de Observável o campo é um link para ServiceNow AI Platform® Tabela observável.

O valor em Observável campo (http://mail.dgtnetworks.com) Vincula a tabela observável e corresponde ao formato que foi trazido do Resposta a incidentes de segurança evento de acionamento de incidente.

. ServiceNow AI Platform® Pode modificar automaticamente as entradas de EDL para que sejam compatíveis com Palo Alto Networks Formato de URL EDL.

Neste exemplo, o observável foi criado com o protocolo http:// (http://mail.dgtnetworks.com E este formato é exibido no campo Observável. O protocolo http:// é removido automaticamente do observável pelo ServiceNow AI Platform® por isso, é compatível com Palo Alto Networks e podem ser recuperados. Como resultado, mail.dgtnetworks.com é exibido em Valor de entrada campo.

O que Fazer Depois

Aprovar entradas de EDL.

Tópicos relacionados

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Envie entradas de EDL da lista de bloqueios para Palo Alto Networks Next-Generation Firewall

Para observáveis determinados como mal-intencionados e não associados a um específico ServiceNow AI Platform Incidente de segurança, você envia entradas de Lista dinâmica externa (EDL) da lista de bloqueios.

Antes de Iniciar

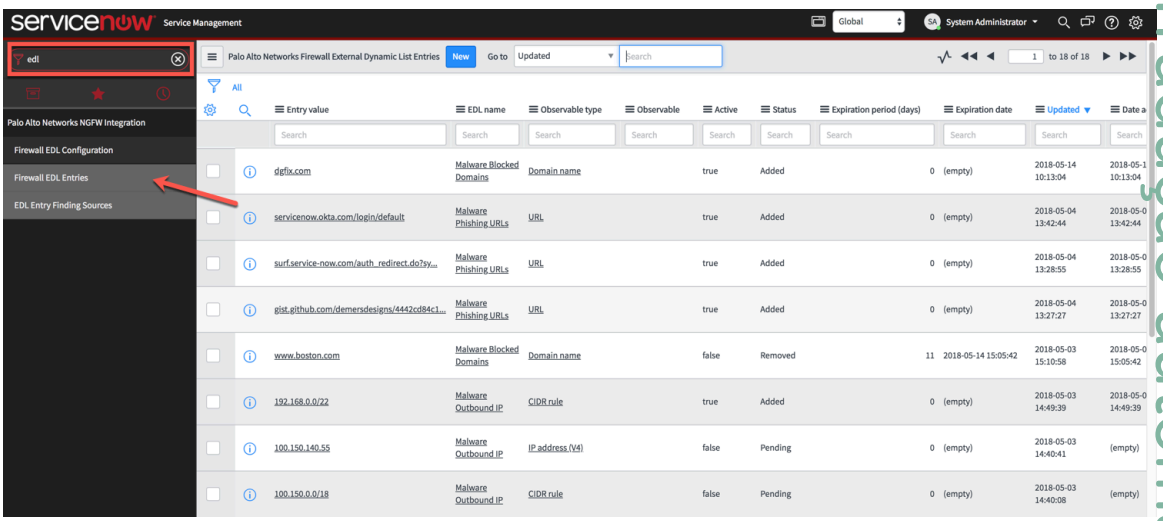
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Quando você deseja bloquear um observável que você determinou como mal-intencionado ou permitir que um observável que você determinou não é mal-intencionado e o observável não está associado a um específico ServiceNow AI Platform Registro de incidente de segurança, você envia entradas de EDL diretamente da lista de bloqueios. Exemplos desses tipos de entradas de EDL podem ser URLs ou domínios para sites específicos.

Procedimento

1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Entradas de EDL de firewall**.



2. Clique em **Entradas de EDL do firewall** módulo.
3. Na lista Entradas da lista dinâmica externa do firewall da Palo Alto Networks, clique em **Novo** .
4. No novo registro exibido, em **Valor de entrada** , insira um valor para o observável.
   Os dois resultados possíveis desta entrada:

   Os campos restantes no formulário são preenchidos automaticamente.

   Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione o EDL ao qual você deseja anexar esta entrada e clique em **Enviar** . Selecione o EDL ao qual você deseja anexar esta entrada antes de definir o Período de expiração.

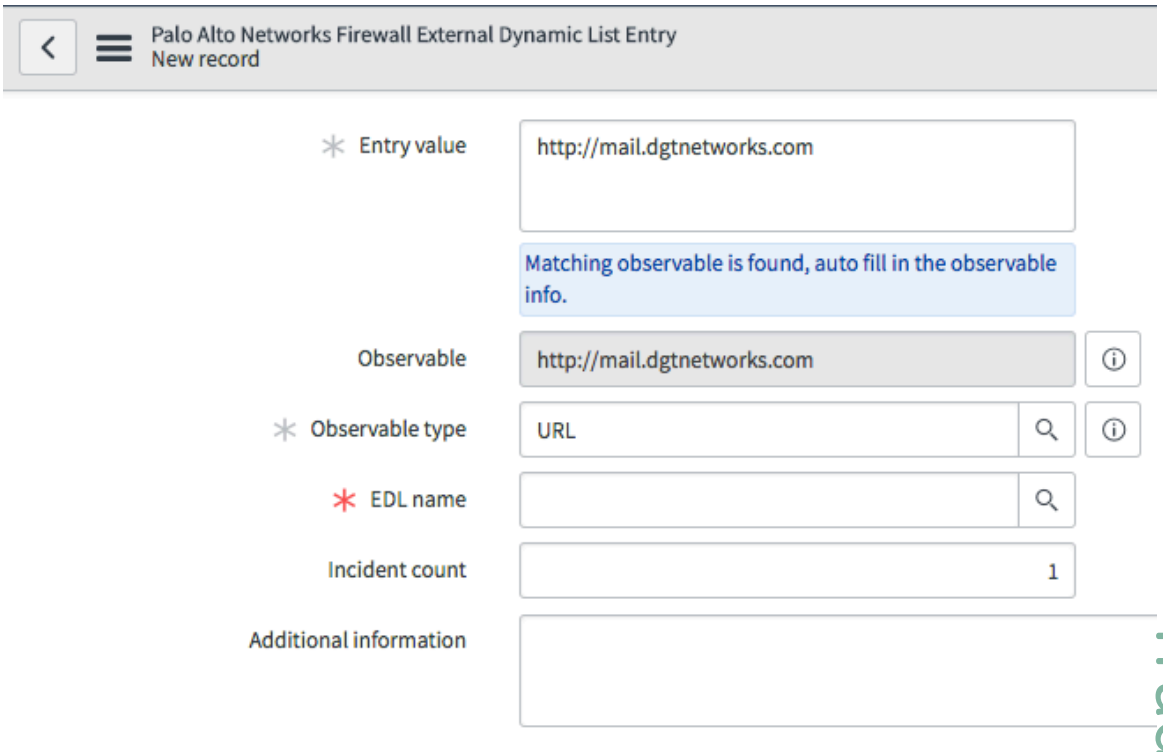
   É exibida uma mensagem instruindo você a preencher o formulário.

   Não foi encontrado um observável correspondente e você deve preencher o formulário. Depois de concluí-lo, selecione o EDL ao qual você deseja anexar o observável e clique em **Enviar** . Um registro observável é criado.

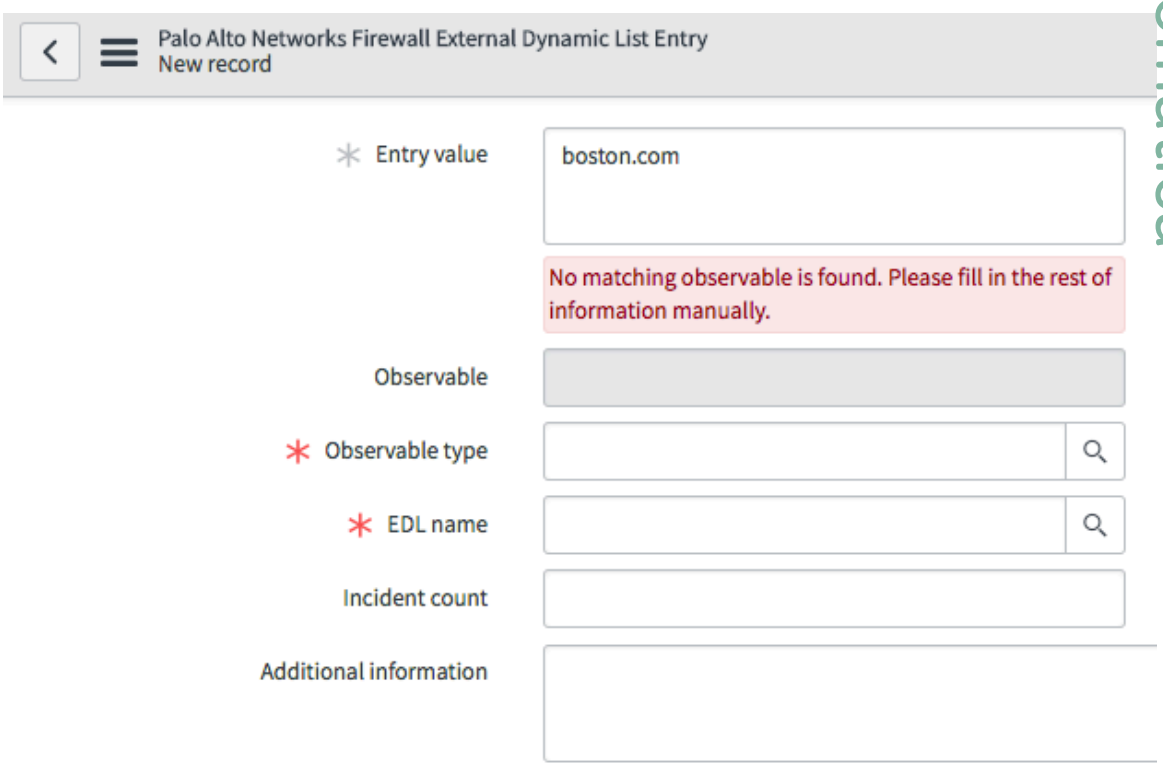
A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique no ícone de pesquisa para selecionar o EDL ao qual você deseja anexar a entrada.
6. Clique em **Enviar**.
   Se você tiver a aprovação de e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
7. Se uma mensagem for exibida solicitando que você preencha o restante das informações manualmente, preencha os campos.

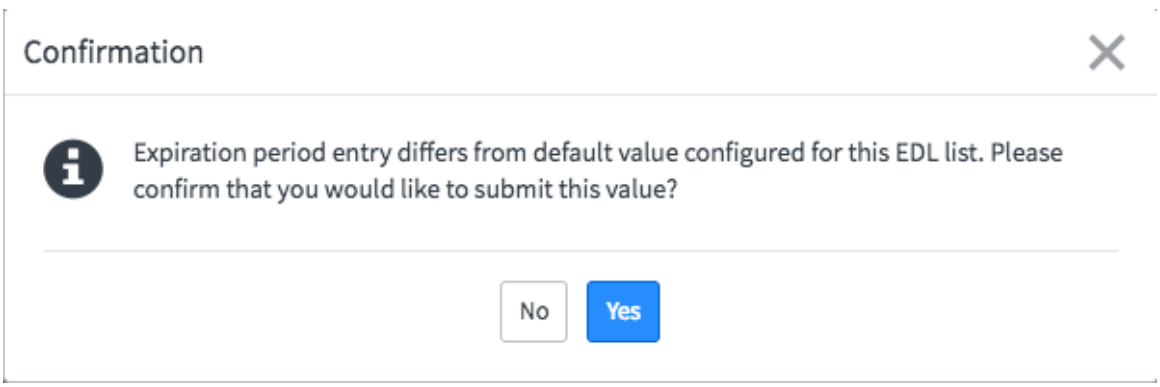


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de observável	Tipo de observável compatível com a caixa de diálogo.
Nome do EDL	EDL ao qual você deseja anexar a entrada. **Nota:** Selecione o EDL ao qual deseja anexar a entrada antes de definir o Período de expiração.
Habilitar substituição (o padrão é selecionado)	Resultado ou origem da pesquisa. Quando configurado, permite que você insira um **Resultado da pesquisa** e a origem usada para encontrar os resultados. Normalmente, esses campos são preenchidos quando um registro de incidente de segurança é criado. Nesse caso, não há resultado de pesquisa ou origem e você preenche esses campos manualmente.
Resultado da pesquisa	Selecione **Desconhecido** ou **Mal-intencionado** .
Origem	Origem que executa uma pesquisa de ameaça na entrada EDL, por exemplo, ThreatCrowd etc.
Período de expiração	O período de expiração herdado do EDL por padrão. Você pode substituir este valor, mas somente durante a criação da entrada. `0` Indica que a entrada EDL nunca expira. Se você mudar este valor, esta entrada ficará ativa para o número de dias que você inserir. Você pode inserir um valor mínimo de `1` e não há valor máximo. Por exemplo, se você inserir `30` Às 2:01 do dia 1 de maio, a entrada de EDL expirará às 2:01 do dia 31 de maio.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada de EDL, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente do EDL selecionado.



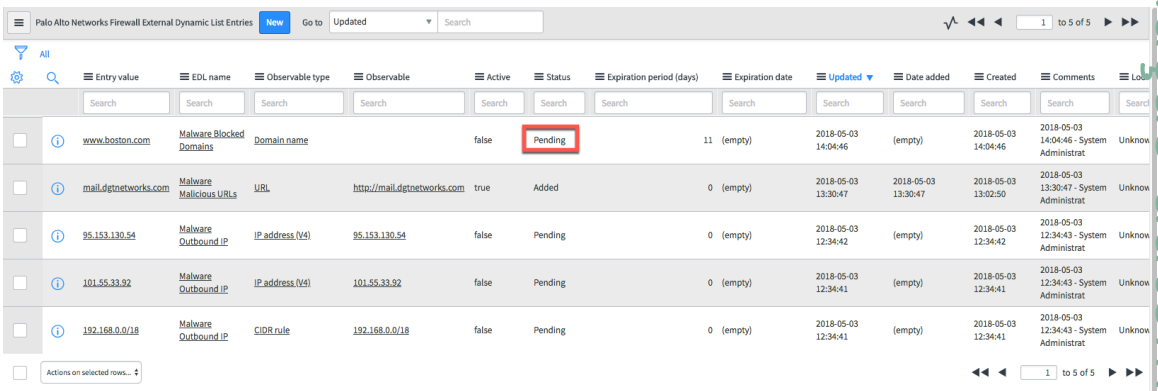
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Escolha uma opção para configurar o período de expiração.

Opção	Descrição
Sim	Confirma sua substituição de expiração, salva o registro e retorna para **Entradas da lista dinâmica externa do firewall da Palo Alto Networks** lista. Se você tiver a aprovação de e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
Não	Cancela a substituição. Neste ponto, você pode mudar o valor de **Período de expiração** . Depois de alterar o valor, clique em **Enviar** para retornar ao **Entradas da lista dinâmica externa do firewall da Palo Alto Networks** lista.

10. Se não for exibido, navegue até **Entradas da lista dinâmica externa do firewall da Palo Alto Networks** E observe que o status da entrada é Pendente.



Agora, a entrada está pronta para aprovação.

O que Fazer Depois

Aprovar entradas de EDL.

Tópicos relacionados

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Aprovar entradas de EDL

Um processo de aprovação para entradas de Lista dinâmica externa (EDL) faz parte do fluxo de trabalho pré-configurado. Você aprova entradas de EDL antes que as entradas sejam ativadas em EDLs. Se você aprovar a entrada de EDL, o firewall recuperará a entrada e seu observável será bloqueado a partir desse ponto em diante.

Antes de Iniciar

Aprovação necessária: A aprovação para entradas de EDL é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização. No exemplo a seguir, ServiceNow AI Platform o administrador tem autoridade de aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

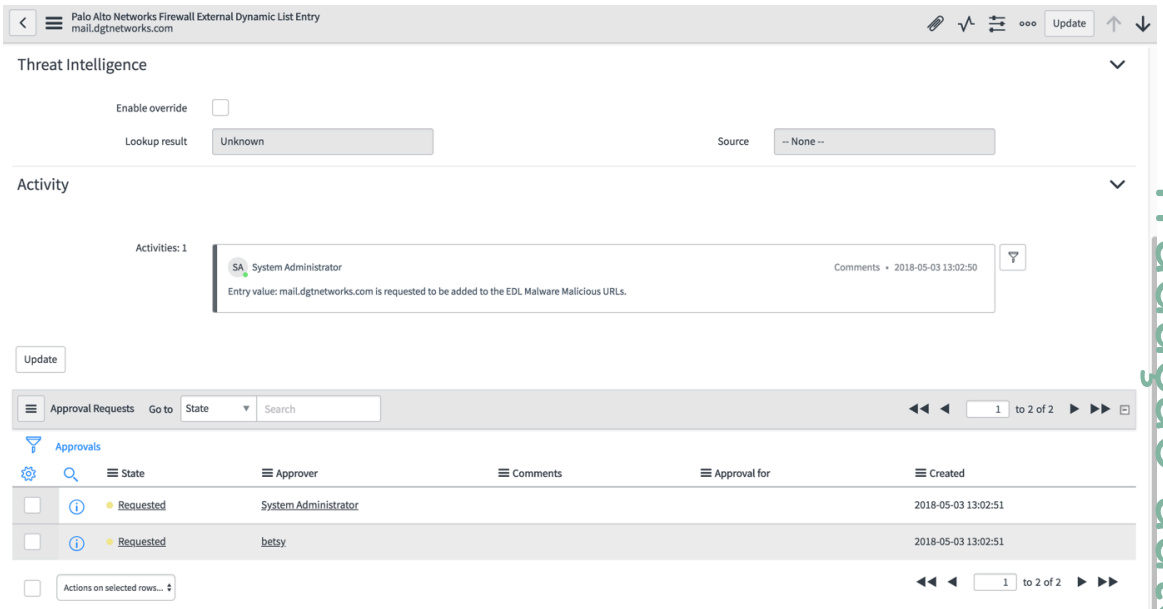
Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada de EDL não é ativada ou desativada no EDL até que seja aprovada.

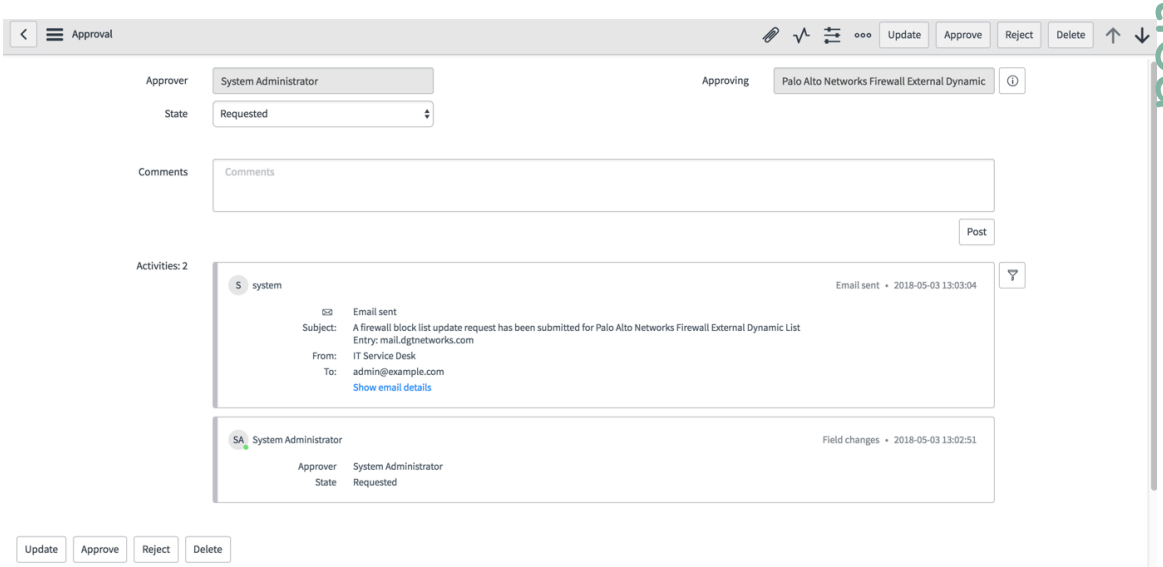
Procedimento

1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Entradas de EDL de firewall** E abra o registro EDL.
2. No registro EDL, role até a seção Solicitações de aprovação.

   Nota: Se você tiver Formulários com guias selecionados em Configurações do sistema, a seção aparecerá como uma guia no registro.



3. Em Solicitações de aprovação, clique em um item no **Estado** coluna para abri-la.
   O registro de aprovação é exibido.



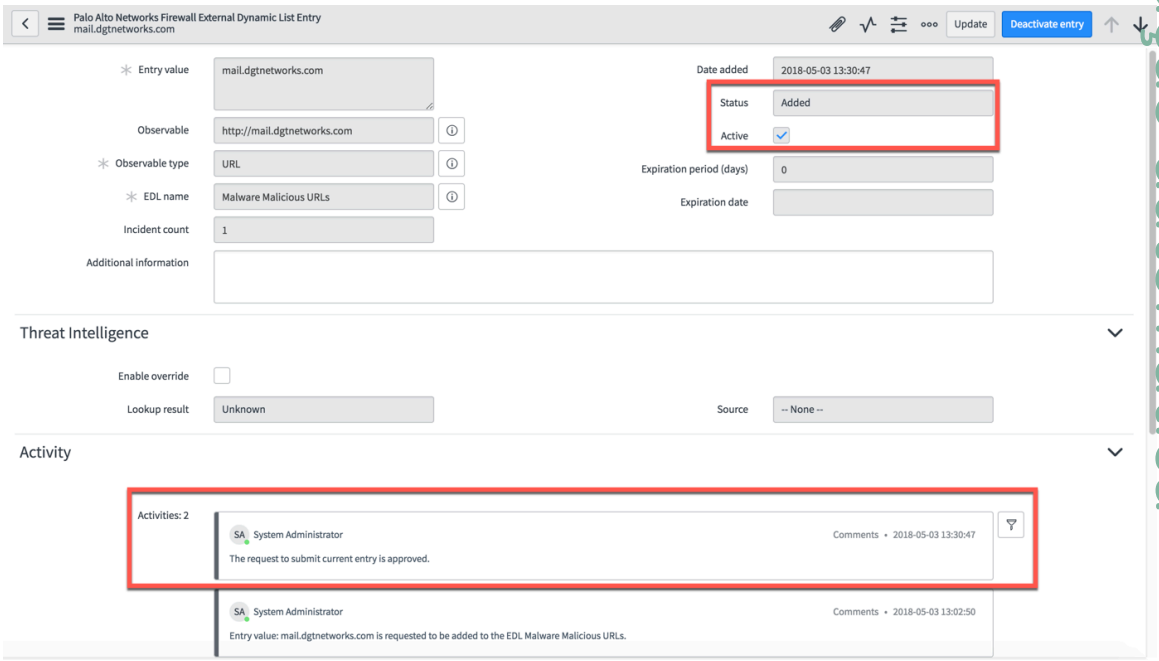
4. Escolha uma opção para aprovar a entrada de EDL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Aprovar	No registro de entrada, **Status** o campo muda para Adicionado e **Ativo** a caixa de seleção está marcada. . **Desativar** o botão é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada EDL foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para **Rejeitado** e **Ativo** a caixa de seleção está desmarcada indicando que a entrada não está bloqueada no firewall. As anotações de trabalho mostram que a solicitação da entrada EDL foi rejeitada.

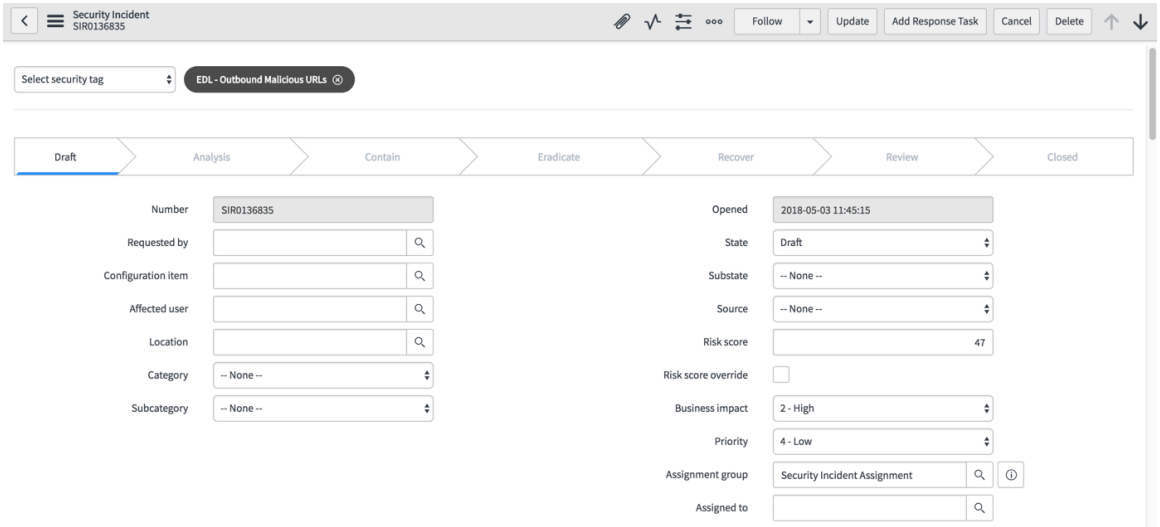
Depois de aprovar a entrada EDL e ela ser ativada, o. Palo Alto Networks Next-Generation Firewall Recupera a entrada de EDL após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado a partir desse ponto em diante. Na figura a seguir, observe que a caixa de seleção Ativo está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.



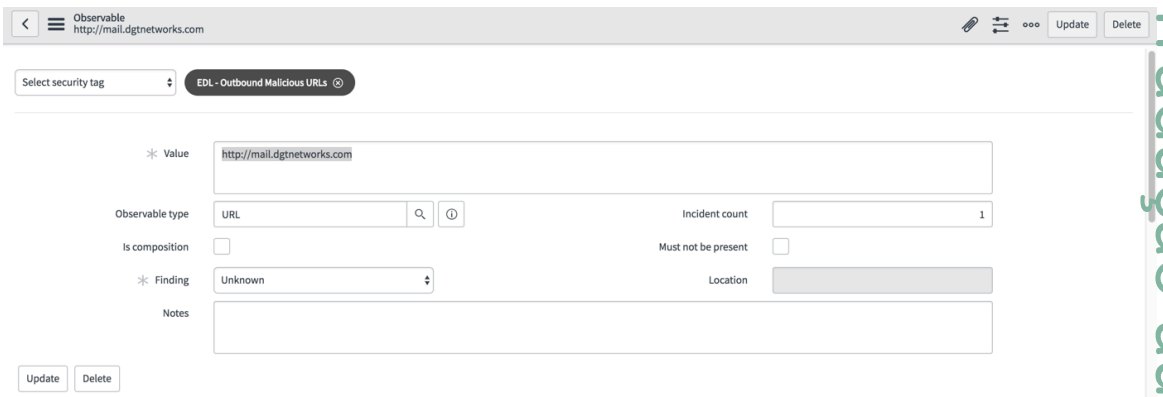
Depois que a entrada EDL é aprovada e ativada, o registro do incidente de segurança é marcado com um marcador de segurança. O marcador é exibido na parte superior do registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O marcador de segurança também é exibido no registro do observável.



Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Há restrições para adicionar entradas de Lista dinâmica externa (EDL) aos EDLs. Se houver conflitos de duplicação, compatibilidade ou CIDR (roteamento entre domínios sem classe) quando você tentar adicionar entradas de EDL aos EDLs, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

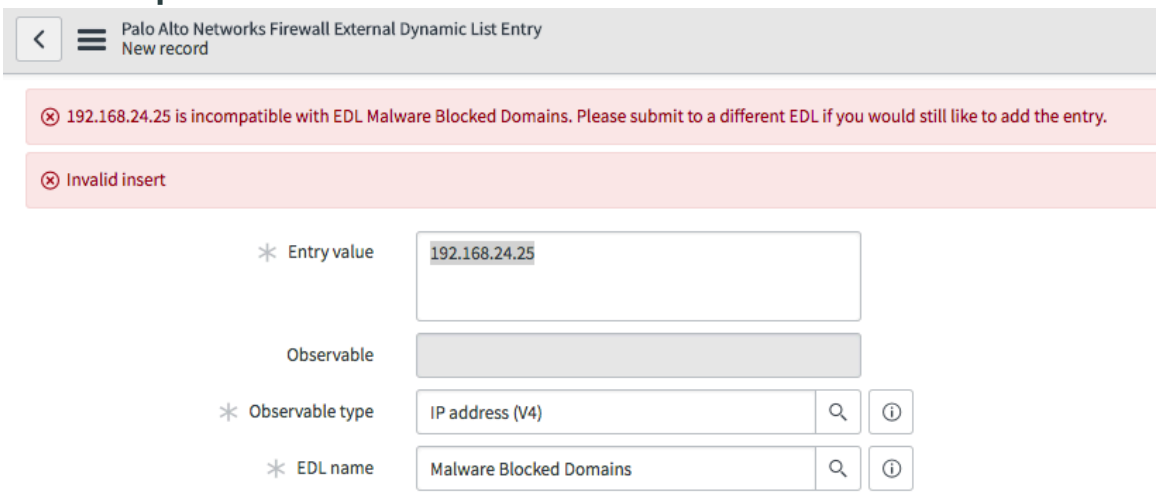
Exceção de compatibilidade

Cada EDL aceita somente entradas compatíveis com seu tipo de observável. Se você criar um EDL de domínio e tentar anexar um endereço IP observável a ele, uma mensagem de erro incompatível será exibida. Por exemplo, um domínio EDL só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

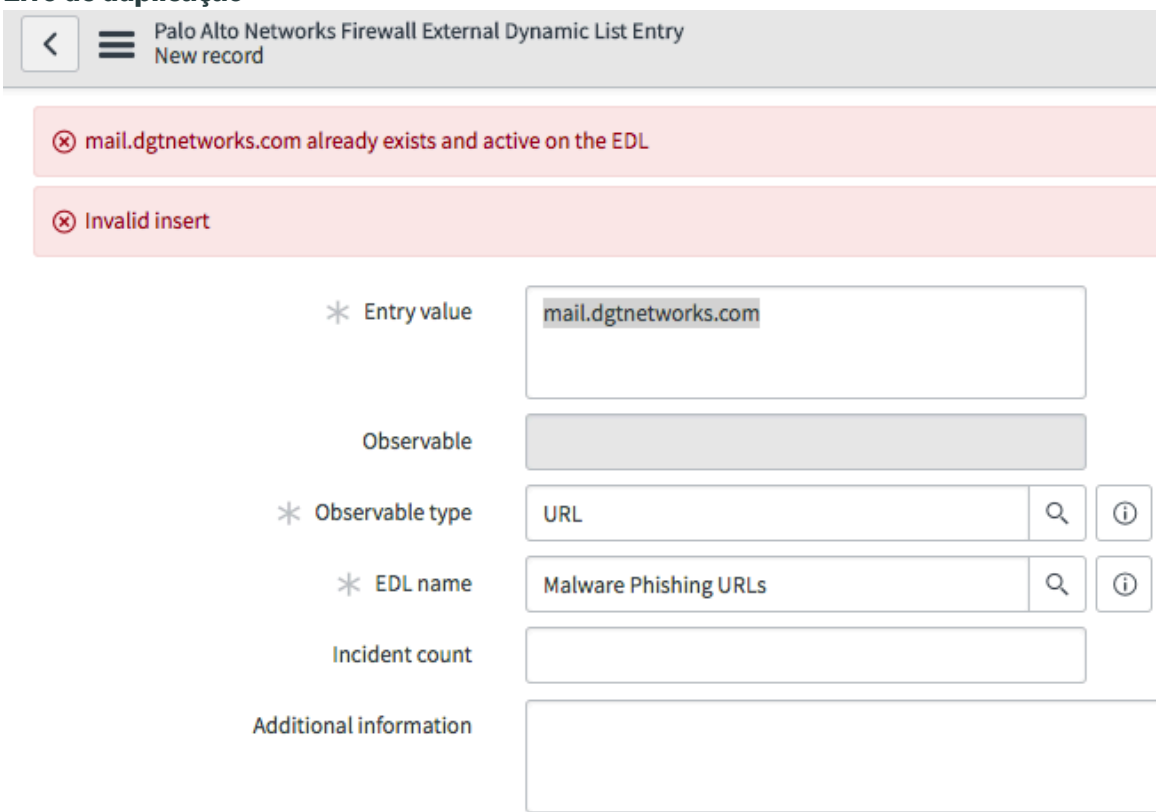
Erro de compatibilidade



Exceção de duplicação

Um observável não pode ser ativado em vários EDLs do mesmo tipo de observável. Se um observável de URL já estiver ativado em um EDL de URL e você tentar ativar o mesmo observável em um EDL de URL de Phishing, uma mensagem de erro de duplicação será exibida.

Erro de duplicação



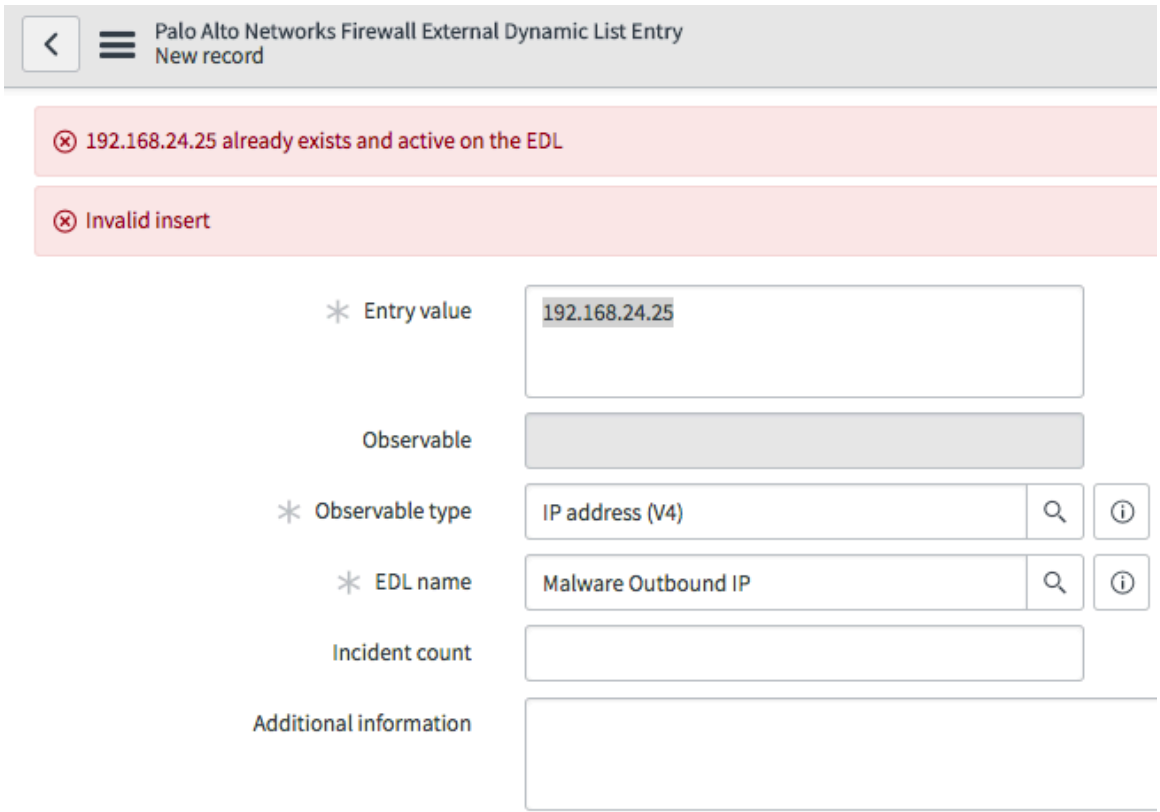
Exceção CIDR (roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a um EDL e este endereço IP fizer parte de um observável de CIDR já em um EDL, um erro de conflito de CIDR será exibido. Este erro indica que o único endereço IP já está incluído no EDL como parte do observável CIDR. Por exemplo, 192.168.24.25 Faz parte do bloco CIDR 192.168.0.0/22 .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conflito de CIDR



(Opcional) Edite o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall

. **Marcador de exibição** Quando você cria o registro de Lista dinâmica externa (EDL), você pode editar os nomes e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

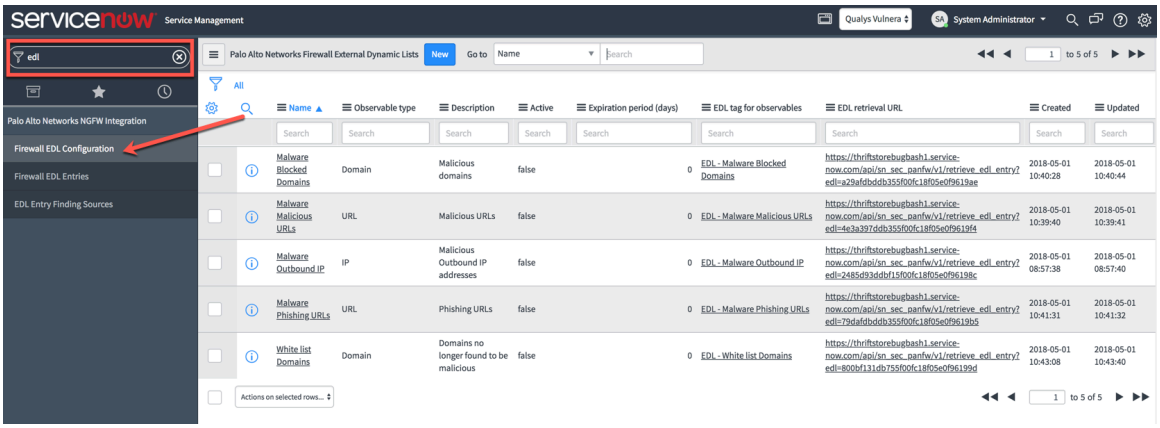
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se ele foi removido de um EDL. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Tradução automática

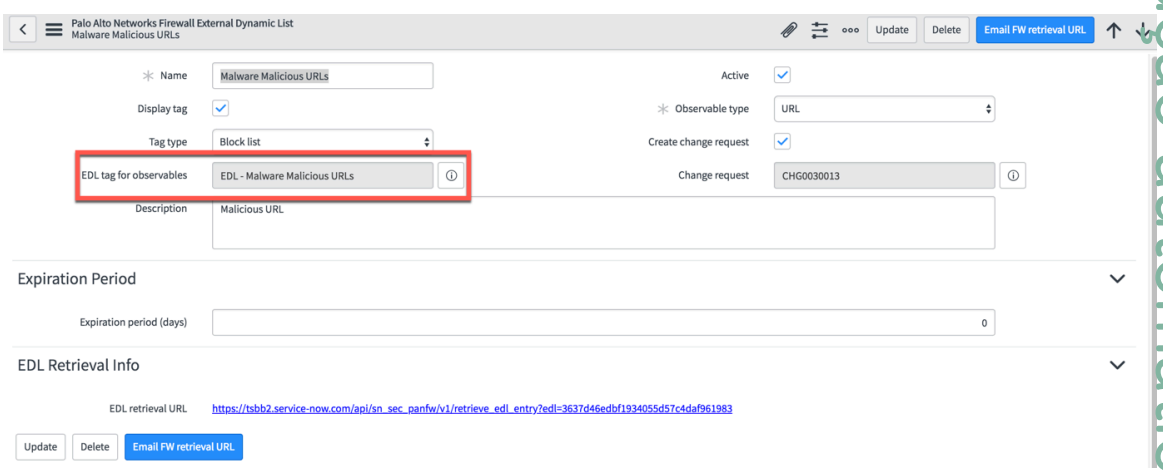
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

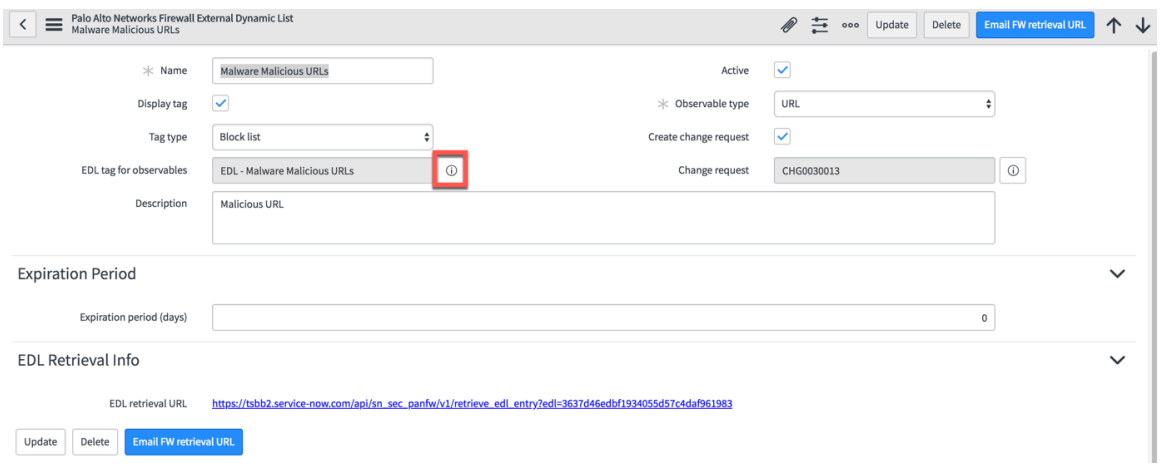
1. Navegar até **Tudo** > **Integração do NGFW da Palo Alto Networks** > **Configuração de EDL de firewall**.



2. Clique em um item no **Nome** coluna para abri-la
   O registro EDL é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor inserido em **Nome** EDL quando você o criou. Por padrão, o nome também inclui um *EDL* Prefixo, por exemplo, EDL - URLs mal-intencionados de malware.



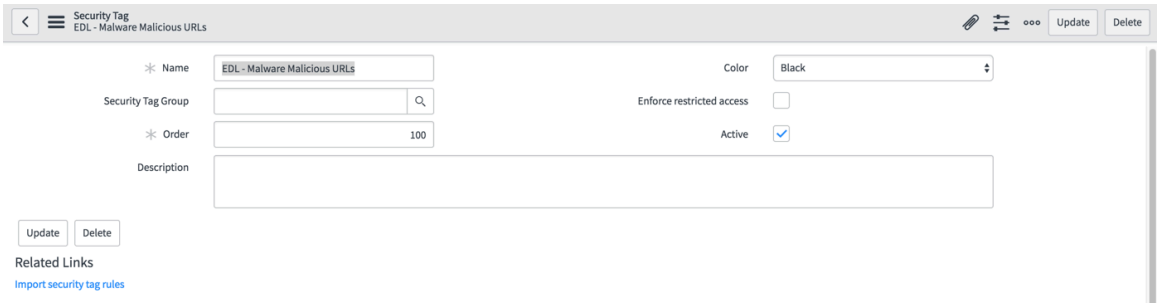
3. Clique no ícone de informações (ⓘ ao lado de **Marcador EDL para observáveis** em seguida **Abrir registro** .



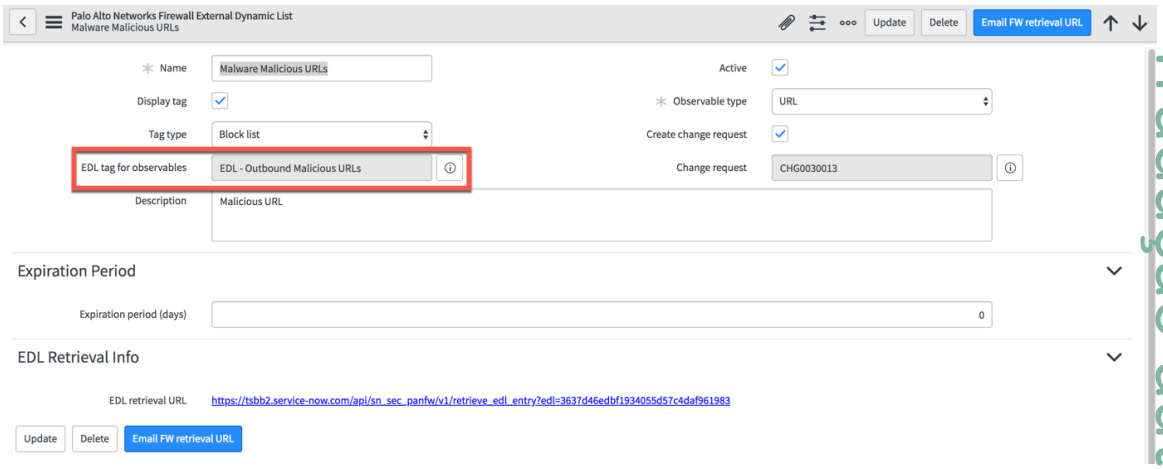
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

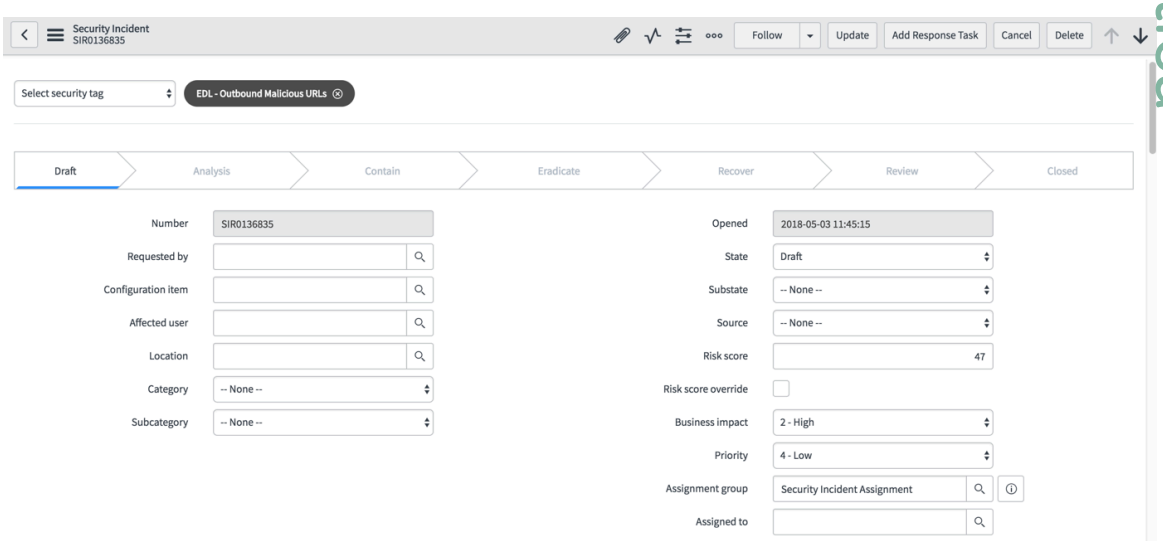
O formulário Marcador de segurança é exibido.



4. Em **Nome** modifique o nome do marcador de segurança e clique em **Atualização** .
   O registro EDL atualizado é exibido com o nome do marcador modificado. No exemplo a seguir, Saída foi adicionado ao nome do marcador. Mantenha EDL prefixo no novo nome do marcador para ajudar você a identificar se o marcador está associado ao Palo Alto Networks Next-Generation Firewall integração.



Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, Domínio) no registro de Incidente de segurança e no registro do observável sempre que o Observable é adicionado a um EDL.



Se um observável já tiver sido adicionado a um EDL e um marcador de segurança for exibido em um incidente de segurança para esse observável, o marcador de segurança EDL também será exibido automaticamente em todos os registros de incidente de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segurança subsequentes criados. Esta duplicação informa que o observável já está em uma lista de bloqueios. Não é necessário adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro de incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desativado de um EDL.

Desinstalar

Se você quiser desinstalar Palo Alto Networks Next-Generation Firewall do seu ServiceNow AI Platform e remover todos os remanescentes da integração, consulte ServiceNow site de documentação para obter instruções sobre como desinstalar aplicações.

Antes de Iniciar

Função necessária: Administrador do sistema (administrador)

Consulte Desinstalar aplicações no Site de documentação do produto da ServiceNow .

PhishTank integração

PhishTank é um sistema de verificação de phishing baseado na comunidade para o qual os usuários enviam ameaças suspeitas e outros usuários no sistema votam para determinar se as ameaças de phishing são legítimas. Quando integrado ao ServiceNow AI Platform Operações de segurança os resultados da inteligência contra ameaças fornecem aos analistas informações adicionais sobre incidentes ou investigações de segurança relacionados a phishing.

. PhishTank A integração executa pesquisas em URLs de sites de phishing em potencial.

O fluxo de trabalho verifica se há novos observáveis conforme eles chegam em incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração de API, os observáveis serão avaliados. Observáveis determinados como mal-intencionados são marcados.

Instalar e configurar PhishTank

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para PhishTank a aplicação se integra corretamente com ServiceNow AI Platform Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tarefas de configuração	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O Administrador do sistema (admin) instala o app e atribui a função de Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	a configuração e verifica os resultados esperados. Esta função também tem acesso ao Operações de segurança módulo.
Obtenha uma chave de API.	Visite PhishTank Site para obter informações sobre chaves de API e para criar uma conta: Site do PhishTank .
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Madrid e versões posteriores Para a versão Madrid e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

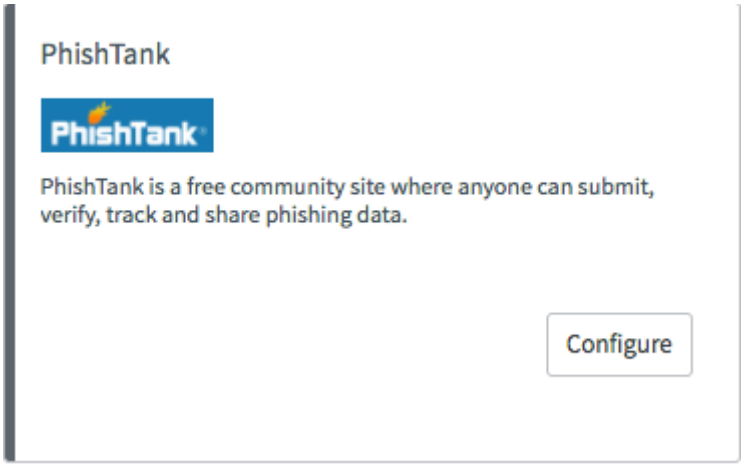
Função necessária: administrador

Procedimento

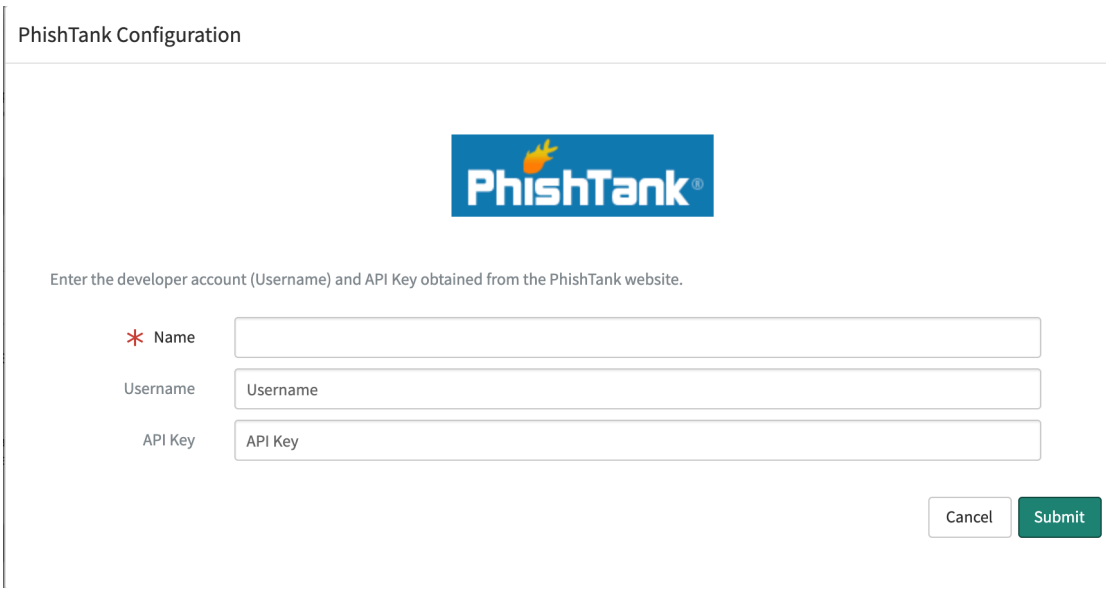
1. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize PhishTank lado a lado.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Em **Configuração do PhishTank** , insira o Nome da configuração, o Nome de usuário (conta de desenvolvedor criada no PhishTank) e a chave de API que você obteve do PhishTank site e clique **Enviar** .



5. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, o PhishTank A chave de API pode ser inválida.

Verifique os resultados esperados para PhishTank

Observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados da pesquisa são exibidos na guia Resultados da pesquisa de ameaças na parte inferior do registro de incidente de segurança.

Antes de Iniciar

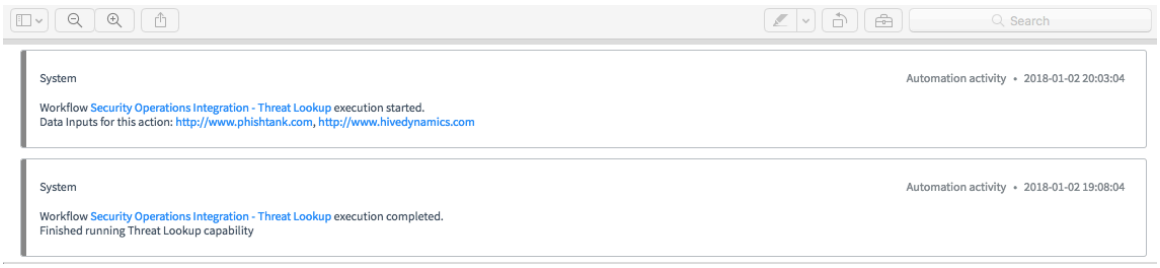
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o formulário de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

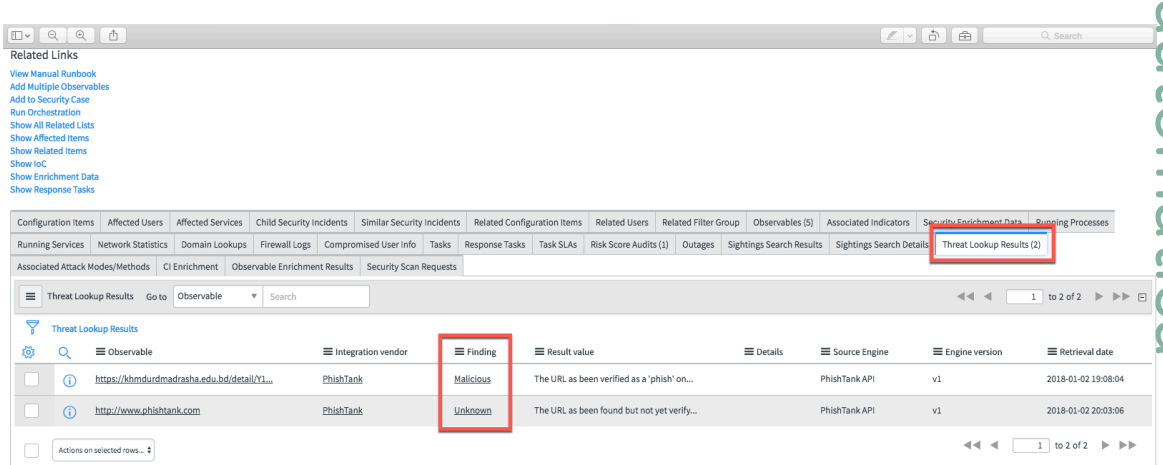


   Depois que a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro de incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

3. Navegue até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas** link relacionado.

   Nota: As figuras nas etapas a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito da moldura da faixa, clique no ícone de engrenagem Configurações. Em **Configurações do sistema** caixa de diálogo exibida, clique em **Formulários** e verifique isso **Formulários com guias** e. **Com o formulário** selecionados.



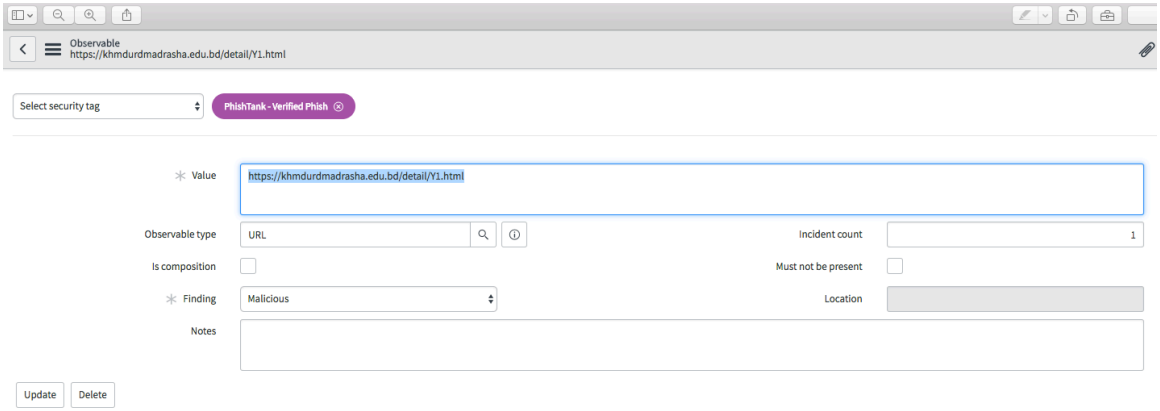
   . **Resultados da pesquisa de ameaças** a guia na parte inferior do registro de incidente de segurança exibe os resultados da pesquisa.

   . **Descoberta** a coluna é exibida Desconhecido para registros não determinados como mal-intencionados. Para resultados correspondentes a mal-intencionados, Mal-intencionado é exibido em **Descoberta** coluna.

4. Em **Observável** , clique em um observável para abrir um registro e exibir mais informações.

Tradução automática

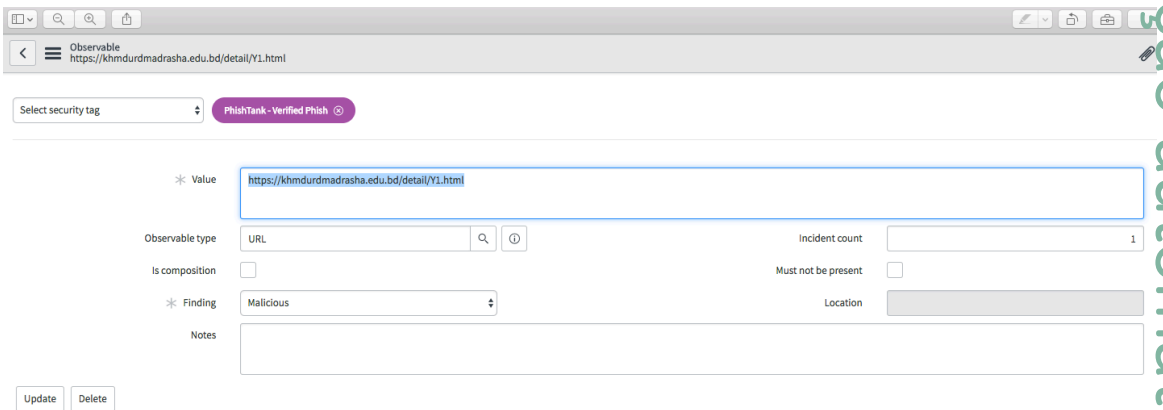
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



No registro observável, para pesquisas correspondentes a mal-intencionadas, Mal-intencionado é exibido **Descoberta** campo. O observável é marcado com Inteligência contra ameaças origem que descobriu que era mal-intencionado, neste caso, o. PhishTank aplicação.

5. Para exibir dados brutos, navegue de volta para o incidente de segurança e clique no ícone de informações azul ao lado de um observável.

6. Na janela exibida, clique em **Registro em aberto** .



O link criado pela API e pelo **Descoberta** campo exibido com os resultados.

Tradução automática

Trouble?

Se você não vir resultados em **Resultados da pesquisa de ameaças** verifique se o observável é um tipo compatível com pesquisa pela integração.

(Opcional) Anexar manualmente um observável para PhishTank

Você pode anexar manualmente observáveis a um incidente de segurança. Anexe observáveis manualmente quando quiser executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

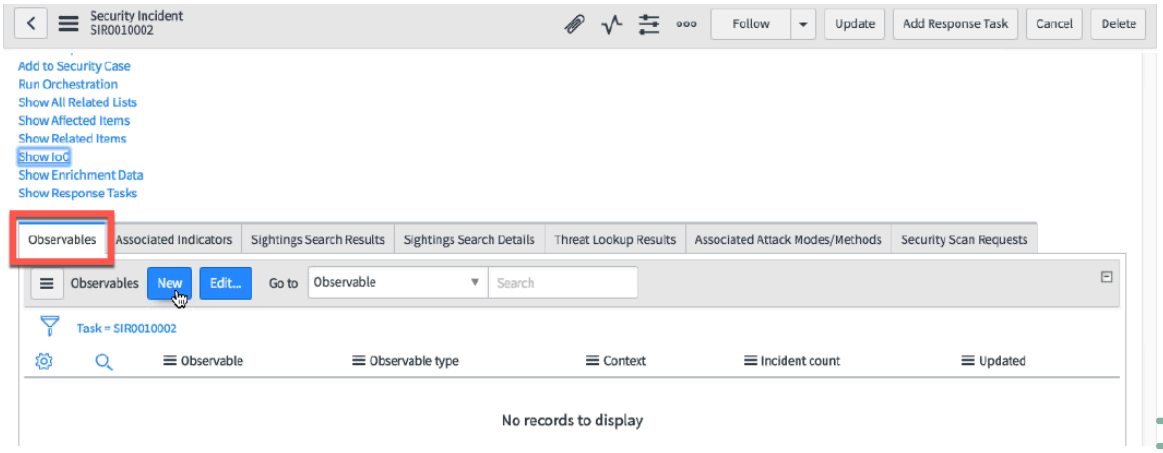
Antes de Iniciar

Função necessária: sn_si.analyst

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

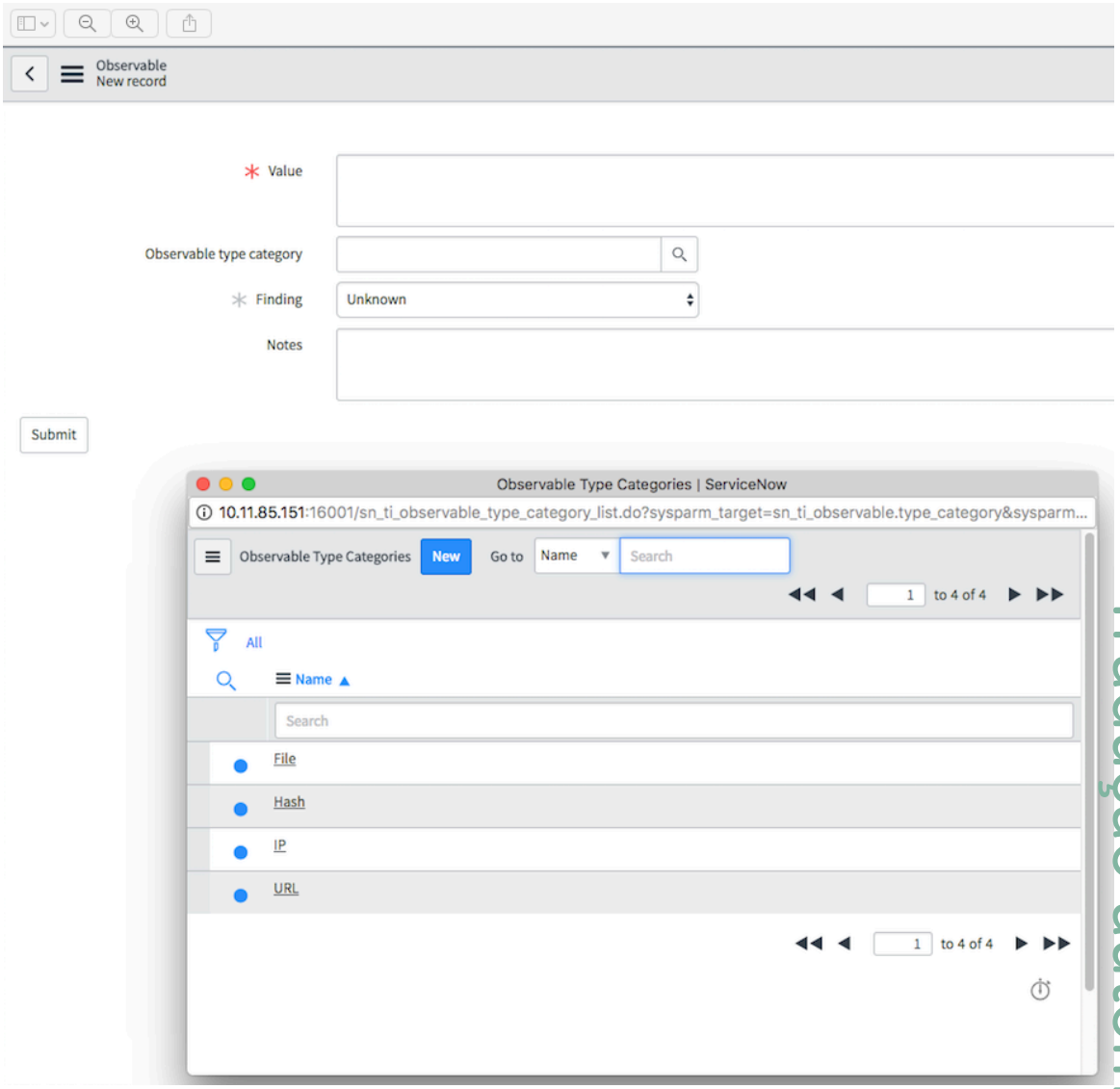
1. Navegue até o incidente de segurança em aberto.
2. No registro de incidente de segurança em aberto, clique em **Mostrar IOC** link em **Links relacionados** para exibir o. **Observáveis** guia.



3. Clique em **Nova**.
   O formulário Observável é exibido.
4. Em **Valor** , insira uma URL.
5. Clique no ícone de pesquisa e no **Categorias de tipo de observável** caixa de diálogo, clique em **URL** na lista para preencher o campo.

Tradução automática

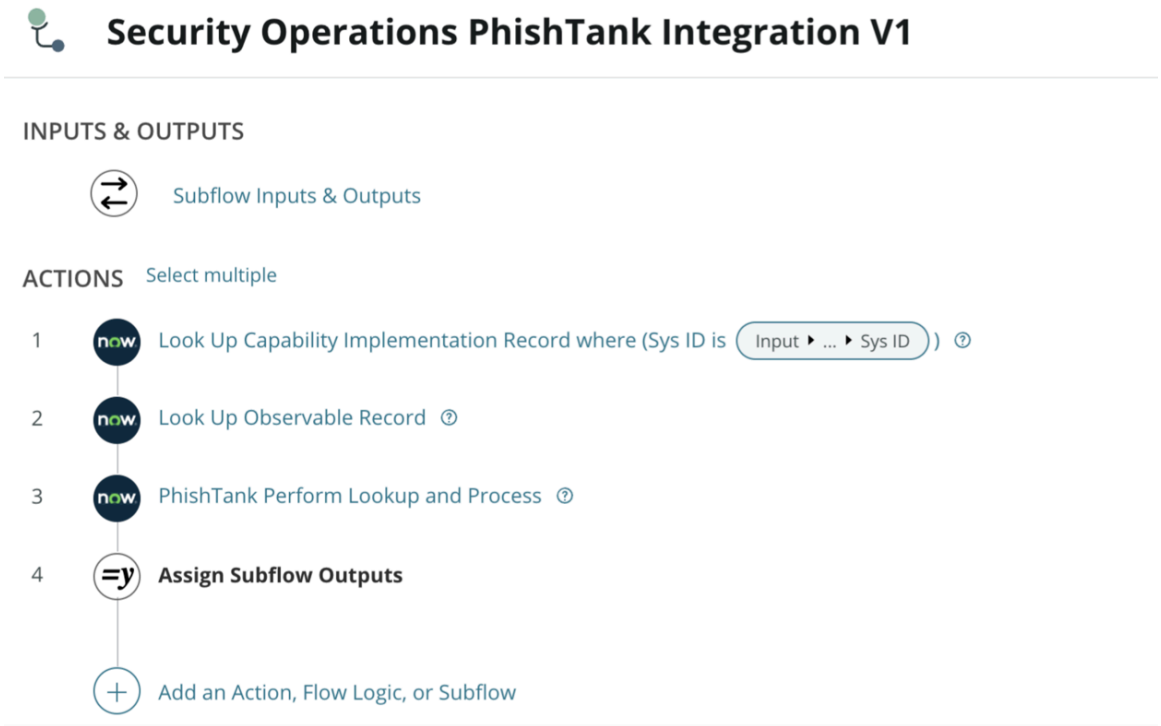
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



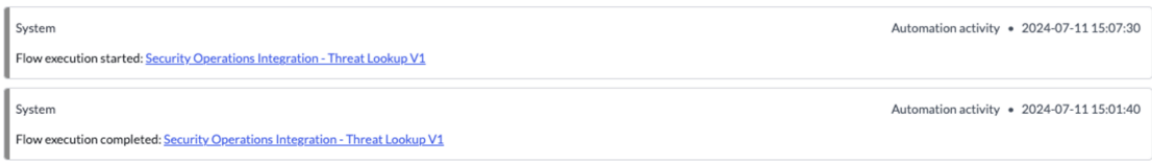
6. Clique em **Enviar**.
   O fluxo é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção Anotações de trabalho no registro de Incidente de segurança.

Tradução automática

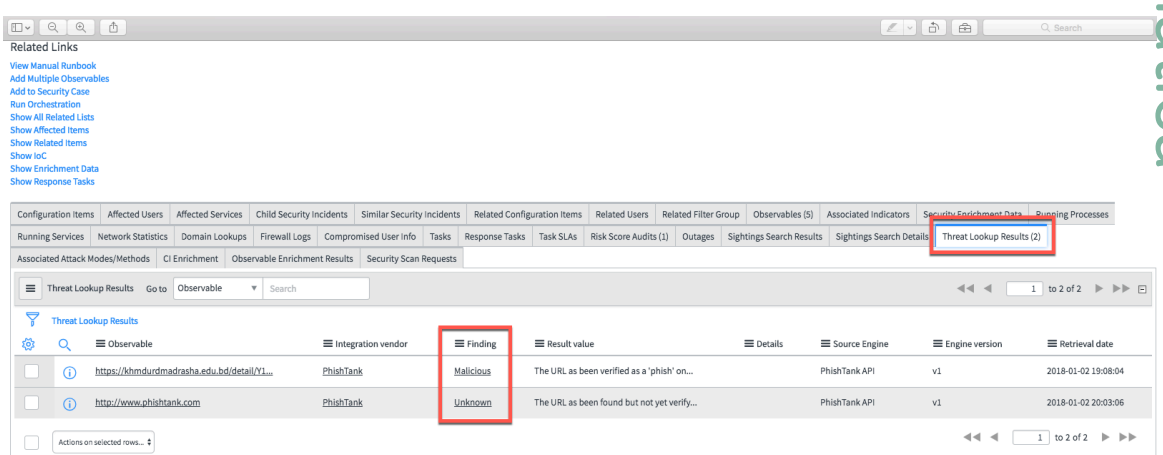
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Navegue até o incidente de segurança e revise as anotações de trabalho.



8. Clique em **Mostrar todas as listas relacionadas** link relacionado na parte inferior do incidente de segurança.
9. Clique em **Resultados da pesquisa de ameaças** para exibir os resultados.



10. Em **Observável** , clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.

11. Na caixa de diálogo exibida, clique em **Registro em aberto** .

Tradução automática

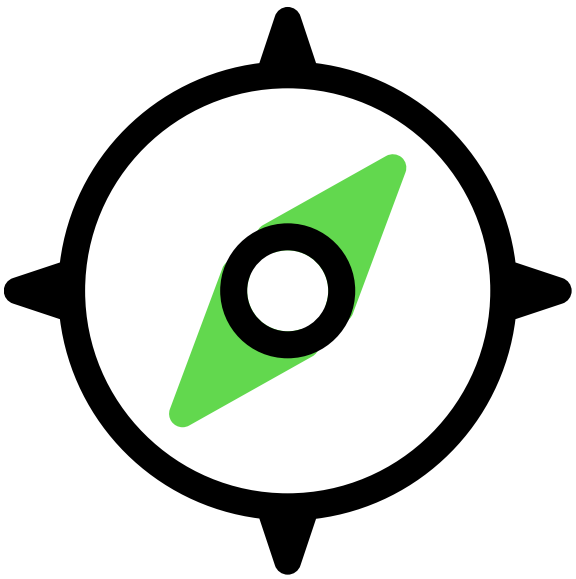
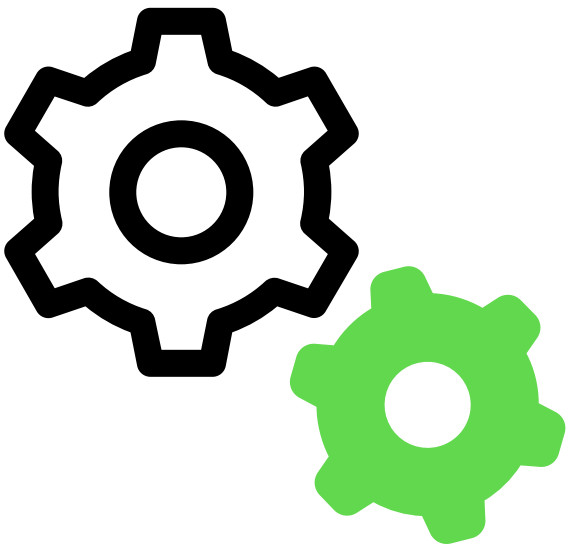
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Proofpoint Integração para Operações de segurança

. Proofpoint A integração DO SIR oferece suporte à ingestão de eventos do Proofpoint. O SIR cria um incidente para cada evento ingerido no qual os analistas podem revisar ou trabalhar.

Iniciar

Explorar	Configurar
	
Saiba mais sobre Proofpoint integração	Configurar Proofpoint Para o Espaço SIR

Tradução automática

Explorar o. Proofpoint Integração para Operações de segurança

Você pode configurar perfis de evento no SIR para ingerir eventos do Proofpoint. O SIR cria um incidente para cada evento ingerido no qual os analistas podem revisar ou trabalhar.

Proofpoint Integração para Operações de segurança usuários

Usuários

Usuário	Descrição
Administrador de segurança	Crie perfis de evento para filtrar os eventos ingeridos. O SIR cria incidentes para esses eventos ingeridos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proofpoint Integração para Operações de segurança benefícios

Proofpoint Integração para Operações de segurança benefícios

Benefício	Recurso	Usuários
Extraia dados do evento para sua instância e crie incidentes de segurança. Revise incidentes de segurança de um único local em busca de eventos considerados suspeitos ou mal-intencionados.	Se as mensagens de e-mail entregues e os cliques permitidos forem considerados mal-intencionados posteriormente, é provável que essas mensagens tenham sido abertas e interagidas por seus funcionários. Para rastrear essas mensagens para revisão, crie automaticamente incidentes de segurança com base nos perfis de evento que você cria e configura para o tráfego de mensagens da integração. Além disso, você também pode habilitar a criação de incidentes de segurança para as mensagens bloqueadas e cliques para fins de auditoria.	Gerentes

Tradução automática

O que explorar a seguir

Para saber mais sobre como configurar e usar o Proofpoint, consulte:

- Configurando o. Proofpoint Integração para Operações de segurança
- Revise as configurações de integração do Proofpoint
- Exiba Proofpoint Painel de análise

Configurando o. Proofpoint Integração para Operações de segurança

Configure sua implementação do Proofpoint Integração para Operações de segurança .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da configuração

1. Instale e configure o. Proofpoint Integração.

   Baixe, instale e ative a aplicação de integração.

2. Crie um perfil de evento para Proofpoint Integração para Operações de segurança.

   Crie um perfil de evento para identificar os eventos que você deseja importar do Proofpoint e as condições que você deseja usar para criar incidentes de segurança a partir dos dados importados.

3. Configurando o. Proofpoint Integração para Operações de segurança

   Revise as configurações de integração para criar os perfis de evento.

Instale e configure o. Proofpoint Integração

Instale e configure o. Proofpoint Integração para Operações de segurança aplicação do ServiceNow® Store em seu ServiceNow AI Platform instância.

Antes de Iniciar
Função necessária: sn_si_admin

Procedimento

1. Baixe o. Proofpoint Integração para Operações de segurança aplicação do ServiceNow® Store e instale-o. Para obter mais informações, consulte Instale uma aplicação da ServiceNow Store .
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Localize Proofpoint Integração para Operações de segurança lado a lado e selecione **Configurar** .
4. No formulário, preencha os campos.

Proofpoint Formulário Configuração de integração

Campo	Descrição
Nome	Nome do Proofpoint Integração para configuração de Operações de segurança.
Principal do serviço	Nome de usuário de Proofpoint locatário.
Segredo	O ID de Proofpoint locatário.

5. Selecione **Enviar**.

Resultado
Depois de validar e enviar a configuração com êxito, a integração será salva na página Integrações de segurança como um bloco.

Crie um perfil de evento para Proofpoint Integração para Operações de segurança

Crie um perfil de evento para identificar os eventos que você deseja importar do Proofpoint produto.

Por Que e Quando Desempenhar Esta Tarefa
Você cria um perfil de evento configurando tipos de evento, mapeamentos e cronogramas de importação. Uma barra de andamento na página exibe todas as etapas e é realçada para a configuração ativa no momento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Navegar até **Tudo** > **Integração do SIR com a Proofpoint** > **Perfil de eventos da Proofpoint**.
2. Na página Perfis de eventos, selecione **Novo** .
3. No formulário, preencha os campos.

   A barra de andamento é exibida começando com Nome.

Formulário de perfil do Proofpoint

Campo	Descrição
Nome	Nome do perfil do evento. Considere usar um nome que inclua o tipo de evento associado: ○ Cliques bloqueados ○ Cliques permitidos ○ Mensagens bloqueadas ○ Mensagens entregues
Origem	A origem configurada para a integração na página Configurações de integração.
Ordem	A ordem na qual este perfil é executado. O valor padrão é 100.
Ativo	Opção para ativar o perfil.
Descrição	Descrição opcional deste perfil de evento.

4. Selecione **Continuar**.
5. Escolha um ou mais tipos de evento movendo-os do **Disponível** coluna para **Selecionado** coluna.
   Os tipos de evento disponíveis são:
   - Cliques bloqueados
   - Cliques permitidos
   - Mensagens bloqueadas
   - Mensagens entregues
6. Selecione **Continuar**.

   As etapas de configuração relacionadas ao tipo ou tipos de evento selecionados são exibidas na barra de andamento.

   Os valores dos Campos de origem são fornecidos a partir dos dados de proteção contra ataque direcionado (TAP) em seu ambiente como referência.

   O mapeamento padrão dos dados dos campos de origem para os campos de destino é exibido na página. Os dados básicos são incluídos como guia, mas você pode modificar esse mapeamento.
7. **Opcional:** Selecione **f(x)** ícone para exibir as traduções padrão incluídas com a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Vários valores de um campo são separados por vírgulas.

8. Selecione **Continuar**.
9. Na página Filtragem e agregações, configure as propriedades na tabela a seguir.

Propriedades de filtragem e agregação

Opção	Descrição
Filtrar com base nas condições de eventos de mensagem	Opção para habilitar a filtragem com base em eventos de mensagem.
Condições do filtro de eventos de mensagem	Condições do filtro de evento de mensagem.
Filtrar com base nas condições de eventos de clique	Opção para habilitar a filtragem com base em eventos de clique.
Condições do filtro de eventos de clique	Clique em Condições de filtro de evento.
Condições de Agregação	Opção para permitir que um incidente de entrada seja anexado a um incidente de segurança aberto em vez de criar um novo.
Campos de incidente com valores correspondentes	Adicione Resposta a incidentes de segurança campos cujos valores devem ser correspondidos para que um incidente seja incluído em uma agregação.
Anotação de trabalho de log para o novo incidente	Opção para permitir que as anotações de trabalho sejam registradas no primário Resposta a incidentes de segurança.
Habilitar relação ThreatID	Opção para habilitar a agregação de todos os incidentes que têm ThreatIDs correspondentes.

10. Selecione **Continuar**.
11. Selecione um dos tipos de importação e a frequência com que você deseja importar dados de evento.

Opção	Descrição
Ingestão de eventos contínuos	Opção para importar eventos em um intervalo regular definido com uma data de início, uma data de término e o intervalo de pesquisa em minutos. ○ **Incremento de pesquisa (minutos)** Intervalo em minutos entre importações ○ **Definir tempo de ingestão de eventos inicial** ○ **Tempo de ingestão inicial de entrada**
Recuperação única	Opção para importar eventos somente uma vez com base na data configurada. Todos os eventos da data selecionada são importados. Forneça uma data de início para a importação do evento (**Desde a data**).

12. Selecione **Concluir**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado
O perfil de evento recém-criado é incluído na lista de perfis de evento existentes na página Perfis de eventos.

Revise as configurações de integração do Proofpoint

Revise as configurações de integração do Proofpoint para modificar as propriedades do sistema do seu ambiente.

Antes de Iniciar
Função necessária: sn_si_admin

Procedimento

1. Navegar até **Tudo** > **Integração do SIR com a Proofpoint** > **Configurações de integração com a Proofpoint**.
2. Modifique as seguintes configurações.

Configurações de integração com a Proofpoint

Nome da Propriedade	Descrição
Tempo limite para as chamadas de restAPI. sn_sec_proofpoint.http_timeout	O tempo limite (em segundos) para buscar dados das chamadas de api. Tipo: Número Inteiro Valor padrão: 3000
Nível de registro em log: depurar, informativo, aviso, erro sn_sec_proofpoint.logging_verbosity	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você pode atualizar o valor para as seguintes opções: ○ erro ○ aviso ○ informações ○ depurar Valor padrão: Não
Impõe um limite ao número de eventos da Proofpoint que podem ser agregados a um único incidente. sn_sec_proofpoint.max_aggregations_per_si	O número máximo de eventos de Proofpoint que podem ser agregados a um incidente. Tipo: Número Inteiro Valor padrão: 100
Imponha um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_proofpoint.max_si_per_day	O número máximo de incidentes que podem ser criados em 24 horas. Tipo: Número Inteiro Valor padrão: 1000
Número de dias, precisamos usar na chamada de api para os principais clicadores, vap. sn_sec_proofpoint.default_days	O número de dias de dados a serem obtidos para os principais clicadores e VAP. Você também pode atualizar o valor para as seguintes opções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
	○ 14 ○ 30 ○ 90 Tipo: Número Inteiro Valor padrão: 90
Sinalizador booliano, se habilitado, ele faz uma chamada de api e preenche os detalhes dos Topclickers. sn_sec_proofpoint.call_topclickers_api	Ative a opção para habilitar e buscar os principais dados do clicker. Tipo: booleano Valor padrão: Verdadeiro
Sinalizador booliano, se habilitado, ele faz uma chamada de api e preenche os detalhes do VAP. sn_sec_proofpoint.call_vap_api	Ative a opção para habilitar e buscar dados do VAP. Tipo: booleano Valor padrão: falso
Restringir o número máximo de usuários a serem exibidos para usuários do TopClickers e do VAP. sn_sec_proofpoint.maxresults	O número máximo de usuários a serem exibidos para os principais clicadores e usuários do VAP. Tipo: Número Inteiro Valor padrão: 100
Habilita/desabilita o uso do período de sobreposição durante a pesquisa programada de eventos do Proofpoint. sn_sec_proofpoint.allow_overlap	Habilite ou desabilite o período de sobreposição quando a pesquisa programada estiver configurada. Tipo: booleano Valor padrão: falso
Tempo de sobreposição em minutos a ser usado durante a pesquisa programada de ProofpointEvents quando a sobreposição estiver habilitada. sn_sec_proofpoint.overlap_time	O tempo de sobreposição em minutos quando a pesquisa programada é configurada. Tipo: Número Inteiro Valor padrão: 5

3. Selecione **Save** (Salvar).

Resultado
Define as configurações de integração com novos valores.

Exiba Proofpoint Painel de análise

. Proofpoint O painel de análise fornece detalhes sobre os usuários do VAP e os principais clicadores.

Por Que e Quando Desempenhar Esta Tarefa
Os usuários mais visados por ataques à segurança são considerados usuários do VAP. Os funcionários que clicam com frequência em links suspeitos e de phishing são considerados os principais clicadores.

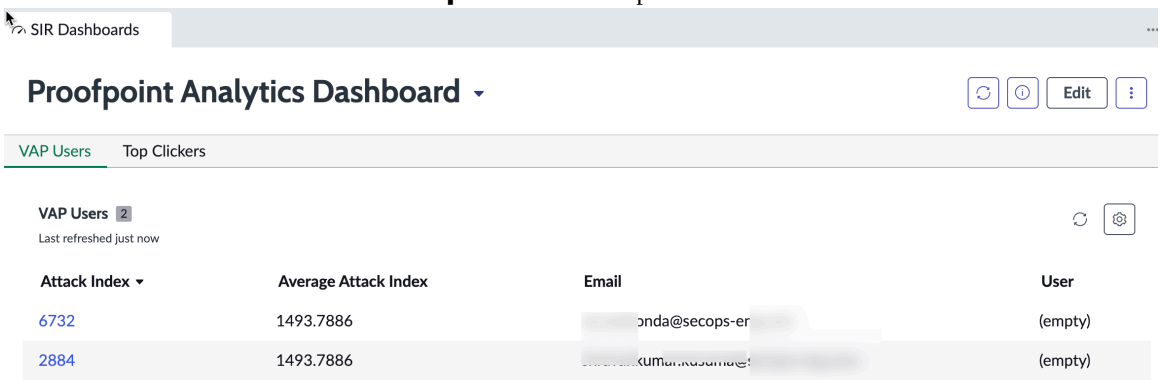
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si_admin

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione **Painéis DO SIR** .
3. Selecione **Painel de análise do Proofpoint** na lista suspensa.



4. Exibir informações sobre usuários do VAP.
   a. Exiba a lista de usuários do VAP selecionando **Usuários do VAP** guia.
   b. Exiba os detalhes de um usuário do VAP selecionando o nome de usuário.
5. Exibir informações sobre os principais clicadores.
   a. Para exibir a lista dos principais clicadores, selecione **Principais Clicadores** guia.
   b. Exiba os detalhes de um clicador superior selecionando o nome de usuário.

Reverse Whois integração

Reverse Whois é um serviço que executa pesquisas em nomes de domínio registrados por indivíduos ou organizações.

Execute pesquisas de domínio usando termos de pesquisa em observáveis que você anexa a um incidente de segurança. . Reverse Whois A API pesquisa registros de domínio com base nos termos de pesquisa inseridos e retorna todos os registros que correspondem a esses termos.

Às vezes, os analistas usam essa integração junto com o. Whois integração para pesquisa de incidentes de segurança. . Whois a integração fornece informações adicionais de aprimoramento com base nas pesquisas de domínio do Reverse Whois integração.

Instalar e configurar Reverse Whois

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para Reverse Whois a aplicação se integra corretamente ao Operações de segurança produto.

Antes de Iniciar
Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções obrigatórias da ServiceNow.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O Administrador do sistema (admin) instala o app e atribui a função de Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração. O administrador de incidentes de segurança também atribui a função Analista de incidentes de segurança (sn_si.analyst). • O analista de incidentes de segurança (sn_si.analyst) executa pesquisas de domínio com Reverse Whois e analisa e trabalha com incidentes de segurança.
Obtenha uma chave de API.	Visite o site da API WhoisXML para obter informações sobre chaves de API e criar uma conta: Site da API WhoisXML . A configuração requer que você insira as chaves de API.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Madrid e versões posteriores Para a versão Madrid e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform

Tradução automática

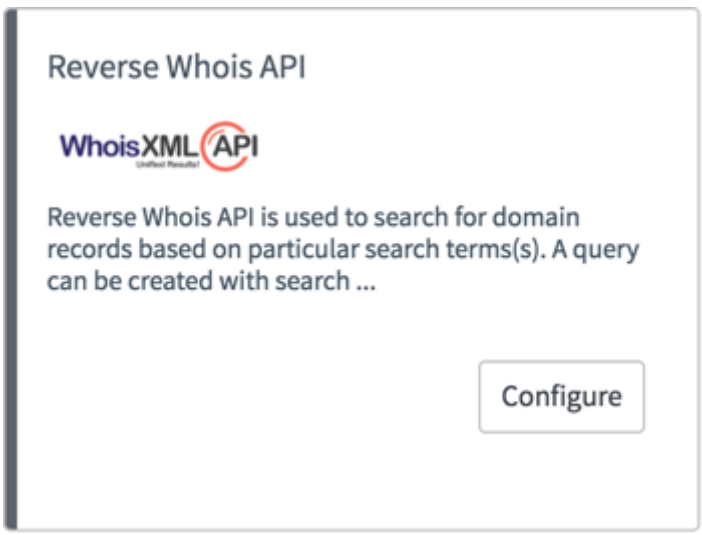
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Função necessária: administrador

Procedimento

1. Se você já instalou e configurou o. Reverse Whois, siga estas etapas:
   a. Exclua a configuração existente.
   b. Instale e crie uma nova configuração usando a chave de API que você obteve.
2. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
3. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize Reverse Whois Bloco de API.
4. Clique em **Configurar**.



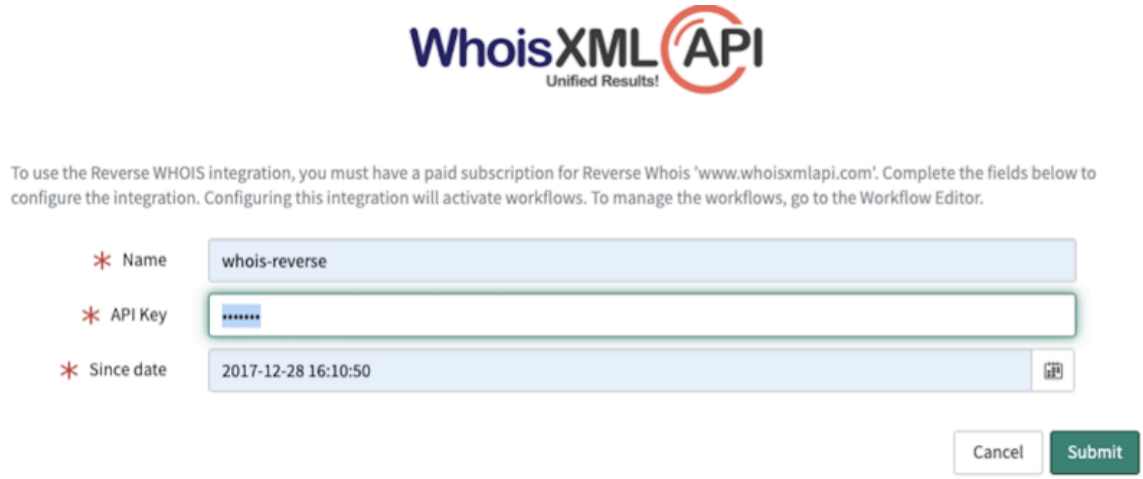
5. Em **Configuração da API Whois reversa** , insira a chave de API que você obteve do Whois Site da API XML.
6. Escolha uma opção na tabela a seguir para filtrar pesquisas de domínio para seus termos de pesquisa.

Descrição	Configuração
Sua pesquisa inclui todos os domínios, ativos e expirados, que foram registrados após a data Desde para os termos de pesquisa inseridos. Esta é a configuração recomendada.	**Desde a data** : Data inserida no formato aaaa-mm-dd. Por exemplo, 1991-06-01 Para 1 de junho de 1991.
Sua pesquisa inclui todos os domínios ativos para os termos de pesquisa inseridos.	**Desde a data** : Campo limpo.

Essas definições de configuração permanecem salvas até que você as altere e se aplique a todas Reverse Whois Pesquisas de API.

Tradução automática

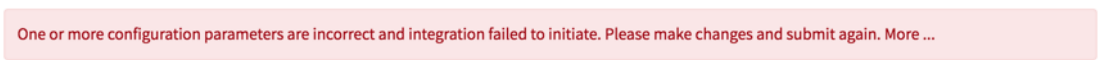
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

Trouble?
Se uma mensagem de erro for exibida, a chave de API poderá ser inválida.

Mensagem de erro



(Opcional) Instale e configure Whois

Instale o. Whois plug-in para fornecer informações adicionais de aprimoramento em suas pesquisas de domínio do Reverse Whois API. Esta pesquisa fornece dados de aprimoramento adicionais no domínio, como data de registro, nome do registrador e país de origem.

Antes de Iniciar

1. Se você não solicitou direito para a aplicação, consulte Obtenha direito para um Operações de segurança produto ou aplicação para Whois Aplicação da ServiceNow Store.
2. Obtenha credenciais para Whois Chave de API do site do produto: Site da API WHOIS .

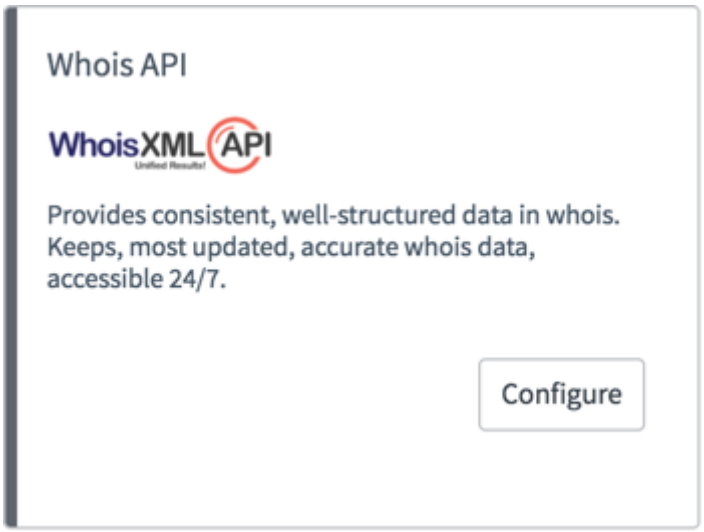
Função necessária: administrador

Procedimento

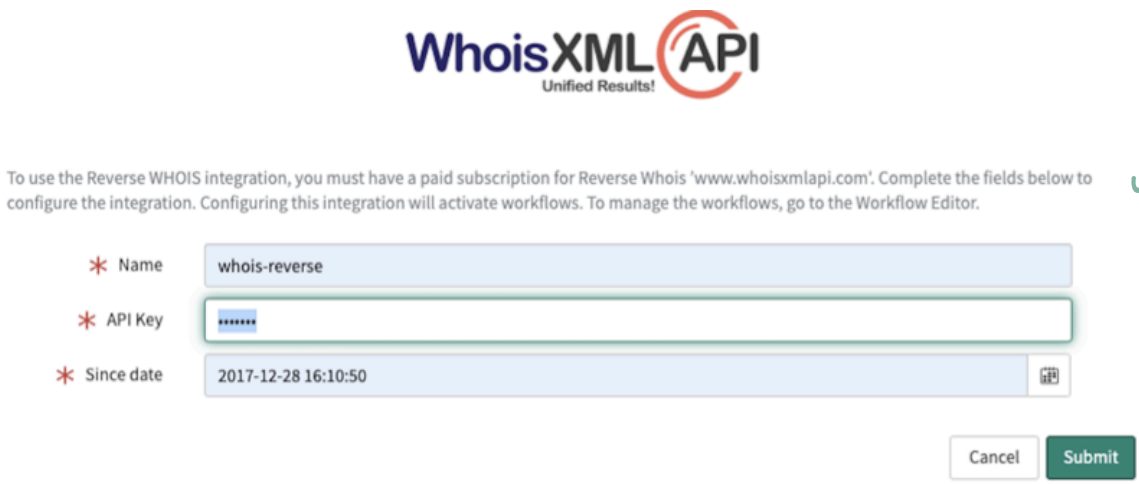
1. Se você não instalou o aplicativo, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize Whois Bloco de API.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



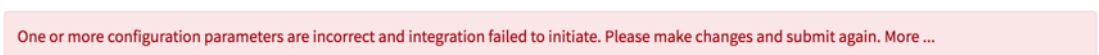
4. Em **Configuração da API WHOIS** Insira a chave de API obtida no site do produto.



5. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Agora você pode executar pesquisas de aprimoramento nos domínios retornados do Reverse Whois integração.

Trouble?
Se uma mensagem de erro for exibida, a chave de API poderá ser inválida.

Solução de problemas



Iniciar pesquisa de Reverse Whois

Inicie pesquisas de domínio usando termos de pesquisa em observáveis que você anexa manualmente a um registro de incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

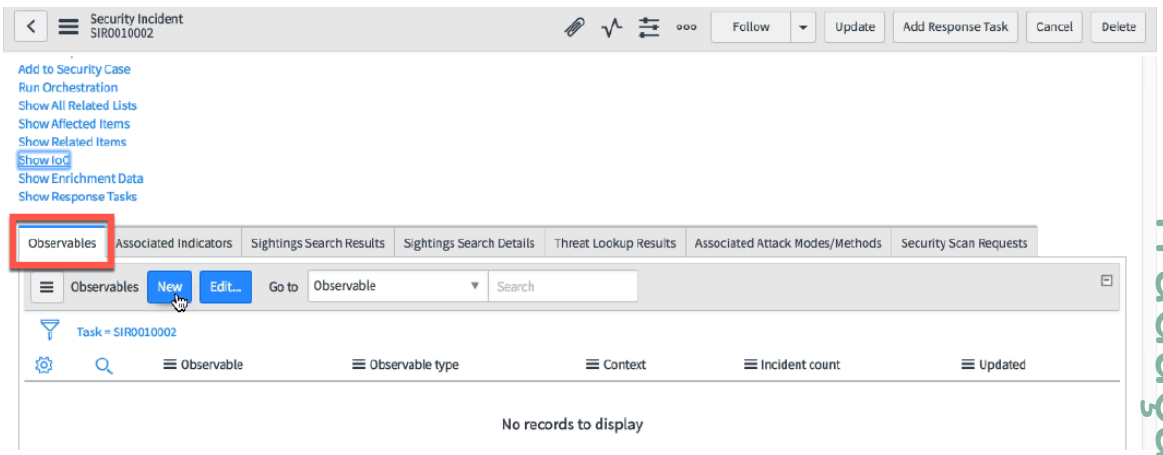
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se não estiver aberto, navegue até **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes** e abra o incidente de segurança com o qual você está trabalhando.
2. Na parte inferior do registro, clique em **Mostrar IOC** Link relacionado para exibir a guia Observáveis.

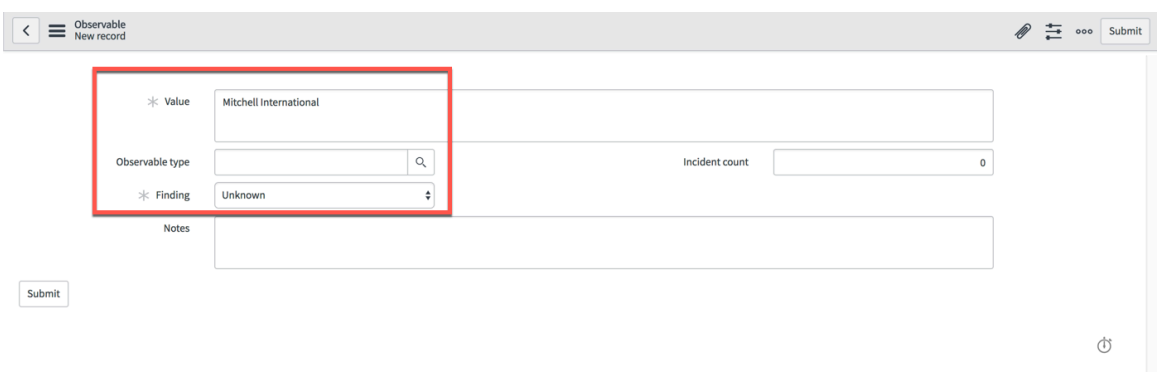
> **Nota:** As figuras nas etapas a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema. Se você não vir guias no incidente de segurança, no canto superior direito do quadro da faixa, clique em **Configurações** ícone de engrenagem. Em **Configurações do sistema** caixa de diálogo exibida, clique em **Formulários** e verifique isso **Formulários com guias** e. **Com o formulário** selecionados.



3. Na guia Observáveis, clique em **Novo** .
4. Preencha os campos.

Campos obrigatórios no novo registro

Campo	Descrição
Valor	Termo de pesquisa exclusivo para um domínio.
Tipo de observável	Este campo é limpo automaticamente.
Descoberta	Este campo é definido automaticamente como **Desconhecido** .



5. Clique em **Enviar**.
   Você retornará ao registro de incidente de segurança e o fluxo iniciará a pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Verifique os resultados da pesquisa no incidente de segurança. Consulte Verifique os resultados esperados para Reverse Whois.

Verifique os resultados esperados para Reverse Whois

Os resultados de aprimoramento são exibidos no **Domínios ReverseWhois** na parte inferior do registro de incidente de segurança. Localize os resultados da pesquisa para verificar se a pesquisa foi executada com sucesso.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Se ainda não estiver aberto, navegue até **Incidentes de segurança** > **incidentes** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando.

   Depois que a aplicação é configurada e você anexa um observável, o fluxo é iniciado automaticamente. As anotações de trabalho no registro de incidente de segurança exibem o status de execução e conclusão da pesquisa.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.

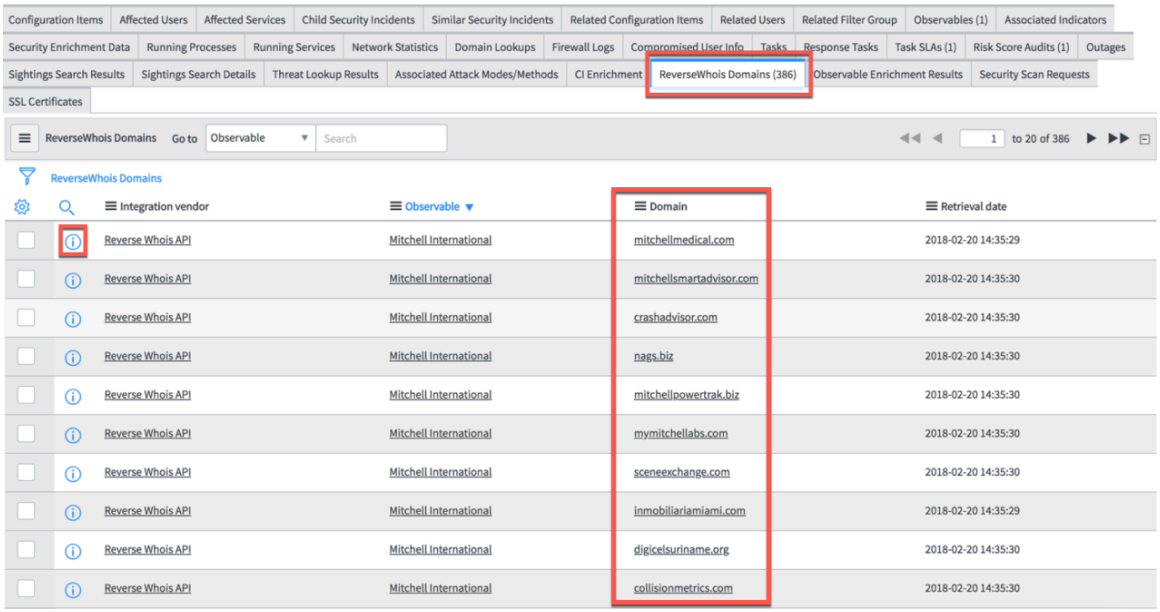
   

3. Navegue até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas** link relacionado.

   Nota: Para os resultados de pesquisa filtrados mostrados na figura a seguir, as definições de configuração no Reverse Whois O bloco de configuração da API foi salvo com **1991-06-01** inserido em **Desde a data** campo.

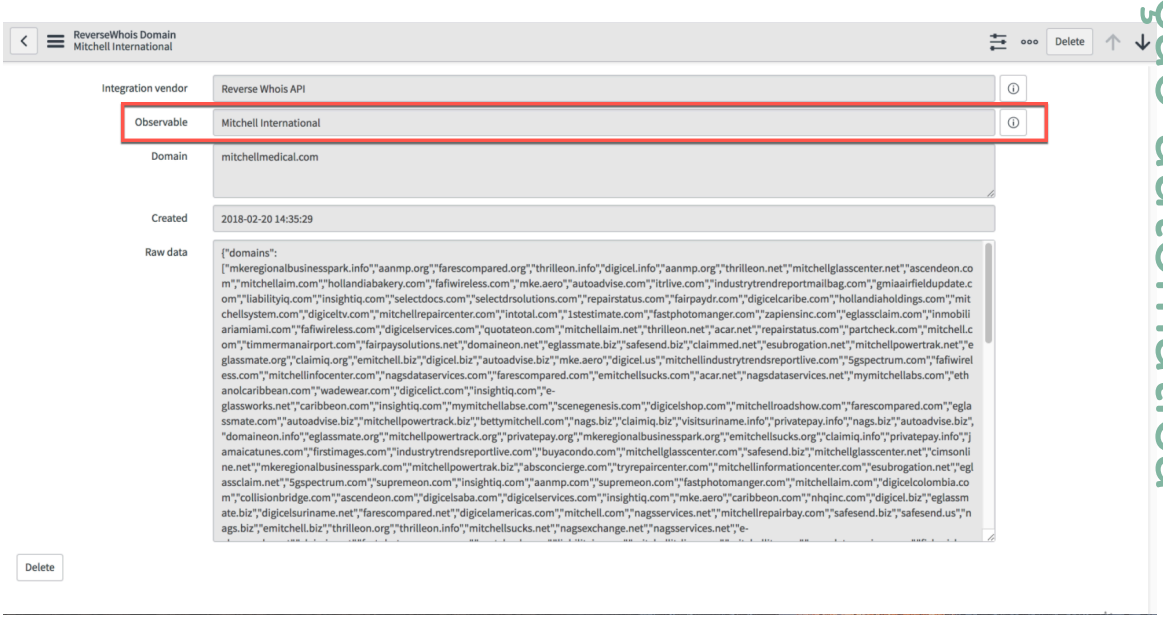
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados de aprimoramento são exibidos no **Domínios ReverseWhois** guia. Os domínios ativos para este observável são exibidos em **Domínio** coluna.

4. Clique no ícone azul de informações ao lado de um item e clique em **Abrir registro** na caixa de diálogo exibida.

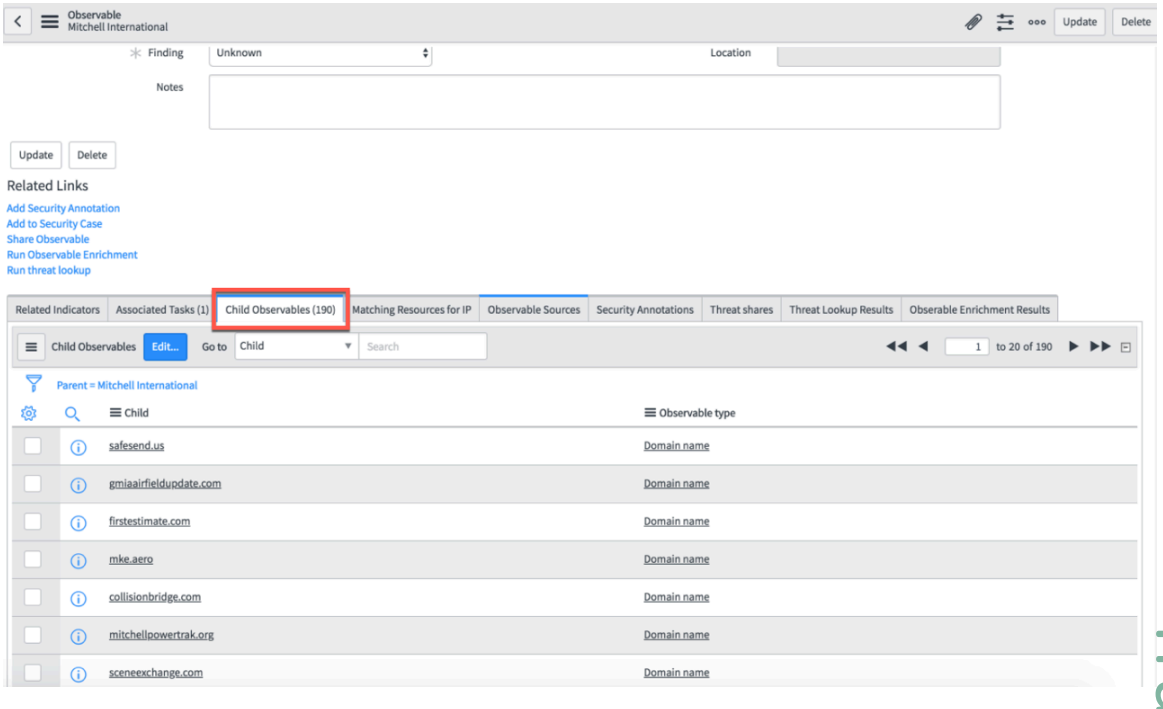


O registro é exibido com detalhes de aprimoramento, incluindo os dados brutos.

5. Navegue de volta para o incidente de segurança e com **Domínios ReverseWhois** selecionado, clique em um observável no **Observável** coluna para abrir um registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os observáveis secundários são exibidos no **Observáveis secundários** No registro do observável. Os observáveis secundários serão gerados somente se Reverse Whois a aplicação retornou domínios.

Trouble?

Se a pesquisa não for concluída com sucesso, verifique se os termos de pesquisa inseridos são compatíveis com a integração. Revise as anotações de trabalho para obter mais informações.

O que Fazer Depois

Para obter mais dados de aprimoramento nos resultados da pesquisa de domínio, você pode executar o. Whois integração para executar pesquisas de aprimoramento nos observáveis secundários retornados pelo Reverse Whois integração. Esses dados de aprimoramento nos observáveis secundários incluem informações sobre data de registro, nome do registrador e país de origem.

(Opcional) Execute a pesquisa de aprimoramento e verifique os resultados esperados para Whois

Execute o. Whois integração para executar pesquisas de aprimoramento nos domínios retornados do Reverse Whois integração.

Antes de Iniciar

Verifique se você instalou e configurou o. Reverse Whois e. Whois plug-ins. Execute essas etapas somente depois de executar a pesquisa de domínio com Reverse Whois plug-in bem-sucedido.

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

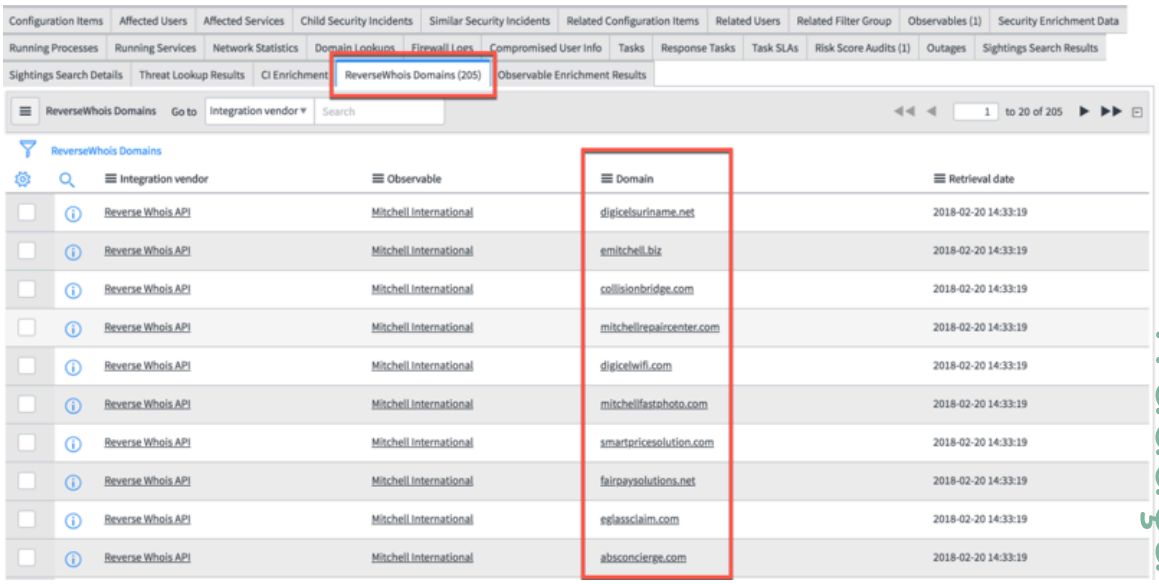
Os resultados são exibidos no **Resultados de aprimoramento do observável** No registro do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

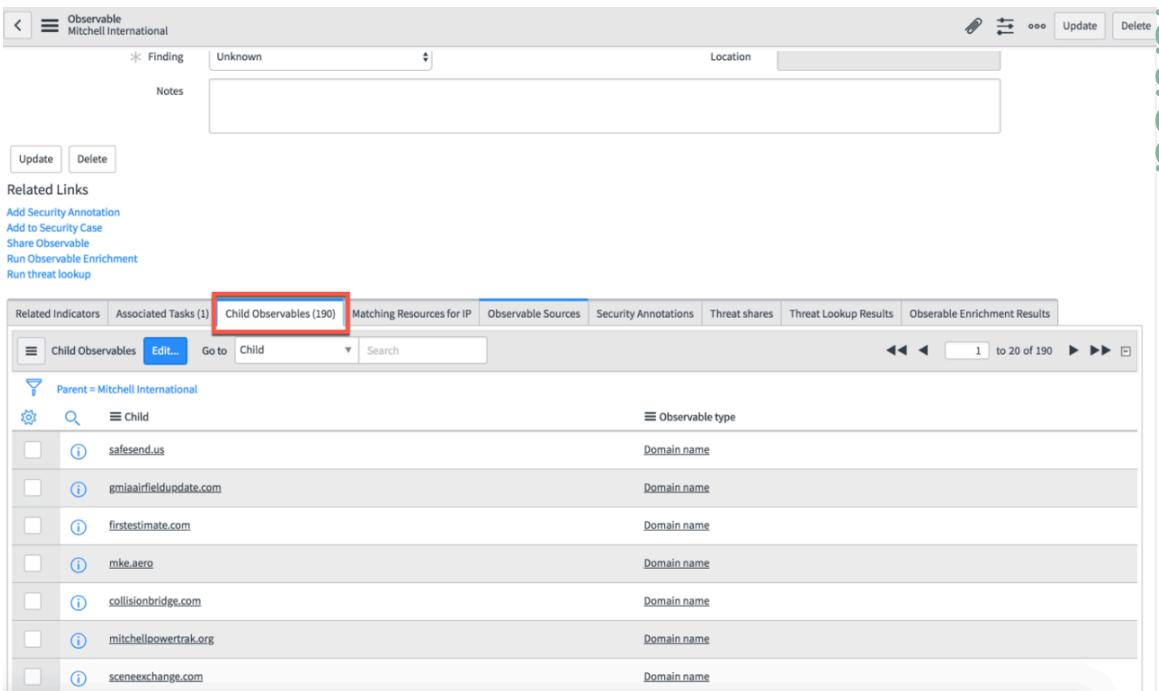
Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **incidentes** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando que executou a pesquisa de domínio com sucesso.
2. Abra o registro e clique em **Mostrar todas as listas relacionadas** link relacionado.
3. Selecione **Domínios Whois revertidos** na parte inferior do registro.



Em **Domínios** , a lista de domínios retornados é exibida.

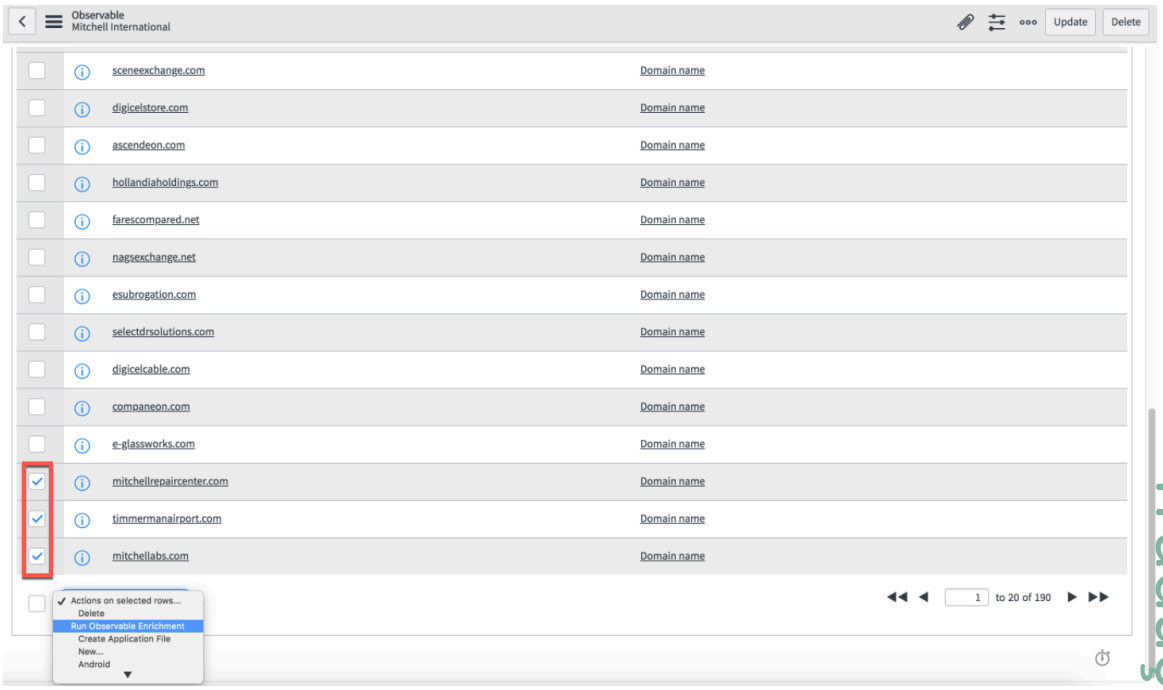
4. Em **Observável** , clique em um observável.
   Em **Observáveis secundários** os observáveis secundários são exibidos. Os observáveis secundários serão gerados somente se a verificação inicial do observável for feita pelo Reverse Whois domínios retornados pela aplicação.



Tradução automática

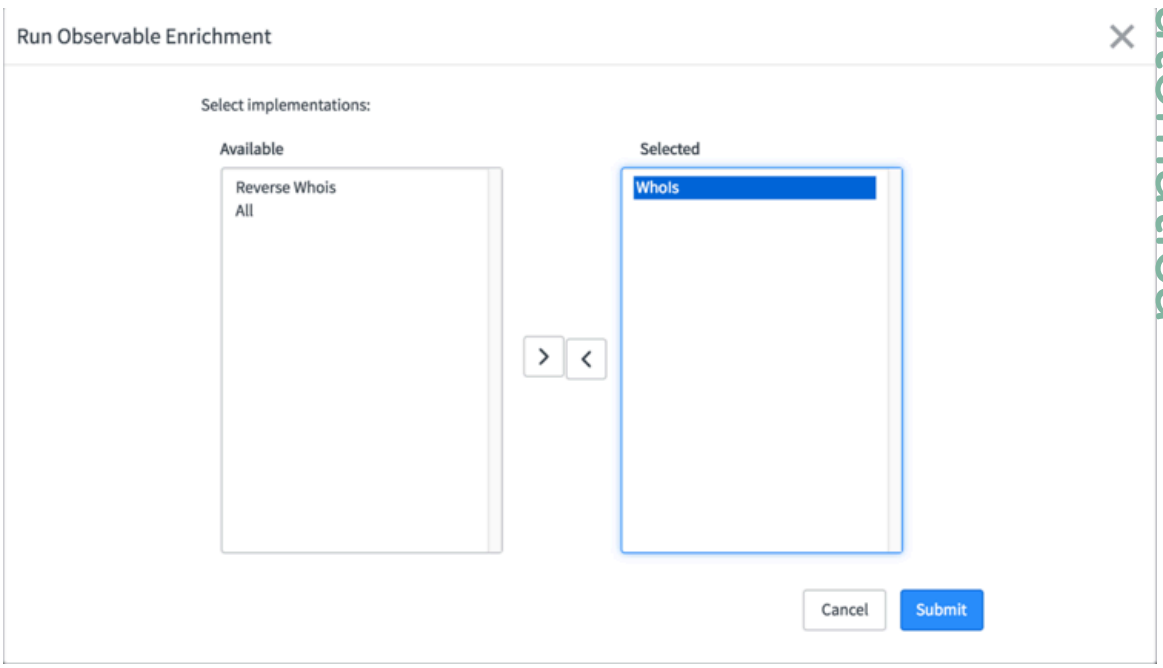
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os observáveis secundários nos quais você deseja executar o aprimoramento do observável, e, no **Ação nas linhas selecionadas** lista de seleção, selecione **Executar aprimoramento de observável** .



. **Executar aprimoramento de observável** a caixa de diálogo é exibida.

6. Mova o. Whois integração de **Disponível** . **Selecionado** e clique em **Enviar** .

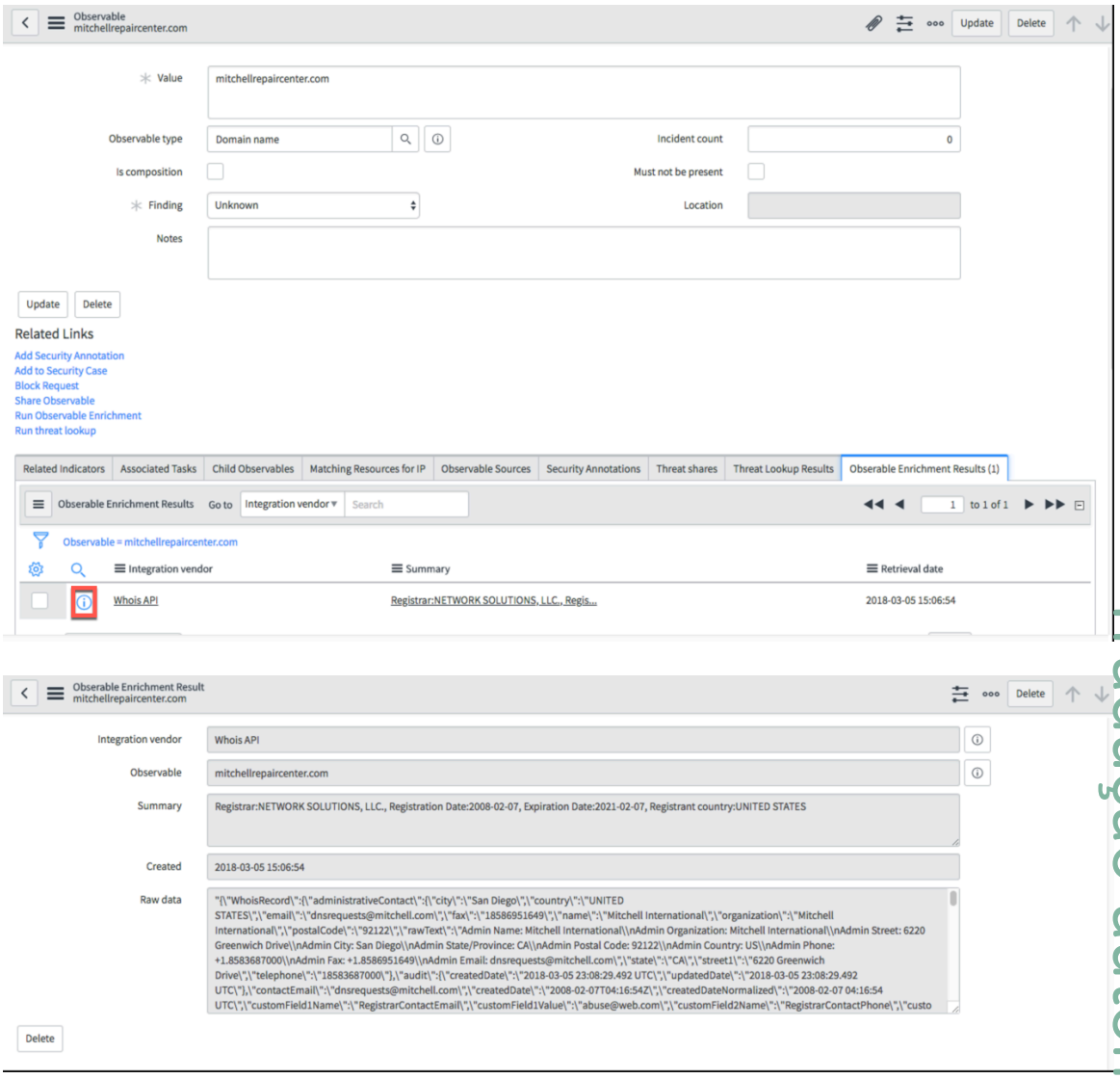


Os resultados são exibidos no **Resultados de aprimoramento do observável** do registro do observável.

7. Clique no ícone azul de informações e clique em **Registro em aberto** na caixa de diálogo exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Mais informações e dados brutos relacionados à pesquisa de domínio original são exibidos, como data de registro, nome do registrador e país de origem.

Trouble?
Se você não puder localizar observáveis secundários ou resultados de aprimoramento, verifique se Reverse Whois a integração foi executada com sucesso e retornou domínios. Além disso, consulte as anotações de trabalho no registro para obter mais informações.

Tópicos relacionados

Instalar e configurar Reverse Whois

Verifique os resultados esperados para Reverse Whois

RISKIQ e. WHOISIQ integração

Com a integração de RISKIQ e. WHOISIQ APIs com ServiceNow AI Platform® Operações de segurança os analistas de segurança recebem dados adicionais de aprimoramento e informações sobre a validade dos sites.

. RISKIQ A API Certificados SSL executa pesquisas em certificados SSL, que incluem detalhes sobre a autoridade de certificação emissora, as organizações que solicitam certificados, os certificados de entidade para os quais são emitidos e o domínio. As

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pesquisas de certificados SSL são realizadas automaticamente quando os incidentes de segurança são criados.

. RISKIQ WHOISIQ A API executa pesquisas em outros tipos observáveis, como domínio, e-mail, nameserver, organização, e número de telefone. Observáveis de URL e domínio são aprimorados automaticamente quando incidentes de segurança são criados.

A integração requer Resposta a incidentes de segurança e. Inteligência contra ameaças produtos.

Observáveis compatíveis com RISKIQ e. RISKIQ WHOISIQ

. RISKIQ A API oferece suporte a pesquisas automáticas de certificados SSL em observáveis de endereço IP, hash de arquivo, número de série do certificado, domínio e URL. Observáveis de URL e domínio são aprimorados automaticamente com WHOISIQ API. Para aprimoramento de observáveis em outros tipos de observáveis com WHOISIQ Criar observáveis e executar pesquisas manualmente a partir da tabela Observáveis.

Observáveis compatíveis

A tabela a seguir lista o tipo de APIs usadas nesta integração e os observáveis compatíveis com cada API. A tabela também indica se uma pesquisa ocorre automaticamente quando os incidentes de segurança são criados ou se a pesquisa é executada manualmente a partir da tabela Observáveis.

Observáveis e pesquisa compatíveis

API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
RISKIQ API de certificado SSL	• Endereço IP • Hash do arquivo (impressão digital do certificado). Consulte a figura a seguir para obter um exemplo de hash de arquivo. • Número de série do certificado ou Número de série. Esta cadeia de caracteres é um ID exclusivo da entidade. Consulte a figura a seguir para obter um exemplo de um número de série de certificado. • Domínio (www.site.com ou site.com)	Pesquisa automatizada quando incidentes são criados. Os resultados são exibidos no **Certificados SSL** do registro de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observáveis e pesquisa compatíveis

API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
	• URL **Nota:** Verificações automáticas são executadas para o formato de URL usando https:// protocolo, por exemplo, https://example.com/index.html	
RISKIQ WHOISIQ API	• Domínio • URL	Pesquisa automatizada quando incidentes são criados. Os resultados são exibidos no **Resultados de aprimoramento do observável** no registro de incidente de segurança.
RISKIQ WHOISIQ API	• Endereço de e-mail • Nome da organização • Número de telefone • Endereço para correspondência	A pesquisa manual é executada a partir da tabela Observáveis. Os resultados são exibidos no **Resultados de aprimoramento do observável** No registro do observável.

Exemplo de hash de arquivo e número de série de certificado

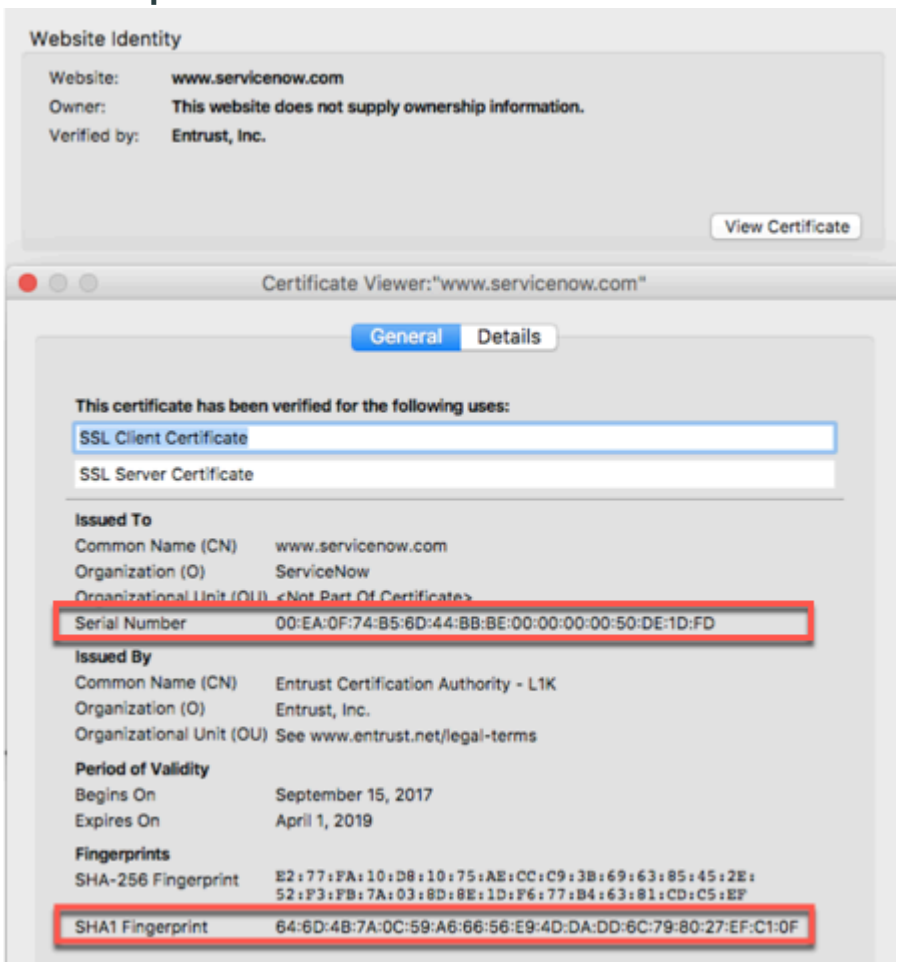
Esta figura mostra um exemplo de observáveis de hash de arquivo e de número de série de certificado usados para as pesquisas de certificado SSL para esta integração. O hash do arquivo se refere a uma impressão digital SHA-1. Este valor é exibido em seu ServiceNow AI Platform instância sem os separadores de dois pontos. Por exemplo, 646D4B7A0C59A66656E94DDADD6C798027EFC10F .

O número de série do certificado observável refere-se ao ID exclusivo ou número de série da entidade. Este valor também é exibido sem os separadores de dois pontos. Por exemplo, 00EA0F74B56D44BBBE000050DE1DFD .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hash do arquivo e número de série do certificado



Instalar e configurar RISKIQ e. WHOISIQ

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para RISKIQ e. WHOISIQ as aplicações se integram corretamente com ServiceNow AI Platform Operações de segurança.

Antes de Iniciar

Função necessária: administrador, RISKIQ e. WHOISIQ administrador.

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções necessárias.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O Administrador do sistema (admin) instala o app e atribui a função de Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao Operações de segurança E atribui

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

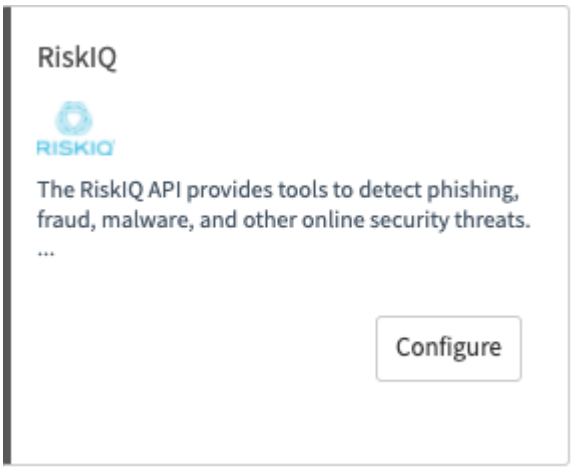
Configuração de tarefa	Descrição
	a função Analista de incidentes de segurança (sn_si.analyst). • O analista de incidentes de segurança (sn_si.analyst) trabalha com registros de incidentes de segurança.
Obtenha um nome de usuário e uma chave de API.	Visite o site para obter informações sobre a chave de API e como criar uma conta: RiskIQ website . A configuração requer que você insira a chave de API.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Madrid e versões posteriores Para a versão Madrid e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Procedimento

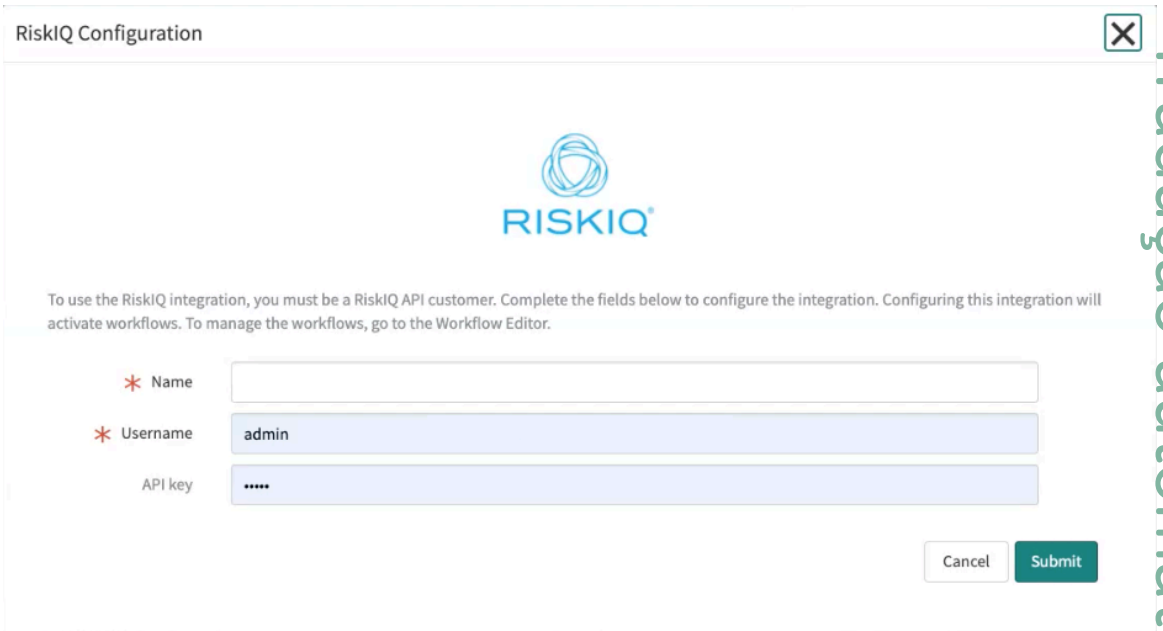
1. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Quando a instalação for concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de integrações** E localize o bloco da API.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo Configuração do RiskIQ exibida, insira **Nome de usuário** e. **Chave de API** .



5. Clique em **Enviar**.

6. Verifique a configuração bem-sucedida.
   Quando a configuração é concluída com sucesso, a página Integrações de segurança com os blocos de integração é exibida.

Trouble?
Se uma mensagem de erro for exibida, o nome de usuário ou a chave de API poderão ser inválidos. Verifique se o nome de usuário e a chave de API estão corretos:

Solução de problemas

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verifique os resultados esperados para RISKIQ Pesquisas de certificados SSL

Quando um incidente de segurança gera observáveis para URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série de certificados, os analistas de incidentes de segurança usam os resultados da pesquisa de certificado SSL para verificar se os sites têm certificados emitidos por uma autoridade de certificação (CA) pública confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para observáveis compatíveis, o. ServiceNow AI Platform Verifica a ocorrência mais recente de URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série do certificado. Estes são os resultados possíveis da verificação:

Uma correspondência exata foi encontrada

Um emissor válido de um certificado SSL é listado no registro de Incidente de segurança.

Nenhum resultado de certificado encontrado

Nenhum resultado está listado no registro de Incidente de segurança.

Uma correspondência exata foi encontrada para um certificado autoassinado ou gerado internamente

Os resultados de um certificado SSL gerado internamente são exibidos no registro de Incidente de segurança.

Não foi encontrada uma correspondência exata para um certificado SSL primário

Um valor de pesquisa retorna várias entradas e um certificado primário não pode ser identificado. Uma mensagem de resumo é exibida no registro de Incidente de segurança.

Procedimento

1. Para exibir os observáveis e verificar os resultados da pesquisa, abra o registro de incidente de segurança com o qual você está trabalhando e localize as anotações de trabalho.

Example

Para ilustrar exemplos dos possíveis resultados de pesquisa para esta integração, suponha que um incidente de segurança tenha sido gerado com os seguintes observáveis:

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Observáveis e local dos resultados da pesquisa

Observável (exemplo)	Resultados da verificação	Descrição e localização
community.servicenow.com	Certificado encontrado com um hash SHA1.	Uma correspondência exata é encontrada e um emissor válido de um certificado SSL é listado. Os resultados da correspondência exata são exibidos no **Certificados SSL** no registro de incidente de segurança.

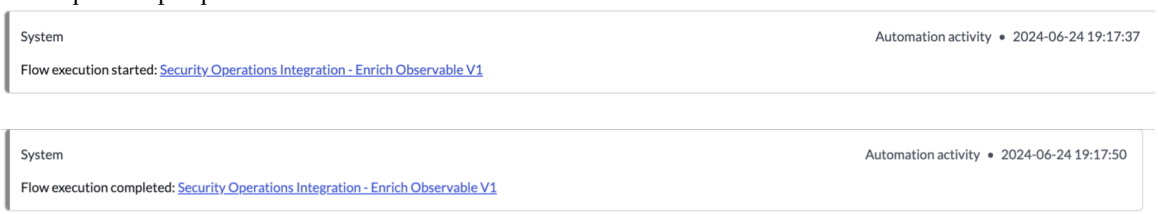
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observável (exemplo)	Resultados da verificação	Descrição e localização
invalidsubdomain.servicenow.com	Nenhum certificado encontrado.	Um resumo que indica que nenhum resultado de certificado foi encontrado é exibido no **Resultados de aprimoramento do observável** no registro de incidente de segurança.
mail.dgnetworks.com	Certificado encontrado com hash SHA1.	Uma correspondência exata é listada para um certificado autoassinado ou gerado internamente. Os resultados são exibidos no **Certificados SSL** no registro de incidente de segurança.
servicenow.com	A pesquisa retornou 138 certificados e um único certificado primário não pôde ser identificado.	Uma correspondência exata não foi encontrada para um certificado SSL primário, porque um valor de pesquisa retorna vários certificados. Um resumo que indica que nenhum certificado primário foi encontrado é exibido no **Resultados de aprimoramento do observável** no registro de incidente de segurança.

Depois que a aplicação é configurada, o fluxo é iniciado automaticamente. O status de pesquisa e os observáveis são exibidos nas anotações de trabalho.

2. Verifique se a pesquisa foi executada com sucesso.



Trouble?
Se você não puder exibir os resultados esperados, verifique se o observável é compatível com a pesquisa de certificado SSL para a integração.

Tópicos relacionados

Observáveis compatíveis com RISKIQ e. RISKIQ WHOISIQ

RISKIQ Pesquisas de certificados SSL que retornam uma correspondência exata

RISKIQ Os resultados da pesquisa de certificado SSL para uma correspondência exata são exibidos no **Certificados SSL** no registro de incidente de segurança. Uma correspondência exata fornece um nome de autoridade de certificação válido, o que ajuda um analista de incidentes de segurança a determinar a validade de um site.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Correspondência exata de um certificado SSL válido

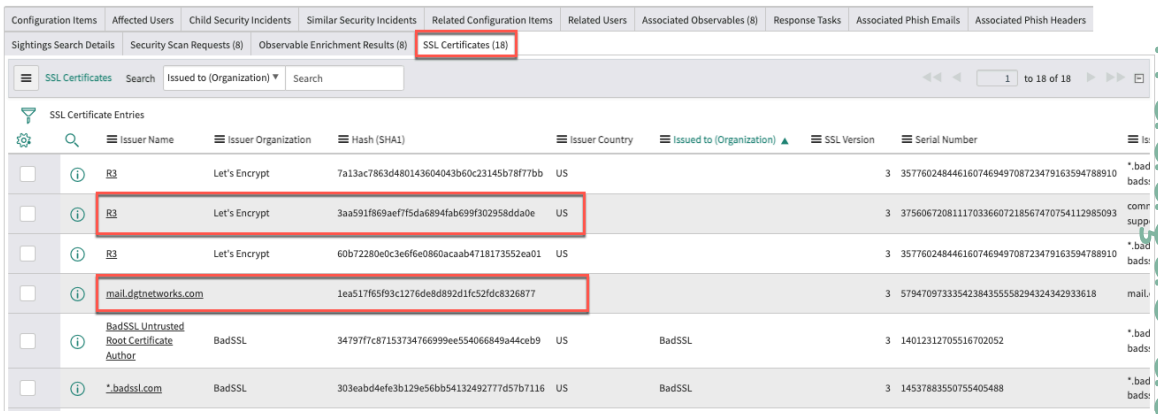
O exemplo a seguir mostra um emissor válido de um certificado SSL de uma correspondência exata nos resultados da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

Nota: As figuras nos exemplos a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema. Se a tela não corresponder à exibição mostrada abaixo, siga as etapas para definir formulários com guias.

1. No canto superior direito da moldura da faixa, clique no ícone Configurações.
2. Em **Configurações do sistema** caixa de diálogo exibida, clique em **Formulários** e verifique isso **Formulários com guias** e. **Com o formulário** selecionados.

1. No registro de incidente de segurança, clique em **Certificados SSL** guia.

Guia Certificados SSL



As informações sobre o nome do emissor do certificado, a organização do emissor e para quem o certificado é emitido (organização) são exibidas junto com outros dados.

18 itens são exibidos em **Nome do emissor** coluna. O segundo item (R3 fornece um nome de autoridade de certificação válido (Criptografar) no **Organização do emissor** coluna.

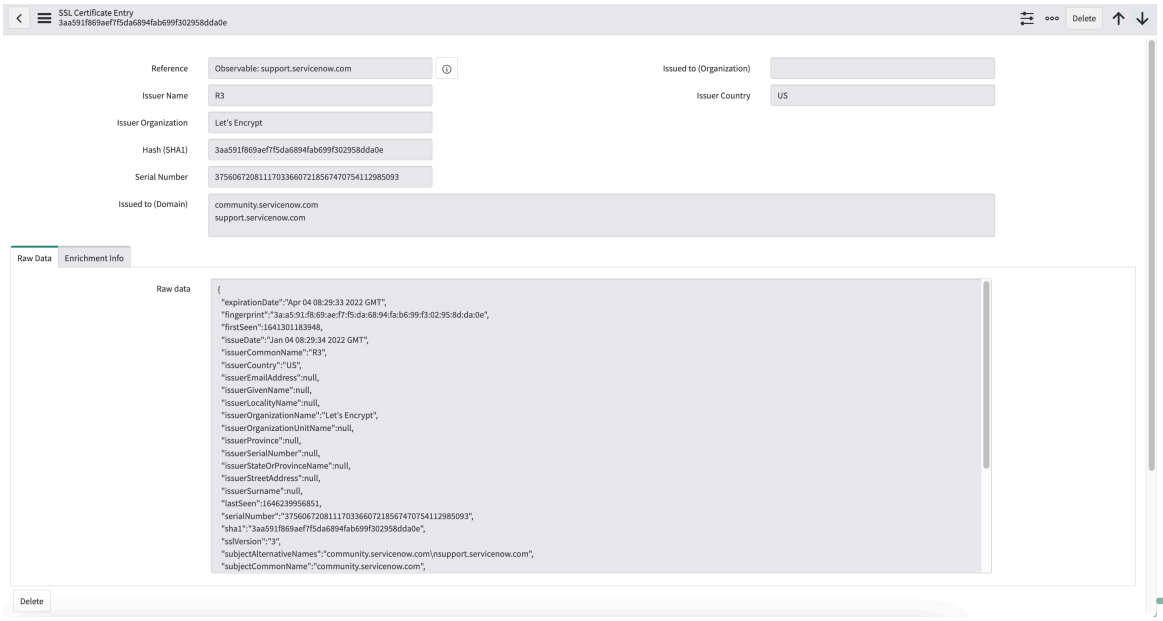
Não há informações no **Organização do emissor** e. **Emitido para** as colunas são exibidas para o segundo item (mail.dgtnetworks.com).

2. Clique no segundo item em **Nome do emissor** , que é (**R3**) para abrir o registro de entrada. Como alternativa, clique no ícone de informações ao lado do item seguido por **Abrir registro** .
3. Selecione **Dados brutos** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Dados brutos



O registro de entrada de certificado SSL inclui o observável no **Dados brutos** em **Nome da entidade** , bem como outros dados.

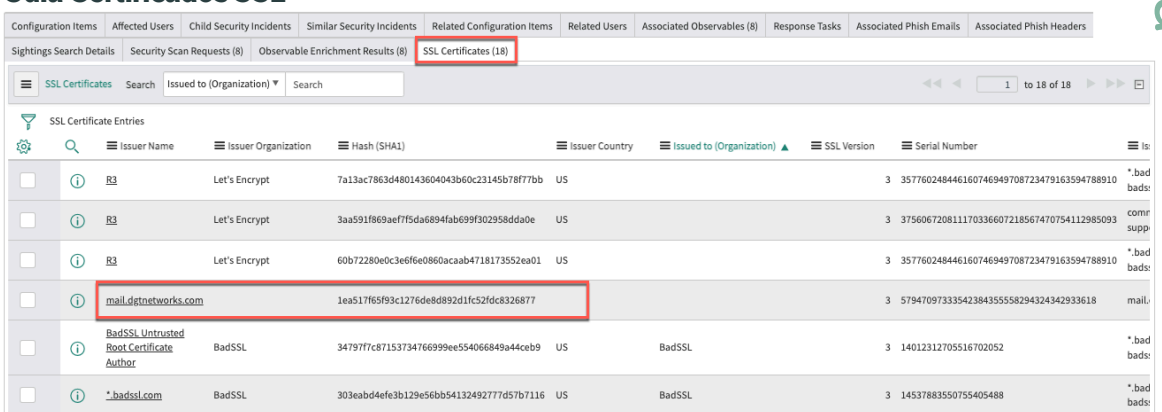
Nota no **Categoria** . Assunto e Emissor corresponder a entidades reconhecíveis em **Nome da entidade** coluna. O emissor deste certificado provavelmente é válido e de uma autoridade de certificação pública confiável. Observe também Assunto e Emissor são entidades diferentes. Essas entidades separadas indicam que o certificado não é um certificado assinado internamente de uma autoridade de certificação desconhecida.

Example: Correspondência exata de um certificado SSL autoassinado

O exemplo a seguir mostra os resultados de um certificado SSL autoassinado da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

1. Navegue de volta para o registro de incidente de segurança. Em **Nome do emissor** , clique no outro item (**mail.dgtnetworks.com**).

Guia Certificados SSL

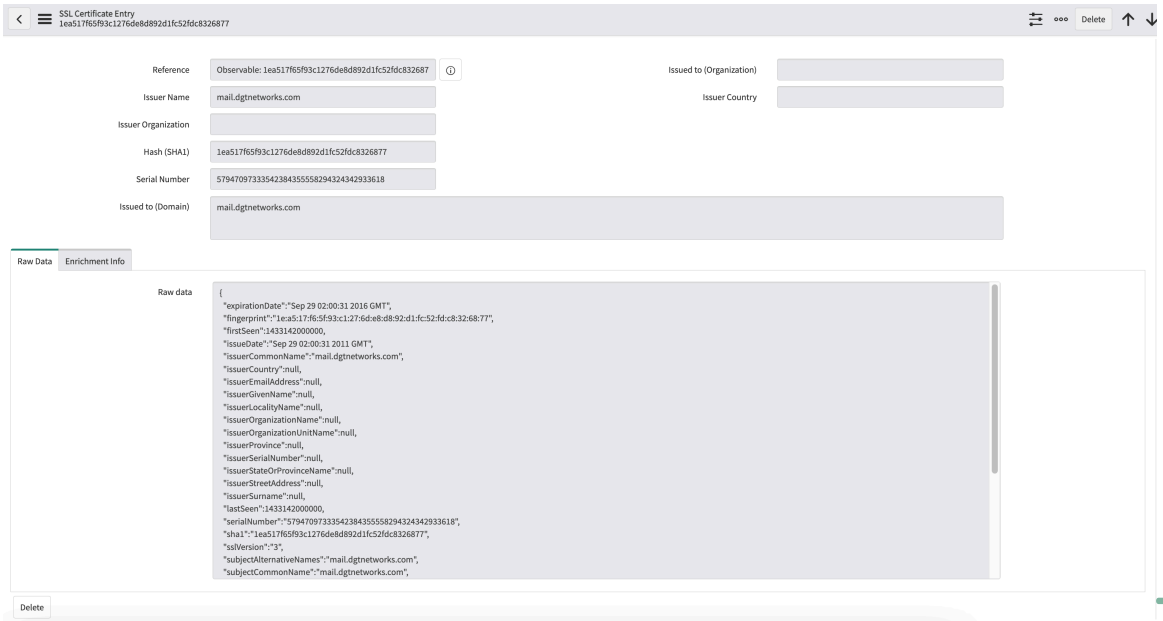


2. No registro em aberto, selecione **Dados brutos** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Dados brutos



. **Categoria** a coluna indica Emissor (mail.dgtnetworks.com e. Dgtsbs.DGTNetworks.local não são autoridades de certificação públicas confiáveis. Observe também o. Emissor e. Assunto são a mesma entidade (Dgtsbs.DGTNetworks.local e cada um contém o nome do observável (dbs). Possivelmente, este certificado é um certificado autoassinado. Certificados autoassinados podem justificar uma investigação adicional, já que esses certificados não são emitidos por uma autoridade de certificação conhecida.

RISKIQ Pesquisas de certificados SSL que retornam vários certificados ou nenhum certificado

Um analista de incidentes de segurança pode usar vários resultados de certificado SSL para determinar se um site faz parte de uma entidade comum e reconhecível. Nenhum resultado de certificado SSL pode indicar que sites com nomes obscuros ou suspeitos não têm certificados confiáveis. Os resultados da pesquisa de observáveis que não retornam certificados SSL ou que retornam vários certificados SSL são exibidos no Resultados de aprimoramento do observável no registro de incidente de segurança.

Example: Nenhum resultado de certificado SSL ou vários resultados de certificado SSL

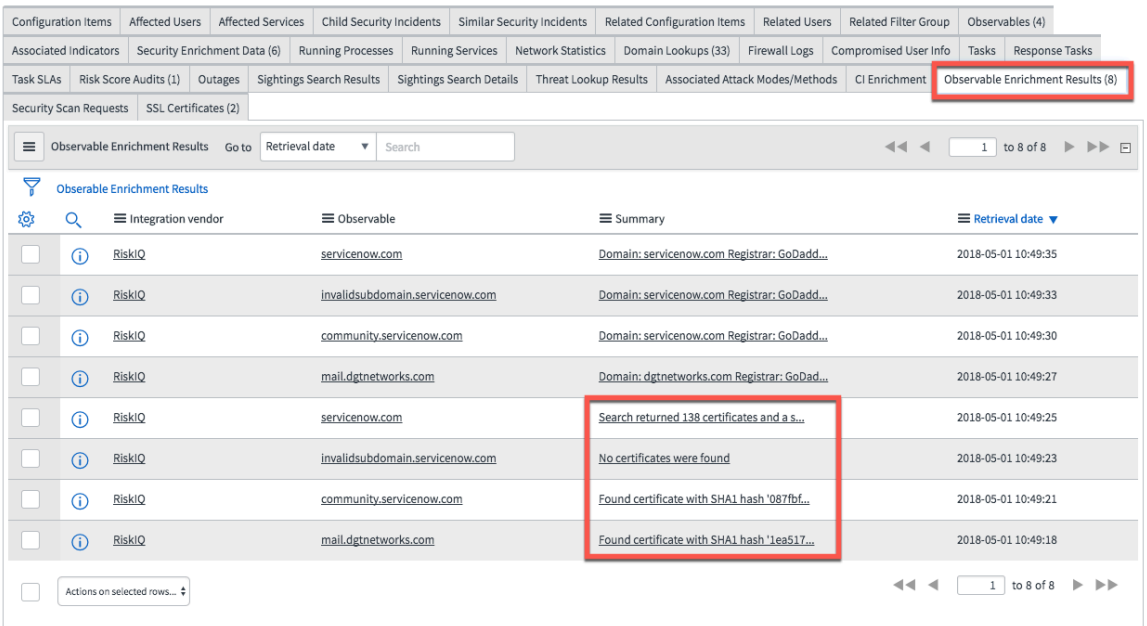
Siga as etapas para exibir os resultados de observáveis que não retornam certificados SSL ou que retornam vários certificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. No registro de incidente de segurança, clique em **Resultados de aprimoramento do observável** guia.

Guia Resultados de aprimoramento do observável

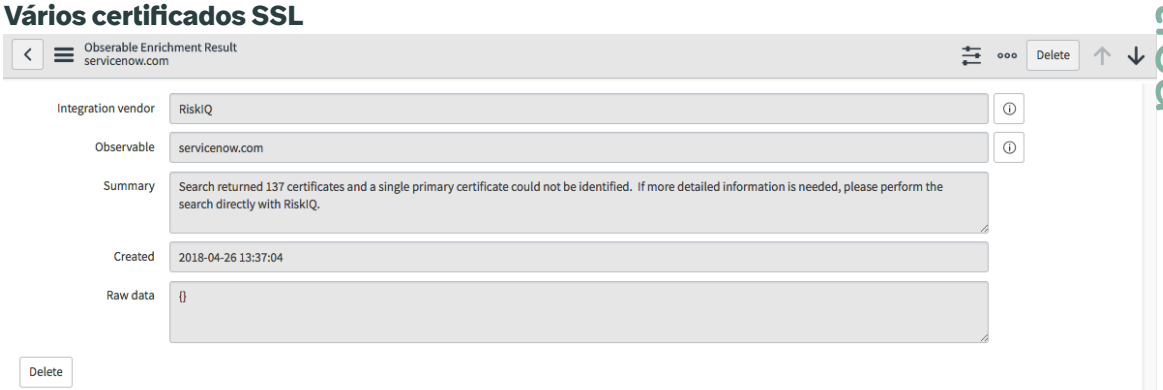


Os resultados de aprimoramento de observável para RISKIQ e. WHOISIQ as pesquisas são exibidas.

Em **Observável** coluna, servicenow.com corresponde a A pesquisa retornou 138 certificados mensagem no **Resumo** coluna. Da mesma forma, invalidsubdomain.servicenow.com corresponde a. Nenhum certificado encontrado em **Resumo** coluna. Esses resumos indicam que vários certificados SSL foram encontrados e que nenhuma correspondência exata para certificados SSL foi encontrada, respectivamente.

2. Em **Observável** , clique em **servicenow.com** .

Vários certificados SSL



A mensagem de resumo exibida no registro indica que vários resultados de certificados SSL foram retornados para servicenow.com E um Certificado SSL primário não pôde ser correspondido. Essa mensagem geralmente é retornada em pesquisas que incluem nomes de domínio comuns, como servicenow.com .

Se você precisar de mais informações sobre um domínio comum, poderá executar a pesquisa diretamente com RISKIQ API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegue de volta para **Resultados de aprimoramento do observável** e no **Observável** , clique em **invalidsubdomain.servicenow.com** .

Nenhum certificado SSL



Nota:

- Se nenhum certificado SSL for encontrado para o observável atual, o campo Resumo exibirá a mensagem, Nenhum certificado encontrado .
- Se nenhum certificado SSL ativo for encontrado para o observável atual, o campo Resumo exibirá a mensagem, Nenhum certificado ativo encontrado .

Verifique os resultados esperados para WHOISIQ Pesquisas de URL

Quando um incidente de segurança gera observáveis para URLs ou domínios, o. WHOISIQ A API executa o aprimoramento do observável automaticamente após a criação do incidente de segurança. Os resultados da pesquisa são exibidos no **Resultados de aprimoramento do observável** e. **Certificados SSL** guias no registro de incidente de segurança.

Antes de Iniciar

Nota: As figuras nas etapas a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema.

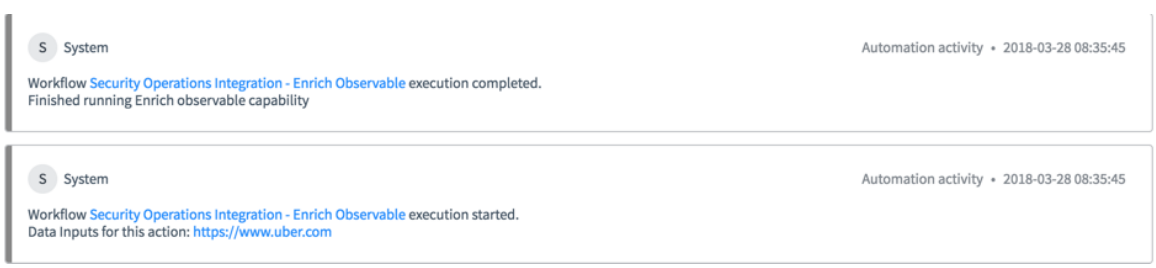
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os resultados de aprimoramento do observável são exibidos no **Resultados de aprimoramento do observável** na parte inferior do registro de incidente de segurança. Para observáveis compatíveis, uma pesquisa de certificado SSL também é executada e os resultados são exibidos no **Guia Certificados SSL** .

Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso nas anotações de trabalho.

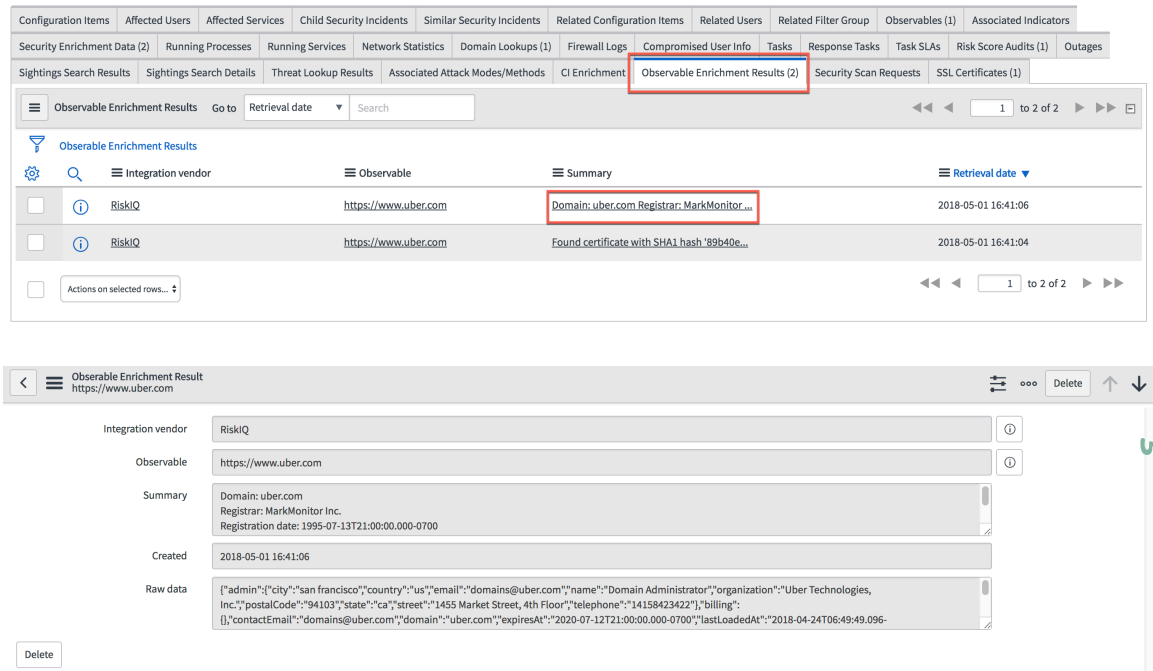


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

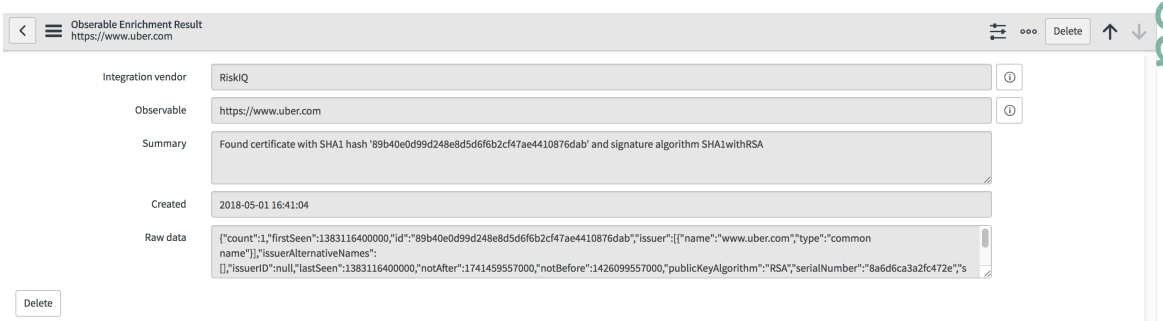
Quando a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro de Incidente de segurança.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.
3. Em Incidente de segurança aberto, clique em **Mostrar todas as listas relacionadas** link relacionado.
4. Clique em **Resultados de aprimoramento do observável** para selecioná-lo.
5. Em **Resumo** , clique no primeiro item, **Registrador: Markmonitor... uber.com** .



O registro exibido contém informações sobre o domínio.

6. Navegue de volta para **Resultados de aprimoramento do observável** , e, no **Resumo** , clique no segundo item, **Certificado encontrado com hash SHA1...** .

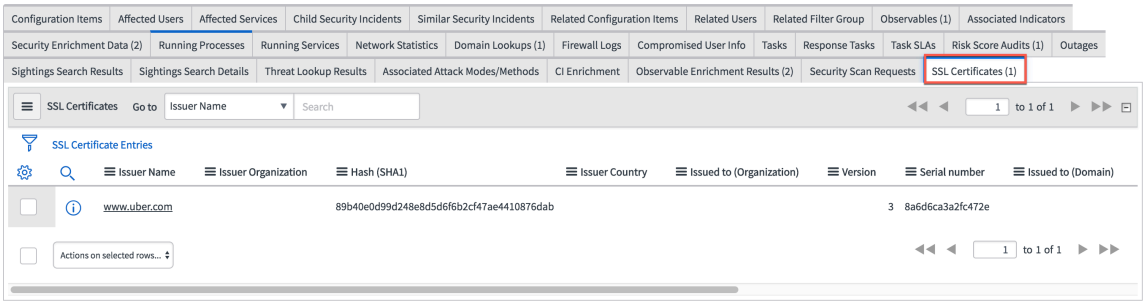


Este registro indica que um certificado SSL foi encontrado com um hash de arquivo.

7. Navegue de volta para o registro de incidente de segurança e clique em **Certificados SSL** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados do certificado SSL para o hash do arquivo também são exibidos aqui.

Trouble?

Se você não puder exibir os resultados esperados, revise as anotações de trabalho. Verifique também se o observável é compatível com a pesquisa pela integração.

Tópicos relacionados

Observáveis compatíveis com RISKIQ e. RISKIQ WHOISIQ

Crie um observável para manual WHOISIQ pesquisas

Os analistas de incidentes de segurança usam informações do aprimoramento de observável com WHOISIQ API para saber mais sobre os endereços de e-mail, nomes e números de telefone das organizações.

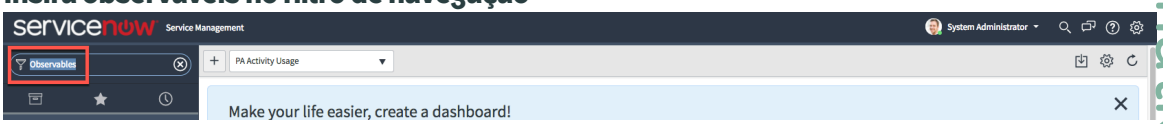
Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

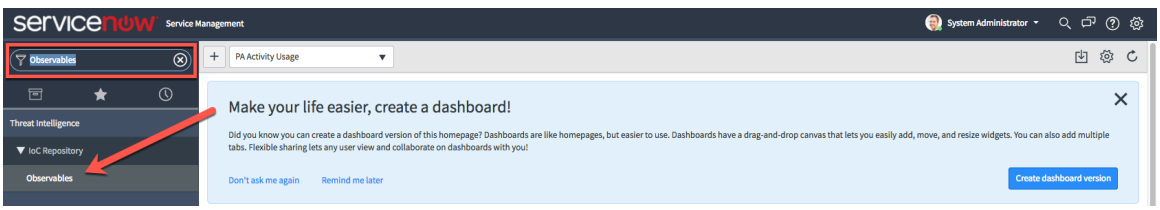
1. Navegar até **Tudo** > **Repositório LOC** > **Observáveis**.

Insira observáveis no filtro de navegação



No painel de navegação, o módulo Observáveis é exibido.

Módulo Observáveis

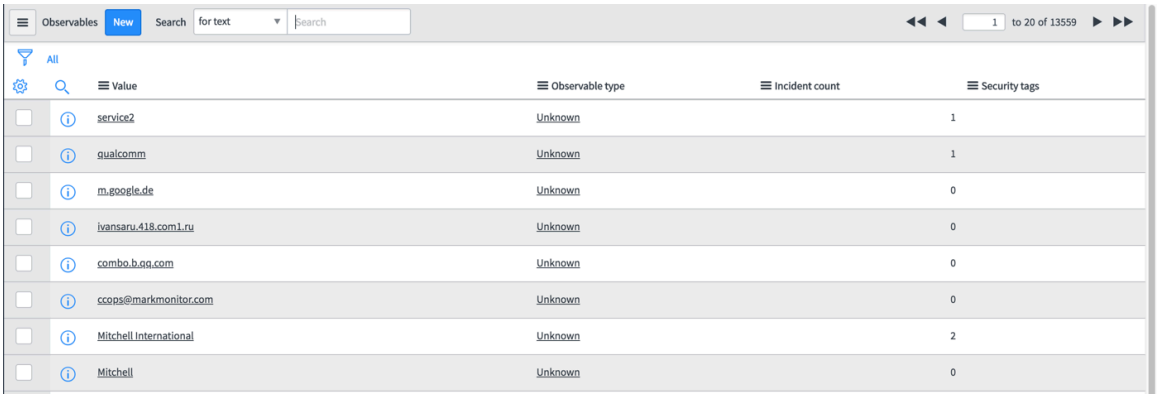


2. Clique em **Observáveis** Módulo para exibir a lista de observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

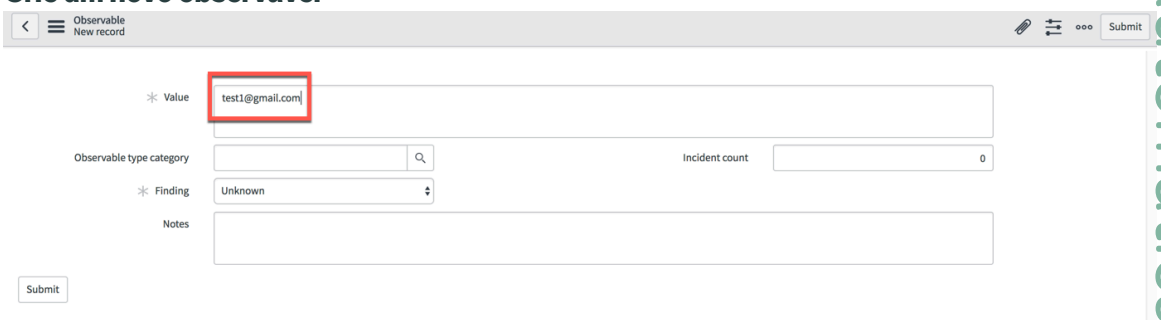
Lista de observáveis



3. Clique em **Novo** para criar um novo observável.
4. No formulário Observável, preencha os campos.

Campo	Descrição
Valor	Endereço de e-mail, nome da organização, número de telefone ou endereço para correspondência. Por exemplo, `test1gmail.com`
Tipo de observável	O campo é limpo automaticamente.
Descoberta	O campo é definido automaticamente como **Desconhecido** .

Crie um novo observável



5. Clique em **Enviar**.
   Você retornará à lista de observáveis. Em **Valor** seu novo observável é exibido.

   Nota: Se você não conseguir localizar seu observável na parte da lista exibida, use a funcionalidade de pesquisa para encontrá-lo.

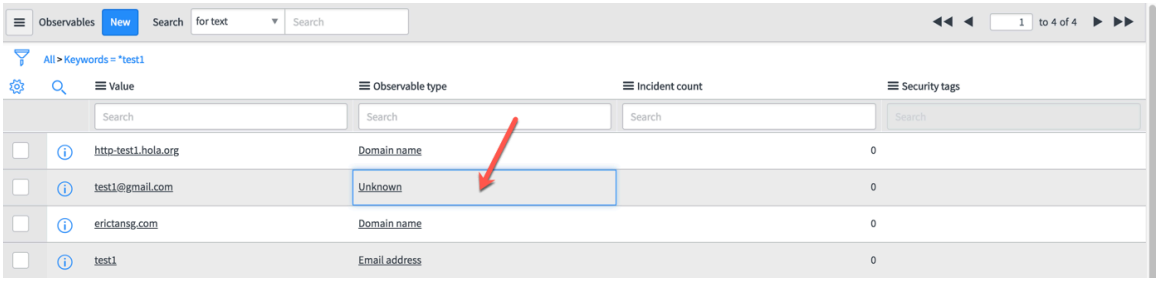
6. Edite o. **Tipo de observável** campo do qual mudar o tipo **Desconhecido** . **Endereço de e-mail** para corresponder ao seu observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em **Tipo de observável** clique uma vez à direita de **Desconhecido** texto para selecioná-lo.

Selecione o campo Tipo de observável

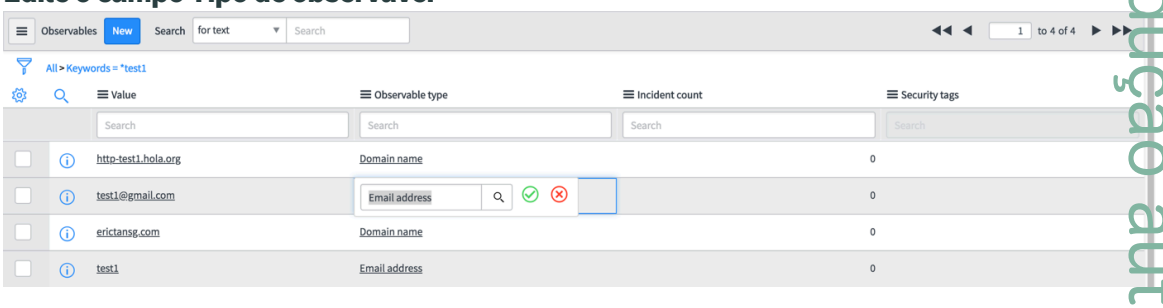


O campo selecionado é destacado em azul.

b. Com o campo destacado em azul, clique duas vezes em qualquer lugar dentro do campo realçado para abrir o editor.

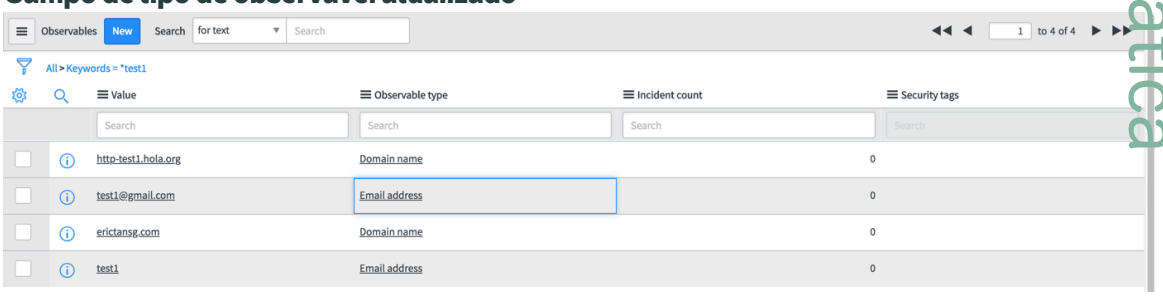
c. No campo exibido, insira o tipo de observável (`Endereço de e-mail` e clique na marca de seleção verde para salvar o valor.

Edite o campo Tipo de observável



Em **Tipo de observável** coluna na lista, `Endereço de e-mail` é exibido para o seu novo observável.

Campo de tipo de observável atualizado



O que Fazer Depois

Se você criou e editou um observável para pesquisa, execute a pesquisa de aprimoramento do observável a partir do registro do observável com WHOISIQ API.

Verifique os resultados esperados para manual WHOISIQ pesquisas

Execute uma pesquisa manual em um observável quando ele não gerar automaticamente um incidente de segurança. Para pesquisas de aprimoramento de observável usando WHOISIQ API Para endereços de e-mail, nomes de organizações, números de telefone ou endereços de correspondência, inicie a pesquisa manualmente na tabela Observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

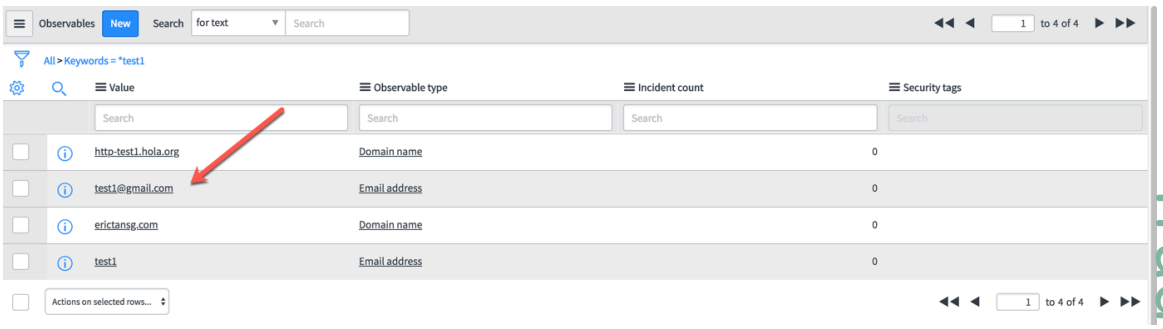
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

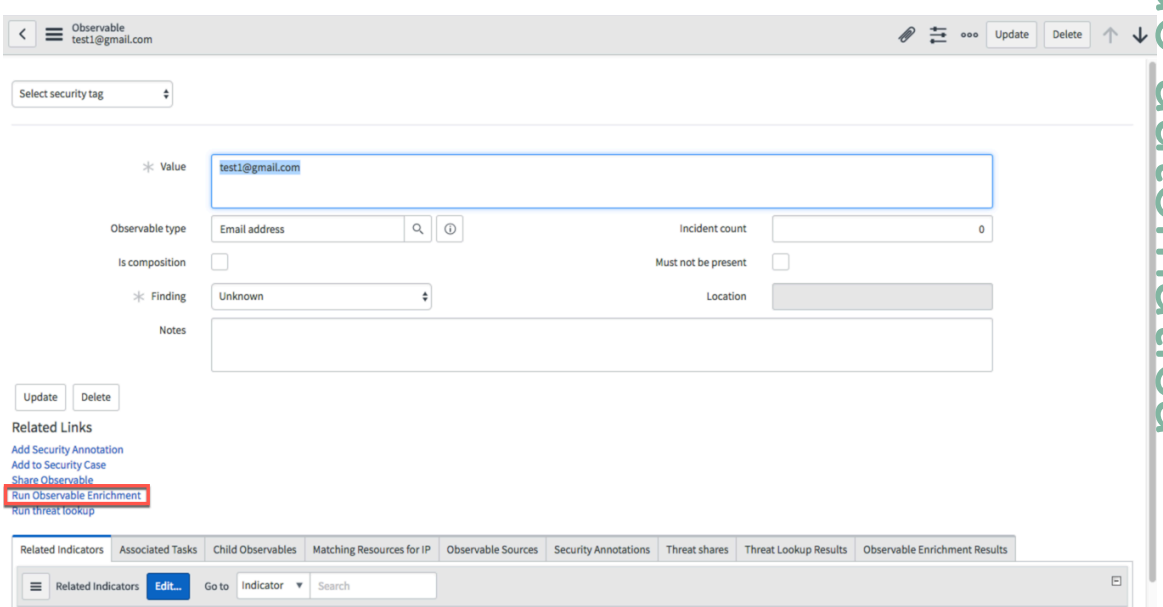
Crie um observável para uma pesquisa manual usando WHOISIQ API. Para obter mais informações sobre como criar e editar um observável, consulte Crie um observável para manual WHOISIQ pesquisas.

Procedimento

1. Navegar até **Tudo** > **Repositório LOC** > **Observáveis** e localize o observável na lista com a qual você está trabalhando.
2. Clique no observável no **Valor** coluna para abrir o registro.



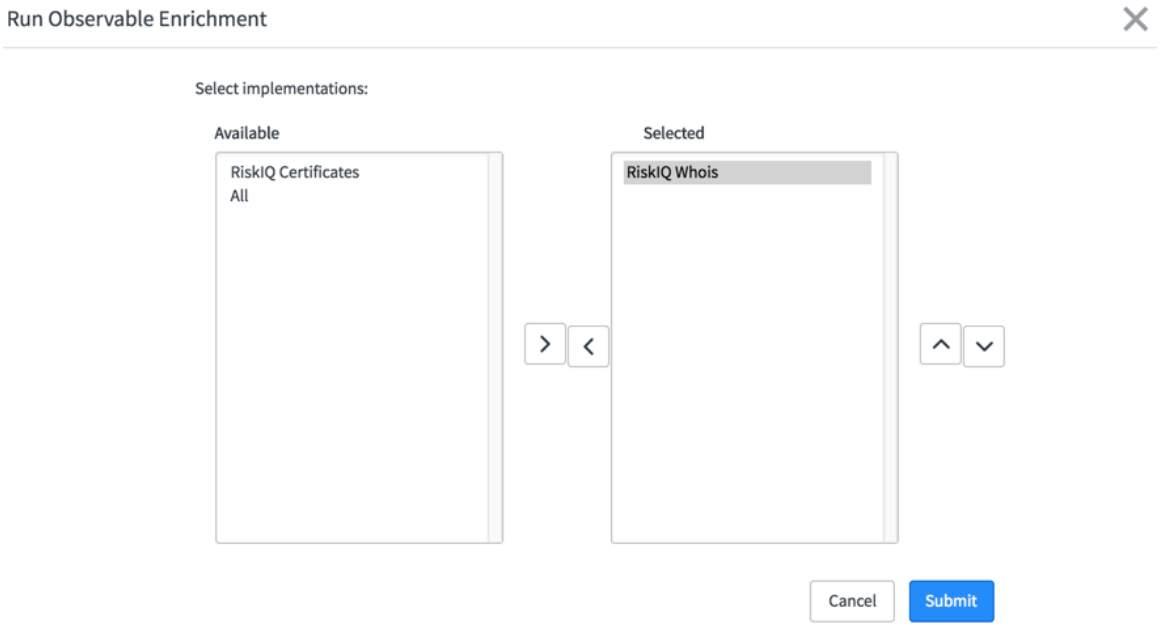
3. Clique em **Executar aprimoramento de observável** link relacionado para executar a pesquisa.



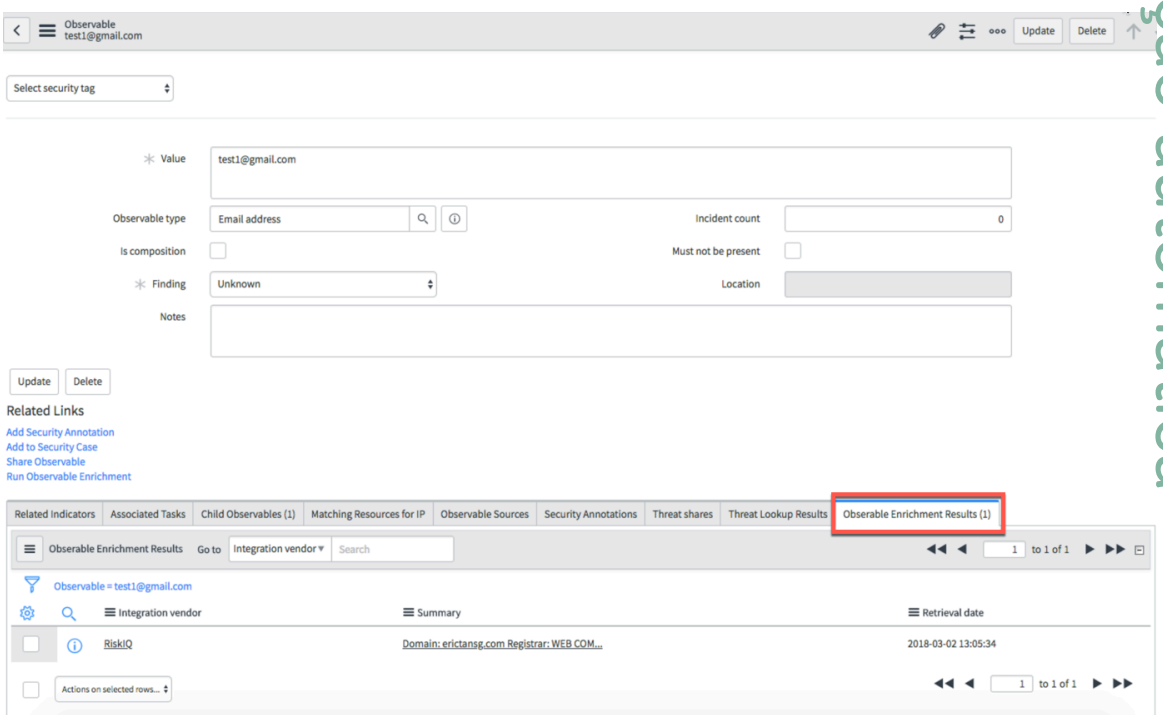
4. Em **Executar aprimoramento de observável** mover **RiskIQ Whois** Para a lista Selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Os resultados da pesquisa são exibidos no **Resultados de aprimoramento do observável** no registro do observável.



Trouble?
Se nenhum resultado for retornado para o observável, uma mensagem será exibida no **Resumo** coluna. Se você não vir resultados, verifique se o observável é compatível com a API.

Tópicos relacionados

Observáveis compatíveis com RISKIQ e. RISKIQ WHOISIQ

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Shodan integração

Shodan é um mecanismo de pesquisa que analisa informações da faixa de serviço de dispositivos conectados em todo o mundo. As faixas de serviço incluem informações sobre um sistema de computador, como nome do host, tipo de dispositivo, sistema operacional, localização geográfica e ISP conectado. Quando integrado ao ServiceNow AI Platform Operações de segurança essas informações de faixa de serviço fornecem aos analistas dados de aprimoramento adicionais e informações para incidentes de segurança ou investigações.

A integração requer Resposta a incidentes de segurança e. Inteligência contra ameaças plug-ins.

. Shodan a integração executa o aprimoramento nos seguintes observáveis:

- Endereços IP
- URLs

A aplicação verifica se há novos observáveis a cada cinco minutos. Se os observáveis forem de um tipo reconhecido pelo Shodan os observáveis são enriquecidos.

Instalar e configurar

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para Shodan a aplicação se integra corretamente com ServiceNow AI Platform Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tarefas de configuração	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • O Administrador do sistema (admin) instala o app e atribui a função de Administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao Operações de segurança módulo.
Obtenha o. Shodan Chave de API.	Crie uma conta e obtenha a chave de API do Shodan site: Site do Shodan .
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Para a versão Madrid e versões posteriores da família, o. Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar

Tradução automática

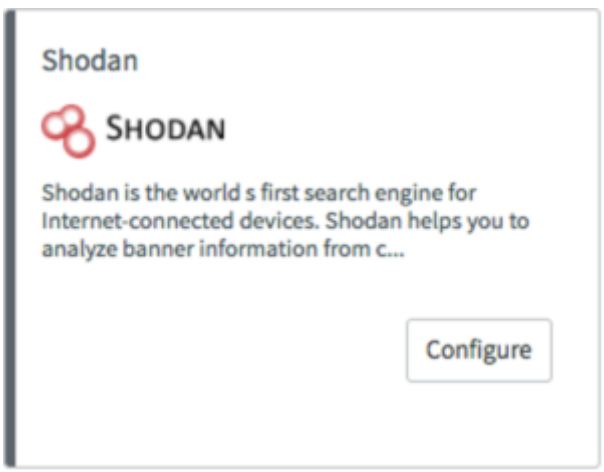
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	e ativar o outro Operações de segurança aplicações exigidas pela integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Framework de integração de segurança **3.** Security Support Common **4.** Orquestração do suporte de segurança Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Função necessária: administrador

Procedimento

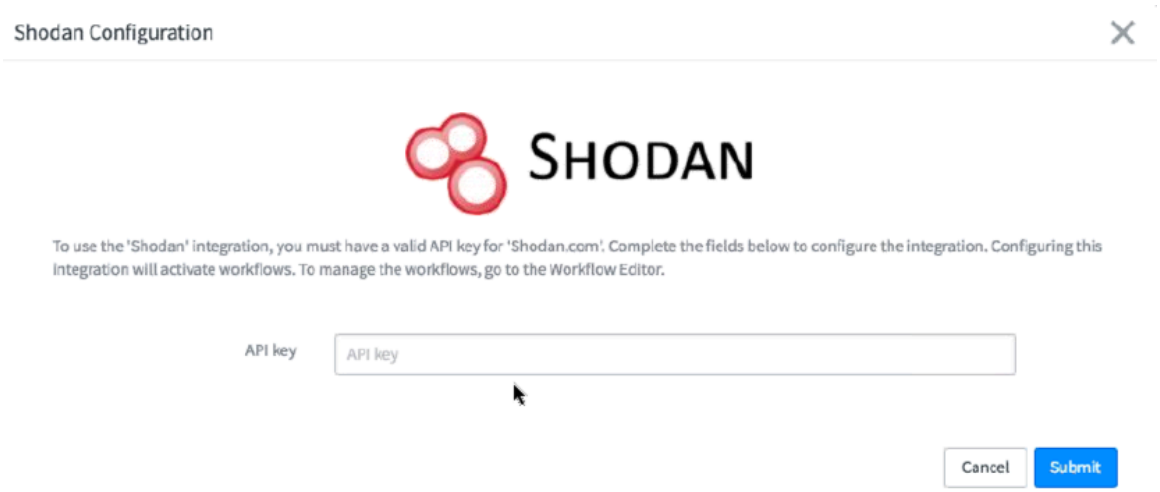
1. Se você não instalou a aplicação para a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize Shodan lado a lado.



3. Clique em **Configurar**.
4. Em **Configuração do Shodan** , insira a chave de API que você obteve do Shodan site e clique **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, o Shodan A chave de API pode ser inválida.

Verifique os resultados esperados

Observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados de aprimoramento são exibidos no **Resultados de aprimoramento do observável** e. **Faixas de rede** guias.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

1. Abra o incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.



   Depois que a aplicação é configurada, o fluxo de trabalho é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

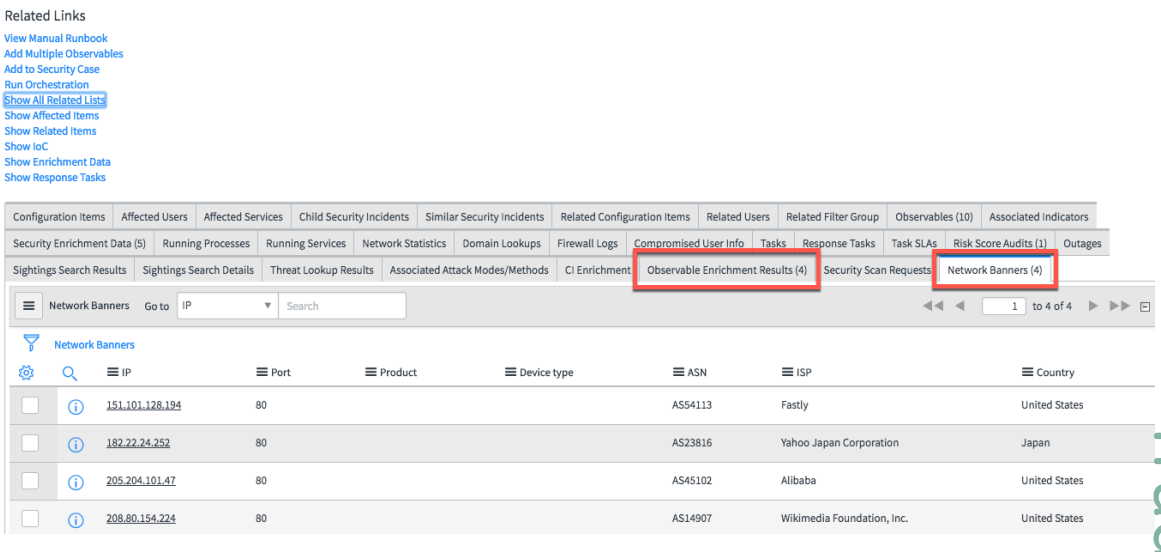
2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

3. Navegue até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas** link em **Links relacionados** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As figuras nas etapas a seguir são mostradas com **Formulários com guias** Configuração ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito da moldura da faixa, clique no ícone de engrenagem Configurações. Em **Configurações do sistema** caixa de diálogo exibida, clique em **Formulários** e verifique isso **Formulários com guias** e. **Com o formulário** selecionados.



Os resultados são exibidos em **Resultados de aprimoramento do observável** e. **Faixas de rede** guias na parte inferior do incidente de segurança.

4. Com **Faixas de rede** selecionado, clique no ícone de informações azul ao lado de um observável.

5. Na caixa de diálogo exibida, clique em **Registro em aberto** para exibir dados brutos e mais detalhes.

Trouble?

Se você não vir resultados em **Resultados de aprimoramento do observável** e. **Faixas de rede** , verifique se o observável é um tipo compatível com pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Shodan

Você pode anexar manualmente observáveis a um incidente de segurança. Anexe observáveis manualmente quando quiser executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

Antes de Iniciar

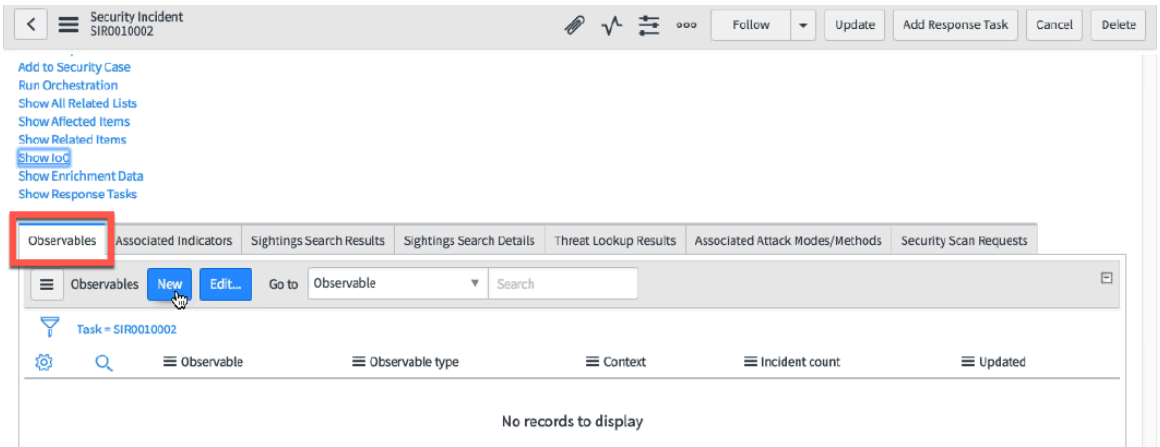
Função necessária: sn_si.analyst

Procedimento

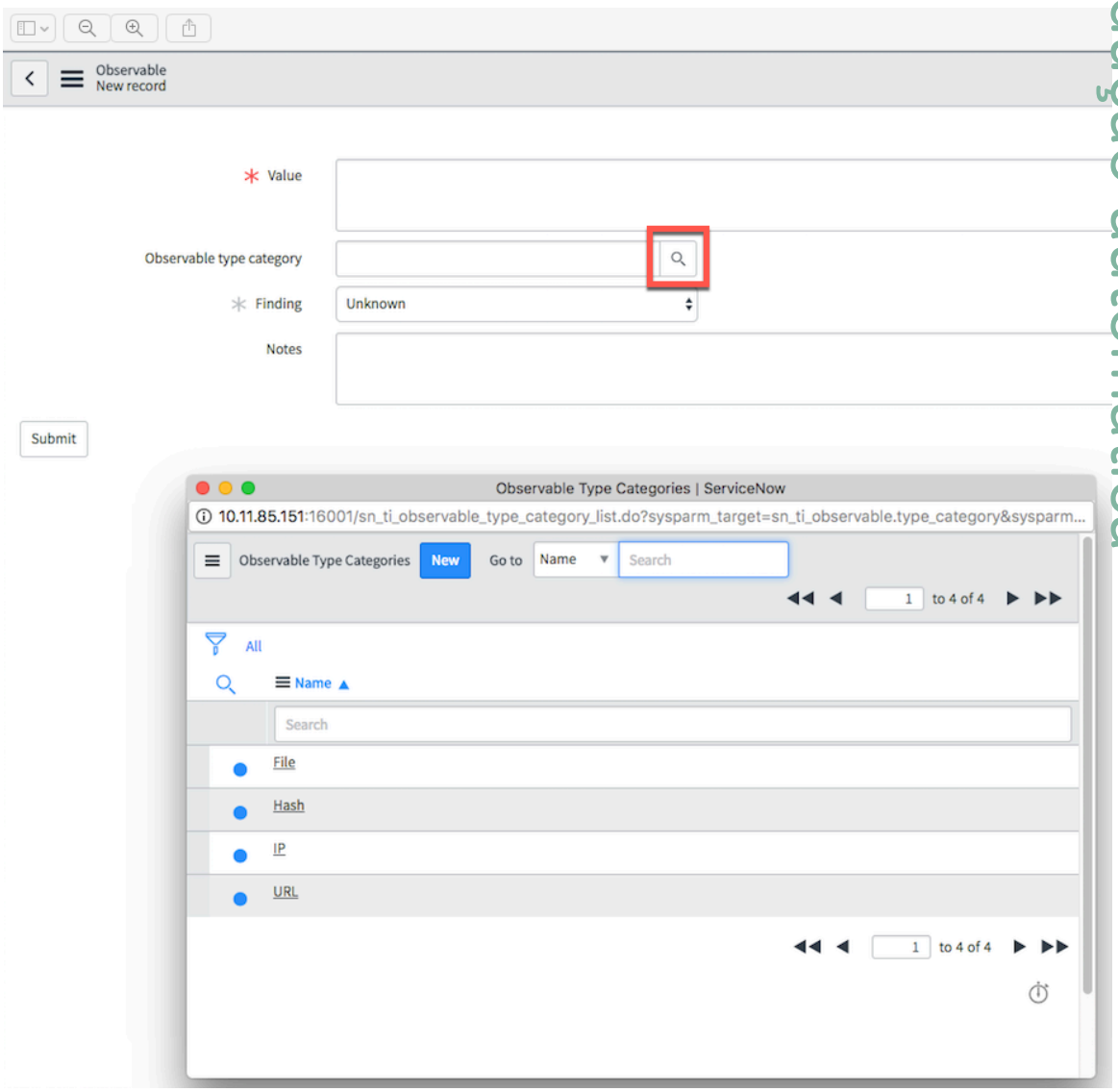
1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. Na parte inferior do registro, clique em **Mostrar IOC** link em **Links relacionados** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Em **Observáveis** clique em **Novo** .
   O formulário Observável é exibido.
4. Em **Valor** Insira um observável (endereço IP ou URL).
5. Clique no ícone de pesquisa e no **Categorias de tipo de observável** , clique no tipo de observável desejado na lista para preencher o campo.



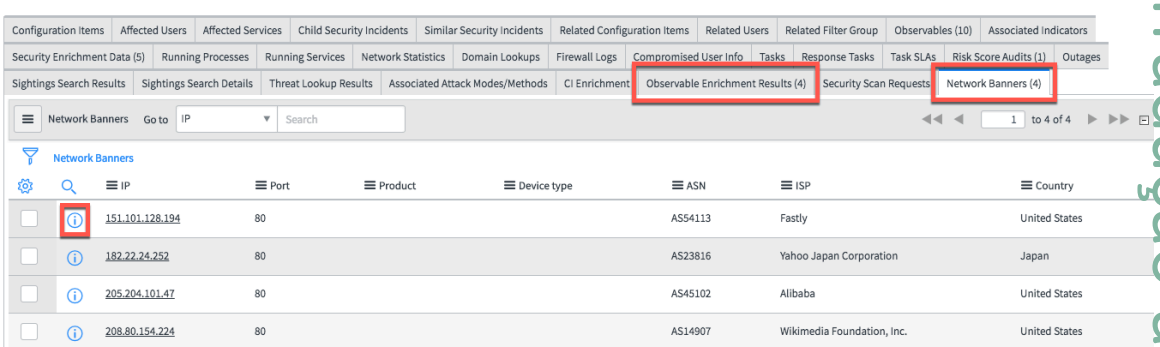
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   O fluxo de trabalho é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção Anotações de trabalho no registro de incidente de segurança.
7. Navegue até o incidente de segurança e revise as anotações de trabalho.



8. Na parte inferior do registro, clique em **Mostrar todas as listas relacionadas** link relacionado.
9. Clique em **Resultados de aprimoramento do observável** ou **Faixas de rede** e clique no ícone de informações azul ao lado de um observável para obter mais informações sobre um item específico.



10. Na caixa de diálogo exibida, clique em **Registro em aberto** para exibir dados brutos e mais detalhes.
11. **Opcional:** Clique no ícone de configurações azul ao lado do ícone de pesquisa para personalizar a saída e a ordem da coluna.
12. Em **Personalizar colunas da lista** , selecione as configurações disponíveis e mova-as para **Selecionado** e clique em **OK** .

Trouble?
Revise **Anotações de trabalho** para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Secureworks CTP Integração de ingestão de tíquete

. Secureworks Counter Threat Platform a integração de ingestão de tíquete permite que você busque automaticamente Secureworks CTP converta-os em incidentes de segurança e execute ações de resposta automatizadas.

Os principais recursos desta integração incluem:

- Ingestão automática de tíquetes selecionados (incluindo anexos) com base em uma programação predefinida.
- Mapeamento de campos de tíquete e evento para Resposta a incidentes de segurança campos.
- Visualização de incidentes de segurança mapeados para os campos de tíquete.
- Filtragem e agregação de tíquetes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Recuperação sob demanda de eventos associados a um tíquete.
- Acompanhamento periódico das principais atualizações dos tíquetes.
- Automatizar atualizações e fechamentos de tíquetes com base no status do incidente SIR
- Atualização do tíquete mestre.
- Sincronização de logs de trabalho do Secureworks com Resposta a incidentes de segurança anotações de trabalho.

Configure seu ServiceNow AI Platform instância do Secureworks CTP integração de ingestão de tíquete

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform instância antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform instância. • Um usuário com ServiceNow AI Platform a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui o. SIR função de administrador (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no ServiceNow AI Platform: ◦ Cria e edita perfis. ◦ E mapeia Secureworks CTP campos de tíquete para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração. ◦ Agenda a ingestão contínua de tíquetes. ◦ Habilita atualizações de tíquete quando um SIR SIR o incidente foi criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Gerenciando funções
Verifique se você está usando as seguintes versões: • API de tíquete do Secureworks 4,0 • API de eventos do Secureworks 1,0 • API de aprimoramento do Secureworks 1,0	Se você tiver acesso ao Secureworks CTP, você tem acesso à API necessária para esta integração. Não há outra configuração especial necessária para a API.
Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você instalar a aplicação para a integração.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. **1.** Resposta a incidentes de segurança **2.** Ingestão de evento e alerta para Operações de segurança(Necessário para integrações DE SIEM): Esta aplicação requer: ◦ Tempo de execução do IntegrationHub da ServiceNow com.glide.hub.integration.runtime ◦ Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in de ingestão de evento e alerta. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Instale e configure o. ServiceNow Aplicação para a integração de ingestão de tíquete do Secureworks CTP

Antes de executar a integração no seu ServiceNow AI Platform, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou o. Secureworks CTP aplicação de tíquete do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize Secureworks CTP Bloco Integração de ingestão de tíquete.



3. Para configurar a aplicação, clique em **Novo** .
4. Como alternativa, se for um **Configurar** é exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo exibida, preencha os campos.

Campo	Descrição
Nome	Nome do Secureworks CTP instância usada para a integração. Somente valores alfanuméricos e hifens (-) podem ser inseridos neste campo.
Descrição	Insira uma descrição para a conta do usuário.
Nome do usuário	Insira o nome de usuário do Secureworks CTP Conta de API. Observe que o nome de usuário diferencia maiúsculas de minúsculas. Para encontrar o nome de usuário, siga estas etapas: ○ Faça login no Secureworks CTP portal. ○ Navegar até **Conta** > **Gestão de contas** > **Credenciais de API**. O nome de usuário é exibido na página Credencial da API.
Senha da API	Insira Secureworks CTP Senha da API. Para encontrar a senha da API, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Faça login no Secureworks CTP portal. ○ Navegar até **Conta** > **Gestão de contas** > **Credenciais de API**. A senha da API é exibida na página Credencial da API. Para obter mais informações sobre como obter o nome de usuário e a senha da API, siga as etapas na seção Gerando uma chave de API persistente do Guia da API de ticketing do Secureworks .

6. Clique em **Enviar**.
   Depois que ela é validada e enviada com sucesso, cada configuração é salva na página Integrações de segurança como um bloco.

Resultado

Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança. No canto superior direito da página, em **Mostrar Configurações** lista de seleção, clique em **Sim** .

Crie um perfil para a integração de ingestão de tíquete do Secureworks CTP

Crie um perfil no seu ServiceNow AI Platform e determinam quais tíquetes precisam ser ingeridos e quais tíquetes serão usados para criar incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de tíquetes ingeridos, os valores de campo dos tíquetes são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será exibido.

A integração permite ingerir tíquetes com base nos perfis que você configura no Operações de segurança ambiente da sua instância. Inicialmente, todos os tíquetes são ingeridos para um tipo de tíquete configurado em um perfil. Os tíquetes ingeridos podem ser filtrados ainda mais para especificar quais tíquetes criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para tíquetes identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de tíquetes ingeridos, os valores de campos individuais nos tíquetes são mapeados para os campos correspondentes em um layout de incidente de segurança para uma visualização.

Identifique a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um tíquete no seu ServiceNow AI Platform instância, navegue até **Integração de ingestão de tíquete do Secureworks** > **Perfis do Secureworks**.
2. Clique em **Nova**.
3. Preencha os campos.

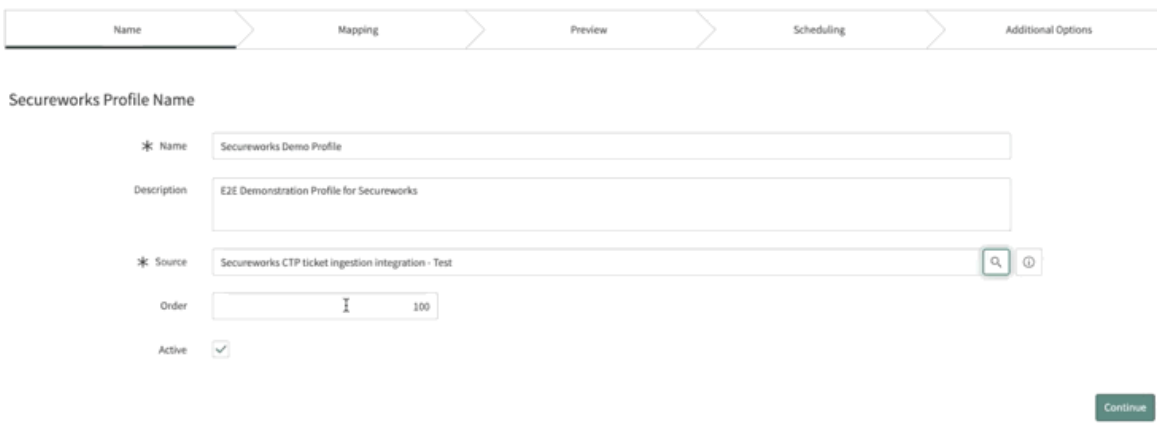
   Um exemplo de um formulário preenchido segue a tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e os nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.
Origem	Selecione a origem de onde você deseja ingerir os dados.
Ordem	O padrão é 100. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. Menor o valor do pedido, maior a prioridade.
Ativo	Esta opção é desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo. **Nota:** Você deve concluir todas as seções no perfil antes de ativá-lo.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois
Mapeie os campos do tíquete.

Mapeamento de campos de tíquete para a integração do SecureWorks CTP

Mapeie os campos de tíquete e evento para os campos no formulário de incidente de segurança.

Para a etapa de mapeamento, você deve primeiro ingerir tíquetes de amostra e, em seguida, garantir que todos os campos de tíquete relevantes sejam mapeados para o local apropriado no Resposta a incidentes de segurança e visualize o incidente de segurança na seção de visualização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O mapeamento dos campos de tíquete de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: Consulte Ingestão de tíquetes do Secureworks de amostra
- Mapeando os campos de tíquete para o incidente de segurança: Consulte Mapeando campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Ingestão de tíquetes do Secureworks de amostra

Selecione os tíquetes de amostra que serão ingeridos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os cinco tíquetes de amostra mais recentes ou fornecer os IDs de tíquete exclusivos para os tíquetes específicos que você deseja usar para sua experiência de mapeamento.
   Em **Preferência de ingestão** lista de seleção, selecione uma das seguintes opções:
   - Recuperar tíquetes mais recentes: Os 5 tíquetes mais recentes são recuperados.
   - Selecionar tíquetes com base no ID do tíquete: Especifique o ID do tíquete a ser recuperado. Você pode especificar um máximo de 5 ids de tíquete separados por vírgulas.
3. Clique em **Buscar dados de amostra** para extrair os dados de tíquete de amostra mais recentes do Secureworks CTP servidor.
   A extração de tíquetes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Os tíquetes recuperados são exibidos como guias individuais. Clique em uma guia para exibir os dados do tíquete. Para cada tíquete, você pode ver os campos do tíquete e seus valores e os detalhes do evento de contribuição que acionou o tíquete.

   Nota: Você verá detalhes dos eventos contribuintes somente se eles tiverem ocorrido nos últimos 7 dias. Eventos com mais de 7 dias não são exibidos.

O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de tíquete para o incidente de segurança.

Mapeando campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Mapeie campos de tíquete ou evento individuais para campos em um ServiceNow AI Platform SIR incidente de segurança.

Mapeamento de campo de tíquete

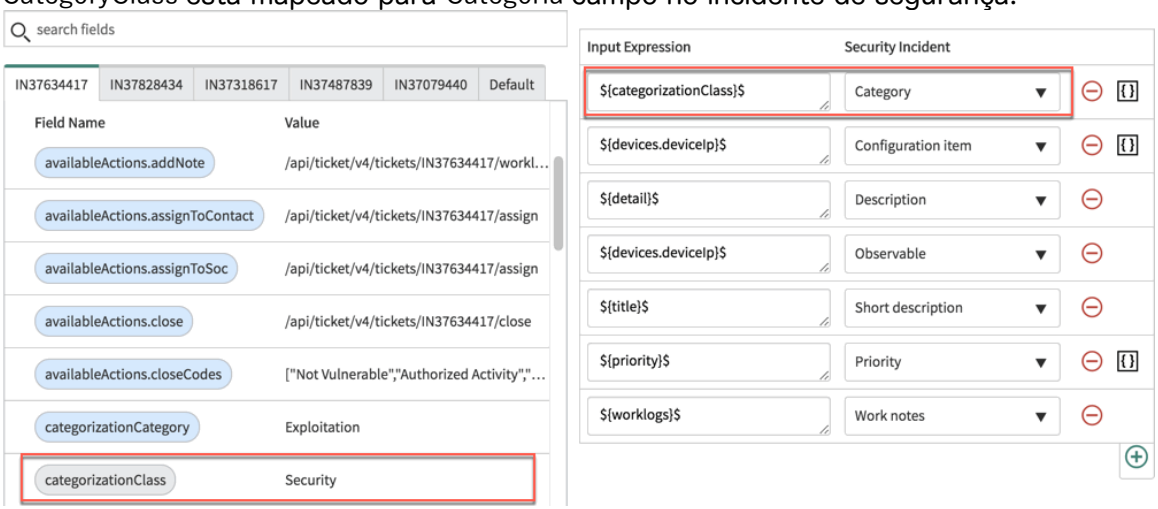
Como um usuário com a função sn_si.admin, use os campos da seção Tíquetes de amostra à esquerda e mapeie-os para os campos de incidente de segurança no **Mapeamento de campo de incidente DO SIR** coluna. Edite a configuração de mapeamento arrastando os campos de tíquete ou evento do lado esquerdo e soltando-os na seção Mapeamento de campo de incidente DO SIR à direita. O mapeamento à direita associa o campo de tíquete de entrada a um campo de incidente de segurança de saída.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
2. Você pode inserir manualmente o nome do campo na coluna Expressão de entrada ou arrastar e soltar o nome do campo. Por exemplo, descrição e solte-o em um campo no **Expressão de entrada** coluna ao lado de um nome de campo no **Incidente de segurança** coluna.

   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, CategoryClass está mapeado para Categoria campo no incidente de segurança.



> **Nota:** Se você inserir o nome do campo Evento manualmente no **Expressão de entrada** , você deve adicionar um prefixo como `Event:eventfield` antes do nome do campo que está sendo mapeado.

Para ajudar você a garantir que nenhum campo de tíquete ou evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de tíquete ajuda a acompanhar os valores de tíquete que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de tíquete importante restante permanece não mapeada.

Campos azuis claros à esquerda indicam que um campo de tíquete ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um tíquete de entrada ou campo de evento a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Esta codificação por cores ajuda você a rastrear o mapeamento.

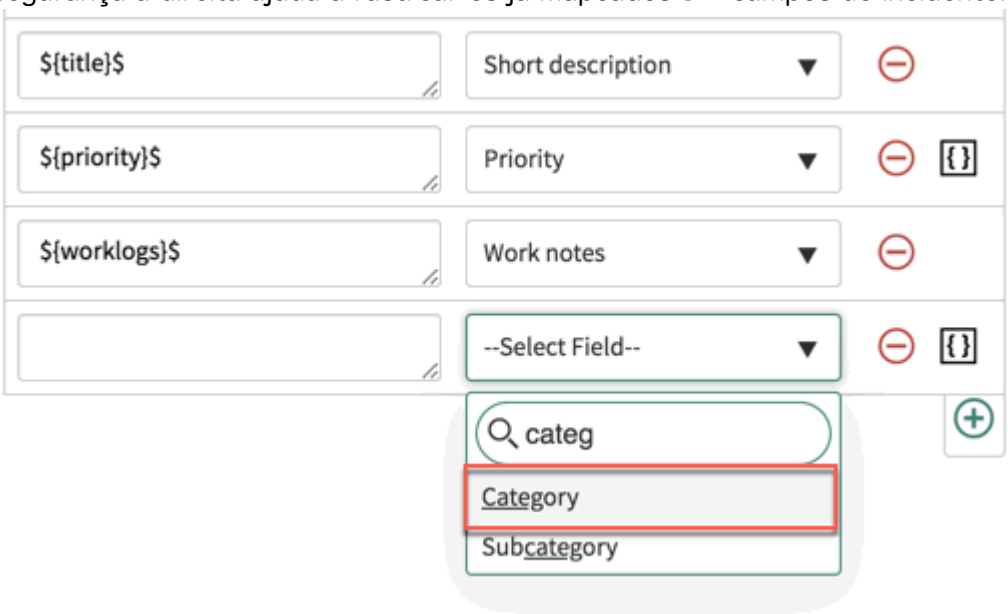
3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário em SIR Na seção Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição. Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida do novo campo, alguns campos são sombreados. Na figura a seguir, Categoria tem um fundo cinza, porque foi mapeada no incidente de segurança. Semelhante à codificação por cores dos campos de tíquete no lado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear os já mapeados SIR campos de incidente.



Nota: Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, selecione o campo de tíquete e arraste-o e solte-o em um campo de incidente de segurança apropriado à direita.

4. Remova campos usando o ícone - ao lado do nome do campo na seção Mapeamento de campo de incidente SIR.

5. Continue o mapeamento adicionando ou removendo valores de campo ao mapeamento.

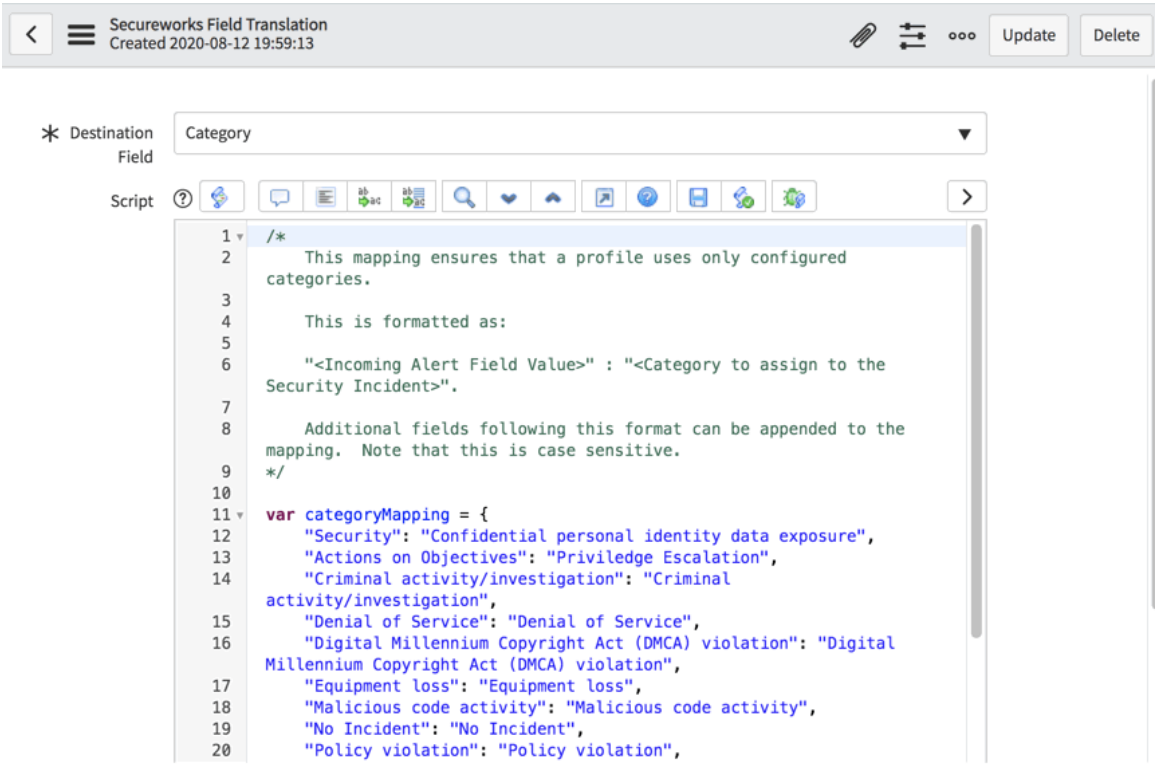
Tradução de campo de formato

Em determinados casos, os campos de tíquete podem não ser traduzidos diretamente para os campos no SIR incidente de segurança. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria Alerta de malware e infecção por vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser traduzidos em uma Atividade de código mal-intencionado comum no campo Categoria no SIR Incidente de segurança usando a funcionalidade Formatar tradução de campo.

Para usar o editor de scripts, clique no ícone ao lado do campo Categoria. O editor de script é exibido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



.

Insira as mudanças no script e clique em **Atualização** Para salvar as mudanças e retornar à página Mapeamento.

Condições de geração de incidentes

Quando a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais tíquetes devem criar incidentes de segurança versus quais tíquetes devem ser filtrados, por exemplo, tíquetes de baixa prioridade. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um tíquete de entrada deve atender para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até **Condições de geração de incidentes** no formulário e selecione **Filtro com base em condições** marque a caixa para habilitar a opção.

   O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos no **Ingestão de tíquete de amostra** seção dos tíquetes ingeridos. Esses campos são dinâmicos e mudam dependendo dos tíquetes que você ingerir. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores de Secureworks CTP tíquete. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao Secureworks CTP console e revise seus tíquetes para as palavras-chave.

   Nota: . `logs de trabalho` , `dispositivos` , `anexos` , `observadores` , `disponivelações` e `CloseCodes` os campos de tíquete podem ter vários valores (pois os valores são armazenados em matrizes). Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar `contém` condição de filtro para esses campos para garantir que os dados sejam filtrados corretamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
   - Se **E.** selecionado, todas as condições devem ser correspondidas.
   - Se **OU** está selecionado, qualquer condição pode ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

   Este tipo de filtragem de condição de geração de incidentes ajuda a restringir os tíquetes e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a regra ou os filtros subjacentes. Se critérios de filtragem adicionais forem definidos, somente os tíquetes que corresponderem a todos os critérios serão mapeados para incidentes de segurança.

Critérios de agregação de tíquete para lidar com tíquetes semelhantes e evitar incidentes duplicados

Defina critérios de agregação de tíquete adicionais que agregue um tíquete de entrada a um existente SIR incidente de segurança em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, esse recurso de agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de tíquete relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

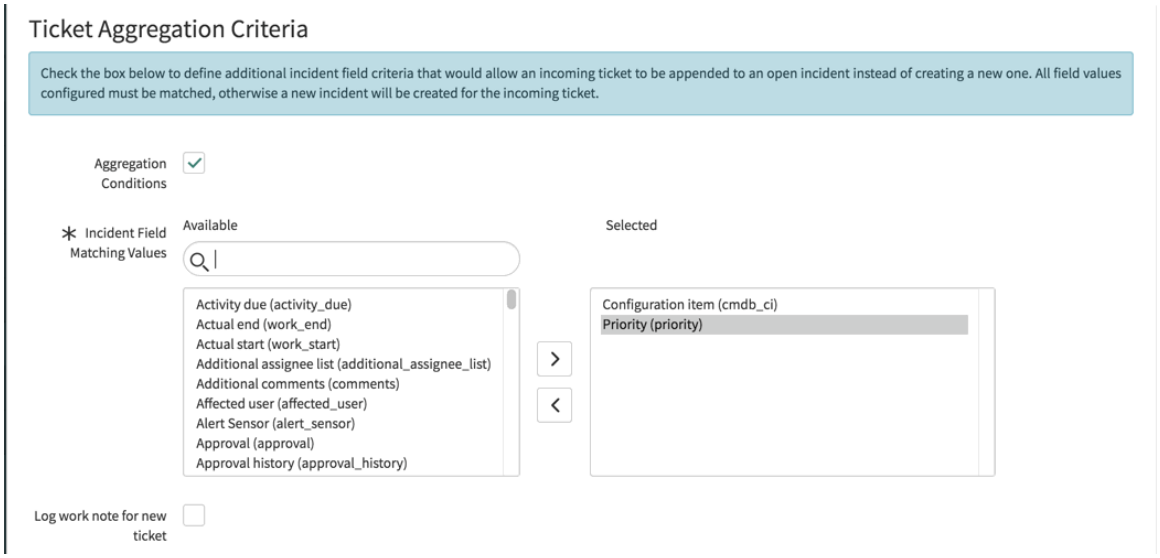
1. Role até **Critérios de agregação de tíquete** no formulário e selecione **Condições de agregação** marque a caixa para habilitar esta opção.

   As colunas Valores de correspondência do campo do incidente são exibidas. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder nos incidentes de segurança existentes na NOW Platform e mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este tíquete de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de tíquete mapeados para eles. Todos os valores devem corresponder. Se somente um subconjunto dos valores for correspondido, as condições de agregação de tíquete não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para obter o mapeamento de campos de vários valores.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se um novo tíquete corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo tíquete será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os tíquetes agregados adicionados em uma lista relacionada em um incidente de segurança. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam você a entender por que esses tíquetes estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida em um incidente de segurança, role para o lado esquerdo do registro em **Links relacionados** e clique em **Mostrar todas as listas relacionadas** link.

Nota: A lista relacionada Tíquetes agregados do Secureworks não está disponível com o sistema de base. Você deve configurar o layout da Lista relacionada e incluí-lo explicitamente com as outras listas relacionadas.

3. (Opcional) Para registrar em log uma anotação de trabalho para um novo tíquete que foi adicionado recentemente no incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra em log que um novo tíquete foi adicionado junto com um link para os detalhes do tíquete e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Valores mapeados com sucesso de um Secureworks CTP tíquete para campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexou tíquetes a incidentes de segurança existentes quando os valores do campo de tíquete correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um SIR incidente de segurança

Visualize os valores mapeados no incidente de segurança

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de tíquete que deseja exibir no incidente de segurança.

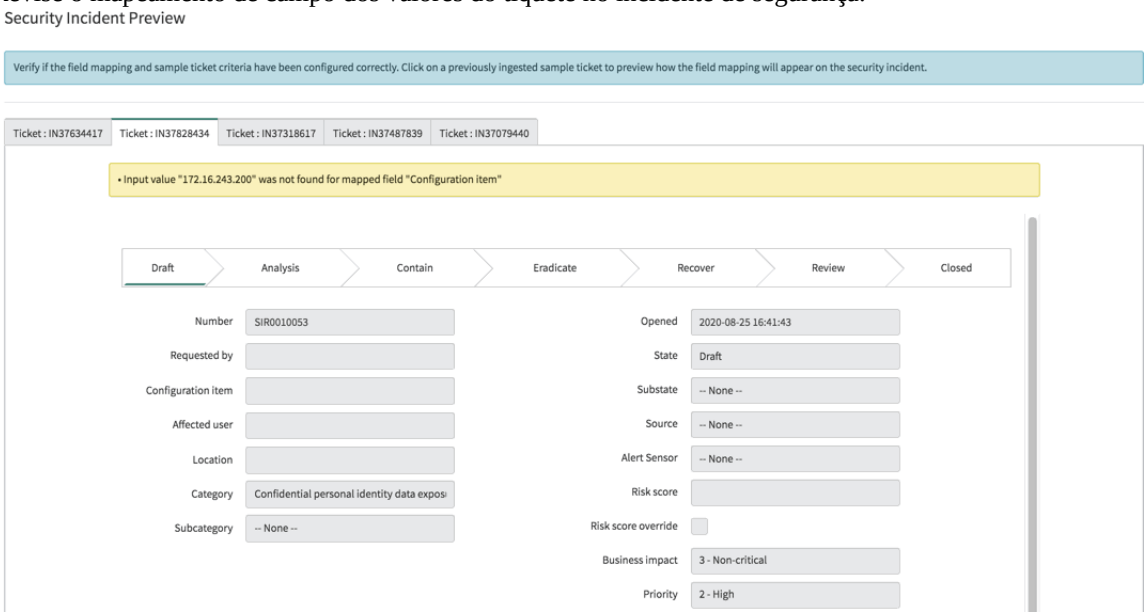
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. Visualizações de SIR Os incidentes de segurança não são salvos como incidentes reais no produto Resposta de incidentes de segurança.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
   Os tíquetes são exibidos como guias.
2. Clique em uma guia para visualizar o incidente de segurança.
   Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores do tíquete no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança. Defina a programação.

Defina a programação para a ingestão de tíquete do Secureworks CTP

Verifique as configurações padrão para recuperação de tíquete ou modifique a programação conforme necessário. Esta etapa permite filtrar a recuperação do tíquete com base em um intervalo de datas e um intervalo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também escolhe com que frequência pesquisará tíquetes futuros que correspondam à configuração do perfil do tíquete. Configure esses intervalos de pesquisa por perfil. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de um minuto é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

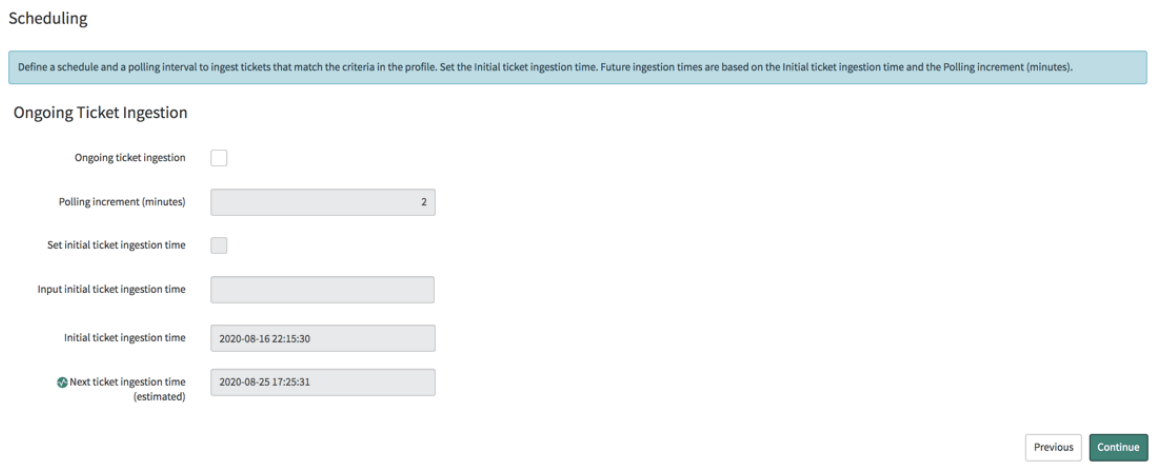
Procedimento
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando os tíquetes são extraídos do Secureworks CTP portal.

Opção	Descrição
Ingestão de tíquete contínua selecionada	Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do Secureworks CTP portal para novos tíquetes a cada cinco minutos. Os incidentes de segurança serão criados se tíquetes forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a ingestão de tíquete em relação à carga do servidor e extrair os dados mais atuais, cinco minutos é a configuração que você pode preferir. No entanto, este valor pode ser modificado conforme necessário.
○ Ingestão de tíquete contínua selecionada ○ Defina o tempo de ingestão do tíquete inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas: ○ Selecione os campos Ingestão de tíquete em andamento e Definir tempo de ingestão de tíquete inicial. ○ Especifique a hora no campo Tempo de ingestão de tíquete inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida no campo Incremento de pesquisa (minutos). Como exemplo de programação, se você tiver um trabalho de tíquete diário que é executado uma vez por dia às 4 hora local, poderá configurar o perfil de tíquete correspondente em seu ServiceNow AI Platform Instância a ser executada às 4:05 hora local para capturar o tíquete imediatamente e criar um incidente de segurança. Insira 04 05 00 no campo Ingestão de tíquete inicial. No campo Incremento de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	pesquisa (minutos), insira 1440 (24 horas) para programar a próxima ingestão de tí–quete para 24 horas a partir da ingestão inicial do tíquete. O horário de ingestão do tíquete inicial e o próximo horário de inges–tão do tíquete são exibidos nos campos. Para definir as configurações neste exem–plo, siga estas etapas: ○ Selecione **Ingestão de tíquete contínua** opção. ○ No campo Incremento de pesquisa (mi–nutos), insira 1440 (24 horas). ○ Selecione **Defina o tempo de ingestão do tíquete inicial** opção. ○ No campo Tempo de ingestão de tíquete inicial de entrada, insira 04 05 00. A hora da próxima ingestão de tíquete é exibida no campo Tempo da próxima ingestão de tíquete (estimado).



Tradução automática

3. Clique em **Continuar** Para navegar até a página Opções adicionais.

Automatize atualizações e fechamento de tíquetes com base no status do incidente SIR

. Secureworks CTP A integração de ingestão de tíquete tem uma interface bidirecional que permite que ambos os tíquetes criem incidentes de segurança, bem como a capacidade de atualizar os tíquetes depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como número do incidente de segurança, grupo de atribuição, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais** .
2. Conclua a configuração para atualizar tíquetes quando o incidente de segurança for criado.

Opção ou Campo	Descrição
Atualizar anotações de trabalho DO SIR com logs de trabalho do Secureworks	Selecione esta opção para habilitar os logs de trabalho do Secureworks e SIR recurso de sincronização de anotações de trabalho. Isso permite que você rastreie atualizações feitas no tíquete em Secureworks CTP depois que o incidente de segurança é criado. **Nota:** ◦ Se o campo Worklogs do Secureworks tiver sido mapeado para o campo Anotações de trabalho DO SIR, os worklogs do Secureworks serão recuperados até que o incidente de segurança seja criado. ◦ Se o recurso de sincronização estiver habilitado, somente os logs de trabalho criados ou atualizados após a criação de um incidente de segurança serão recuperados.
Atualizar tíquetes do Secureworks após a criação do incidente SIR	Selecione esta opção para atualizar o. Secureworks CTP tíquete e adicione comentários adicionais quando um incidente de segurança é criado a partir do tíquete. Isso pode ocorrer para os tíquetes de gatilho iniciais que criam o incidente de segurança, bem como tíquetes agregados.
Comentários iniciais retornados ao tíquete do Secureworks	Quando um incidente de segurança é criado, o tíquete é atualizado automaticamente em Secureworks CTP com comentários. Você pode modificar o texto padrão e usar o formato "nome do campo" para adicionar ou modificar todos os campos disponíveis no formulário de incidente de segurança.
Fechar tíquetes do Secureworks após o fechamento do incidente SIR	Selecione esta opção se quiser usar a opção de fechamento automatizado de tíquete. Isso pode ocorrer para os tíquetes de gatilho iniciais que criam o incidente de segurança, bem como tíquetes agregados. Quando um incidente de segurança é encerrado, o tíquete correspondente é encerrado automaticamente em Secureworks CTP junto com o mesmo código de fechamento do incidente de segurança e os comentários de fechamento padrão especificados no perfil. **Nota:** Você não pode usar esta opção para atualizar o status do tíquete mestre.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou Campo	Descrição
Comentários de fechamento publicados novamente no tíquete do Secureworks	Os comentários de fechamento padrão são exibidos aqui. Você pode editar o texto padrão e usar o formato "nome do campo" para adicionar ou modificar todos os campos disponíveis no formulário de incidente de segurança.

3. Clique em **Concluir** para concluir a configuração e mover o perfil para **Aguardando** estado.
   Uma caixa de diálogo de confirmação é exibida. Você configurou o perfil com sucesso. Ative este perfil para extrair tíquetes do Secureworks CTP portal baseado em sua programação.

Opcional: Copie um perfil do Secureworks CTP

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis para economizar tempo.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Tudo** > **Integração de ingestão de tíquete do Secureworks** > **Perfil do Secureworks**.
2. Na lista Perfis do Secureworks exibida, selecione um perfil que você deseja copiar e, no **Ações nas linhas selecionadas** lista de seleção, clique em **Cópia** .
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém (cópia). Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que **Ativo** o status da coluna é definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois
Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

O formulário de resposta a incidentes de segurança muda após a ingestão do tíquete

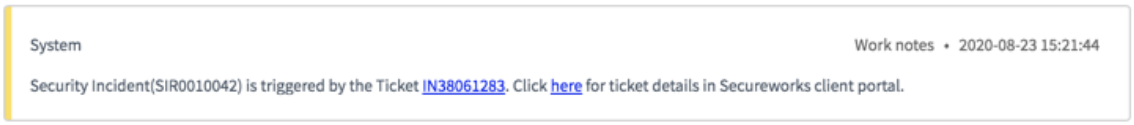
Depois de um Secureworks CTP o tíquete foi ingerido, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada com detalhes do tíquete que acionou o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



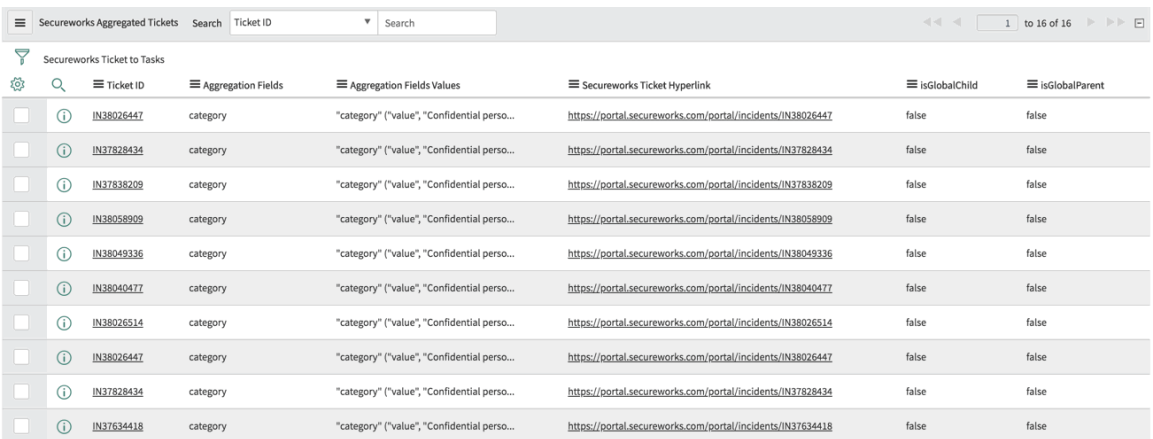
Clique no link do tíquete para navegar até o registro de tíquete interno do Secureworks para tarefa. . **Clique aqui** o hiperlink leva você para Secureworks CTP painel onde você pode exibir os detalhes do tíquete.

Se você tiver selecionado **Anotação de trabalho em log para o novo tíquete** Nos Critérios de agregação de tíquete, conforme descrito na página Criar perfil: Mapeamento, uma anotação de trabalho é publicada quando o tíquete é agregado.



Tíquetes agregados

Clique **Listas relacionadas** > **Tíquetes agregados do Secureworks** para exibir o tíquete agregado ao incidente de segurança. Clique no hiperlink do tíquete para exibir o tíquete no Secureworks CTP painel.



Criar incidente de segurança: Selecione um tíquete na lista e clique em **Ações** e clique em **Criar incidente de segurança** . Esta opção cria um novo incidente de segurança para o tíquete e este tíquete é desagregado do incidente de segurança primário.

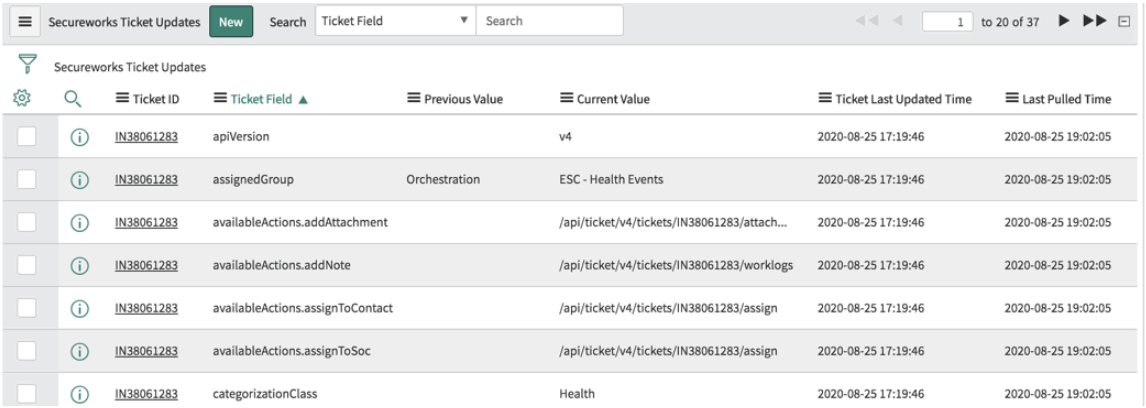
Excluir registro de tíquete: Selecione um tíquete na lista e clique em **Ações** e clique em **Excluir** . Esta opção exclui o registro do tíquete.

Atualizações de tíquete do Secureworks

Mostra os campos de tíquete padrão e rastreia as mudanças nos tíquetes durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir atualizações de tíquete diretamente sem navegar até Secureworks CTP painel. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.

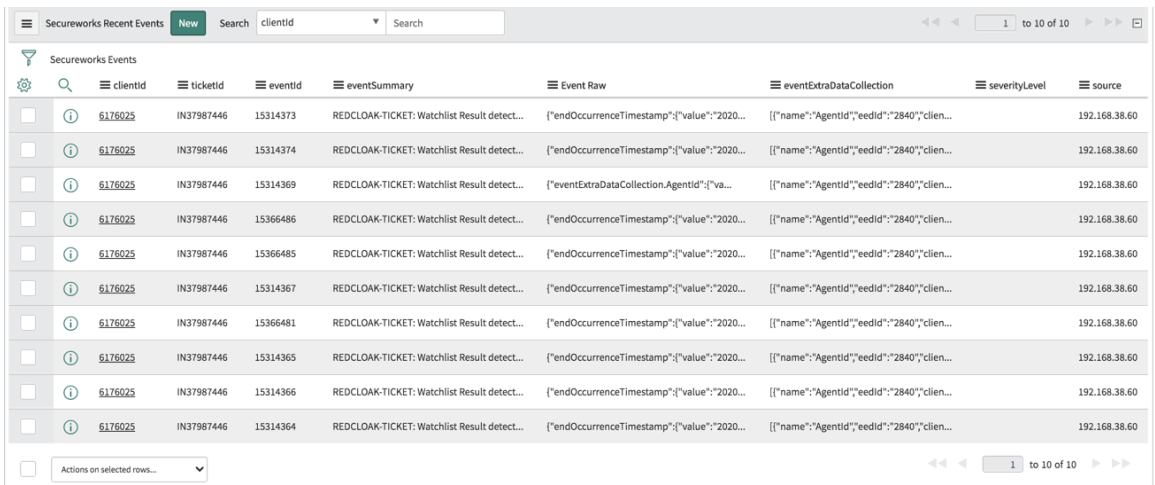
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Eventos recentes do Secureworks

Clique em **Buscar eventos recentes do Secureworks** opção em **Links relacionados** Para exibir os eventos mais recentes do Secureworks.



Por padrão, um número máximo de 50 eventos será exibido. Você pode modificar essa configuração padrão nas Configurações de integração do Secureworks.

Exiba os tíquetes do Secureworks e os incidentes de segurança correspondentes

Importados Secureworks CTP Os tíquetes são armazenados inicialmente na tabela Importação de tíquete. Exibir todos os Secureworks CTP tíquetes que foram importados antes da aplicação de qualquer condição de filtro.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Integração de ingestão de tíquete do Secureworks** > **Importação segura de tíquete**.
2. Você pode exibir todos os Secureworks CTP tíquetes que foram importados antes de serem agregados ou que quaisquer condições de filtro sejam aplicadas.
3. Clique em um ID de tíquete para ver os dados brutos do tíquete.
4. Navegar até **Ingestão de tíquete do Secureworks** > **Tíquete do Secureworks para tarefa**.
   . Secureworks CTP os tíquetes com os incidentes de segurança correspondentes são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aviso de fechamento do tíquete principal do Secureworks CTP

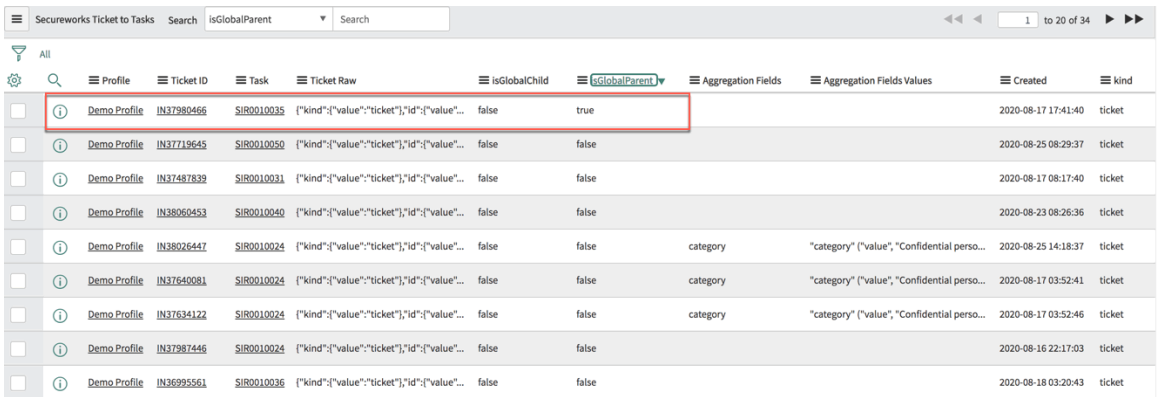
Antes de fechar um incidente de segurança criado por um Secureworks CTP tíquete mestre, você deve verificar se todos os tíquetes secundários associados ao tíquete mestre estão encerrados.

Antes de Iniciar

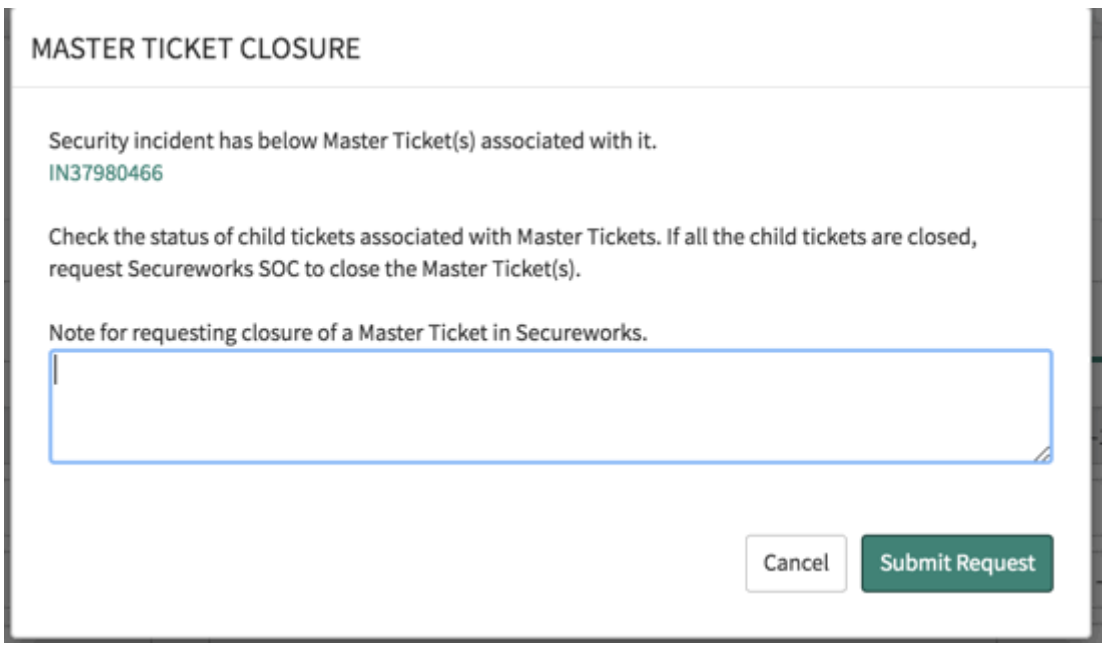
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Ingestão de tíquete do Secureworks** > **Tíquete do Secureworks para tarefa**.
   . Secureworks CTP os tíquetes com os incidentes de segurança correspondentes são exibidos.



2. Clique no incidente de segurança com **IsGlobal Parent** campo definido como **verdadeiro.**
3. Altere o estado do incidente de segurança para **Encerrado** , especifique os códigos de fechamento e clique em **Salvar** .
   A seguinte caixa de diálogo é exibida.



Este incidente de segurança está associado a um tíquete mestre do Secureworks. Um tíquete mestre pode ter um ou mais tíquetes secundários associados a ele. Antes que o tíquete mestre possa ser fechado, você deve primeiro verificar se todos os tíquetes secundários associados a este tíquete mestre estão encerrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

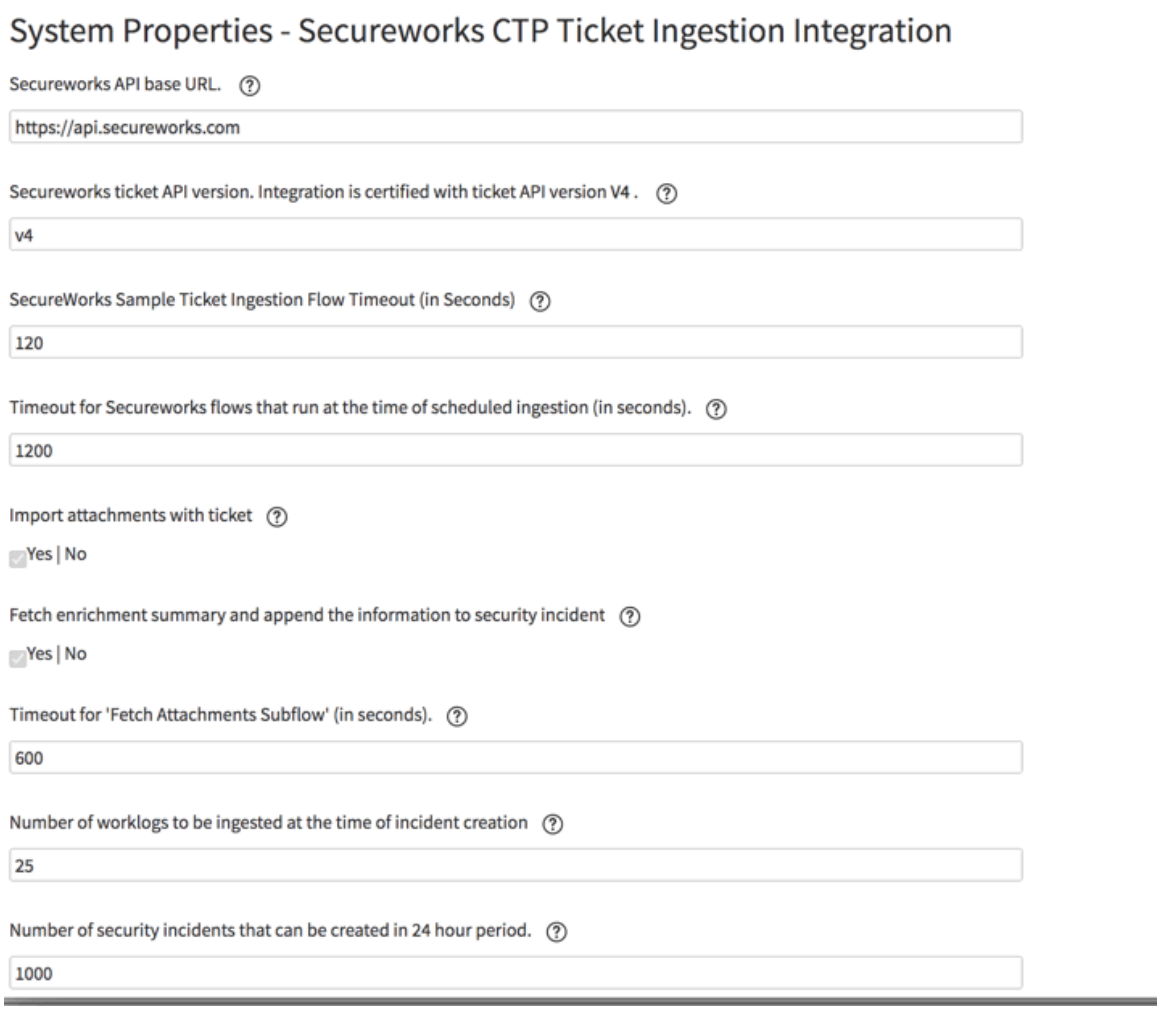
4. Adicione uma anotação solicitando o fechamento do tíquete mestre no Secureworks e clique em **Enviar solicitação** .
   O tíquete mestre agora foi reatribuído à equipe SOC do Secureworks.
5. Depois que a solicitação for enviada, você poderá fechar o incidente de segurança.
6. Navegar até **Aplicação** > **Módulo**.

Definições de configuração

Use esta opção para modificar Secureworks CTP propriedades do sistema padrão da integração de ingestão de tíquete.

Para modificar as propriedades do sistema, faça login como um usuário com *sn_si.admin* e navegue até **Integração de ingestão de tíquete do Secureworks** > **Configurações de integração do Secureworks**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.



Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Integração da Resposta a incidentes de segurança com Zscaler

Você pode usar Integração da Resposta a incidentes de segurança com Zscaler produto para conectar seu Zscaler Internet Access Logs do servidor (ZIA) com ServiceNow AI Platform. Esta integração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

permite que você exiba painéis, crie alertas personalizados e ajude a investigar incidentes de segurança.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

. Zscaler o produto de gateway de internet e web é entregue a partir da nuvem. Ele fornece os principais pontos de dados e informações sobre seu ambiente de segurança empresarial. Integração da Resposta a incidentes de segurança com Zscaler conecta o. Zscaler Internet Access produto com seu ServiceNow AI Platform instância. Usando o. Zscaler produto no ServiceNow AI Platform, você obtém mais informações sobre o uso da internet da sua organização.

Principais recursos da integração

Esta integração inclui os seguintes recursos principais:

- Pesquisa de reputação de observáveis em relação à biblioteca de ameaças global que o Zscaler o produto mantém.

  Nota: . Zscaler a biblioteca de ameaças global lista as ameaças por tendências, país de origem, destino de destino, volume e várias categorias de ameaça. Esta biblioteca de ameaças global permite que você investigue seus observáveis em relação ao cenário de ameaças globais.

- Manutenção de observáveis em uma lista de bloqueios ou lista de permissões no Zscaler produto.
- Capacidade de buscar e revisar relatórios de área restrita do Zscaler Produto para um hash MD5. O recurso Sandbox em nuvem no Zscaler o produto executa e analisa arquivos em um ambiente virtual para detectar comportamento mal-intencionado.
- Alertas de segurança de eventos do Paciente 0 gerados no Zscaler produto quando um usuário baixa um arquivo mal-intencionado desconhecido.
- Várias listas de categorias de URL que atuam como listas de bloqueio ou listas de permissão, conforme definido em Zscaler produto.
- ServiceNow AI Platform Incidentes de segurança que podem ser marcados para identificar a categoria de URL à qual os observáveis são adicionados.
- Períodos de expiração que mantêm o tamanho das entradas da lista de categorias de URL expirando ou removendo automaticamente as entradas mais antigas.
- Fluxo de trabalho de aprovação para adicionar e remover observáveis das listas de categorias de URL.
- Entradas de categoria de URL que podem ser vinculadas a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Conheça esta integração

Identificador do documento	Título do documento
Zscaler site de documentação do produto	Zscaler Product Documentation

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificador do documento	Título do documento
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece com Integração da Resposta a incidentes de segurança com Zscaler

Ativar e configurar o. Zscaler Internet Access produto para fazer interface com seu ServiceNow AI Platform instância e. Resposta a incidentes de segurança produto.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique o necessário ServiceNow AI Platform e. Resposta a incidentes de segurança funções.	Estas funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria, ativa e remove as listas de categorias de URL. ◦ Atribui a função sn_si.analyst. • A função sn_si.analyst cria entradas e funciona com incidentes de segurança.
Verifique se o ServiceNow as aplicações principais são instaladas e ativadas antes de configurar esta integração.	. ServiceNow IntegrationHub Instalador do Enterprise Pack [o plug-in com.glide.hub.integrations.enterprise] é necessário. . Resposta a incidentes de segurança o plug-in (com.snc.security_incident) é obrigatório. Este plug-in instala automaticamente todas as dependências do Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações para a integração. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, instale e ative cada aplicação uma de cada vez na seguinte ordem: 1. Resposta a incidentes de segurança Dependência (com.snc.si_dep) 2. Framework de integração de segurança 3. Security Support Common

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	4. Orquestração do suporte de segurança **5.** Inteligência contra ameaças Suporte Comum **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Resposta a incidentes de segurança
Verifique Zscaler versões.	• Esta integração é compatível com Zscaler Internet Access versão 1,0 ou posterior. • Esta integração é testada com o seguinte Zscaler versões: ◦ Zscaler Client Connector para Windows - 3,0 ◦ Zscaler Client Connector para macOS - 3,0 ◦ Zscaler Client Connector para Linux - Beta ◦ Zscaler Cloud Connector - 6,1
Verifique se você tem o necessário Zscaler e configuraram acesso ao Zscaler Internet Access APIs.	• Você deve ter as credenciais de administrador para Zscaler Internet Access. • Você deve ter uma assinatura de API de serviço de nuvem válida. Zscaler O suporte deve fornecer sua chave. • Você deve ter Zscaler Internet Access credenciais de administrador (nome de usuário e senha). A autenticação de API é baseada em uma combinação da chave de API e. Zscaler Internet Access credenciais de administrador. **Nota:** Para obter mais informações sobre como gerenciar o. Zscaler Internet Access Chaves de API, consulte Documentação do Zscaler .

Configure o acesso ao Zscaler Internet Access APIs

Configure o acesso ao Zscaler Internet Access servidor para autenticar a conexão segura entre ServiceNow AI Platform e Zscaler servidor.

Antes de Iniciar

Função necessária: administrador do Zscaler Internet Access

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Após Zscaler Habilita sua assinatura de API para o serviço de nuvem da sua organização, ela está disponível em Zscaler Internet Access Página de gestão de chaves de API com o URL de base. Sua organização só pode ter uma chave de API ou token. Exclua a chave ou token existente antes de adicionar um novo.

A URL base da API é `Cloud_Name/api/v1` . Verifique Zscaler nome da nuvem que foi provisionado para sua organização e use-o para substituir `(Cloud_Name)` No URI de base. Alguns exemplos da URL base são:

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Nota: Para obter mais informações sobre Zscaler Internet Access portal de administração, consulte Documentação de gestão de chaves da API Zscaler e o. Documentação do Portal Zscaler .

Procedimento

1. Faça login como administrador do Zscaler Internet Access portal de administração.
2. Navegar até **Administração** > **Segurança de API de serviço em nuvem**.
3. Clique em **Adicionar chave de API** .
   Se você não vir **Adicionar chave de API** excluir a chave existente.
   A nova chave de API é imediatamente válida e é exibida na guia .

Resultado

Você recuperou o URL base e a chave de API para configurar o acesso Zscaler em ServiceNow AI Platform instância.

Instalar e configurar Integração da Resposta a incidentes de segurança com Zscaler

Instale e configure o. Integração da Resposta a incidentes de segurança com Zscaler Produto de acesso à Internet do ServiceNow Store para começar a usar a integração em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe o. Integração da Resposta a incidentes de segurança com Zscaler produto do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE Integração da Resposta a incidentes de segurança com Zscaler lado a lado e clique **Configurar** > **Criar nova configuração**.
4. No formulário, preencha os campos.

Tradução automática

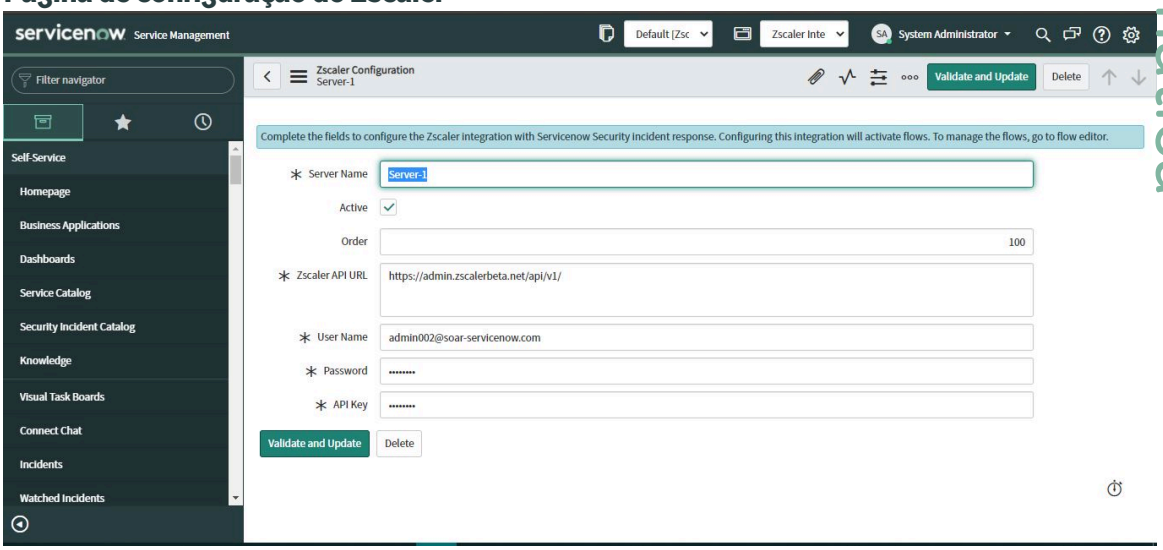
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Zscaler Formulário de configuração

Campo	Descrição
Nome do servidor	Zscaler nome do servidor. Por exemplo, ZSserver.
Ativo	Indicador de que o perfil está ativo.
Ordem	Prioridade de fluxo. O valor desse campo indica a ordem dos fluxos de trabalho quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Zscaler URL DA API	URL base que hospeda o. Zscaler API. Por exemplo, https://example.zscalerbeta.net
Nome de usuário	Nome de usuário do Zscaler Internet Access conta de administrador.
Senha	Senha do Zscaler Internet Access conta de administrador.
Chave de API	Chave de API que você obteve do Zscaler Internet Access portal de administração.

O exemplo a seguir mostra a página de configuração do Zscaler.

Página de configuração do Zscaler



5. Clique em **Validar e atualizar** .

Resultado

Depois de validar e salvar esta configuração, retorne ao Zscaler Página Configurações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar Zscaler Internet Access Listas de categorias de URL

Adicione as categorias de URL que estão disponíveis no Zscaler Produto de acesso à Internet para ServiceNow AI Platform Instância para especificar uma ação para cada URL para que você tenha acesso fácil para filtragem granular e criação de política.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

. Integração da Resposta a incidentes de segurança com Zscaler Fornece uma lista de permissões padrão e listas de categorias de URL da lista de proibições para ajudar a filtrar o conteúdo.

As categorias de URL que você adiciona no ServiceNow AI Platform a instância já deve estar em seu Zscaler Internet Access ambiente. Você não pode usar Integração da Resposta a incidentes de segurança com Zscaler Para criar categorias de URL em Zscaler.

Nota: Para obter mais informações sobre listas de categorias de URL no Zscaler produto, consulte Documentação do Zscaler sobre Categorias de URL .

Procedimento

1. Navegar até **Tudo** > **Integração do Zscaler** > **Listas de categorias de URL do Zscaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário Listas de categorias de URL

Campo	Descrição
Origem	Nome do servidor. Você pode exibir somente o configurado anteriormente Zscaler Internet Access Servidores da lista de categorias de URL.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Categoria de URL	Campo habilitado depois que você seleciona a origem. Você pode exibir a lista de categorias de URL que são criadas em Zscaler.
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao mudar este valor, qualquer observável adicionado a esta categoria de URL ficará ativo pelo número de dias que você inserir. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias.
Marcador de exibição	Marcador de segurança que aparece no SIR incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando você habilita **Marcador de exibição** . Zscaler O campo Marcador para observáveis está disponível no formulário.
Criar solicitação de mudança	Solicitação de mudança e tarefas de mudança em seu ServiceNow AI Platform Instância dos registros anexados à lista de categorias de URL. Quando você habilita **Criar solicitação de mudança** . **Solicitação de mudança** o campo está disponível no formulário.
Requer Aprovação	Lista de grupos de aprovadores. Depois de enviar uma solicitação, uma aprovação é necessária do grupo para concluir a solicitação. Quando você habilita **Aprovação necessária** . **Aprovadores para adicionar observáveis** e. **Aprovadores para remover observáveis** os campos estão disponíveis no formulário. ○ **Aprovadores para adicionar observáveis** : Selecione os aprovadores usando a Pesquisa para adicionar os observáveis do **Lista de categorias de URL do Zscaler** página. Esta opção permitirá que você adicione o(s) grupo(s) de usuários para aprovações. ○ **Aprovadores para remover observáveis** : Selecione os aprovadores para remover os observáveis usando a pesquisa do **Lista de categorias de URL do Zscaler** página. Esta opção permitirá que você remova os grupos de usuários da lista de aprovação.
Descrição	Descrição do Zscaler Lista de categorias de URL. Use este campo para adicionar mais detalhes sobre o registro da categoria de URL.

4. Clique em **Enviar**.
   Um envio bem-sucedido aciona uma notificação por e-mail para o grupo de aprovação.

Envie observáveis de um registro de incidente de segurança para uma lista de categorias de URL

Envie observáveis anexados a um registro de incidente de segurança para uma lista de categorias de URL configurada usando a solicitação Permitir ou bloquear. Adicionar observáveis à lista de permissões ou bloqueios para verificações de segurança permite que os usuários revisem o conteúdo desses URLs e obtenham acesso ao conteúdo confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

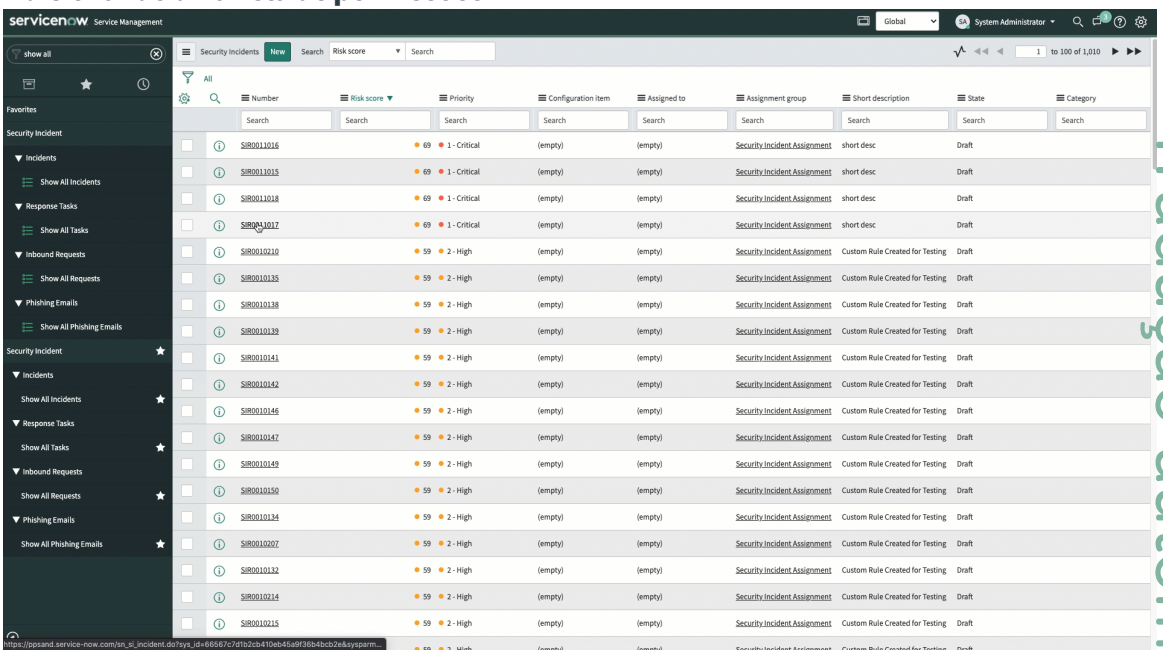
Por Que e Quando Desempenhar Esta Tarefa

Você envia entradas de observáveis usando a ação Permitir ou bloquear solicitação da lista relacionada Observáveis associados. Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicarão uma invasão. Use a lista de Categorias de URL configuradas anteriormente para selecionar o observável que você deseja enviar. Depois de enviar a solicitação, uma solicitação de aprovação será enviada para o seu grupo de aprovação.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**.
   Neste exemplo, você vê como selecionar um incidente de segurança e um observável e como adicionar uma lista de permissões.

Adicionando uma lista de permissões



2. Selecione o incidente de segurança que você deseja associar ao Zscaler solicitação de permissão ou bloqueio.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
   Se você não encontrar observáveis, clique em **Novo** .
4. Selecione um observável e, no menu Ações, clique em **Solicitação de permissão/bloqueio** .
5. Na caixa de diálogo Permitir/bloquear solicitação, selecione se deseja executar a solicitação de permissão ou bloqueio no observável.
6. Clique em **Enviar**.
7. Exiba as anotações de trabalho para ver o status do seu envio e os marcadores de segurança.
   Clique nos links nas anotações de trabalho para obter mais informações sobre o status ou para analisar os detalhes no Flow Designer. Marcadores de segurança são metadados no registro de resposta e definem quem deve ter acesso a tipos específicos de conteúdo de segurança.
8. Para exibir o status do observável selecionado, navegue até **Integração com Zscaler** > **Entradas da lista de categorias de URL do Zscaler**.
9. Na página Entradas da lista de categorias de URL do Zscaler, clique no observável para exibir o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprovar observáveis para listas de categorias de URL

Aprove observáveis que são adicionados a uma Lista de categorias de URL para que as entradas de observáveis estejam nas listas de permissão ou negação apropriadas.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Integração com Zscaler** > **Aprovações do Zscaler**.
2. Selecione o registro a ser aprovado.
3. Clique em **Aprovar**.
   O grupo de aprovadores recebe uma notificação por e-mail para a solicitação de aprovação. Depois que os aprovadores clicam em **Aprovar/Rejeitar** no e-mail, o status muda para aprovado.

Envie o incidente de segurança para Zscaler Lista de categorias de URL

Envie entradas diretamente para observáveis que não estão associados a um específico ServiceNow AI Platform registro de incidente de segurança para que as entradas observáveis estejam nas listas de permissão ou negação apropriadas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também pode adicionar observáveis à lista de categorias de URL diretamente do registro do observável.

Procedimento

1. Navegar até **Tudo** > **Integração com Zscaler** > **Entradas da lista de categorias de URL do Zscaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário Entradas de listas de categorias de URL

Campo	Descrição
Valor de Entrada	Nome do observável. Se um observável correspondente for encontrado, o restante do formulário será preenchido automaticamente. Se nenhum observável correspondente for encontrado, você deverá preencher o restante das informações manualmente.
Observável	Valor (por exemplo, endereço IP ou hash) associado ao observável.
Tipo de Observável	Classificação observável, como um endereço IP ou hash de arquivo.
Lista de categorias de URL	Categoria de URL. Por exemplo, se uma organização usa example.com para serviços do Office 365, então

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Zscaler Categoriza example.com como Serviços profissionais e Office 365.
Origem	Nome do servidor. Você pode exibir somente o configurado anteriormente Zscaler Servidores da lista de categorias de URL.
Contagem de incidentes	Número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Status	Se o observável for Aprovado ou Rejeitado.
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao alterar este valor, qualquer observável adicionado a esta categoria de URL ficará ativo pelo número de dias que você inserir. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias. **Nota:** Se você mudar o período de expiração padrão da entrada da lista de categorias de URL, verá um aviso de que o período difere do período configurado na lista de categorias de URL selecionada.
Informações adicionais	Campo em que você pode adicionar mais detalhes sobre o observável.

4. Clique em **Enviar**.

Execute uma pesquisa de ameaças usando Zscaler biblioteca de ameaças global

Execute uma pesquisa de ameaças em um observável usando Zscaler Internet Access biblioteca global de ameaças do produto. Zscaler Oferece suporte a pesquisas em IPs, URLs e domínios do tipo observáveis.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. Quando um observável é associado a um incidente de segurança pela primeira vez, todas as

Tradução automática

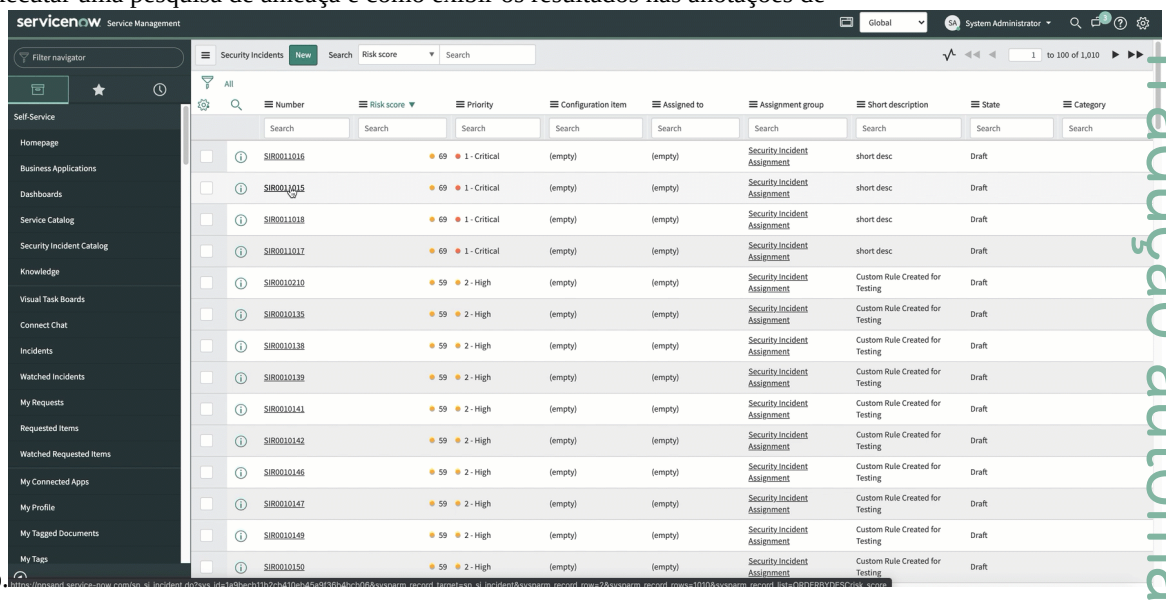
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

implementações de pesquisa de ameaças ativas no ServiceNow AI Platform execute uma pesquisa de ameaça automática. Você pode exibir os resultados em relação à lista relacionada Resultados de pesquisa de ameaças.

Por padrão, a configuração com a menor ordem é selecionada para executar a pesquisa de ameaças Zscaler Internet Access biblioteca global de ameaças do produto. Você também pode executar a pesquisa de ameaças manualmente.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a pesquisa de ameaças.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
4. Selecione o observável e, no menu Ações, clique em **Executar Pesquisa de ameaças** .
   Neste exemplo, você vê como selecionar um incidente de segurança e um observável, como executar uma pesquisa de ameaça e como exibir os resultados nas anotações de trabalho.



Tradução automática

Resultado

Depois de iniciar a pesquisa de ameaças, você pode exibir as anotações de trabalho para ver o status do seu envio.

Enviar para Zscaler Análise de área restrita

Use Zscaler Internet Access serviço de área restrita de produtos para analisar arquivos em um ambiente virtual para detectar comportamento mal-intencionado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

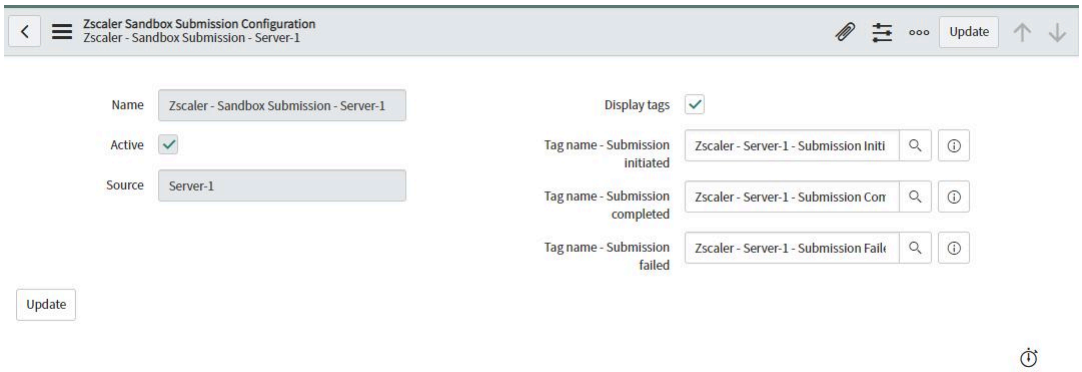
Ao criar um Zscaler configuração, a. Zscaler O envio da Sandbox é criado por padrão no módulo Configuração da Sandbox do Zscaler.

Os campos de nome e origem são preenchidos automaticamente e a configuração é habilitada por padrão. Você pode editar somente o marcador de exibição e as opções ativas. Zscaler Internet Access O produto permite que você busque somente o relatório de área restrita para observáveis do tipo hash MD5.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A análise do arquivo associado ao hash MD5 deve estar concluída e o relatório correspondente deve estar no Zscaler sandbox. Se o hash MD5 que você envia não tiver um relatório em Zscaler, você recebe uma mensagem de erro.

Envio da Sandbox do Zscaler



Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a análise de área restrita.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
4. Selecione um observável do tipo de hash MD5 e, no menu Ações, selecione **Enviar para Sandbox** . Crie um observável de tipo de hash MD5 se você não encontrar um observável de tipo de hash MD5 existente.
5. Na caixa de diálogo Envio de arquivo, selecione **Zscaler - Envio da área restrita - Servidor** Na configuração de envio e clique em **Enviar para a área restrita** .
   Depois de iniciar o envio da área restrita, você pode exibir as anotações de trabalho para ver o status do seu envio. Um marcador também é anexado ao incidente de segurança.
6. Nas anotações de trabalho, clique no link na publicação Resultado de envio da área restrita.

Resultado

Você também pode exibir os resultados na guia Mostrar todas as listas relacionadas e resultados de envio da área restrita.

Configurar alertas por e-mail para eventos de Paciente 0

Configurar Zscaler Internet Access Produto para identificar e verificar se há arquivos desconhecidos e potencialmente maliciosos, como eventos do Paciente 0, para que você possa proteger sua rede contra arquivos maliciosos.

Antes de Iniciar

Função necessária: sn_si.admin, Zscaler Internet Access administrador

Por Que e Quando Desempenhar Esta Tarefa

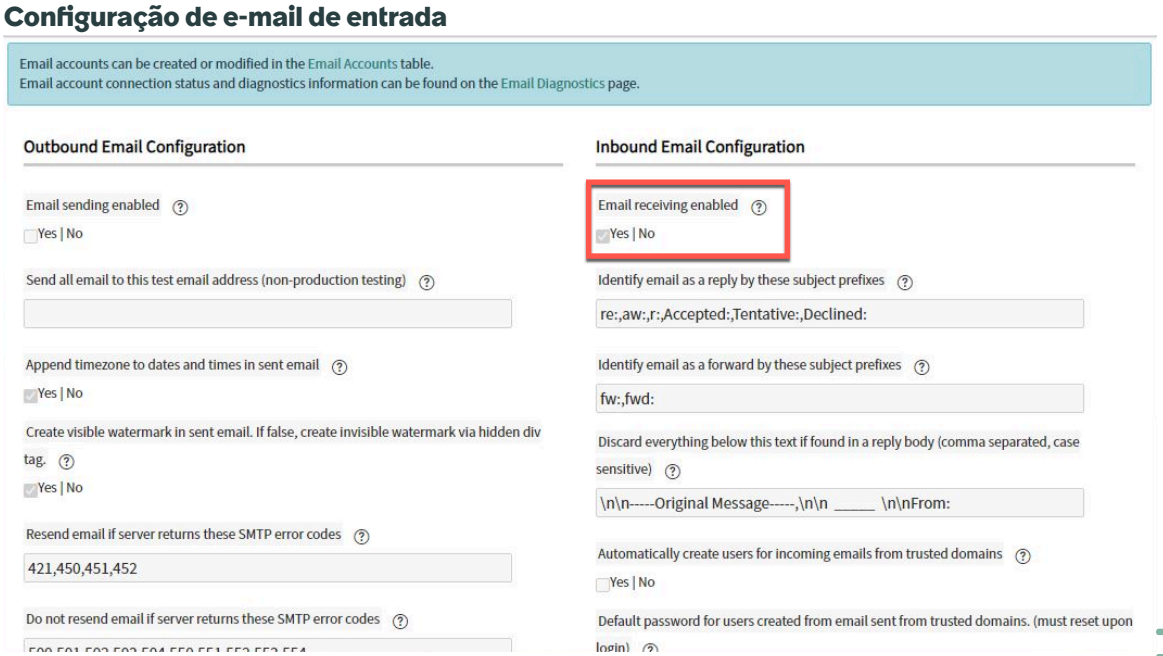
O paciente O é uma classe de alerta que inclui um arquivo desconhecido que tem permissão para download, mas é considerado mal-intencionado. O evento do paciente 0 é classificado como crítico. Você pode configurar ServiceNow AI Platform Para receber alertas por e-mail em intervalos regulares para eventos de Paciente 0.

Procedimento

1. Navegar até **Tudo** > **Caixas de Correio do Sistema** > **Administração** > **Propriedades do E-mail**.
2. Na seção Configuração de e-mail de entrada, selecione **Recebimento de e-mail habilitado** opção.

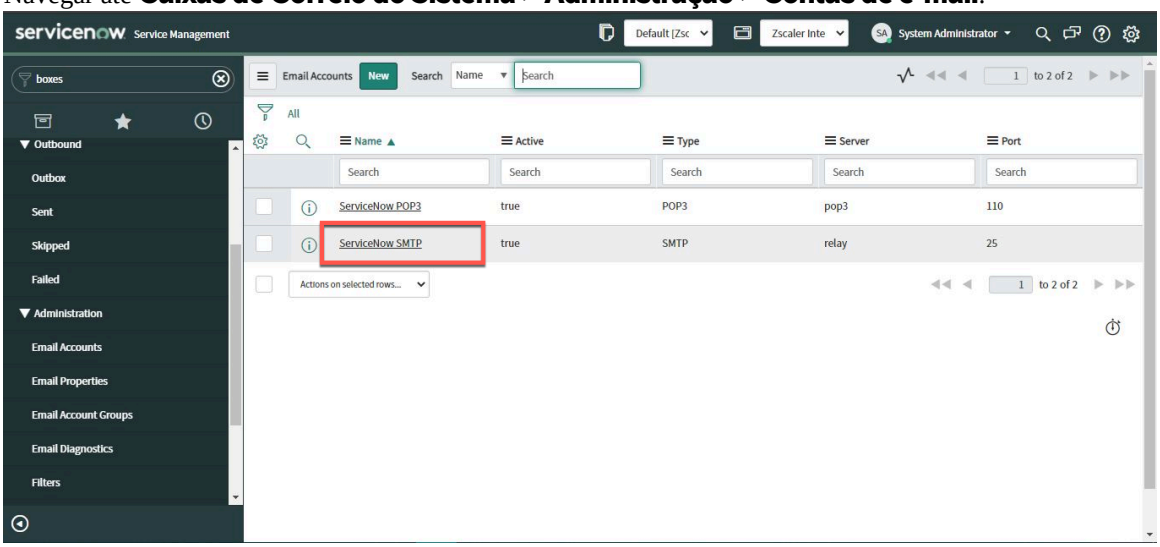
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Salvar**.

4. Navegar até **Caixas de Correio do Sistema** > **Administração** > **Contas de e-mail**.

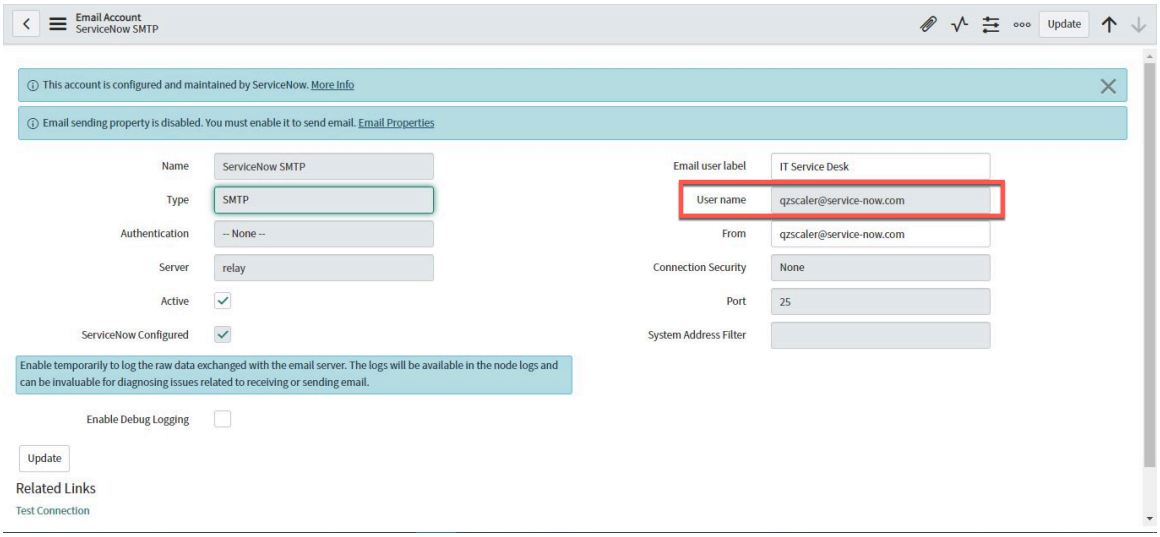


5. Selecione **ServiceNow SMTP** conta de e-mail.
   Anote o nome de usuário. O nome de usuário identificado aqui é ServiceNow AI Platform endereço de e-mail que você usa para configurar no Zscaler Para alertas de Paciente 0.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de usuário do ServiceNow AI Platform Conta SMTP



6. Faça login no Zscaler Internet Access portal de administração.

> **Nota:** Para obter mais informações sobre Zscaler Internet Access portal de administração, consulte Documentação do Zscaler .

7. Navegar até **Administração** > **Alertas** > **Publicar Alertas**.
8. Clique em **Adicionar assinatura de alerta** .
9. No formulário, preencha os campos.

Formulário Adicionar assinatura de alerta

Campo	Descrição
E-mail	ServiceNow AI Platform Endereço de e-mail da conta SMTP.
Descrição	Campo para adicionar mais detalhes sobre os alertas do Paciente 0.

10. Clique em **Salvar**.

ServiceNow Operações de segurança Visão geral do complemento Splunk

. ServiceNow Operações de segurança complemento para Splunk permite um Splunk administrador de software para coletar dados e criar incidentes e eventos no ServiceNow AI Platform.

O complemento é instalado a partir de Splunkbase.

> **Importante:** Splunk Também é compatível com o ambiente MSP (Provedor de serviços gerenciados).

Configuração de integração do Splunk

Procedimentos de configuração para ServiceNow Operações de segurança Complemento do Splunk Incluir o download do arquivo de complemento no Splunk, a instalação do complemento e a configuração do ServiceNow instância em que incidentes e eventos de segurança são criados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária

Antes de executar os procedimentos de configuração de integração do Splunk, certifique-se de definir um usuário de integração com as funções sn_si.integration_user e sn_si.analyst em sua instância da ServiceNow. Para executar importações, você precisa da função import_transformer para obter permissão de leitura e gravação nas tabelas de segurança. A função sn_si.integration_user deve ser definida com a parte import_transformer da função.

Baixe a aplicação Operações de segurança da ServiceNow

A primeira etapa na configuração da integração da ServiceNow-to-Splunk é baixar o. ServiceNow Operações de segurança Aplicação do Splunkbase.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra Splunkbase.
2. Pesquisar Integração de operações de segurança da ServiceNow .
3. Baixe a aplicação.

Instale o complemento Operações de segurança da ServiceNow para Splunk

Instale o. **Complemento de Operações de segurança da ServiceNow para Splunk** Para vincular Splunk a. ServiceNow.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o Splunk.
2. Clique em **Aplicações** ícone de engrenagem ou **Gerenciar aplicações** item de menu de atalho.
3. Clique em **Instale o app do arquivo** .
4. Clique em **Escolha Arquivo** , selecione sn_sec_ops.spl e clique em **Upload** .
5. Se solicitado, reinicie Splunk.
   . ServiceNow Operações de segurança O complemento para Splunk está instalado e pronto para ser configurado.

Configure ou mude a instância em que incidentes ou eventos são criados

Para configurar ou mudar o. ServiceNow Instância em que novos incidentes de segurança e eventos de segurança são criados, use a ação Configuração na lista de aplicações.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Aberto **Splunk** .
2. Clique em **Aplicações** ícone de engrenagem ou **Gerenciar aplicações** item de menu de atalho.
3. Na lista de aplicações, pesquise **ServiceNow** aplicativos que usam o filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

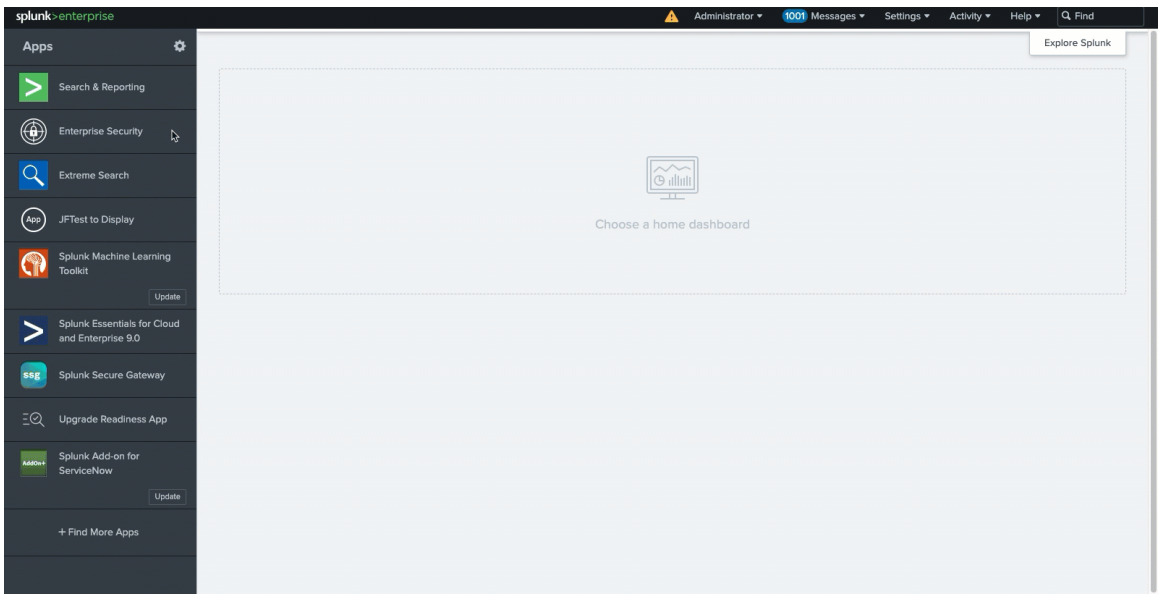
4. Procure **Integração de operações de segurança da ServiceNow** e clique no correspondente **Configurar** ação.
5. No formulário, preencha os campos.

Campo	Descrição
Especifique o ServiceNow Server	
URL	URL do Splunk Enterprise Security console ou Splunk Cloud instância. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica** ou **Autenticação do OAuth 2,0** . ○ Se você estiver usando o Nome de usuário da conta de API e a Senha da API para configuração, habilite o. **Autenticação básica** caixa de seleção. O padrão é desabilitado. ○ Se você estiver usando autenticação OAuth 2,0 para a configuração, habilite o. **Autenticação do OAuth 2,0** caixa de seleção. O padrão é desabilitado.
Autenticação básica	
Nome do usuário	Nome de usuário que você criou para sua conta de usuário da API no Splunk Enterprise Security console.
Senha	Senha que você criou para sua conta de usuário de API no Splunk Enterprise Security console.
Confirmar Senha	Locatário a senha para confirmá-la.
Autenticação do OAuth 2,0	
ID de cliente	ID do cliente do app criado no ServiceNow Server.
Segredo do cliente	Segredo do cliente do app criado no ServiceNow Server.
Redirecional URL	O URL para o qual será redirecionado. Você pode copiar e colar este URL no URL de redirecionamento do registro da ServiceNow.
Proxy opcional	
URL do proxy	URL do proxy para seu Splunk Enterprise Security console ou Splunk Cloud instância.
Porta	Endereço da porta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do usuário	Nome de usuário que você criou para a conta de proxy no Splunk Enterprise Security console.
Senha	Senha que você criou para a conta de proxy no Splunk Enterprise Security console.
Confirmar Senha	Locatário a senha para confirmá-la.
Configuração do nível de registro em log	
Nível de registro em log	O nível de logs de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **informações** ○ **error** ○ **aviso** ○ **depurar** Por padrão, o valor é **informações**.
Seleção de API	
Seleção de API	Selecione uma das seguintes APIs: ○ API da tabela ○ API do Import Set



6. Clique em **Salvar**.
7. Como alternativa, procure **Integração de ingestão de eventos da ServiceNow** e clique no correspondente **Configurar** ação.

   A Integração de ingestão de eventos da ServiceNow é configurada em três guias diferentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Splunk primário** : A configuração padrão ou primária do Splunk.
- **Splunk secundário** : (Opcional) O backup ou a segunda configuração do Splunk.
- **Nível de registro em log** : O nível de logs de relatórios gerados pela integração, ou seja, o nome do tipo de informação.

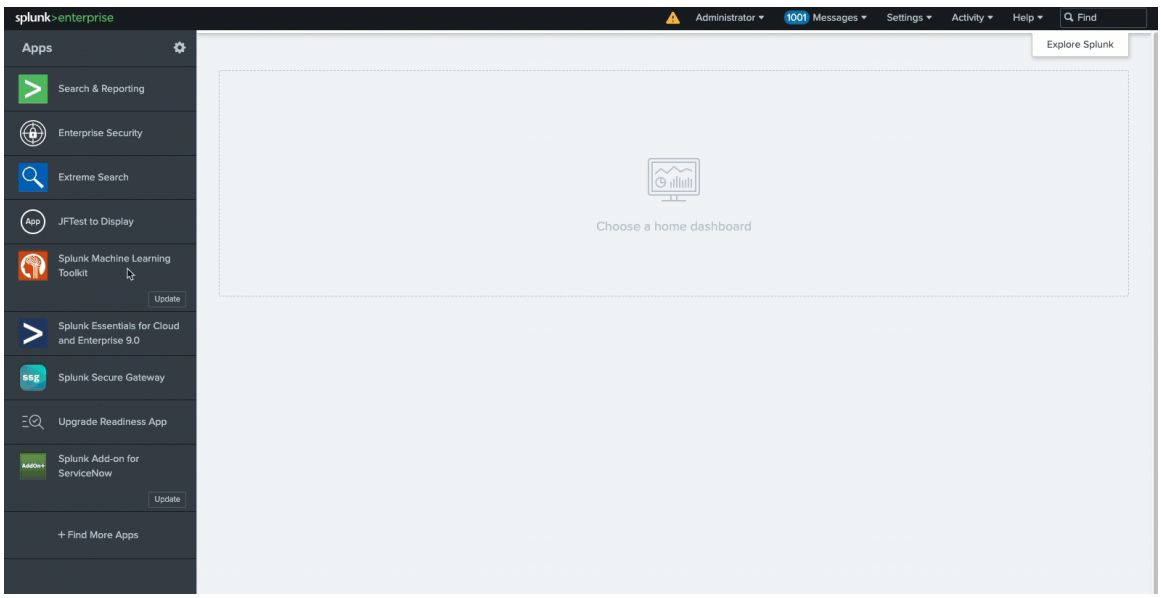
8. Selecione **Splunk primário** guia.
9. No formulário, preencha os campos.

Campo	Descrição
Rótulo da ação do fluxo de trabalho	Nome do Splunk Enterprise Security console primário ou Splunk Cloud instância primária usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `SplunkES2` .
URL	URL do Splunk Enterprise Security console primário ou Splunk Cloud instância primária. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Endpoint	Endpoint para seu Splunk Enterprise Security console primário ou Splunk Cloud instância primária.
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica** ou **Autenticação do OAuth 2,0** . ◦ Se você estiver usando o Nome de usuário da conta de API e a Senha da API para configuração, habilite o. **Autenticação básica** caixa de seleção. O padrão é desabilitado. ◦ Se você estiver usando autenticação OAuth 2,0 para a configuração, habilite o. **Autenticação do OAuth 2,0** caixa de seleção. O padrão é desabilitado.
Autenticação básica	
Nome do usuário	Nome de usuário que você criou para sua conta de usuário da API no Splunk Enterprise Security console.
Senha	Senha que você criou para sua conta de usuário de API no Splunk Enterprise Security console.
Confirmar Senha	Locatário a senha para confirmá-la.
Autenticação do OAuth 2,0	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID de cliente	ID do cliente do app criado no ServiceNow Server. Para obter informações sobre como obter o ID do cliente, consulte Configure o registro de aplicações na instância da ServiceNow
Segredo do cliente	Segredo do cliente do app criado no servidor. Para obter informações sobre como obter o segredo do cliente, consulte Configure o registro de aplicações na instância da ServiceNow
Redirecional URL	O URL para o qual será redirecionado. Você pode copiar e colar este URL no URL de redirecionamento do registro da ServiceNow. Para obter informações, consulte Configure o registro de aplicações na instância da ServiceNow
Configuração de proxy opcional	
URL do proxy	URL do proxy para seu Splunk Enterprise Security console secundário ou Splunk Cloud instância secundária.
Porta	Endereço da porta.
Nome do usuário	Nome de usuário que você criou para a conta de proxy no Splunk Enterprise Security console secundário.
Senha	Senha que você criou para a conta de proxy no Splunk Enterprise Security console secundário.
Confirmar Senha	Locatário a senha para confirmá-la.



10. **Opcional:** Selecione **Splunk secundário** guia.
11. **Opcional:** No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Rótulo da ação do fluxo de trabalho	(Optional) Nome do Splunk Enterprise Security console secundário ou Splunk Cloud instância secundária usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira SplunkES2 .
URL	URL do Splunk Enterprise Security console secundário ou Splunk Cloud instância secundária. O URL deve incluir a porta da API, por exemplo: https://mysplunkserver.com:8089
Endpoint	Endpoint para seu Splunk Enterprise Security console secundário ou Splunk Cloud instância secundária.
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica** ou **Autenticação do OAuth 2,0** . ○ Se você estiver usando o Nome de usuário da conta de API e a Senha da API para configuração, habilite o. **Autenticação básica** caixa de seleção. O padrão é desabilitado. ○ Se você estiver usando autenticação OAuth 2,0 para a configuração, habilite o. **Autenticação do OAuth 2,0** caixa de seleção. O padrão é desabilitado.
Autenticação básica	
Nome do usuário	Nome de usuário que você criou para sua conta de usuário da API no Splunk Enterprise Security console.
Senha	Senha que você criou para sua conta de usuário de API no Splunk Enterprise Security console.
Confirmar Senha	Locatário a senha para confirmá-la.
Autenticação do OAuth 2,0	
ID de cliente	ID do cliente do app criado no ServiceNow Server.
Segredo do cliente	Segredo do cliente do app criado no ServiceNow Server.
Redirecional URL	O URL para o qual será redirecionado. Você pode copiar e colar este URL no URL de redirecionamento do registro da ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Configuração de proxy opcional	
URL do proxy	URL do proxy para seu Splunk Enterprise Security console secundário ou Splunk Cloud instância secundária.
Porta	Endereço da porta.
Nome do usuário	Nome de usuário que você criou para a conta de proxy no Splunk Enterprise Security console secundário.
Senha	Senha que você criou para a conta de proxy no Splunk Enterprise Security console secundário.
Confirmar Senha	Locatário a senha para confirmá-la.

12. Selecione **Nível de registro em log** guia.
13. No formulário, preencha os campos.

Campo	Descrição
Nível de Log	O nível de logs de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **informações** ○ **error** ○ **aviso** ○ **depurar** Por padrão, o valor é **informações** .

14. Clique em **Salvar**.
    Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, **Atualização** e. **Excluir** os botões são exibidos conforme mostrado na figura a seguir.

    Nota: Você precisa usar autenticação básica ou somente autenticação OAuth 2,0. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

    Cada evento é validado e enviado com sucesso Splunk A configuração do servidor é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, clique em **Sim** .

Configure o registro de aplicações na instância da ServiceNow

Registre a aplicação com a instância para usar a autorização OAuth.

Antes de Iniciar
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

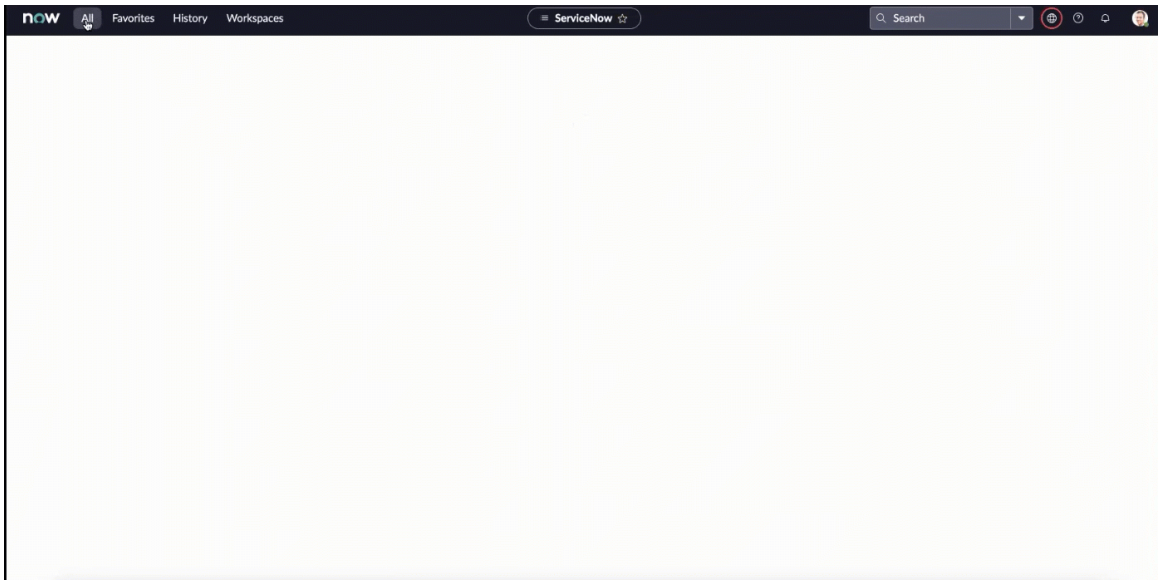
1. Navegar até **Tudo** > **OAuth de Sistema** > **Registro de aplicações**.
2. Clique em **Nova**.
3. Clique em **Criar um endpoint da API do OAuth para clientes externos**.
4. No formulário, preencha os campos.

Campo	Descrição
Nome	Um nome exclusivo que identifica a aplicação para o qual você solicitou acesso ao OAuth.
ID de cliente	(Somente leitura) O ID exclusivo gerado automaticamente da aplicação. A instância usa o ID de cliente ao solicitar um token de acesso.
Segredo do cliente	A cadeia de caracteres do segredo compartilhado que a instância e a aplicação cliente ou site usam para autorizar as comunicações entre si. A instância usa o segredo do cliente ao solicitar um token de acesso. Deixe este campo em branco para que a instância gere automaticamente um segredo do cliente. Para exibir segredos de cliente existentes, clique no ícone do cadeado.
URL de redirecionamento	O URL de retorno de chamada para o qual o servidor de autorização é redirecionado. Insira quantos URLs forem necessários para todos os consumidores de token possíveis. A instância corresponde ao URL da solicitação de entrada para um dos URLs de redirecionamento. Se nenhuma correspondência for feita, a instância usará o primeiro URL de redirecionamento.
URL do logotipo	O URL que contém uma imagem a ser usada como logotipo da aplicação. O logotipo aparece na página de aprovação quando o usuário recebe uma solicitação para conceder acesso a uma aplicação cliente a um recurso restrito na instância.
Aplicação	O nome da aplicação.
Acessível de	Defina o escopo da aplicação. Selecione uma das seguintes propriedades: ○ **Todos os escopos da aplicação** ○ **Somente este escopo da aplicação**
Ativo	Marque a caixa de seleção para ativar o registro da aplicação.
Tempo de vida do token de atualização	O número de segundos que um token de atualização é válido. A instância usa o valor de tempo de vida ao solicitar um token de atualização. Por padrão, os tokens de atualização expiram em 100 dias (8.640.000 segundos).
Tempo de vida do token de acesso	O número de segundos que um token de acesso é válido. A instância usa o valor de tempo de vida ao so-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	licitar um token de acesso. Por padrão, os tokens de acesso expiram em 30 minutos (1800 segundos).
Comentários	Informações adicionais a serem associadas à aplicação.



5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
6. Clique em **Enviar**.

Comandos de pesquisa manual

Os comandos de pesquisa manual são inseridos em qualquer janela de pesquisa. Você pode criar um incidente ou evento de segurança. Após o comando, há pares de nomes de campos e valores usados para criar o registro desejado.

Evento de segurança

O comando do evento de segurança, **snseevento** cria um evento em ServiceNow Com a classificação Segurança.

Esses eventos podem ser revisados por conta própria ou regras de alerta no ServiceNow ou ações manuais podem transformar um evento ou coleção de eventos em um incidente de segurança.

Se o evento se tornar um incidente de segurança e cada parâmetro for enviado para o evento, esses dados serão usados para preencher o incidente de segurança da seguinte forma:

Evento de segurança

Nome do Parâmetro	Necessários	Uso	Usar no incidente de segurança
node	Sim	O nó representa o servidor ou o item de configuração do evento. Este nó é mapeado para	Usar no incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Evento de segurança

Nome do Parâmetro	Necessários	Uso	Usar no incidente de segurança
		um IC existente no ServiceNow.	
tipo	Sim	A categoria do evento.	Descrição resumida
recurso	Sim	O item de configuração.	Descrição resumida
origem	Não	A origem desses dados. Por padrão, o servidor Splunk gera os dados.	Log de atividades
external_url	Não	O URL de detalhamento a ser usado em ServiceNow Para voltar aos dados do Splunk sobre este evento. Por padrão, este URL contém o link de resultado para qualquer alerta ou um link para a página de pesquisa padrão do Splunk.	URL externo acessado por meio de **Detalhamento** Botão no formulário Incidente de segurança
time_of_event	Não	A hora em que o evento foi registrado no Splunk.	N/D
Todos os outros valores (categoria, subcategoria no exemplo)	Não	Qualquer campo que não faça parte do campo de informações no evento. Se um incidente de segurança for criado, ele será usado.	Se o campo existir e não estiver preenchido, o incidente de segurança usará esse valor. Por exemplo, a categoria passada pelo evento se torna a categoria do novo incidente de segurança. Se um campo com este nome não existir, o valor será colocado no log de atividades.

Tradução automática

Incidente de segurança

O comando Incidente de segurança, **snseincidente** Cria um Incidente de segurança em seu ServiceNow instância.

Incidente de segurança

Parâmetro	Necessários	Uso
short_description	Sim	Uma descrição resumida de uma linha do incidente.
categoria	Não	A categoria do incidente de segurança. Se esta categoria não existir, ela será criada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Parâmetro	Necessários	Uso
subcategoria	Não	A subcategoria. Se esta subcategoria não existir, ela será criada.
cmdb_ci	Não	O item de configuração do incidente de segurança. Este item deve ser mapeado para um IC existente no ServiceNow.
descrição	Não	A descrição mais longa e detalhada do incidente.

Há muitas colunas úteis possíveis - qualquer coisa no mapa de transformação de incidente de segurança pode ser usada. Se novas colunas forem adicionadas ao incidente de segurança, elas também serão usadas, desde que estejam no mapa de transformação. Algumas colunas úteis: Location, priority, assignment_group, assigned_to, affected_user, attack_vector e watch_list.

Ações de evento do Splunk

Ao revisar os logs do Splunk, você pode criar rapidamente eventos de segurança e incidentes de segurança a partir de qualquer item no log usando as ações de evento.

Clicar em uma dessas ações cria um comando de pesquisa manual preenchido com os dados na entrada de log e executa-o para gerar o novo registro.

Essas ações são facilmente configuradas para adicionar campos em seus dados normalizados. No Splunk, usando **Configurações** > **Campos** > **Ações de Fluxo de Trabalho**, você pode selecionar e editar qualquer uma dessas ações usando os campos de pesquisa manual.

Você pode escolher onde a ação será mostrada, para quais campos e modificar a cadeia de caracteres de pesquisa que contém um comando de pesquisa para criar seu registro.

Alertas Splunk de registro único

Em qualquer alerta, você pode especificar eventos de segurança ou incidentes de segurança a serem criados quando o alerta for disparado.

Abra ou crie seu alerta e, ao editar ações, selecione o tipo de registro desejado e preencha a caixa de diálogo de alerta.

Alertas Splunk de campo personalizado de vários registros

Alertas de vários registros (definidos usando **Crie vários incidentes de segurança da ServiceNow** e. **Crie vários eventos de segurança da ServiceNow** ações do gatilho) pode criar registros automaticamente com qualquer conjunto de campos compatíveis.

Agem de forma diferente das outras ações de alerta em que os valores padrão são fornecidos. No entanto, a maioria dos dados vem do resultado da pesquisa desse alerta.

Nota: Em versões anteriores do complemento e desta documentação, alertas com script eram compatíveis. Esse recurso foi descontinuado e substituído por estas instruções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um alerta Splunk de campo personalizado de vários registros

Para criar um alerta Splunk de vários registros com campos personalizados, você deve criar uma pesquisa projetada para corresponder às colunas da ServiceNow que deseja preencher.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegue até **Pesquisa** .
2. Em **Pesquisa** crie uma pesquisa que gera seus dados de registro.
   Consulte exemplos para critérios de pesquisa recomendados.
3. Clique em **Salvar como** e selecione **Alerta** .
4. Defina o nome, as permissões e a programação, conforme necessário.
5. Clique em **Adicionar ações** .
6. Faça uma das seguintes seleções.
   - Para criar um evento por resultado de sua pesquisa, selecione **Crie vários eventos de segurança da ServiceNow** .
   - Para criar um incidente por resultado da sua pesquisa, selecione **Crie vários incidentes de segurança da ServiceNow** .
7. Defina todos os padrões, conforme necessário.
   Se o campo no resultado da pesquisa estiver em branco ou não estiver presente, os padrões serão usados. Se houver um valor no resultado, os padrões serão substituídos.

Exemplos de alerta Splunk de campo personalizado de vários registros

Ao criar alertas Splunk de vários registros com campos personalizados, você precisa definir critérios de pesquisa para gerar dados de alerta. Exemplos de critérios de pesquisa para incidentes de segurança e eventos de segurança são mostrados.

Pesquisa de incidentes de segurança

Para um incidente de segurança, este critério cria uma pesquisa para preencher colunas na tabela de incidentes de segurança.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Pesquisa de evento de segurança

Para um evento de segurança, esta é a mesma pesquisa, mas preenche os campos de evento. Se este evento for transformado em um incidente de segurança e todos os campos que não existirem no evento forem preenchidos, eles serão transferidos para o incidente de segurança. Caso contrário, eles permanecerão no campo de informações adicionais do evento e do alerta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Nota: Os critérios de pesquisa usados adicionarão quantos registros forem encontrados na pesquisa. Pode adicionar 5 ou 10,000,000,000 registros. Este NÃO é um método recomendado para a transferência em massa de dados. A intenção desse método é adicionar um registro por chamada REST à instância da ServiceNow.

Relatório de erros do Splunk

Sempre que ocorre um problema de conectividade com sua instância da ServiceNow, um erro é registrado no Splunk com informações descrevendo o problema.

As mensagens de erro são armazenadas em um novo índice chamado **servicenow** com tipo de origem **servicenow** .

Para pesquisar logs de erro, certifique-se de especificar o. **servicenow** índice em sua pesquisa. Como alternativa, consulte a documentação atual do Splunk sobre como adicionar o novo **servicenow** índice para os índices de pesquisa padrão.

Splunk Enterprise Event Ingestion integração para Operações de segurança por ServiceNow

. Splunk Enterprise integração de dados de evento e alerta com Resposta a incidentes de segurança(SIR) permite que os analistas de incidentes de segurança coletem e processem logs de segurança e dados de eventos relacionados.

Visão geral

Os dados são coletados em tempo real e usados por analistas para identificar e relatar possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser processados em alertas acionados que são ingeridos automaticamente com esta integração. Eventos de segurança individuais podem ser encaminhados manualmente sob demanda do Splunk Enterprise interface de pesquisa e emissão de relatórios no Resposta a incidentes de segurança produto do ServiceNow AI Platform para criar incidentes de segurança. Você pode recuperar eventos notáveis de Splunk Enterprise pesquise com a configuração de cluster do cabeçote de pesquisa. Você pode conseguir isso usando a URL e a porta de API de qualquer cabeçalho de pesquisa que faça parte do cluster.

Esta integração fornece a um analista do SOC (Security Operations Center, centro de operações de segurança) visibilidade de eventos e dados de alertas relacionados. Esses dados podem ser integrados ao ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança para investigação e correção adicionais. Perfis para Splunk alertas ingeridos contínuos e eventos encaminhados são criados em seu ServiceNow AI Platform instância. Esses perfis personalizam a diferença Splunk os campos alerta e evento são exibidos em SIR incidentes de segurança. Um mapeamento padrão de campos de alerta é fornecido que pode ser editado e aumentado para atender às necessidades específicas do cliente.

Principais recursos

Esta integração inclui os seguintes recursos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie vários perfis de ingestão de alertas para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda do seu Splunk Console para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk Valores de campo de alerta e evento aos campos de incidente de segurança SIR associados.
- Uma visualização do SIR layout de incidente de segurança com base em alertas ou eventos de amostra para validar a configuração do perfil.
- Ingerir alertas históricos, bem como alertas futuros contínuos em intervalos configuráveis.
- Agregue eventos ou alertas aos existentes SIR incidentes de segurança com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.

Versões da ServiceNow AI Platform compatíveis

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações.

A seguir Operações de segurança as aplicações devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila:

1. Framework de integração de segurança
2. Security Support Common
3. Orquestração do suporte de segurança
4. Resposta a incidentes de segurança

Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

ServiceNow Complementos

. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterpriseé necessário somente se você preferir encaminhar eventos manualmente do seu Splunk Enterprise console em seu ServiceNow AI Platform instância. Isso ServiceNow o complemento está disponível em splunkbase .

Isso ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise a aplicação no splunkbase não é necessária para a ingestão automatizada de alertas que é compatível com a integração.

Versões compatíveis com Splunk

Esta integração oferece suporte à versão 6,0 ou posterior do Splunk Enterprise. A integração também oferece suporte ao Splunk Serviço de nuvem empresarial.

MID Server

Esta integração requer um MID Server instalado e configurado em seu ServiceNow AI Platform® instância para se conectar ao Splunk se o Splunk o servidor está implantado em

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

sua rede corporativa. Se você estiver usando Splunk Cloud Um MID Server não é necessário. Para obter mais informações sobre MID Servers, consulte MID Server .

Arquitetura de integração e conexão de sistemas

Para obter mais informações sobre a arquitetura da integração, incluindo termos principais e detalhes de conexão de sistemas externos, consulte Arquitetura de integração e conexão de sistemas externos para Splunk Enterprise Event Ingestion integração.

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para Splunk Enterprise Security Integração de ingestão de evento notável. Você pode usar esta lista para monitorar seu andamento conforme trabalha nas tarefas da integração.

As imagens usadas nos tópicos a seguir foram geradas para a versão Kingston do ServiceNow AI Platform. Para obter informações sobre a interface do usuário de San Diego, consulte Gerencie ameaças à segurança usando o Espaço do analista de segurança .

Os tópicos a seguir são numerados. Siga os tópicos listados abaixo na ordem em que são apresentados para uma instalação e configuração suaves da aplicação.

Configure seu ServiceNow AI Platform® instância do Splunk Enterprise Event Ingestion integração

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

Procedimento

1. Verifique se você atribuiu o necessário ServiceNow AI Platform® E Resposta a incidentes de segurança (SIR).

   As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform® instância.

   - Um usuário com ServiceNow AI Platform® a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin).
   - Se você quiser encaminhar eventos manualmente de Splunk Enterprise para esta integração, um usuário com ServiceNow AI Platform® a função de administrador atribui um usuário com a função (sn_sec_splunk_v2.api_account_access) no ServiceNow AI Platform®. Esta função permite a um usuário com Splunk Enterprise Função de administrador para acessar a API no ServiceNow AI Platform® necessário para o encaminhamento manual de eventos para esta integração.

     A função (sn_sec_splunk_v2.api_account_access) não será necessária para a integração se você estiver ingerindo alertas automaticamente do Splunk Enterprise em seu ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um usuário com **sn_si.ingestion_profile_admin** a função supervisiona as seguintes tarefas no ServiceNow AI Platform®:
  - Cria e edita perfis de alerta e evento.
  - Seleciona e mapeia valores de alertas e eventos para ServiceNow AI Platform® incidentes de segurança.
  - Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração.
  - Agenda a ingestão de alertas em andamento.
  - Atribui a função de analista de incidentes de segurança (sn_si.analyst).
  - Usuários com sn_si.analyst trabalham com incidentes de segurança.

Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Gerenciando funções .

2. Verifique se você está usando a versão 6,0 ou posterior do Splunk API.

   Se você tiver acesso ao Splunk Enterprise, você tem acesso à API necessária para esta integração. Não há outra configuração especial necessária para a API.

3. Verifique se você instalou e configurou um MID Server.

   Um MID Server em seu ServiceNow AI Platform® a instância é necessária para se conectar ao Splunk se o Splunk o servidor está implantado em sua rede corporativa. Para obter mais informações sobre MID Servers, consulte MID Server

   Se você estiver usando Splunk Cloud Um MID Server não é necessário.

4. Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas.

   . Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração.

   Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila.

   a. Resposta a incidentes de segurança
   b. Framework de integração de segurança
   c. Security Support Common
   d. Orquestração do suporte de segurança

   Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

O que Fazer Depois

Você configurou com sucesso seu ServiceNow AI Platform® instância da integração. A próxima etapa é instalar o. Splunk Enterprise Event Ingestion aplicação do ServiceNow Store para a integração. Para obter mais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

informações, consulte Instale e configure o. ServiceNow aplicação para Splunk Enterprise Event Ingestion integração.

Se você não salvou pesquisas em seu Splunk Enterprise console para ingestão ou se você estiver executando a configuração inicial desta integração em seu Splunk Enterprise e Operações de segurança produto do seu ServiceNow AI Platform® instância simultaneamente, consulte Salve pesquisas em seu Splunk Enterprise console para Splunk Enterprise Event Ingestion integração para obter mais informações.

Se você quiser exportar eventos manualmente e sob demanda do seu Splunk Enterprise console para a integração, consulte Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise integração de ingestão de evento para obter mais informações.

Instale e configure o. ServiceNow aplicação para Splunk Enterprise Event Ingestion integração

Antes de executar a integração no seu ServiceNow AI Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform® instância.

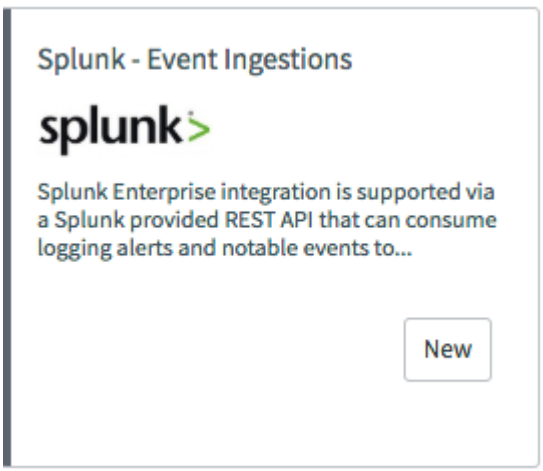
Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Se você não instalou o. Splunk Enterprise Event Ingestion aplicação do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize Splunk Bloco Ingestões de evento.
3. Para configurar a aplicação, clique em **Novo** .



4. Como alternativa, se for um **Configurar** é exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestões de evento exibida, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

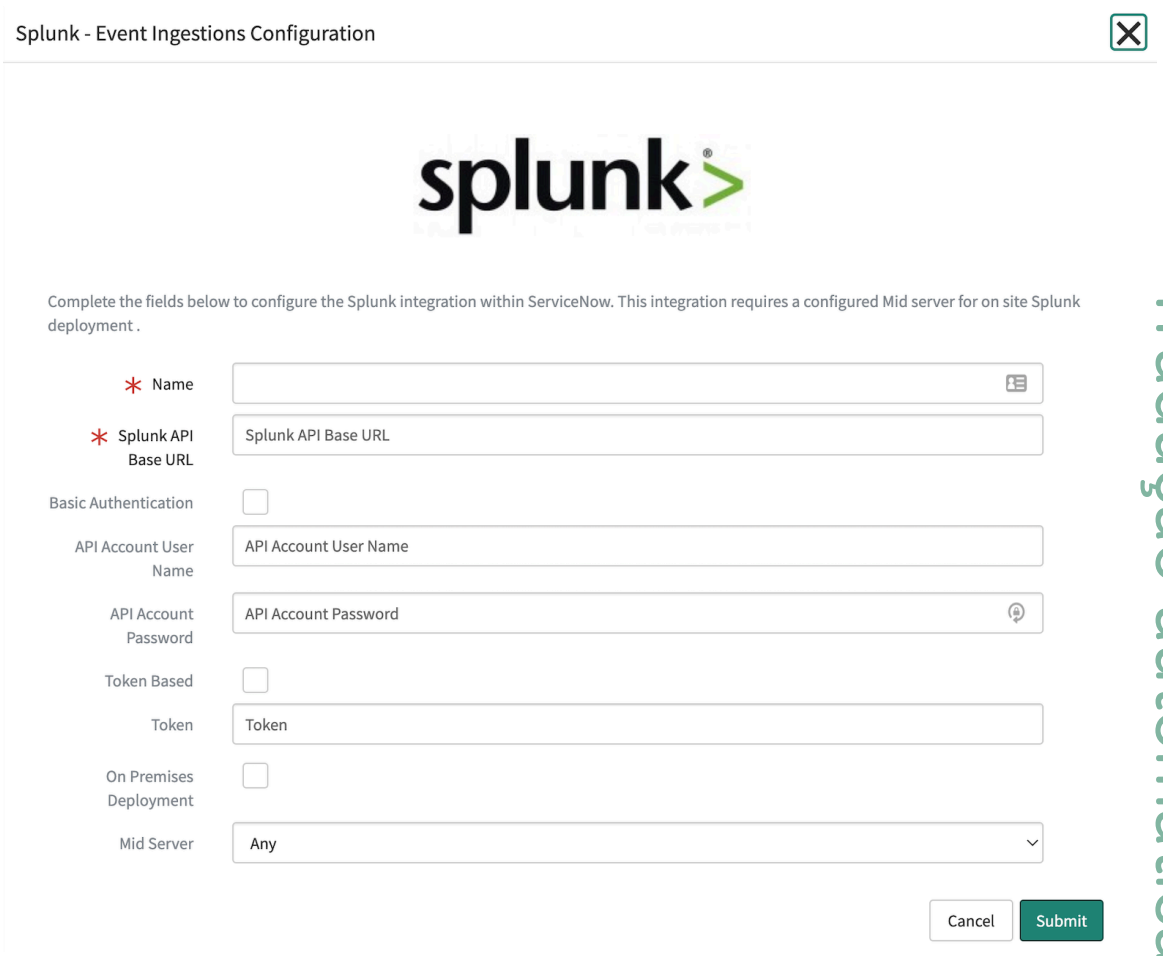
Campo	Descrição
Nome	Nome do Splunk Enterprise console ou Splunk Cloud instância usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `HQ-EUA` ou `SEDE EUA` .
URL base da API Splunk	URL do Splunk Enterprise console ou Splunk Cloud instância.
Autenticação básica	O padrão é desabilitado. Se você estiver usando o Nome de usuário da conta de API e a Senha da API para configuração, habilite a caixa de seleção.
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário individual no Splunk Enterprise console.
Senha da API	Senha que você criou para sua conta de usuário individual no Splunk Enterprise console.
Baseado em token (disponível a partir da versão 12,0.0)	Autenticação baseada em token que você criou para sua conta de usuário de API no Splunk Enterprise console.
Token	Token que você criou para sua conta de usuário de API no Splunk Enterprise console.
MID Server	MID Server específico que está configurado em seu ambiente. Somente MID Servers ativos e validados estão disponíveis nesta lista de seleção.
Implantação no Local	O padrão é desabilitado. Se você estiver usando a versão baseada em nuvem de Splunk Enterprise verifique se a caixa de seleção está desmarcada. Se esta opção estiver habilitada, a lista de seleção DO MID Server será exibida. Se você estiver usando uma versão no local de Splunk Enterprise, Siga estas etapas para selecionar um MID Server. **a.** Marque a caixa de seleção. Uma lista de seleção é exibida. O padrão é **Qualquer** . **b.** Selecione **Qualquer** Somente se este MID Server estiver configurado para Splunk Enterprise Event Ingestion integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	c. Na lista de seleção, selecione ServiceNow AI Platform® MID Server que você configurou em sua instância para esta integração específica.

A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão no local de Splunk Enterprise Com um MID Server.



Cada um Splunk Enterprise alerta que você ingesta do seu Splunk Enterprise o console requer um perfil de evento exclusivo em seu ServiceNow AI Platform® instância. No entanto, a origem que você configura no formulário Configuração de ingestões de evento pode ser reutilizada para vários ServiceNow AI Platform® perfis, desde que cada perfil ingere exclusivo Splunk alertas acionados.

6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, **Configurar** e. **Excluir** os botões são exibidos conforme mostrado na figura a seguir.

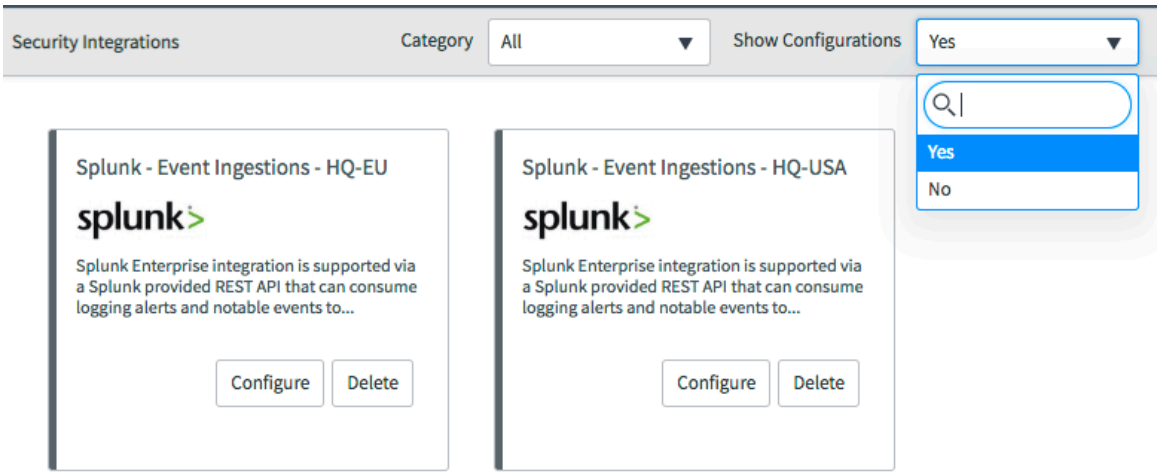
> **Nota:** Você precisa usar Autenticação básica ou Autenticação baseada em token somente. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

Cada evento é validado e enviado com sucesso Splunk A configuração do servidor é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim** .



Trouble?

Se uma mensagem de erro for exibida depois que você clicar em **Enviar** insira suas informações novamente e clique em **Enviar** .

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Defina as configurações de ingestão de evento do Splunk Enterprise

Use as configurações de ingestão de evento do Splunk Enterprise para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Navegar até **Tudo** > **Splunk Integration** > **Configurações do Splunk Integration**.
2. No formulário, preencha os campos.

Configurações do Splunk Integration

Campo	Descrição
Número máximo de alertas a serem exibidos na criação do perfil. sn_sec_splunk_v2.max_alerts_to_display	Opção para definir o número máximo de alertas que você deseja exibir ao criar um perfil de evento. Por padrão, o valor é definido como 500.
Número máximo de incidentes de segurança a serem criados em um dia. sn_sec_splunk_v2.max_si_per_day	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 1000.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número máximo de eventos a serem obtidos do Splunk por chamada. sn_sec_splunk_v2.max_events_per_call	Opção para definir o número máximo de eventos a serem recuperados do Splunk para cada chamada. Por padrão, o valor é definido como 100.
O número de dias que um item permanece na tabela de fila após concluir/errar para fins de informações ou depuração. sn_sec_splunk_v2.queue_item_expire	Opção para definir o número de dias para que um item permaneça na tabela de fila após a conclusão ou a ocorrência de erro devido a informações ou fins de depuração. Por padrão, o valor é definido como 14.
Número de dias para reter os dados de importação de evento, evento para tarefa e alertas disparados. sn_sec_splunk_v2.retention_period	Opção para determinar o número de dias que você deseja reter os dados de importação de evento, evento para tarefa e alertas disparados. Por padrão, o valor é definido como 30.
Ative esta configuração para atualizar as configurações de origem existentes do Splunk para suporte à autenticação baseada em token. Você precisará atualizar a configuração de integração com os detalhes do token depois que essa configuração estiver habilitada. sn_sec_splunk_v2.upgrade_existing_tile	Opção para atualizar a configuração de origem do Splunk existente para suporte à autenticação baseada em token de uma versão existente. **Nota:** Depois que você fizer upgrade para a nova versão, o campo de token ficará indisponível. Você precisa habilitar esta configuração para obter a autenticação baseada em token, após a qual você precisa atualizar a configuração de integração com detalhes do token. Por padrão, o valor é definido como Não
Nível de registro em log - depuração, informações, aviso, erro. sn_sec_splunk_v2.logging.detalhamento	
Duração em segundos da pesquisa do Splunk. sn_sec_splunk_v2.sid_ttl	Por padrão, o valor é definido como 14.
Número de minutos de sobreposição a serem adicionados ao buscar os eventos do Splunk (para superar o atraso de indexação do Splunk). sn_sec_splunk_v2.overlap_time	Por padrão, o valor é definido como 0.
Tamanho do lote da regra de alerta a ser usado para disparar consultas de pesquisa do Splunk durante a ingestão. sn_sec_splunk_v2.rules_batch_size	Por padrão, o valor é definido como 50.
Limite de eventos por alerta acionado para lidar com pico.	Por padrão, o valor é definido como 1000.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
sn_sec_splunk_v2.spike_events_limit	
O caractere delimitador para dividir os valores em mapeamentos de campo. sn_sec_splunk_v2.delimiter	

3. Selecione **Save** (Salvar).

Crie e nomeie um perfil de evento

Crie um perfil de evento em seu ServiceNow AI Platform e determine qual Splunk alertas criam incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Antes ServiceNow AI Platform Resposta a incidentes de segurança(SIR os incidentes de segurança são criados a partir de alertas ingeridos, os valores de campo dos alertas são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será exibido.

De uma perspectiva de integração usando APIs disponíveis, Splunk os eventos são encaminhados individualmente e manualmente como eventos discretos ou são combinados em alertas acionados que são ingeridos automaticamente no Operações de segurança do seu ServiceNow AI Platform instância. Os fluxos de trabalho de integração ingerem diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo.

Esses alertas são ingeridos com base nos perfis que você configura no Operações de segurança ambiente da sua instância. Inicialmente, todos os alertas são ingeridos para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados ainda mais para especificar quais alertas criam incidentes de segurança. Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para alertas identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de alertas ingeridos, os valores de campos individuais nos alertas filtrados são mapeados para os campos correspondentes em um layout de incidente de segurança para uma visualização.

Nomes de alerta para perfis de evento em seu ServiceNow AI Platform a instância deve ser exclusiva e só pode ser mapeada para um perfil de evento ativo a qualquer momento. Estes são os nomes de alertas acionados que você configurou em Splunk serviço como parte da configuração da integração. Para obter mais informações sobre como configurar alertas em seu Splunk Enterprise ambiente, consulte Salve pesquisas em seu Splunk Enterprise console para Splunk Enterprise Event Ingestion integração.

. ServiceNow AI Platform ingere alertas específicos usando os fluxos de trabalho da integração. Todos os alertas que atendem aos critérios de seleção em seu Splunk inicialmente, o console enterprise é ingerido em seu ServiceNow AI Platform instância.

Um perfil em seu ServiceNow AI Platformé um encapsulamento de um Splunk alerta em seu Splunk console empresarial. Há um relacionamento um para um entre os alertas que são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ingeridos com um perfil e as conexões com seu Splunk console empresarial: um alerta para uma conexão. Há uma única conexão https para um cabeçalho de pesquisa em seu Splunk Enterprise console. Vários alertas podem vir de um único cabeçalho de pesquisa. Se você se conectar a vários cabeçalhos de pesquisa em seu Splunk Enterprise, você deve criar vários perfis em seu ServiceNow AI Platform instância para ingerir esses alertas.

Etapas para criar perfis para ingestão de alertas programada

Procedimento

1. Para criar um perfil de evento para um alerta, em seu ServiceNow AI Platform instância, navegue até **Integração com Splunk ES** > **Perfis de eventos do Splunk ES**.
2. . Splunk O formulário Perfil de evento não for exibido, clique em **Nome** Na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

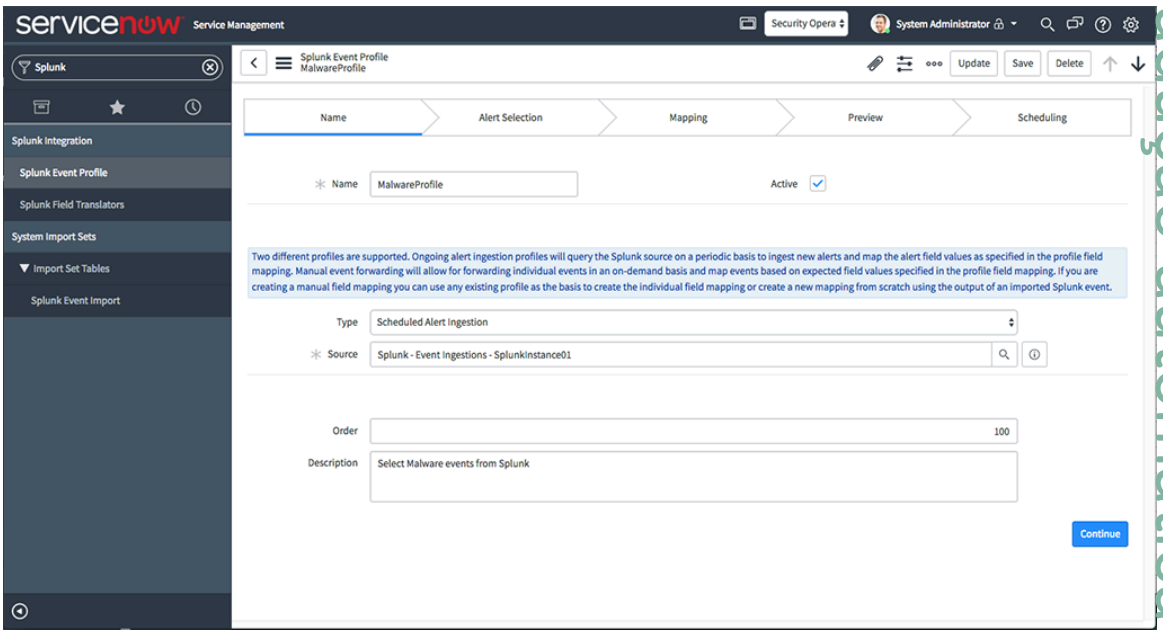
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.
Ativo	A caixa de seleção está desmarcada por padrão. A opção Ativo está desabilitada e não está disponível para seleção até que você conclua todas as etapas de configuração do perfil e clique em **Concluir** .
Tipo	Selecione o tipo de perfil na lista de seleção. ○ Ingestão de alerta programada - Este tipo de perfil oferece suporte a alertas acionados que são ingeridos em uma programação que você configura. Preencha os campos e clique em **Continuar** Para prosseguir para a etapa Seleção de alerta do perfil. ○ Encaminhamento manual de eventos - Este tipo de perfil oferece suporte a eventos individuais que são encaminhados manualmente do seu Splunk Enterprise console sob demanda. Consulte as etapas a seguir para preencher o formulário para esses tipos de perfis.
Tipo de Origem	Splunk servidor ou término de pesquisa que você configurou para ingerir alertas. Se você tiver vários Splunk servidores configurados, selecione o servidor

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	apropriado para os tipos de alerta que você planeja ingerir para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido para um alerta programado.



5. Para um perfil com um alerta programado, escolha uma opção para continuar com a configuração do perfil.

Opção	Descrição
Continuar	Salve o perfil e o andamento na etapa Seleção de alerta.
Atualizar	Salve as atualizações neste perfil e retorne ao Splunk Lista de perfis de evento.
Salvar	Salve este perfil e permaneça na página.
Excluir	Exclua este registro de perfil e retorne ao Splunk Lista de perfis de evento.

Etapas para criar perfis para encaminhamento manual de eventos

6. Para criar um perfil compatível com o encaminhamento manual de eventos, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

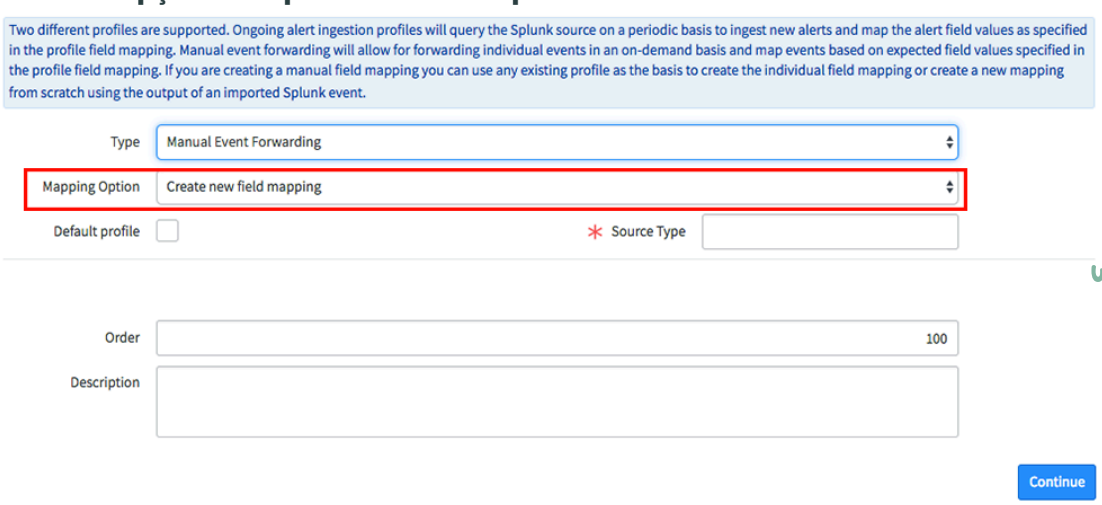
Para eventos que você encaminha sob demanda do seu Splunk console enterprise, você pode basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos que você encaminha manualmente não são programados no perfil de evento.

a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos** .

b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

Consulte as figuras e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Criar nova opção de mapeamento de campo



Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para seu evento. Se você não tiver um mapeamento de campo existente semelhante ao perfil que está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos Splunk eventos. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este perfil é o único perfil ativo e usado para cada Splunk mapeamento de campo de evento para um SIR incidente de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	segurança. Um perfil se encaixa em todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, a opção Tipo de origem permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base em Splunk tipo de origem. Se você quiser gerenciar eventos de log de firewall de forma diferente dos eventos de detecção de endpoint, e eles tiverem diferentes Splunk tipos de origem, você pode criar diferentes perfis de evento com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você criou um grande número de perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para obter um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Selecione o perfil existente para a opção de mapeamento de campo



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar o perfil existente para mapeamento de campo	Um mapeamento de campo existente para o seu evento. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil. **i.** À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. **ii.** Em Splunk Lista Perfis de evento exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos Splunk eventos. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este perfil é o único perfil ativo. É usado para cada Splunk mapeamento de campo de evento para um SIR incidente de segurança. Um perfil se encaixa em todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver selecionada. Se disponível, a opção Tipo de origem permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base em Splunk tipo de origem. Se você quiser gerenciar eventos de log de firewall de forma diferente dos eventos de detecção de endpoint, e eles tiverem diferentes Splunk tipos de origem, você pode criar diferentes perfis de evento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

O que Fazer Depois

Você concluiu com sucesso as etapas para criar perfis para alertas agendados e encaminhamento manual de eventos. Para perfis para encaminhamento manual de eventos, você concluiu a configuração do perfil. A próxima etapa é carregar dados de anexo na etapa de mapeamento.
Para perfis para alertas agendados, a próxima etapa é selecionar alertas para ingestão automática.

Selecione Alertas programados para Splunk Enterprise Event Ingestion integração

Depois de criar um perfil para um alerta programado, selecione um Splunk alerta para este perfil que você deseja mapear para um ServiceNow AI Platform Resposta a incidentes de segurança incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Exiba os alertas disponíveis em seu ServiceNow AI Platform para que você saiba quais valores de campo estão disponíveis para mapeamento. Selecione um alerta para verificar se você recebeu os resultados esperados no layout do formulário básico antes de mapear os valores para campos em SIR incidentes de segurança. Você só pode selecionar um alerta na lista neste formulário.

Procedimento

1. Se a página Seleção de alerta não for exibida, selecione-a na barra de andamento para exibi-la.
   Por padrão, a aplicação principal de Pesquisa e emissão de relatórios está selecionada.
2. Se o alerta a ser ingerido fizer parte de um diferente Splunk aplicativo, selecione **Seleção do aplicativo Splunk** e escolha o seu Splunk aplicativo do **Aplicativo selecionado** lista.
3. Em **Lista de alertas** , escolha um alerta e mova-o para a partir de **Disponível** coluna para **Selecionado** coluna.

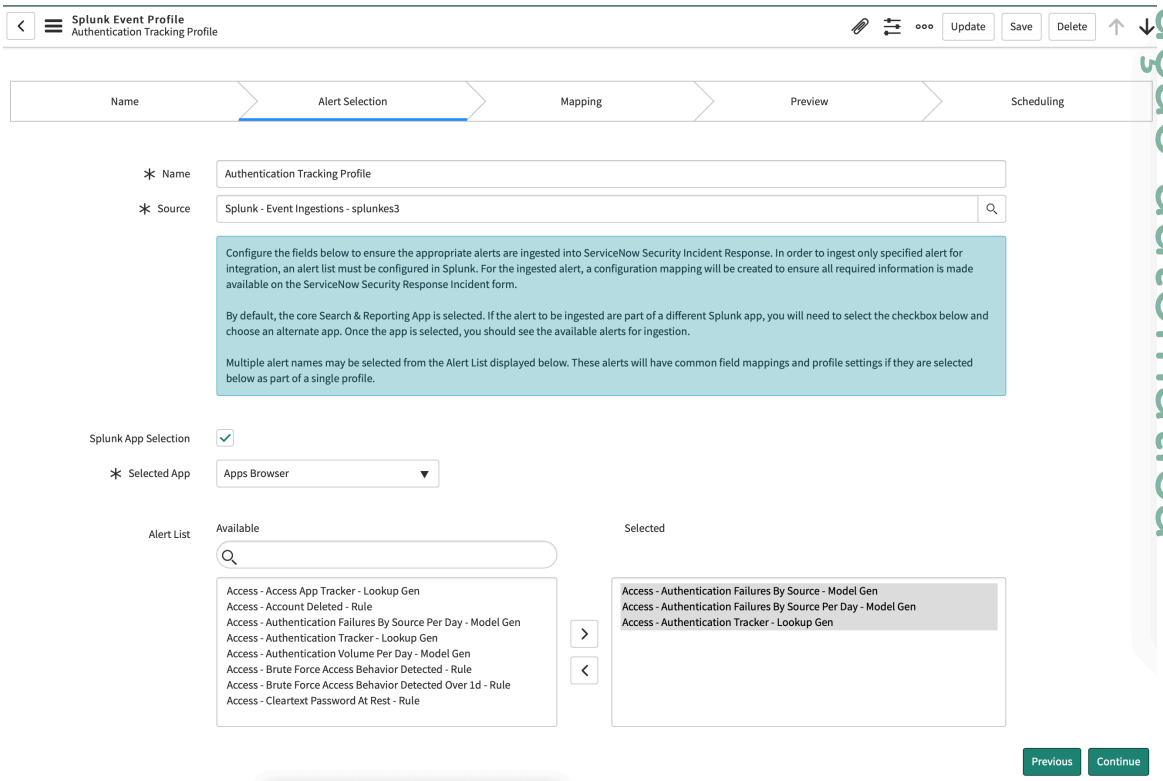
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode escolher vários alertas. Se os alertas forem selecionados como parte de um único perfil, os alertas terão mapeamentos de campo comuns e configurações de perfil.

A lista de alertas neste formulário corresponde à lista de alertas em seu Splunk console. Até 500 alertas são exibidos neste formulário. Se houver mais de 500 alertas listados no console do Splunk na página Alertas, somente os primeiros 500 alertas serão exibidos neste formulário em seu ServiceNow AI Platform instância.

Opção	Descrição
No campo de pesquisa Lista de alertas, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione um alerta e, com as teclas de seta, mova o alarme selecionado de **Disponível** . **Selecionado** .
Na Lista de alertas, clique duas vezes em um alerta.	. **Selecionado** a coluna é preenchida com sua seleção.
Na Lista de alertas, clique uma vez em uma regra de alarme.	O alarme é selecionado. Com as teclas de seta, mova o alerta selecionado de **Disponível** . **Selecionado** .



4. Escolha uma opção para continuar.

Opção	Descrição
Ou, como alternativa, clique em Mapeamento na barra de andamento	O formulário Mapeamento é exibido. **Mapeamento** está selecionado na barra de andamento. A próxima etapa é mapear

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	campos de alerta para um SIR incidente de segurança.
Atualizar	Seus dados são salvos e a lista Perfis de evento do Splunk é exibida.
Anterior	. **Nome** a etapa é exibida.
Excluir	Exclua este perfil de evento e a lista Perfis de evento do Splunk será exibida.

O que Fazer Depois

Você selecionou com sucesso um alerta para um perfil de alerta programado. A próxima etapa é mapear valores de alerta para campos em um incidente de segurança.

Mapeamento de alertas e eventos para Splunk Enterprise Event Ingestion integração

Depois de identificar as origens para ingestão de alertas programada ou encaminhamento manual de eventos, a próxima etapa é mapear campos de evento individuais para os campos em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Visão geral de alertas e eventos de mapeamento

Para a etapa de mapeamento, como um usuário com **sn_si.ingestion_profile_admin** , você ingira alertas de amostra do seu Splunk Enterprise ou você exporta dados de evento para um Splunk Enterprise evento.

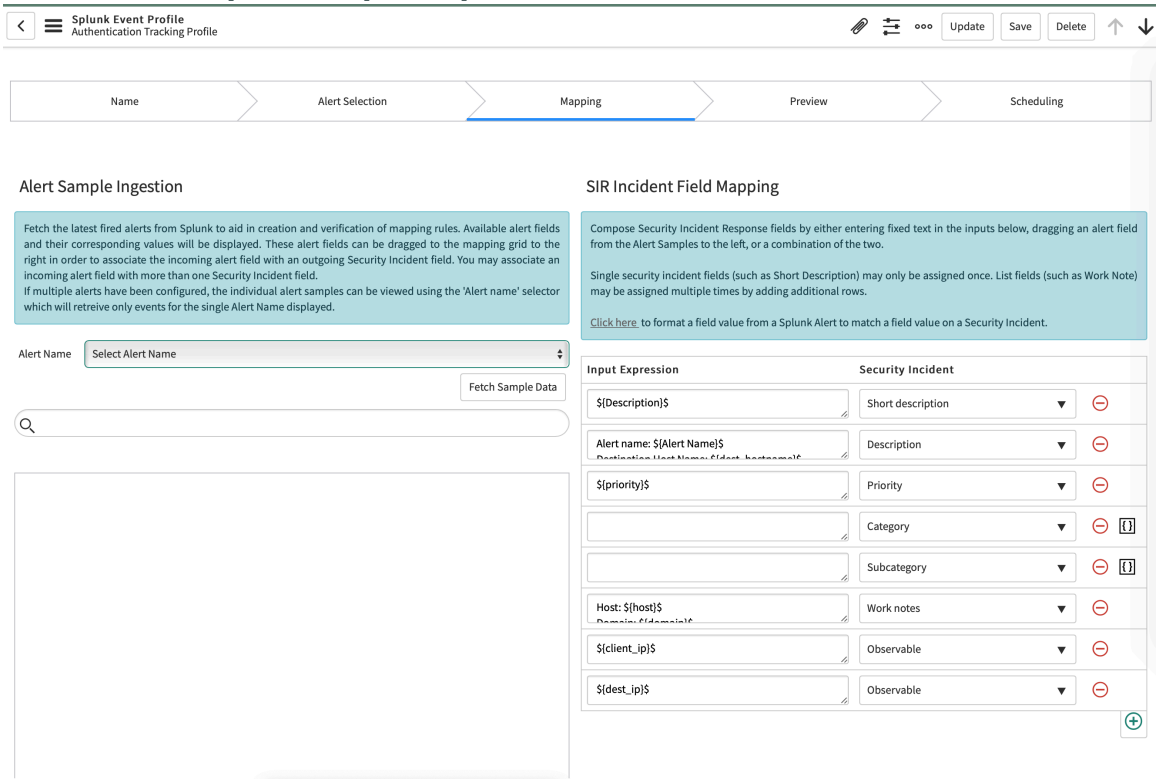
As figuras a seguir são exemplos das grades de mapeamento padrão fornecidas para cada tipo de perfil de evento. Este mapeamento padrão pode ser editado. Esta modificação permite personalizar os campos que preenchem o incidente de segurança. Com a etapa de mapeamento, você pode visualizar como adicionar ou remover campos de evento afeta o. SIR valores do campo de incidente de segurança.

Selecione **Nome do alerta** e depois de clicar em para **Buscar dados de amostra** . Splunk os valores do campo de alerta são preenchidos no lado esquerdo do formulário quando alertas de amostra são ingeridos pelo perfil. . Splunk campos de alerta que você mapeia para SIR campos de incidente de segurança.

Tradução automática

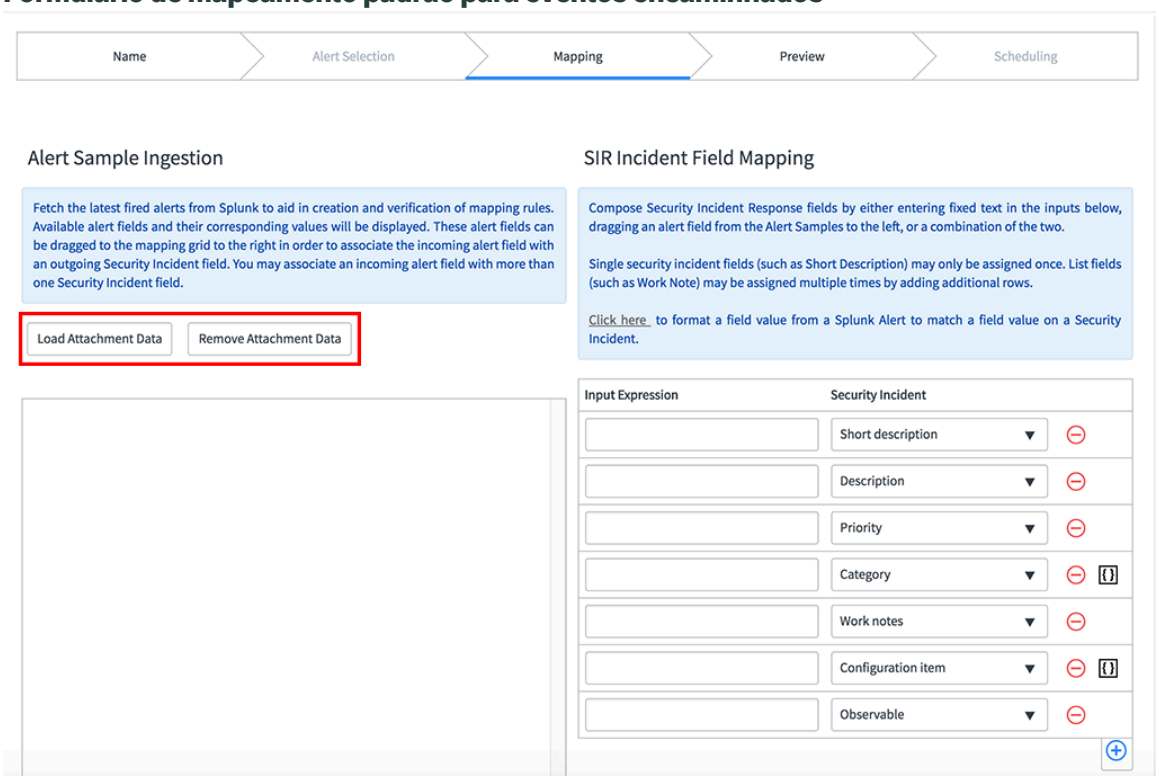
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de mapeamento padrão para alertas



Depois de clicar para carregar dados de anexo para eventos encaminhados, o. Splunk os campos de evento são preenchidos no lado esquerdo do formulário. . Splunk campos de dados mapeados para SIR campos de incidente de segurança.

Formulário de mapeamento padrão para eventos encaminhados



Você pode preferir revisar alguns alertas de amostra em seu Splunk console para ingerir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada, **Mapeamento** na

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento.

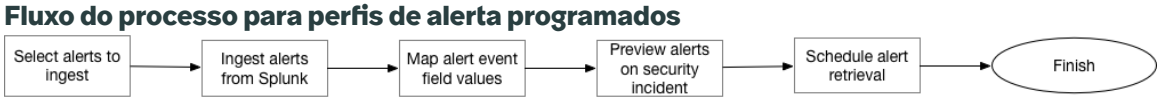
Mapeamento de alertas e exportação de eventos sob demanda do seu Splunk o console enterprise inclui os seguintes conceitos e tarefas:

- Busque dados de amostra para perfis de alerta ingeridos automaticamente. Depois que os dados são obtidos (extraídos) de um alerta disparado no Splunk Enterprise os campos de alerta disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento. As guias são exibidas para você exibir os valores de um ID de alerta que você extraiu. Verifique se todos os campos críticos da seção Ingestão de amostra de alerta à esquerda do formulário estão mapeados para a grade à direita do formulário.
- Se necessário, carregue dados de amostra de evento para qualquer perfil de evento encaminhado manualmente. Os dados de amostra desses eventos são exportados em um .xml arquivo do Splunk Enterprise e carregados em seu ServiceNow AI Platform® instância. Os dados importados são exibidos na seção Ingestão de amostra de alerta à esquerda do formulário.
- Edite a configuração de mapeamento arrastando alertas do lado esquerdo e soltando-os na grade de mapeamento à direita. A grade de mapeamento à direita associa o campo Alerta de entrada a um campo de incidente de segurança de saída.
- Personalize a grade de mapeamento adicionando ou removendo campos. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Defina condições de filtro para que você possa especificar quais alertas serão ingeridos em SIR e quais alertas são filtrados.
- Defina critérios de campo de incidente adicionais que agreguem um alerta de entrada a um existente SIR incidente de segurança para evitar incidentes duplicados. Esta filtragem adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de eventos de segurança relacionados em um único incidente de segurança.
- Em determinados casos, os valores do campo de evento no Splunk O console do Enterprise pode não ser traduzido diretamente para os campos no SIR incidente de segurança. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de scripts, os valores de campo Alerta de malware e Infecção por vírus no Splunk O console é convertido em Atividade de código mal-intencionado no campo Categoria no SIR incidente de segurança.

Perfis de alerta programados

Depois de criar um perfil de alerta programado, o fluxo do processo para a configuração é mostrado na figura a seguir.

Fluxo do processo para perfis de alerta programados



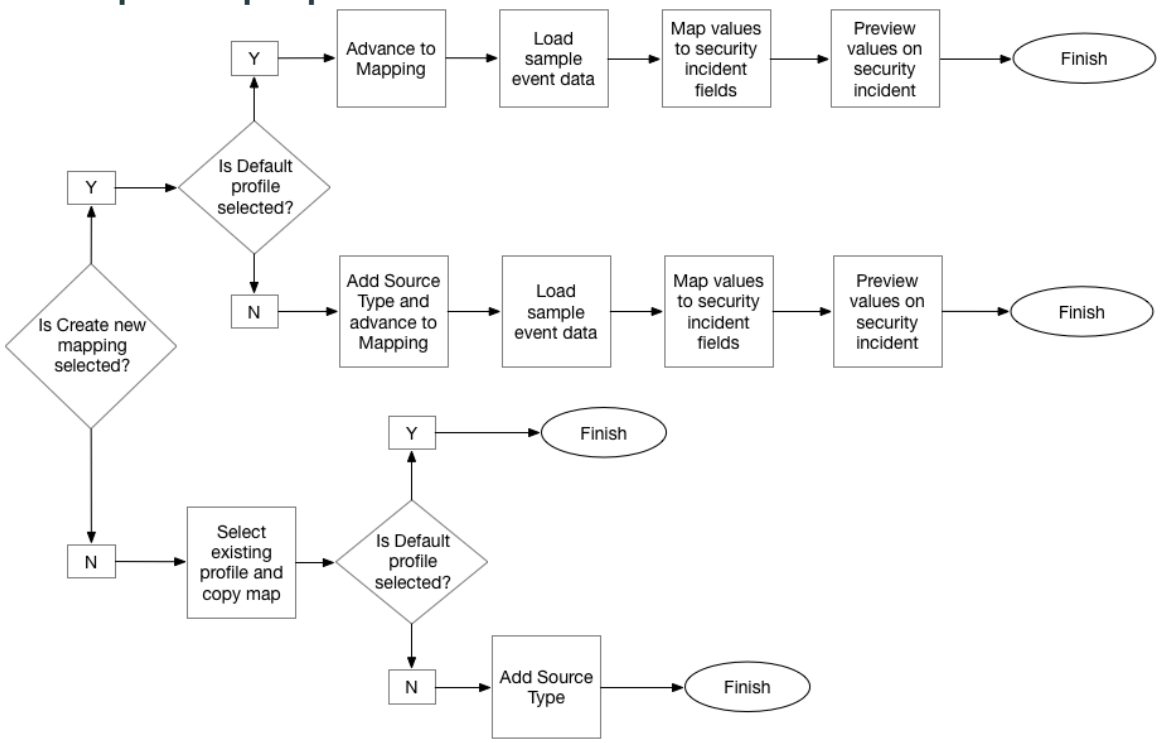
Perfis de encaminhamento de eventos manuais

Depois de criar um perfil para um evento, o fluxo do processo para a configuração é mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo do processo para perfis de evento



A próxima etapa é ingerir alertas acionados ou exportar dados e mapear valores para SIR campos de incidente de segurança.

Alertas de mapa para Splunk Enterprise Event Ingestion integração

Durante a etapa de mapeamento de campo de evento, você mapeia campos de evento individuais de alertas acionados ou dados de evento importados para campos em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa
A grade de mapeamento pré-configurada dos campos de incidente de segurança padrão pode ser editada. A codificação por cores dos campos de evento ajuda a monitorar os valores de campo que você já mapeou. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Mapeie até cinco alertas da coluna Ingestão de amostra de alerta à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no SIR incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para um perfil com um alerta programado, abaixo de Ingestão de amostra de alarme, selecione o alerta no **Nome do alerta** e clique em **Buscar dados de amostra** para extrair a instância mais recente de um alerta disparado do Splunk Enterprise console.

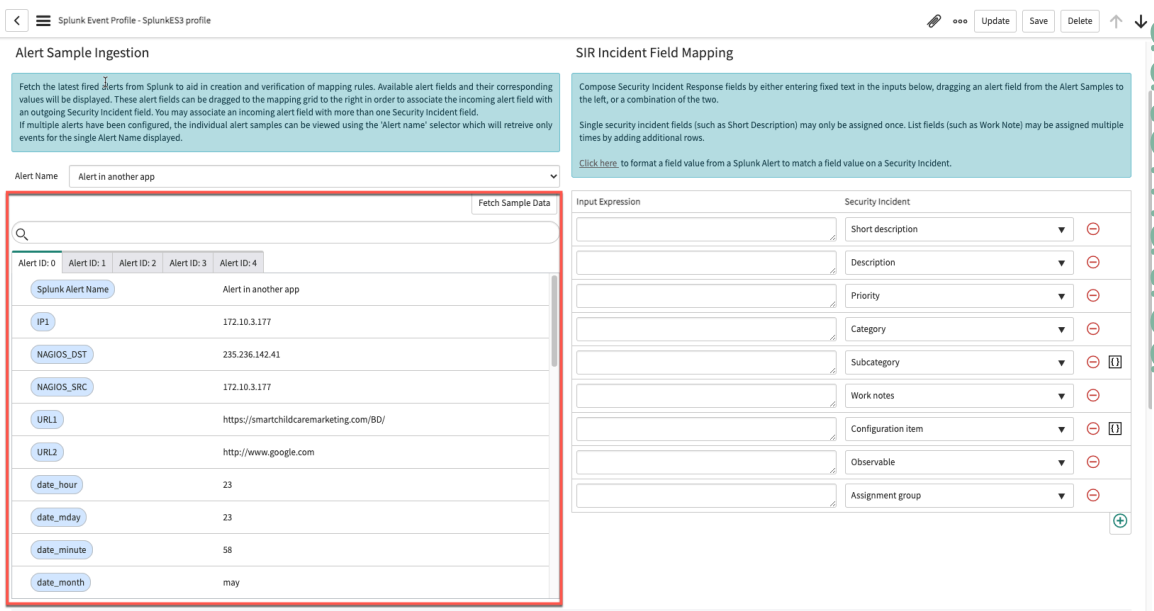
   Os alertas são exibidos como guias. Você pode ingerir até cinco dos alertas mais recentes.

   A extração de eventos de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

   Nota: Um campo de mapeamento adicional, **Nome do alerta do Splunk** , é adicionado pela integração para permitir o rastreamento de um evento para a regra de alerta de origem em Splunk. Isso pode ser útil em cenários em que vários Splunk os alertas são combinados em um único perfil.

   Quando um único campo contém vários valores, esses valores são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR. Por exemplo, os endereços IP de origem, nomes de ativos ou URLs podem ter várias entradas de campo observável ou vários ICs, que são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR.

   Na figura a seguir, os pares de valor de nome de campo para o alerta ingerido ou o evento de amostra importado são exibidos no lado esquerdo deste formulário depois que a extração é concluída. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



3. Para perfis de alerta programados, prossiga para a etapa cinco para mapear os valores.
4. Como alternativa, para um perfil para um tipo de evento que você deseja exportar do seu Splunk Enterprise siga estas etapas para carregar dados de anexo em seu ServiceNow AI Platform® instância.

   a. Se ainda não estiver conectado, faça login em Splunk Enterprise console.

   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados do evento que você deseja exportar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, malware é um termo de pesquisa usado para todos os eventos de malware que você pode encaminhar com o fluxo de trabalho desta integração.

c. Expanda o evento e, na coluna Campo, selecione os campos que você deseja importar.

Esses campos são os pares campo-valor que são exportados e exibidos na página Mapeamento do seu ServiceNow AI Platform® instância.

d. Em seu Splunk Enterprise No canto superior direito da página Pesquisar, clique em **Exportação** ícone.

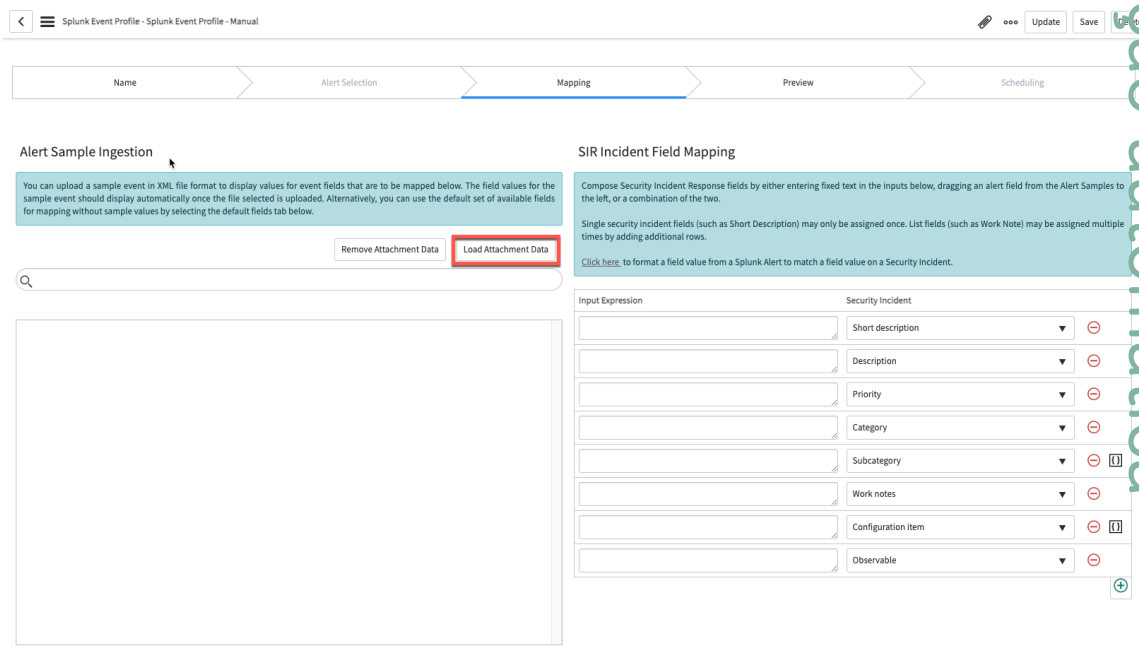
e. Na lista do campo Formato na caixa de diálogo exibida, clique em **Formato XML** .

f. Opcional: Insira um novo nome de arquivo.

g. Clique em **Exportar**.
O arquivo é baixado para seu ServiceNow AI Platform® instância.

h. Se a página Mapeamento ainda não estiver exibida em seu ServiceNow AI Platform® instância, clique em **Mapeamento** na barra de andamento.

i. Na coluna Ingestão de amostra de alerta, clique em **Carregar dados do anexo** .



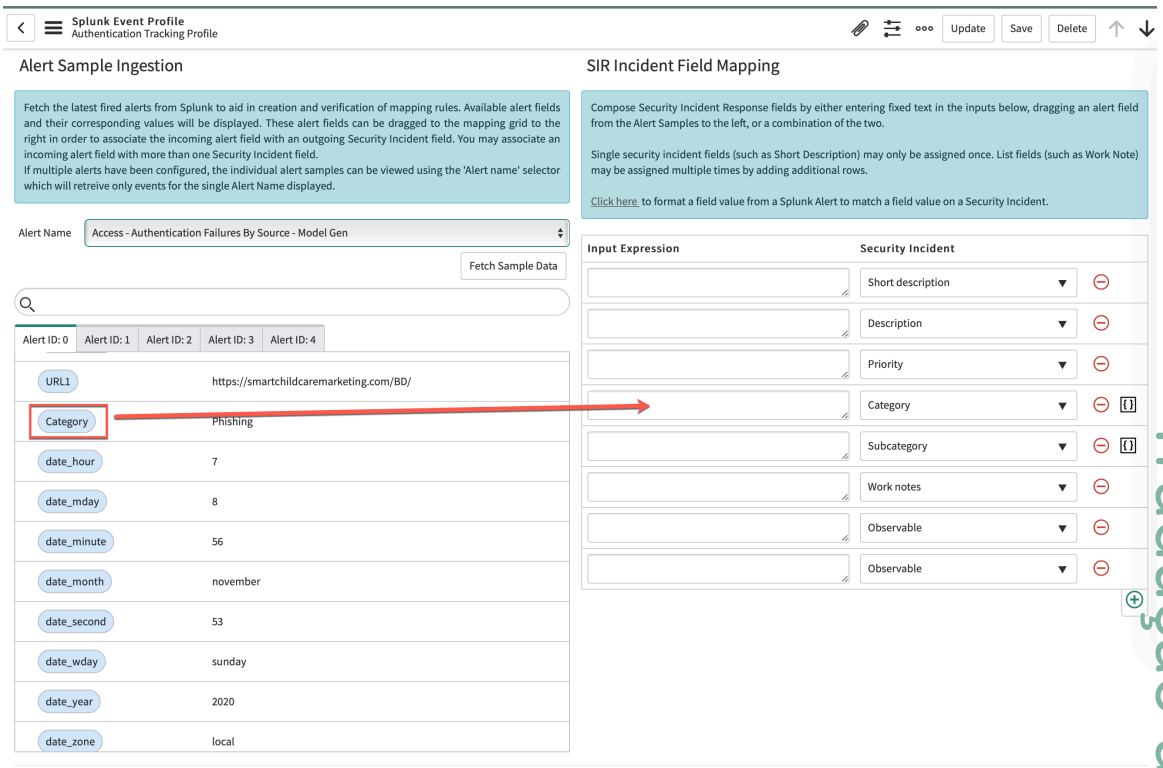
j. Na caixa de diálogo exibida, clique em **Escolha Arquivos** e navegue até .xml arquivo exportado e clicado **Aberto** .
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

Na figura a seguir, os pares de dados para um alerta programado ingerido são exibidos no lado esquerdo deste formulário. Pares de valores para eventos importados também são exibidos neste lado do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
6. Arraste o nome do campo, por exemplo, categoria E solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.



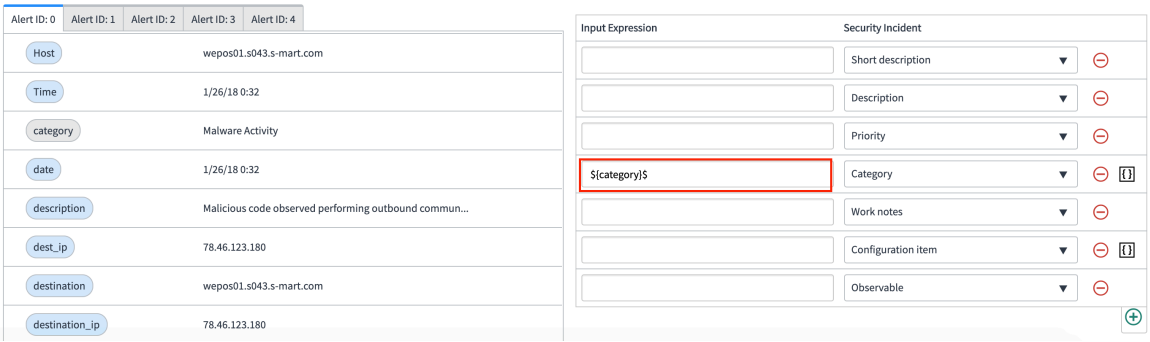
O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, categoria está mapeado para categoria campo no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar você a garantir que nenhum evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Campos azuis claros à esquerda indicam que um campo ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação por cores ajuda a rastrear o mapeamento, porque, em determinados casos, os campos de evento de alerta só podem ser atribuídos uma vez. Por exemplo, você só pode atribuir valores a campos como Descrição resumida uma vez. No entanto, você pode atribuir campos de lista, como anotação de trabalho, várias vezes, adicionando linhas adicionais à grade de mapeamento.

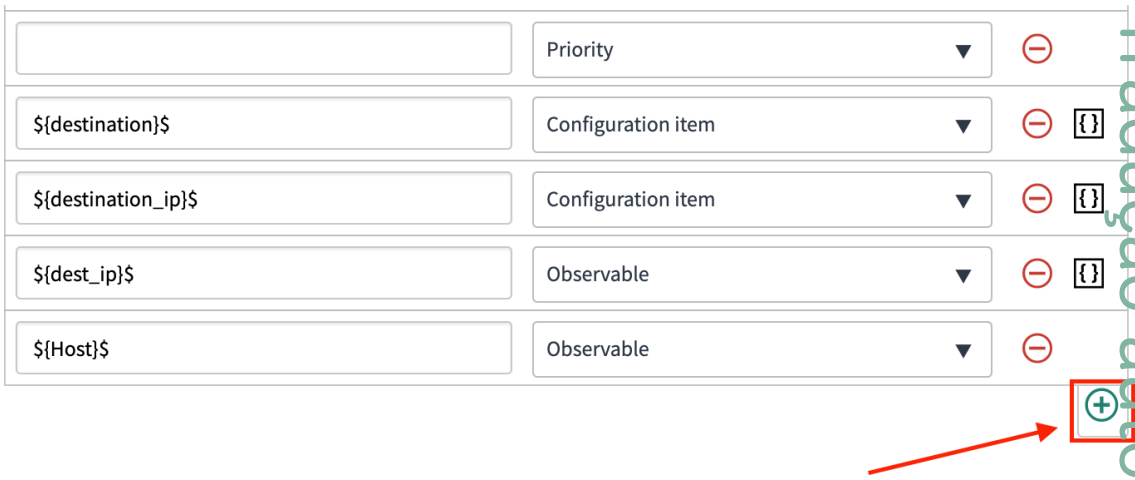
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Para adicionar campos ao mapeamento padrão do incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de adição.



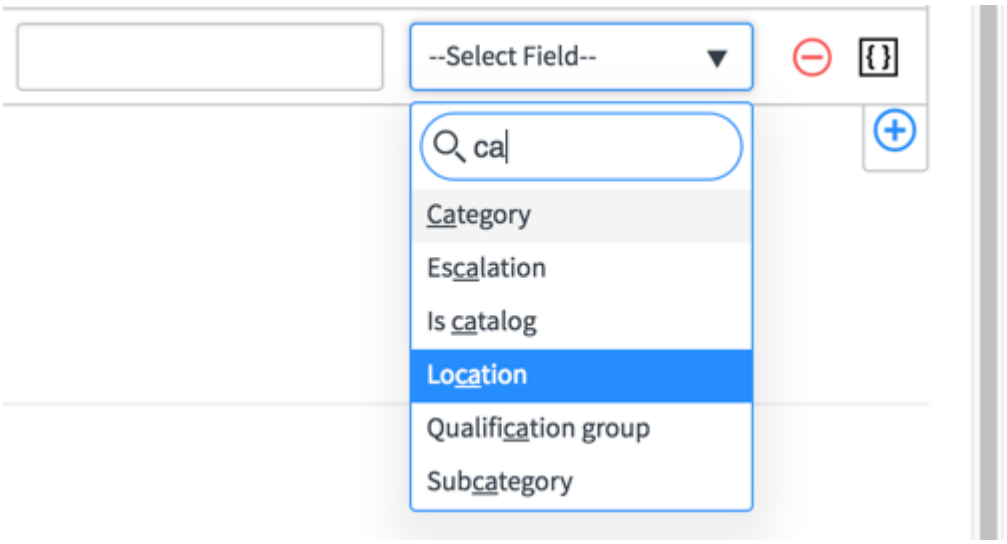
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Na lista expandida do novo campo, alguns campos são sombreados. Na figura a seguir, Categoria tem um fundo cinza, porque foi mapeado no incidente de segurança. Semelhante à codificação por cores para campos de alerta no lado esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear o mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

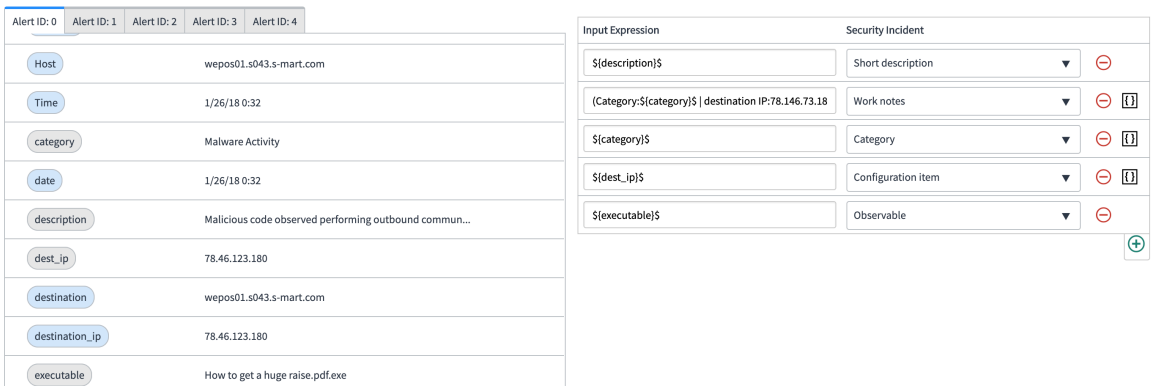


Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar **ID do alerta** Que você deseja no campo Expressão de entrada.
Com o recurso de arrastar, mapeie-o ao lado do novo campo.

8. Continue o mapeamento adicionando ou removendo campos e adicionando valores ao mapa.
A figura a seguir é um exemplo de uma grade de mapeamento editada. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Os valores são separados por espaços e sinais de pontuação (IP de destino:78.146.73.180).



Na visualização, esses valores são exibidos nas anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à grade e há vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e os sinais de pontuação inseridos no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

A imagem a seguir é um exemplo de como os valores na imagem anterior são exibidos no incidente de segurança.

Related Items

Field Name	Field Value
Work Note	Category: Malware Activity | destination IP: 78.46.123.180
Work Note	Source: MalwareDemoData Top 100 events with 15 host machines

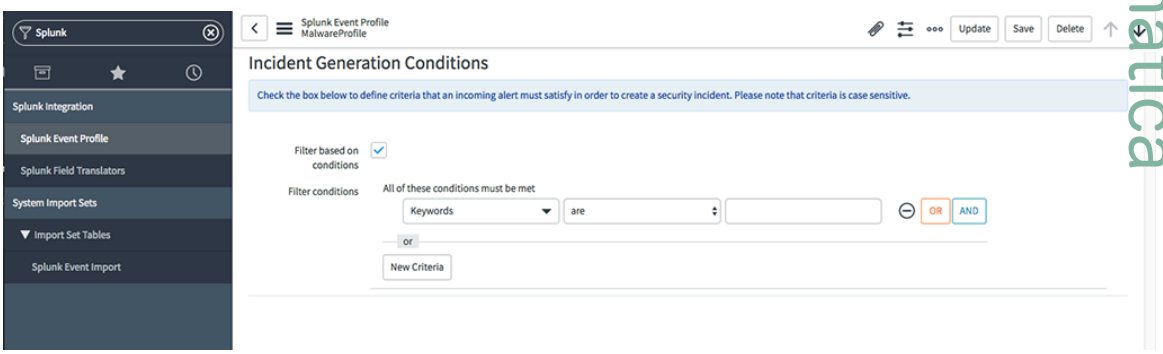
Condições de filtragem de geração de incidentes

9. **Opcional:** Depois de concluir as etapas de mapeamento no nível de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de filtro para definir critérios adicionais que um alerta de entrada deve atender para criar um SIR incidente de segurança.
Para definir condições de filtragem, siga estas etapas.

   a. Role até a seção Condições de geração de incidentes no formulário e selecione **Filtro com base em condições** marque a caixa para habilitar a opção.

   (Optional) O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de alerta para o alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo de Splunk alerta de que você ingesta ou o evento que você encaminha manualmente. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores de Splunk Enterprise alerta ou evento. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao Splunk Enterprise console e revise seus alertas e eventos para as palavras-chave.



   b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

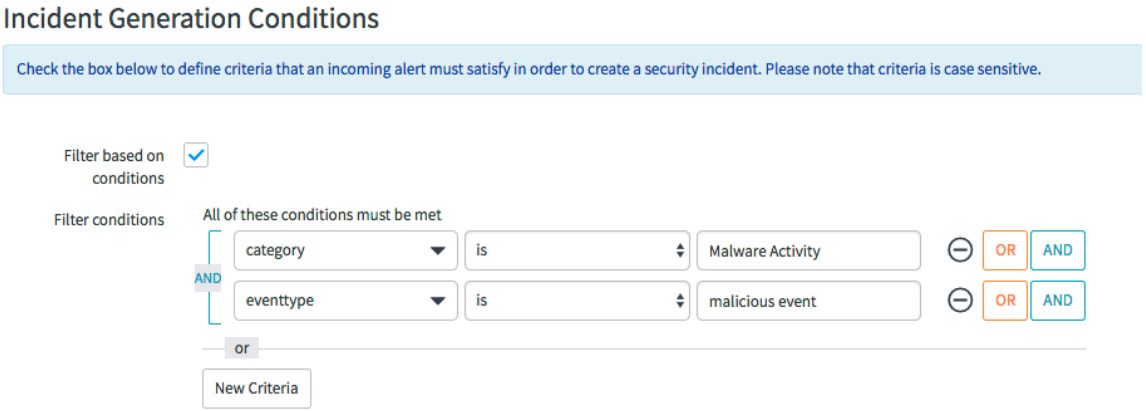
   c. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
   Se **E.** selecionado, todas as condições devem ser correspondidas. Se **OU** está selecionado, qualquer condição pode ser correspondida.

   d. **Opcional:** Na segunda linha, defina uma segunda condição de filtro.

   (Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



(Optional) Você definiu as condições de acionamento para que os incidentes de segurança sejam criados somente quando as duas condições de filtragem inseridas forem correspondidas.

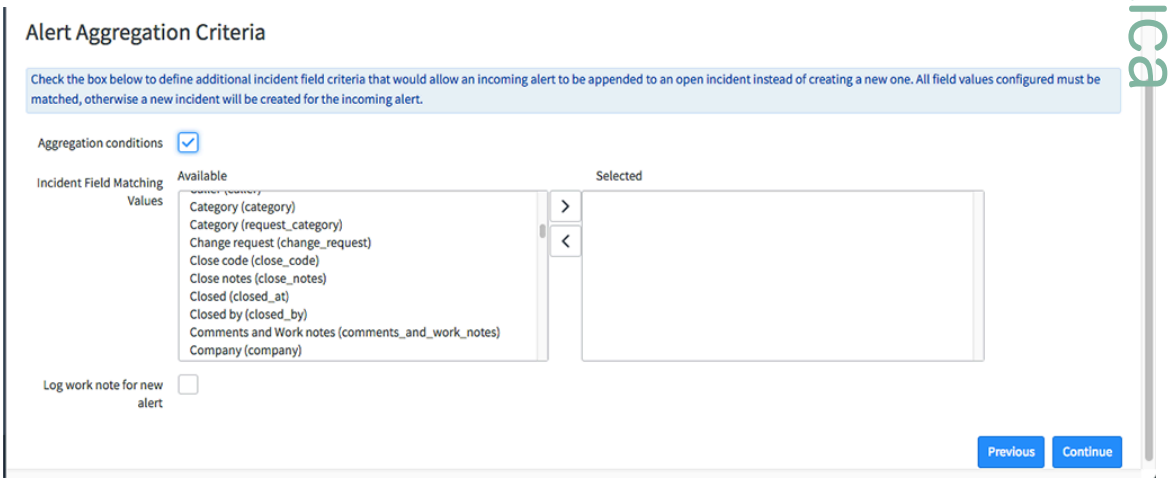
Esse tipo de filtragem ajuda a isolar eventos de segurança e limita o número de incidentes de segurança criados. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem precisar mudar o. Splunk ou a configuração de alerta acionada.

Alertas de agregação para evitar incidentes duplicados

10. Opcional: Para evitar a possível criação de incidentes de segurança duplicados, defina critérios de campo de incidente adicionais para que os alertas de entrada sejam agregados a um incidente de segurança em aberto. Para definir esses critérios, siga estas etapas.

a. Role até a seção Critérios de agregação de alertas no formulário e marque a caixa de seleção Condições agregadas para habilitar esta opção.

(Optional) As colunas Valores de correspondência do campo do incidente são exibidas. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.



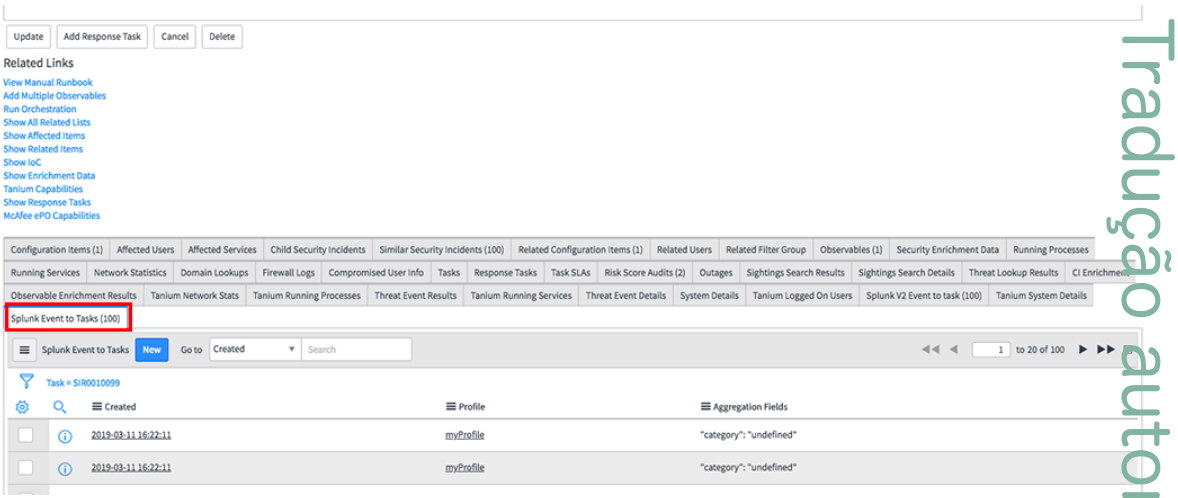
b. Na lista Disponível, selecione os valores de campo que você deseja corresponder nos incidentes de segurança existentes em seu ServiceNow AI Platform E mova-os para a lista Selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Se você preferir revisar os valores de campo em incidentes de segurança a serem usados para esses critérios, navegue até **incidentes** > **Mostrar todos os incidentes**.

Se um novo alerta corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos no Splunk Evento para lista relacionada de tarefas. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam você a entender por que os alertas são adicionados a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique em **Mostrar todas as listas relacionadas** link.



c. Opcional: Para registrar em log uma anotação de trabalho para um novo alerta que foi adicionado recentemente no incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra em log que um novo alerta foi adicionado junto com um link para os detalhes do alerta.

Valores mapeados com sucesso de um Splunk alerta ou evento para campos em um SIR incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos ao existente SIR incidentes de segurança.

11. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de scripts, consulte Use o editor de scripts para formatar valores de alerta para Splunk Enterprise Event Ingestion integração.

12. Escolha um para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Visualização está selecionado na barra de andamento. A próxima etapa é visualizar os campos mapeados em um SIR incidente de segurança.
Atualizar	Seus dados são salvos e Splunk A lista Perfis de evento é exibida.
Anterior	O formulário Seleção de alerta é exibido.
Excluir	Exclua este perfil de evento e o. Splunk A lista Perfis de evento é exibida.

O que Fazer Depois

A próxima etapa é visualizar os valores mapeados no incidente de segurança.

Visualize o incidente de segurança do Splunk Enterprise Event Ingestion integração

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um ServiceNow AI Platform® Resposta a incidentes de segurança(SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

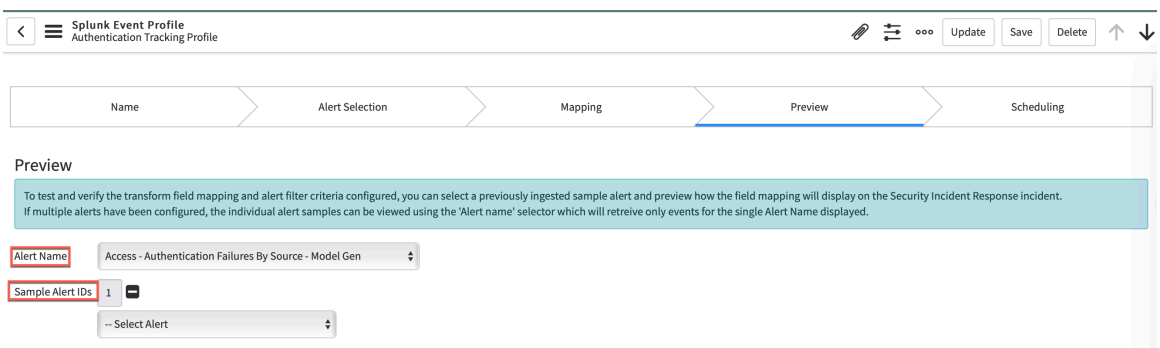
Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. Visualizações de SIR os incidentes de segurança não são salvos como incidentes reais no SIR produto.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
2. Selecione **Nome do alerta** e, em seguida, selecione um item no **IDs de alerta de amostra** lista.

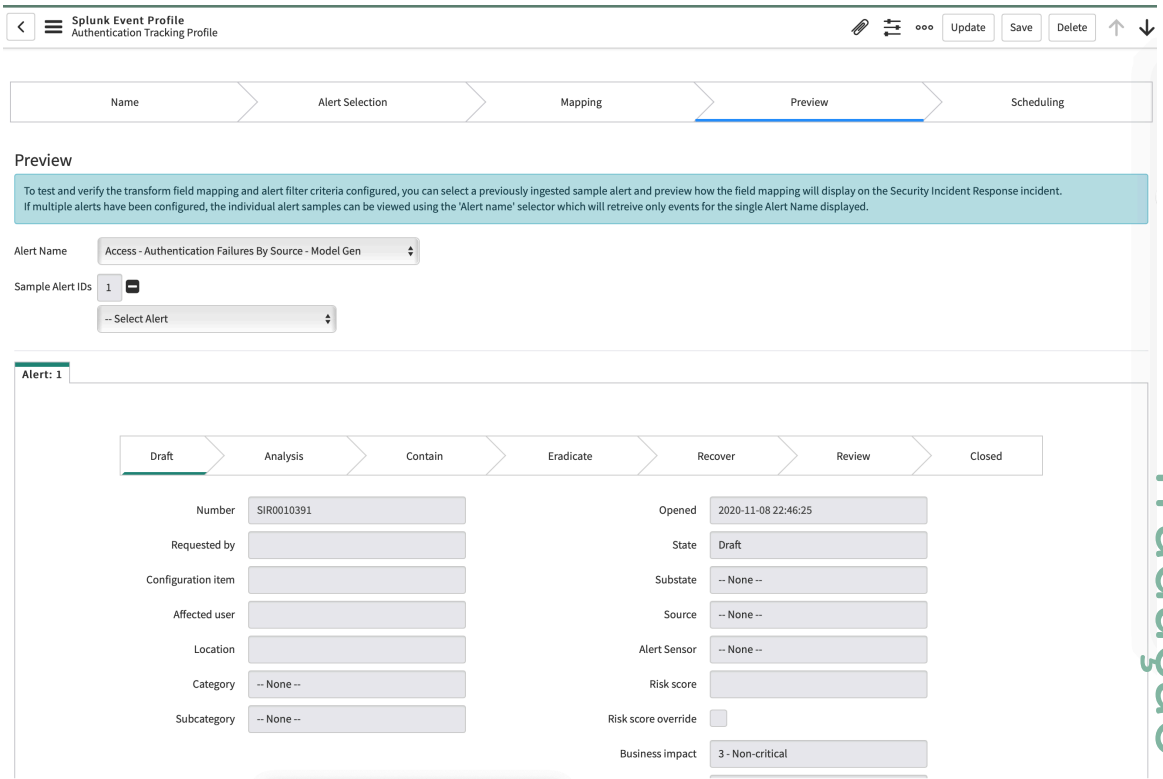


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.

3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



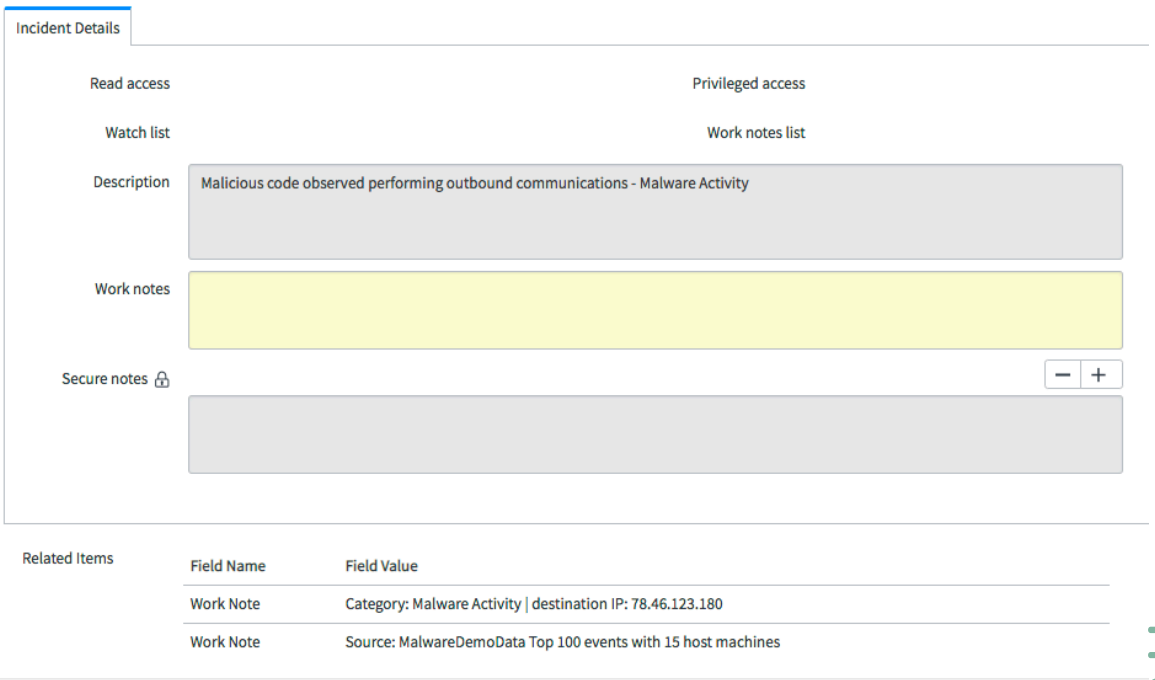
A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um campo no incidente de segurança não existe para um valor ou o campo não é compatível com o valor mapeado. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para Item de configuração campo.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um SIR incidente de segurança após todas as mensagens de erro serem resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos do Splunk Enterprise console. O primeiro campo de anotações de trabalho não tem valor. Este campo foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotação de trabalho adicionais que têm valores foram adicionados à grade de mapeamento durante a etapa de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Depois de corrigir os erros e verificar se os campos estão do jeito desejado, escolha uma opção para continuar.

Opção	Descrição
Continuar	O formulário Programação é exibido para perfis com alertas programados. **Programação** está selecionado na barra de andamento.
Encerrar	Para perfis com configurados para encaminhamento manual de eventos, clique em **Concluir** . Não há etapa de programação para perfis com dados de evento que são exportados sob demanda diretamente do Splunk Enterprise console.
Atualizar	Seus dados são salvos e você retorna para Splunk Lista de perfis de evento.
Anterior	A etapa Mapeamento na barra de andamento é exibida.
Excluir	Exclua este perfil de evento e o. Splunk A lista Perfis de evento é exibida.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será Programar e recuperar alertas para Splunk Enterprise Event Ingestion integração.

Programar e recuperar alertas para Splunk Enterprise Event Ingestion integração

Para perfis de ingestão de alertas automatizados, esta etapa é a etapa final da configuração do perfil de evento. Durante esta etapa, você pode verificar as configurações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

padrão para recuperação de alertas ou modificar a programação conforme necessário. Esta etapa permite filtrar sua recuperação de alertas com base em um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Depois de concluir todas as etapas na barra de andamento da configuração do perfil, conforme mostrado na figura a seguir, você concluiu a configuração dos perfis para encaminhamento manual de eventos. Não há programação disponível para eventos encaminhados manualmente do seu Splunk Enterprise console. Para perfis para ingestão automatizada de alertas, você escolhe se deseja ingerir alertas históricos durante a etapa Programação. Você também escolhe a frequência com que pesquisará alertas futuros que correspondam à configuração do perfil de alerta.

Barra de andamento



Para perfis de ingestão de alertas automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação de alertas. Esta etapa é a etapa final do processo de configuração do perfil de evento para perfis de alerta programados.

Configure esses intervalos de pesquisa por perfil. O desempenho do Splunk a integração de ingestão de evento é afetada pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Em Splunk Enterprise console, você define um alerta a ser acionado com base em incrementos ou em um horário específico. Use esta configuração para ajudá-lo a configurar a programação no seu ServiceNow AI Platform para que o tempo seja incrementado em seu Splunk Enterprise sincronização do console com a programação que você configurou no seu ServiceNow AI Platform instância.

Procedimento

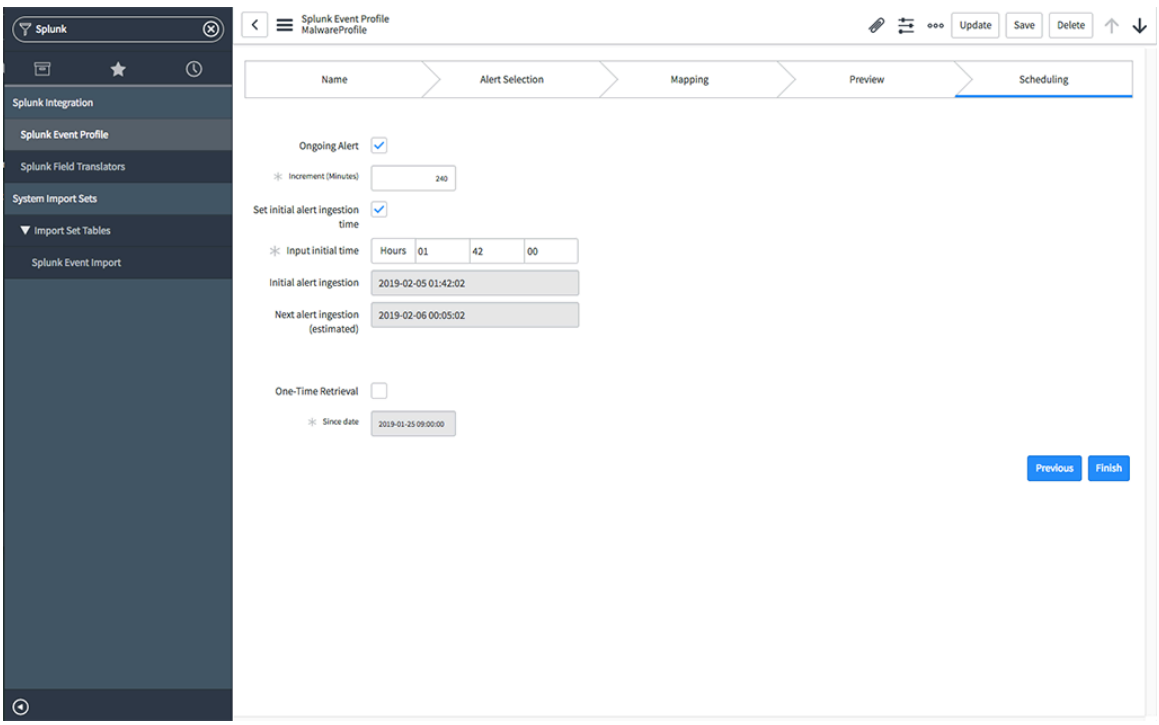
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando os alertas são extraídos do Splunk Enterprise console.

Opção	Descrição
◦ Campo Alerta contínuo selecionado ◦ Campo Recuperação única limpo	Alerta contínuo Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do Splunk Enterprise servidor para novos alertas a cada cinco minutos. Os incidentes de segurança serão criados se alertas acionados forem encontrados e os critérios de filtragem forem correspondidos. Para equilibrar a ingestão de alertas em relação à carga do servidor e extrair os dados mais atuais,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cinco minutos é a configuração que você pode preferir. No entanto, este valor pode ser modificado conforme necessário.
○ Campo de alerta contínuo limpo ○ Campo Recuperação única selecionado	Recuperação única Use esta configuração se quiser que uma extração única ingere alertas com base em eventos históricos. Quando configurado, um perfil é usado uma vez para recuperar alertas acionados, incluindo alertas de eventos históricos baseados em um intervalo de datas. À direita do **Desde a data**, clique no ícone de calendário. No calendário exibido, selecione a data em que você deseja começar a extrair alertas. Começando com **Desde a data** alertas acionados são recuperados até a data atual. Depois que os alertas forem extraídos, esta configuração não recuperará alertas acionados para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os alertas encontrados para o intervalo inserido.



Como exemplo de programação, se você tiver um diário Splunk Alerta que é executado uma vez por dia às 4 hora local, você pode configurar o perfil de alerta correspondente em seu ServiceNow AI Platform Instância a ser executada às 4:05 hora local para capturar o alerta imediatamente e criar um incidente de segurança. Insira `04 05 00` em **Ingestão de alerta inicial** campo. Em **Incremento (minutos)** campo, insira `1440` (24 horas) para programar a próxima ingestão de alerta para 24 horas a partir da ingestão de alerta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

inicial. A hora de ingestão do alerta inicial e a hora da próxima ingestão do alerta são exibidas nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, selecione **Alerta contínuo** marque a caixa para habilitar esta opção.

   b. Em **Incremento (minutos)** campo, insira `1440` (24 horas).

   c. Clique em **Selecione Ingestão de alerta inicial** Caixa de seleção para habilitar a edição dos campos Ingestão de alerta inicial e Próxima ingestão de alerta.

   d. No campo Ingestão de alerta inicial, insira `04 05 00` .
   Em **A próxima ingestão de alerta (estimada)** a hora da próxima ingestão de alerta é exibida.

4. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Este perfil está ativado e extrai alertas do Splunk Enterprise console baseado em sua programação. Há um limite de 1 000 incidentes de segurança que podem ser criados em um período de 24 horas. Até 100 eventos são por alerta disparado. Eventos subsequentes serão ignorados depois que os limites forem atingidos.

Arquitetura de integração e conexão de sistemas externos para Splunk Enterprise Event Ingestion integração

O tópico a seguir descreve a arquitetura de integração desenvolvida para oferecer suporte à ingestão de alertas acionados do Splunk Enterprise console. Esta informação esclarece, em alto nível, o funcionamento conceitual da integração. Ele também explica por que há etapas de configuração necessárias antes de instalar a aplicação do ServiceNow Store.

Principais termos usados para esta integração

Os termos-chave a seguir são usados durante a instalação e a configuração. Para obter mais informações sobre esses termos, consulte Site de documentação do produto da ServiceNow e o. Site da Splunk e recursos em Recursos do Splunk página.

ServiceNow AI Platform

Uma empresa ServiceNow produto. . ServiceNow AI Platformé a base sobre a qual componentes individuais, como Resposta a incidentes de segurança(SIR IT Service Management (ITSM) e outros produtos são criados.

ServiceNow Splunkbase add

. ServiceNow aplicação que está instalada no seu Splunk Enterprise console que oferece suporte à opção de encaminhamento de eventos manual da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Isso ServiceNow O complemento Splunkbase não é necessário para a ingestão automatizada de alertas fornecida pela integração.

Resposta a incidentes de segurança (SIR)

. ServiceNow AI Platform aplicação que rastreia o andamento de incidentes de segurança desde a descoberta e a análise inicial, até contenção, erradicação e recuperação, e até a revisão e fechamento finais pós-incidente.

Splunk Enterprise

Um produto automatizado de gestão de eventos de incidentes de segurança (SIEM) ou serviço em nuvem que coleta dados usados para análise e gestão de incidentes. Este serviço está em um host que às vezes também é chamado de Splunkneste guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk alerta

Uma pesquisa que você configura e salva em Splunk para verificar dados específicos com base nos parâmetros configurados no Splunk Enterprise serviço. Quando você extrai alertas de Splunk você também extrai todos os eventos associados a esse alerta.

Splunk alerta acionado

Uma pesquisa configurada no Splunk Enterprise console que retorna resultados e sinaliza esses resultados como alertas acionados. Os alertas acionados são ingeridos do Splunk console em seu ServiceNow AI Platform instância desta integração. Os alertas acionados têm um ou mais Splunk eventos.

Splunk evento

Um ou mais elementos de dados que resultam nos alertas acionados do Splunk serviço. Do seu ServiceNow AI Platform instância, você pode pesquisar qual Splunk eventos acionados ServiceNow AI Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre o. ServiceNow AI Platform e aplicações externas, fontes de dados e serviços. Normalmente, esta aplicação é necessária para integração com tecnologias no local e, para isso Splunk Enterprise Event Ingestion O MID Server facilita a comunicação entre o. ServiceNow AI Platform e a instância no local de Splunk Enterprise. Um MID Server não será necessário se você estiver integrando seu ServiceNow AI Platform instância com um Splunk Cloud instância.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com SIR produto em seu ServiceNow AI Platform instância.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage com e analisa incidentes de segurança no ServiceNow Resposta a incidentes de segurança produto.

Administrador de perfil de incidente de segurança (sn_si.ingestion_profile_admin)

O usuário com esta função configura o plug-in, cria, edita, exclui e mantém perfis de ingestão para Azure Sentinel, Splunk e Splunk ES Integration para SIR produto em seu ServiceNow AI Platform instância.

Conexão de sistemas externos

Um perfil de evento é um contêiner que você cria, nomeia e configura para uma conexão singular e chama para Splunk serviço para extrair os alertas acionados mais atuais que correspondem a critérios específicos. Alertas acionados que correspondem ao seu perfil foram extraídos de Splunk, você seleciona quais desses alertas deseja exibir como ServiceNow AI Platform Resposta a incidentes de segurança SIR incidente de segurança. Uma exibição padrão do Splunk Enterprise os campos de alerta estão disponíveis e você edita este mapeamento de campos de alerta para os campos em um SIR incidente de segurança para atender às suas necessidades. Você visualiza seu mapeamento para verificar se todos os valores de campo de alerta necessários estão preenchidos no SIR incidente de segurança. Para concluir a configuração do perfil de alerta, programe a recuperação de alertas e ative o perfil. Depois de ativar o perfil no ServiceNow AI Platform, você está pronto para ingerir históricos e em andamento Splunk alertas automaticamente.

Como um usuário com a função sn_si.admin, se você determinar que um novo alerta acionado é semelhante aos alertas ingeridos anteriormente, poderá agregar novos alertas acionados aos existentes SIR incidentes de segurança. Você define critérios para especificar valores de campo de destino correspondentes em Splunk Enterprise perfil de alerta que define quando um incidente de segurança existente é atualizado e quando um novo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

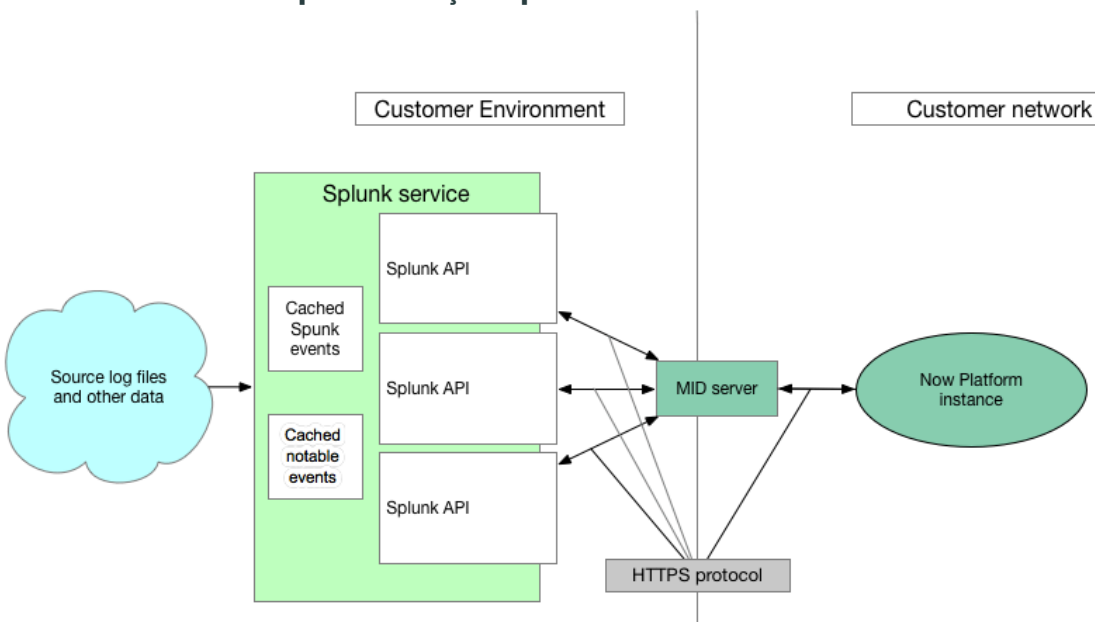
incidente de segurança é criado. Se o recurso de agregação estiver habilitado em seu perfil de evento, quando o conjunto de importação for transformado, seu ServiceNow AI Platform a instância verifica se há um registro existente na tabela de destino que tenha o mesmo valor nos campos de destino e origem. Se um registro existente com um valor correspondente na tabela de destino for encontrado, esse registro será atualizado. Se nenhum registro correspondente for encontrado, um novo registro será criado na tabela de destino. Se habilitada, a opção de agregação atualizará os incidentes de segurança existentes com novos alertas acionados e você evitará a criação de vários incidentes de segurança. Para obter mais informações sobre como atualizar registros usando opções de agregação, consulte Atualizando registros usando aglutinação .

Esta aplicação usa Splunk Serviço de API para recuperar informações do Splunk serviço. Uma conexão HTTPS de saída do MID Server para este ambiente é necessária para que a integração funcione corretamente.

Depois que ele é conectado ao Splunk, a integração oferece suporte à extração e ingestão de alertas e eventos acionados que acionam incidentes de segurança.

O fluxo de dados básico é ilustrado nas figuras a seguir. Em cada figura, seu ServiceNow AI Platform extraindo (ingerindo) dados. Splunk não está enviando dados para alertas programados.

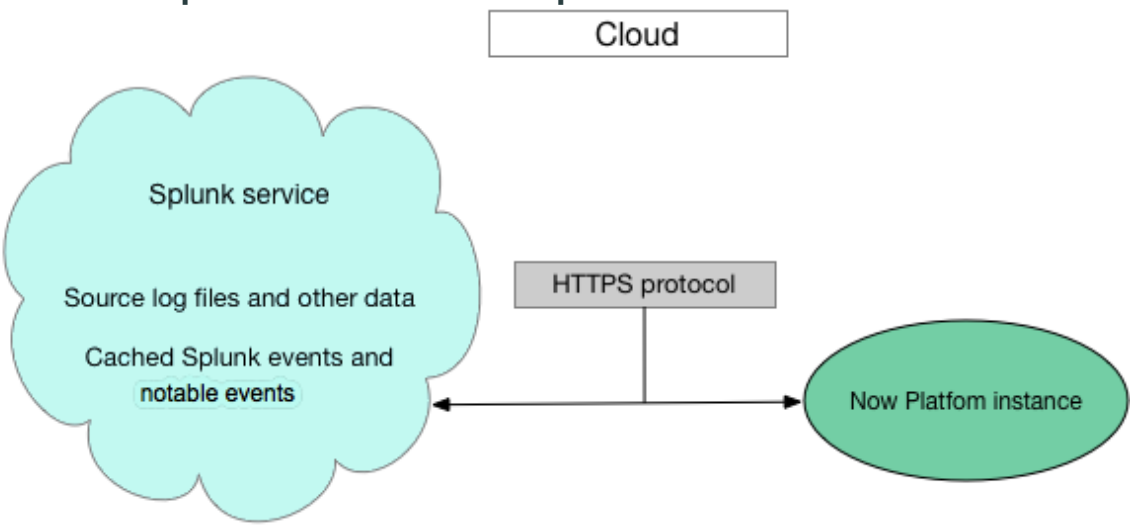
Conexão com no local Splunk Serviço empresarial com MID s únicos servidor



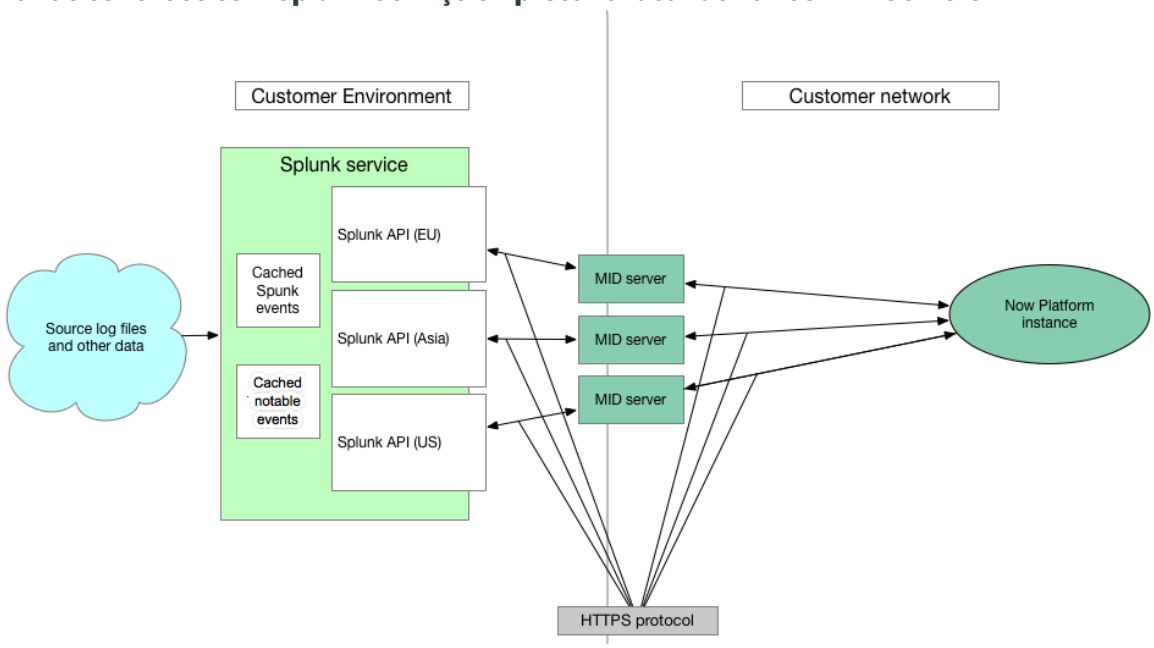
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conexão a um Splunk instância de nuvem corporativa



Várias conexões com Splunk Serviço empresarial usando vários MID Servers



Tradução automática

Cópia Splunk Enterprise Event Ingestion perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar Splunk Enterprise Event Ingestion configurações de perfis de um ServiceNow AI Platform instância para um diferente ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Esta funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em um ServiceNow AI Platform instância, por exemplo, em não produção, para outra ServiceNow AI Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações exportadas e importadas incluem nome de perfil, regras de correlação, mapeamentos, filtros, critérios de agregação,

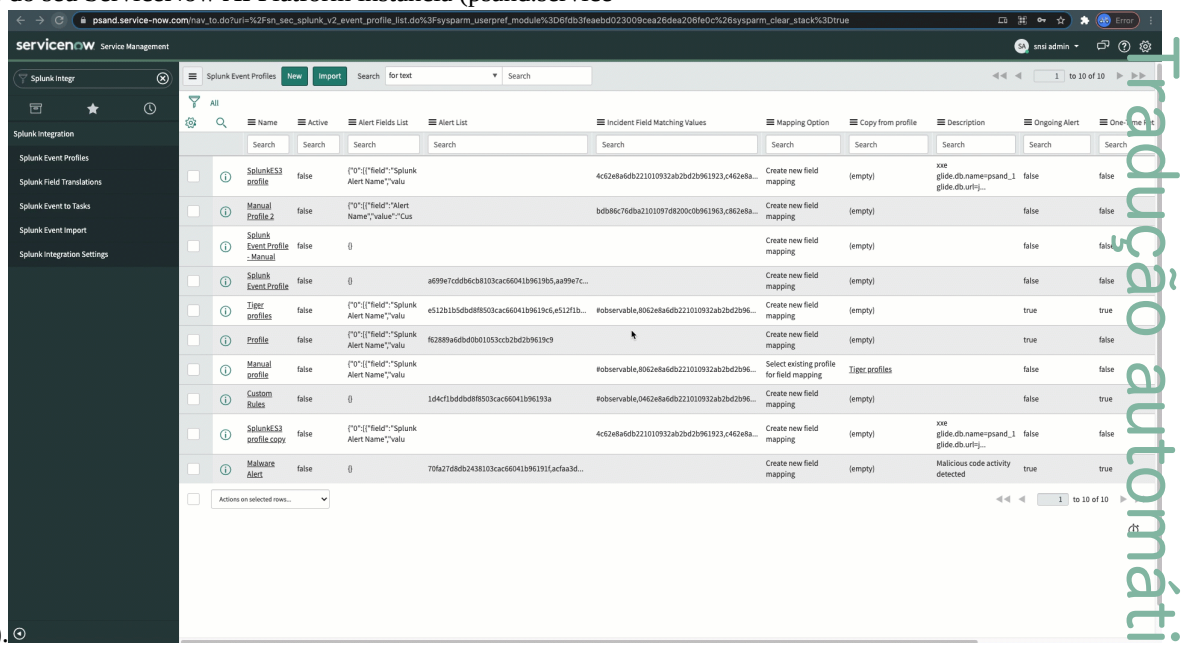
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

traduções de campo, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Nota: Quando você exporta um tipo de perfil de encaminhamento de evento manual, os dados do anexo usados para o mapeamento de campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

Procedimento

1. Navegar até **Tudo** > **Splunk Integration** > **Perfis de eventos do Splunk**.
2. Selecione um perfil que você deseja exportar para outro ServiceNow AI Platform instância.
   Você pode selecionar vários perfis para exportação.
3. No menu Ações, clique em **Exportação** .
4. Quando a mensagem de exportação concluída for exibida, clique em **Download** .
   A ilustração a seguir mostra como exportar um Splunk Perfil (Perfil manual 2) do seu ServiceNow AI Platform instância (psand.service-now.com).

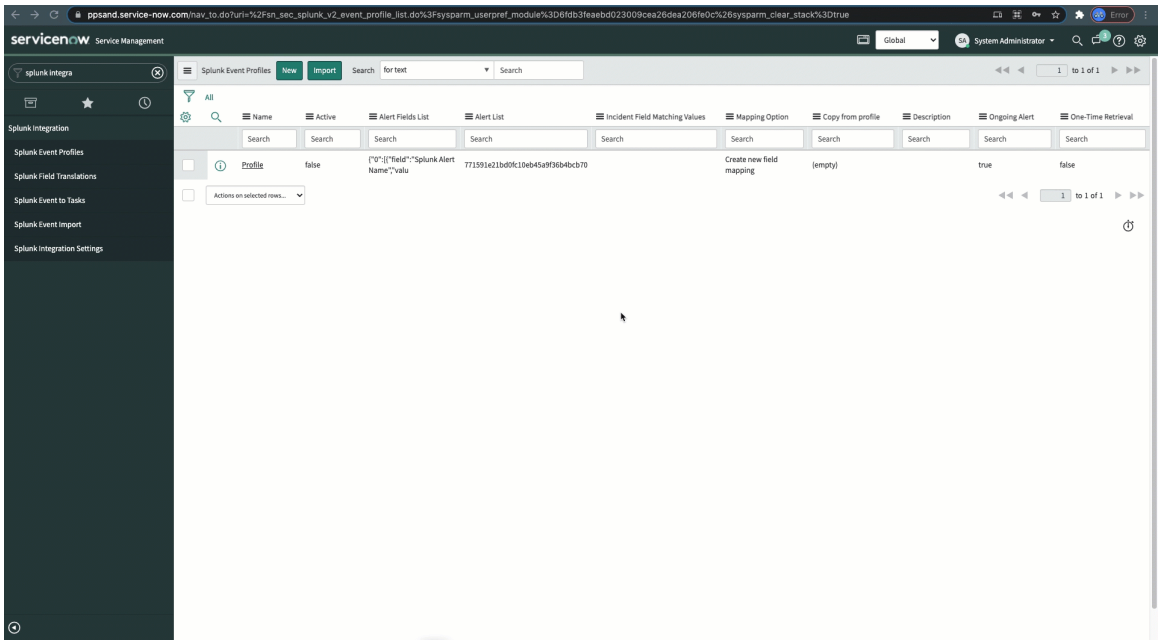


   O arquivo payload.xml exportado é baixado em seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campo, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

   Agora você pode prosseguir para importar o perfil em outro ServiceNow AI Platform instância.
5. Navegar até **Splunk Integration** > **Perfis de eventos do Splunk**.
6. Clique em **Importar**.
7. Clique em **Escolha o arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Upload** (Carregar).
9. Clique em **Fechar e recarregar perfis** .
   A ilustração a seguir mostra como importar um Splunk Perfil (Perfil manual 2) do ServiceNow AI Platform instância (psand.service-now.com) para outra ServiceNow AI Platform instância (ppsand.service-now.com).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outro ServiceNow AI Platform instância.

Verifique se a Origem exportada (Splunk Conta de API e. Splunk E as definições de configuração do MID Server são válidas e estão disponíveis no importado ServiceNow AI Platform instância. Atualize seu Splunk Enterprise Event Ingestion configuração, se necessário.

10. **Opcional:** Verifique as configurações DO MID Server após importar um perfil.
11. **Opcional:** Navegar até **Operações de segurança** > **Configurações de Integração**.
12. **Opcional:** Selecione Splunk Enterprise Event Ingestion bloco configuração e clique em **Atualização** .
13. **Opcional:** Revise e atualize os detalhes de origem e DO MID Server conforme necessário.

Copie um perfil de evento para Splunk Enterprise Event Ingestion integração

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis de alarme para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Copiar um perfil existente e suas configurações associadas é opcional.

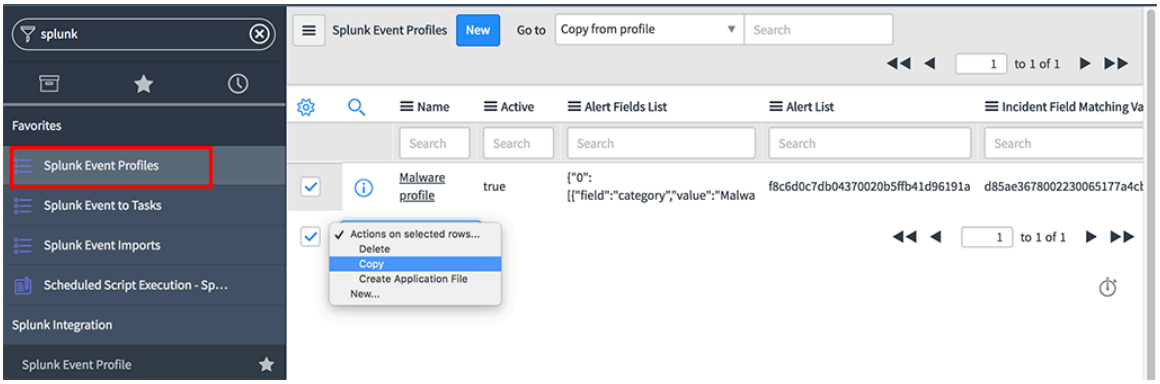
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

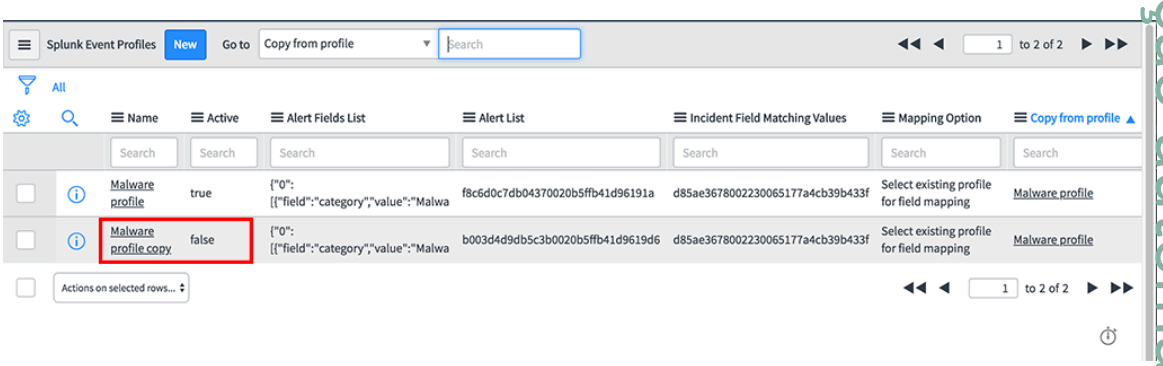
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Splunk Integration** > **Perfil de evento do Splunk**.
2. Em Splunk Lista Perfis de evento exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Cópia** .



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise integração de ingestão de evento

Se você quiser exportar eventos manualmente e sob demanda do seu Splunk Enterprise console para esta integração, instale e configure o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise aplicação em seu Splunk Console empresarial ou instância do Splunk Cloud.

Antes de Iniciar

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in de complemento do splunkbase que é necessário para ingestão manual de eventos. Se você não instalou a aplicação para a integração do ServiceNow Store, consulte Instale e configure o. ServiceNow aplicação para Splunk Enterprise Event Ingestion integração e siga as instruções para instalá-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: ServiceNow AI Platform administrador (admin)

Por Que e Quando Desempenhar Esta Tarefa
Instalação e configuração do ServiceNow O complemento de ingestão de evento de operações de segurança é opcional.

Se você quiser exportar eventos manualmente e sob demanda do seu Splunk Enterprise console para integração, download, instalação e configuração do ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise do splunkbase em seu Splunk Enterprise console.

Isso ServiceNow o complemento de extensão é necessário para que os incidentes de segurança possam ser criados a partir de eventos exportados manualmente em seu ServiceNow AI Platform instância. Isso ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise a aplicação está disponível em splunkbase .

Para encaminhamento manual de eventos, você pode identificar até dois diferentes ServiceNow AI Platform endpoints (instâncias) em seu Splunk Enterprise console. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. PESQUISE ServiceNow Operações de segurança Complemento de ingestão de evento de operações de segurança para Splunk Enterprise.

   > **Nota:** Verifique se você selecionou ServiceNow Operações de segurança Complemento de ingestão de evento para Splunk Enterprise. Há adicionais ServiceNow complementos exibidos nesta lista. Estes addons são para diferentes ServiceNow Splunk e elas não são necessárias para esta integração.

   c. Baixe a aplicação.

   d. Abra seu Splunk Enterprise conta.

   e. Na página Aplicativos, clique no ícone de engrenagem ou em **Gerenciar aplicações** atalho na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicativos exibida, clique em **Instale o app do arquivo** .

   g. Clique em **Escolha Arquivo** , selecione ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise e clique em **Upload** .

   h. Se solicitado, reinicie Splunk Enterprise.
   . ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise está instalado em seu Splunk Enterprise console empresarial. A próxima etapa para configurar o complemento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Para configurar o complemento, siga estas etapas.

a. Em Splunk Enterprise, clique em **Aplicações** ícone de engrenagem ou **Gerenciar aplicações** na lista suspensa do menu.

b. Na lista de aplicações exibida, em **Ações** , clique em **Configurar** para ServiceNow Operações de segurança Complemento de ingestão de evento para Splunk Enterprise.

c. Preencha o formulário.

A figura a seguir é um exemplo de um formulário preenchido em seu Splunk Enterprise console.



Campo na seção Especificar instância primária da ServiceNow	Descrição
Rótulo da ação do fluxo de trabalho	Nome do ServiceNow AI Platform fluxo de trabalho para sua instância de produção (primária). Este nome é o nome de um ServiceNow AI Platform instância que seus usuários que estão monitorando Splunk Os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	eventos são identificados como uma instância primária, por exemplo, Ingestão de eventos da ServiceNow (produção). O padrão para este campo é Ingestão de eventos da ServiceNow (produção). Em seu Splunk Enterprise Este nome de fluxo de trabalho é exibido para a instância de produção (primária) no expandido Ações de evento lista suspensa de uma pesquisa. Este nome é o nome da sua instância de produção. Você pode editar o nome.
URL	O URL do ServiceNow AI Platform Instância que você inseriu no campo Rótulo de ação de fluxo de trabalho anterior. Copie o URL no seu navegador e cole-o neste campo no formulário.
Endpoint	Caminho da API de base. Para obter mais informações, consulte a figura que segue a tabela. Se você não tiver um valor para o endpoint do seu ServiceNow AI Platform instância de produção, siga estas etapas. **a.** Faça login no seu ServiceNow AI Platform instância de produção como um usuário com a função de administrador do sistema (administrador). **b.** Insira REST APIs com script no painel de navegação. **c.** Depois que o painel de navegação for atualizado, selecione **REST APIs com script** módulo exibido. **d.** Se a ingestão de evento não estiver listada na coluna Nome do REST APIs com script lista exibida, no campo de pesquisa na parte superior, insira Ingestão de evento . **e.** Na coluna Caminho da API base na página atualizada, copie este valor e cole-o no campo Endpoint do formulário. Um exemplo de caminho de api base é, /api/sn_sec_splunk_v2/event_ingestion .
Nome do usuário	Nome de usuário do ServiceNow AI Platform instância. Este nome é o nome de usuário do ServiceNow AI Platform instância na qual você atribuiu a um usuário a função (sn_sec_splunk_v2.api_account_access) para encaminhamento manual de eventos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	Para obter mais informações sobre como atribuir esta função, consulte Configure seu ServiceNow AI Platform instância do Splunk Enterprise Event Ingestion integração.
Senha	Senha do ServiceNow AI Platform instância. Esta senha é a senha do ServiceNow AI Platform instância na qual você atribuiu a um usuário a função (sn_sec_splunk_v2.api_–account_access) para encaminhamento manual de eventos.
(Opcional) Campos na seção Especificar instância secundária da ServiceNow	Descrição Esses campos são opcionais. Você não precisa especificar uma instância secundária.
Rótulo da ação do fluxo de trabalho	Nome do ServiceNow AI Platform fluxo de trabalho para sua instância secundária (preparação). Este nome é o nome de um ServiceNow AI Platform instância que seus usuários que estão monitorando Splunk os eventos são identificados como uma instância secundária, por exemplo, ServiceNow Ingestão de evento (preparação). Em seu Splunk Enterprise Este nome de fluxo de trabalho é exibido para a instância de preparação (secundária) na lista suspensa Ações de evento expandidas de uma pesquisa. Isso ServiceNow AI Platform a instância é sua instância de preparação. Você pode editar o nome.
URL	O URL do ServiceNow AI Platform Instância que você inseriu no campo Rótulo de ação de fluxo de trabalho anterior para o secundário ServiceNow AI Platform instância. Copie o URL no seu navegador e cole-o neste campo no formulário.
Endpoint	Caminho da API de base. O valor do caminho da API base para sua instância secundária é o mesmo valor do caminho da API base para sua instância primária. Consulte a figura anterior do formulário para obter mais informações.
Nome do usuário	Nome de usuário do ServiceNow AI Platform instância de preparação. O usuário deve ter a função (sn_sec_splunk_v2.api_account_access).

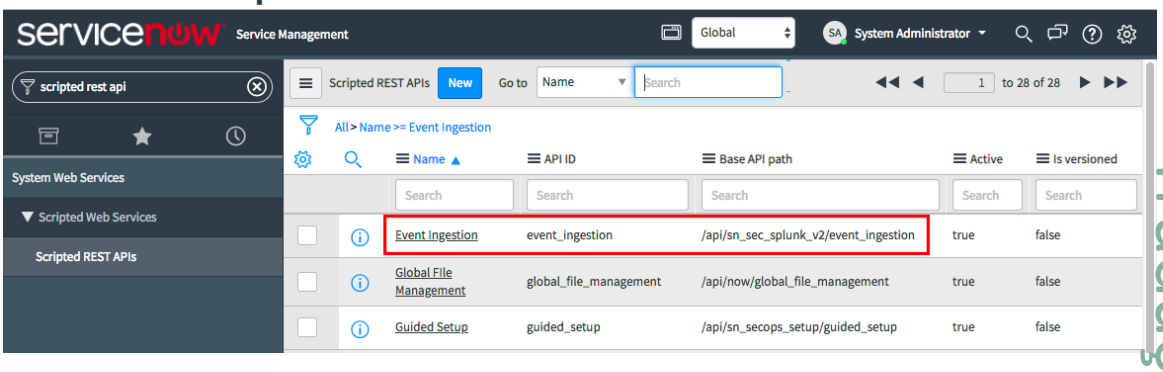
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
Senha	Senha do ServiceNow AI Platform instância de preparação. O usuário deve ter a função (sn_sec_splunk_v2.api_account_access).

A figura a seguir é um exemplo da lista REST APIs com script em seu ServiceNow AI Platform. A lista exibe o local do valor de endpoint de um ServiceNow AI Platform instância que você insere no formulário como parte da configuração para ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise extensão em seu Splunk Enterprise console.

REST APIs com script no ServiceNow AI Platform



3. No formulário de configuração do seu Splunk Enterprise console, clique em **Salvar** para salvar suas edições.

Após alguns momentos, na parte superior esquerda do formulário em seu Splunk Enterprise uma mensagem é exibida informando que o registro foi atualizado com sucesso.

Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) do seu ServiceNow AI Platform As instâncias que você criou no formulário estão disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa em seu Splunk Enterprise console.

O que Fazer Depois

Se você ainda não salvou as pesquisas em seu Splunk Enterprise console, a próxima etapa é salvar pesquisas como alertas em seu Splunk Enterprise console.

Salve pesquisas em seu Splunk Enterprise console para Splunk Enterprise Event Ingestion integração

As etapas a seguir para salvar pesquisas em seu Splunk Enterprise o console é fornecido para um usuário com Splunk Enterprise função de administrador.

Antes de Iniciar

Se você já tiver pesquisas salvas e alertas acionados em seu Splunk Enterprise não é necessário modificar essas pesquisas para esta integração.

A integração do ServiceNow AI Platform® Operações de segurança produto com Splunk o serviço de notificação de eventos extrai informações de evento e alerta do Splunk.

Antes de ingerir alertas em seu Operações de segurança, configure pesquisas em seu Splunk Enterprise para que você extraia automaticamente os eventos de segurança relevantes no Splunk Enterprise que você deseja salvar como alertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você não tiver pesquisas salvas e alertas acionados estabelecidos para notificação quando ocorrerem eventos de segurança importantes em seu Splunk Enterprise siga estas etapas para salvar as pesquisas.

Função necessária: Splunk Enterprise administrador

Procedimento

1. Faça login na sua conta Splunk Enterprise.
2. Clique em **Pesquisa** guia.
3. No campo Nova pesquisa exibido, insira um valor para o alerta, por exemplo, Malware.
4. Para exibir os eventos relacionados à sua pesquisa, à direita do campo Nova pesquisa, clique no ícone de pesquisa ou pressione Enter.
   Os resultados da pesquisa com eventos são exibidos.
5. Para salvar a pesquisa como um alerta, no canto superior direito da página, expanda a lista de seleção Salvar como e selecione **Alerta** .
6. No formulário exibido, preencha os campos.

Campo	Descrição
Título	Nome descritivo do alerta, por exemplo, Eventos de malware. Depois de salvar esta pesquisa como um alerta, os eventos de um alerta dispararam no Splunk os serviços são processados automaticamente em alertas acionados usando esses dados de pesquisa. Este título de alerta acionado é usado no perfil de evento que você cria em ServiceNow AI Platform instância para identificar quais eventos são ingeridos em sua instância para ServiceNow AI Platform® Resposta a incidentes de segurança SIR criação de incidente de segurança.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este alerta de outros alertas.
Tipo de alerta	Nos campos exibidos, selecione **Programado** para pesquisar este alerta em uma programação, ou **Tempo real** para pesquisar continuamente este alerta.
Acionar resultados	Você pode preferir definir uma das seguintes condições de filtro: ○ O número de resultados é maior ou menor que ○ Uma vez (uma vez) para cada resultado
Ações de gatilho	Adicione ações para acionar este alerta. Expanda a lista Adicionar seleção e clique em **Adicionar a Alertas acionados** para que ele seja exibido no formulário. Você pode preferir esta configuração para os alertas que você ingerem em seu ServiceNow AI Platform instância.

7. Clique em **Salvar**.
   Seu alerta é salvo e exibido na guia Alertas na página Pesquisar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. Splunk o serviço extrai os eventos correspondendo aos critérios configurados no alerta. Os eventos são armazenados em cache e você solicita esses eventos de seus perfis que configurou em seu ServiceNow AI Platform instância. Porque a extração de ingestão de eventos ocorre de um cache no Splunk, esta ingestão do seu ServiceNow AI Platform não afeta o desempenho do seu Splunk plataforma.

O que Fazer Depois

Você concluiu com sucesso a configuração necessária para a integração em seu Splunk Enterprise console. Se você ainda não instalou a aplicação para a integração do ServiceNow Store, a próxima etapa é instalar a aplicação para a integração e configurá-la.

Use o editor de scripts para formatar valores de alerta para Splunk Enterprise Event Ingestion integração

Use o editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Além dos campos mapeados diretamente dos valores de alerta extraídos e dos valores de alerta inseridos manualmente, você pode usar opcionalmente o editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. O editor de script muda os valores de um Splunk alerta para que os valores que são compatíveis com ServiceNow AI Platform® Resposta a incidentes de segurança Os incidentes de segurança são mapeados para os campos Categoria, Item de configuração (IC) e Observável.

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

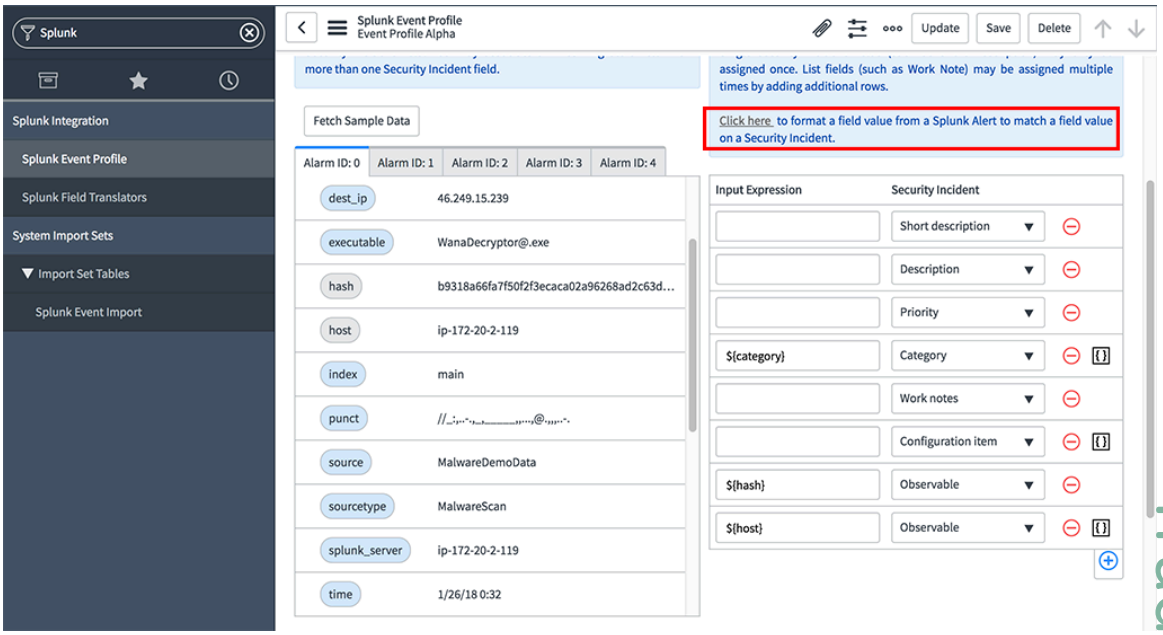
Em determinados casos, Splunk Enterprise Os valores de alerta são mapeados para os campos Categoria, Item de configuração (IC) e Observável no SIR incidente e não são compatíveis. Você pode preferir editar os valores mapeados. Se você quiser traduzir o valor de um Splunk Enterprise alerta para um valor compatível com esses campos no SIR incidente de segurança, use o editor de scripts.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de scripts.

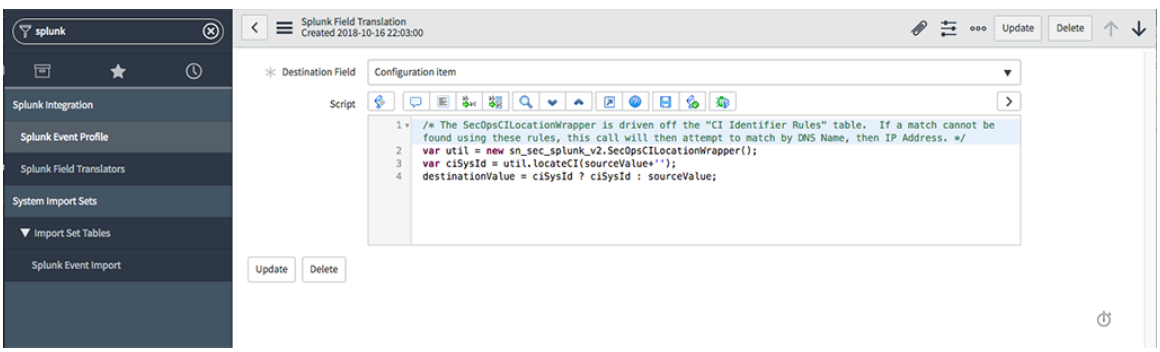


2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete [] ao lado de um campo para abrir o editor de script desse campo.

   Em determinados casos, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um alerta, por exemplo, um valor para o item de configuração pode não ser correspondido.

   Se não for possível encontrar uma correspondência para um nome de host em ServiceNow AI Platform® CMBD Para o campo Item de configuração, você pode editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido em Campo de destino. A imagem a seguir mostra o editor com Item de configuração Campo como o Campo de destino.



4. Insira as mudanças no script e clique em **Atualização** para salvar suas mudanças.
   . Splunk A tabela Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para Splunk Enterprise Event Ingestion integração

Use esta check-list para orientá-lo em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem resultados esperados para a integração.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe seu andamento com a instalação, a instalação e a configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima etapa. Cada linha da tabela lista tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Funções necessárias: As funções são listadas para cada etapa abaixo.

Procedimento

1. Como um usuário com ServiceNow AI Platform função de administrador, configure seu ServiceNow AI Platform instância.
   - Atribuir usuários com **sn_si.ingestion_profile_admin** (ou sn_si.admin) e sn_si.analyst conforme necessário.
   - Instale e configure um MID Server se o Splunk o servidor está implantado em sua rede corporativa.
   - Verifique se o ServiceNow Resposta a incidentes de segurança os plug-ins estão ativados para sua versão do ServiceNow AI Platform.
   - Se você quiser encaminhar eventos manualmente do seu Splunk Enterprise console em seu ServiceNow AI Platform, verifique se você atribuiu a função (sn_sec_splunk_v2.api_account_access) a um usuário com Splunk Enterprise permissão de administrador da empresa.

   Para obter mais informações, consulte Configure seu ServiceNow AI Platform instância do Splunk Enterprise Event Ingestion integração.

   Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.
2. Como um usuário com ServiceNow AI Platform função de administrador, instale e configure o. Splunk Enterprise Event Ingestion aplicação do ServiceNow Store.
   a. Baixe e instale o aplicativo em seu ServiceNow AI Platform instância.
   b. Configure a aplicação e conecte-se ao seu Splunk Enterprise console.

   Para obter mais informações, consulte Instale e configure o. ServiceNow aplicação para Splunk Enterprise Event Ingestion integração.
3. **Opcional:** Se você pretende exportar eventos manualmente do seu Splunk Enterprise console para seu ServiceNow AI Platform execute as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. . Splunk Enterprise administrador, instale, configure e habilite o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise do splunkbase em seu Splunk Enterprise console.

b. . Splunk Enterprise se ainda não estiver configurado, salve as pesquisas como alertas em Splunk Enterprise console.

(Optional) Para obter mais informações, consulte Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise integração de ingestão de evento e Salve pesquisas em seu Splunk Enterprise console para Splunk Enterprise Event Ingestion integração.

4. Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** criar e nomear um perfil de evento.

Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do seu Splunk Enterprise console.

- Para um alerta programado, selecione um alerta disponível.
- Para perfil para dados exportados manualmente, crie um novo mapa ou copie um mapa existente.

Para obter mais informações, consulte Crie e nomeie um perfil de evento.

5. Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** valores de função, mapa ingeridos ou dados de anexo que são exportados de Splunk Enterprise. ServiceNow AI Platform incidentes de segurança.

a. Buscar dados de amostra para um alerta programado.

b. Exporte dados de anexo manualmente de Splunk Enterprise para um evento.

c. Edite a configuração de mapeamento padrão.

d. Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de scripts.

Para obter mais informações, consulte Mapeamento de alertas e eventos para Splunk Enterprise Event Ingestion integração e Alertas de mapa para Splunk Enterprise Event Ingestion integração.

6. Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** visualizar os dados de Splunk Enterprise exibido em um ServiceNow AI Platform incidente de segurança.

Corrija erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida.

Para obter mais informações, consulte Visualize o incidente de segurança do Splunk Enterprise Event Ingestion integração.

7. Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** programar recuperação de alerta para um perfil com um alerta programado.

Para obter mais informações, consulte Programar e recuperar alertas para Splunk Enterprise Event Ingestion integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk Enterprise Security integração de ingestão de evento

. Splunk Enterprise Security integração de ingestão de evento notável com Resposta a incidentes de segurança(SIR) permite que os analistas de incidentes de segurança coletem e processem dados de eventos notáveis (conhecidos como notáveis).

Visão geral de Splunk Enterprise Security integração de ingestão de evento

Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados por analistas para identificar e responder a possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser correlacionados a eventos notáveis em Splunk Enterprise Security e, em seguida, ingerido automaticamente com esta integração. Eventos notáveis individuais podem ser encaminhados manualmente sob demanda do Splunk Enterprise Security Console de Revisão de incidentes e interface de emissão de relatórios no Resposta a incidentes de segurança produto do ServiceNow AI Platform para criar incidentes de segurança.

Esta integração fornece a um analista do SOC (Security Operations Center, centro de operações de segurança) visibilidade de eventos notáveis e dados de eventos de contribuição relacionados. Esses dados podem ser integrados ao ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidentes de segurança para investigação e correção adicionais. Os perfis são criados em seu ServiceNow AI Platform instância para lidar com diferentes tipos de eventos notáveis que são criados por meio de pesquisas de correlação em Splunk Enterprise Security. Esses perfis personalizam a diferença Splunk os campos de evento são exibidos em SIR incidentes de segurança.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de eventos notáveis para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware e tentativas de acesso não autorizado.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda do seu Splunk ES Console de revisão de incidentes para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk Valores de campo de evento notáveis para campos de incidente de segurança SIR associados.
- Uma visualização do SIR layout de incidente de segurança com base em exemplos de eventos notáveis para validar detalhes de mapeamento de eventos.
- Ingerir eventos notáveis históricos, bem como eventos notáveis contínuos, novos e atualizados em intervalos configuráveis.
- Filtre eventos notáveis que não atendem aos critérios de geração de incidentes SIR, por exemplo, eventos de baixa prioridade, eventos que ainda não atingiram um status específico e assim por diante.
- Agregue eventos ou alertas aos existentes SIR incidentes de segurança com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualize eventos notáveis com base nas condições de criação e/ou fechamento de incidentes de SIR por meio de uma interface bidirecional para manter Splunk ES atualizações de eventos notáveis em sincronia com ServiceNow Status do incidente SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões da ServiceNow AI Platform compatíveis

O plug-in com.snc.si_dep é necessário para esta integração. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações.

A seguir Operações de segurança as aplicações devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação tranquila:

1. Framework de integração de segurança
2. Security Support Common
3. Resposta a incidentes de segurança

Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

ServiceNow Complementos

. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk ESé necessário somente se você preferir encaminhar eventos manualmente do seu Splunk Enterprise Security Console de Revisão de incidentes em seu ServiceNow AI Platform instância. Isso ServiceNow o complemento está disponível em splunkbase .

Isso ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise a aplicação no splunkbase não é necessária para a ingestão automatizada de alertas que é compatível com a integração.

Versões compatíveis com Splunk

Esta integração foi testada com Splunk Enterprise versão 8.0.1 e com Splunk Enterprise Security aplicação versão 6,2.1.

MID Server

Esta integração requer um MID Server instalado e configurado em seu ServiceNow AI Platform® instância para se conectar ao Splunk serviço quando Splunk o servidor está implantado em sua rede corporativa. Se você estiver usando Splunk Cloud Um MID Server não é necessário. Consulte MID Server Para obter mais informações sobre MID Servers.

Referências

Referência	Identificador do documento	Título do documento
1	Splunk site do produto	Site do produto Splunk Enterprise Security .

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para Splunk Enterprise Security Integração de ingestão de evento notável. Você pode usar esta lista para monitorar seu andamento conforme trabalha nas tarefas da integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais termos usados nesta integração

Esta seção descreve alguns dos principais termos usados nesta integração.

Os termos-chave a seguir são usados durante a instalação e a configuração. Para obter mais informações sobre esses termos, consulte Site de documentação do produto da ServiceNow e o. Site da Splunk e recursos em Recursos do Splunk página.

ServiceNow AI Platform

Uma empresa ServiceNow produto. . ServiceNow AI Platformé a base sobre a qual componentes individuais, como Resposta a incidentes de segurança(SIR IT Service Management (ITSM) e outros produtos são criados.

ServiceNow Splunkbase add

. ServiceNow aplicação que está instalada no seu Splunk Enterprise Security console que oferece suporte à opção de encaminhamento de eventos manual da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Isso ServiceNow O complemento Splunkbase não é necessário para a ingestão automatizada de eventos notáveis fornecida pela integração que extrai eventos do Splunk.

Resposta a incidentes de segurança (SIR)

. ServiceNow AI Platform aplicação que rastreia o andamento de incidentes de segurança desde a descoberta e a análise inicial, até contenção, erradicação e recuperação, e até a revisão e fechamento finais pós-incidente.

Splunk Enterprise Security

Splunk Enterprise Security Ajuda as equipes a obter visibilidade em toda a organização e inteligência de segurança para monitoramento contínuo, resposta a incidentes, operações de SOC e fornecer aos executivos uma janela para o risco comercial. Splunk Enterprise Securityé uma solução de segurança premium que requer uma licença paga. Este serviço está em um host ou em uma oferta de nuvem Splunk que é chamada de Splunkneste guia.

Splunk Enterprise Security evento notável

Quando uma pesquisa de correlação identifica um evento ou um padrão de eventos, ela cria um evento notável. As pesquisas de correlação filtram os dados de segurança e correlacionam entre eventos para identificar um tipo específico de incidente (ou padrão de eventos) e, em seguida, criar eventos notáveis.

Splunk evento

Um ou mais elementos de dados que resultam nos eventos notáveis do Splunk serviço. Do seu ServiceNow AI Platform instância, você pode pesquisar qual Splunk eventos acionados ServiceNow AI Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre o. ServiceNow AI Platform e aplicações externas, fontes de dados e serviços. Normalmente, esta aplicação é necessária para integração com tecnologias no local e, para isso Splunk Enterprise Security Integração de ingestão de evento, o MID Server facilita a comunicação entre o. ServiceNow AI Platform e a instância no local de Splunk Enterprise Security. Um MID Server não será necessário se você estiver integrando seu ServiceNow AI Platform instância com um Splunk Cloud instância.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com SIR produto em seu ServiceNow AI Platform instância.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage com e analisa incidentes de segurança no ServiceNow Resposta a incidentes de segurança produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure seu ServiceNow AI Platform® instância do Splunk Enterprise Security integração

A seção a seguir lista as tarefas de configuração que você deve concluir em ServiceNow AI Platform® instância antes de instalar a aplicação do ServiceNow Store.

Função necessária: sn_si.ingestion_profile_admin.

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração suaves.

1. Verifique se você atribuiu o necessário ServiceNow AI Platform® e. Resposta a incidentes de segurança(SIR) funções.

   As funções a seguir são necessárias para a instalação, a configuração e o uso da integração em seu ServiceNow AI Platform® instância.

   - Um usuário com ServiceNow AI Platform® a função de administrador (admin) instala a aplicação do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin).
   - Se você quiser encaminhar eventos notáveis manualmente de Splunk Enterprise Security para esta integração, um usuário com ServiceNow AI Platform® a função de administrador atribui um usuário com a função (sn_sec_splunkes.api_account_access) no ServiceNow AI Platform®. Esta função permite a um usuário com Splunk Enterprise Security Função de administrador para acessar a API no ServiceNow AI Platform® necessário para o encaminhamento manual de eventos para esta integração.

     A função (sn_sec_splunkes.api_account_access) não será necessária para a integração se você estiver ingerindo eventos notáveis automaticamente do Splunk Enterprise Security em seu ServiceNow AI Platform® instância.

   - Um usuário com **sn_si.ingestion_profile_admin** a função supervisiona as seguintes tarefas no ServiceNow AI Platform®:
     - Cria e edita perfis de evento.
     - Seleciona e mapeia valores de Splunk Enterprise Security. ServiceNow AI Platform® incidentes de segurança.
     - Visualiza os detalhes do incidente de segurança para obter precisão antes de finalizar a configuração.
     - Ingestão de eventos notáveis em andamento.
     - Habilita atualizações de eventos notáveis quando um incidente SIR é criado e encerrado.
     - Atribui a função de analista de incidentes de segurança (sn_si.analyst).
     - Usuários com sn_si.analyst trabalham com incidentes de segurança.

   Para obter mais informações, consulte Gerenciando funções .

2. Atribua o. Splunk função do usuário.

   Atribua uma função de usuário Analista de segurança (ess_analyst) em Splunk ES para executar todas as atividades relacionadas à integração no Splunk servidor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Verifique se você está usando a versão 7.2.6 ou posterior do Splunk API. Versões anteriores não são compatíveis.

   Se você tiver acesso ao Splunk Enterprise Security, você tem acesso à API necessária para esta integração. Não há outra configuração especial necessária para a API.

4. Verifique se você instalou e configurou um MID Server.

   . MID Server em seu ServiceNow AI Platform® a instância é necessária para se conectar ao Splunk se o Splunk o servidor está implantado em sua rede corporativa. Para obter informações, consulte MID Server .

   Se você estiver usando Splunk Enterprise Security Serviço em nuvem, um MID Server não é necessário.

5. Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas.

   . Resposta a incidentes de segurança O plug-in de dependência (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao Resposta a incidentes de segurança produto. Instale e ative este plug-in antes de instalar e ativar o outro Operações de segurança aplicações exigidas pela integração.

   Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila.

   a. Resposta a incidentes de segurança
   b. Framework de integração de segurança
   c. Suporte de segurança comum

   Para obter mais informações sobre como instalar o. Operações de segurança aplicações principais, consulte Obtenha direito para um Operações de segurança produto ou aplicação e. Ativar um ServiceNow Store aplicação.

Você configurou com sucesso seu ServiceNow AI Platform® instância da integração. A próxima etapa é instalar o. Splunk Enterprise Security Aplicação de ingestão de evento notável do ServiceNow Store para a integração. Para obter mais informações, consulte Instalar e configurar Splunk Enterprise Security Integração de ingestão de evento notável.

Se você quiser exportar eventos notáveis manualmente e sob demanda do seu Splunk Enterprise Security console para a integração, consulte Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise Security Integração de ingestão de evento notável para obter mais informações.

Instalar e configurar Splunk Enterprise Security Integração de ingestão de evento notável

Antes de executar a integração no seu ServiceNow AI Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente ao Resposta a incidentes de segurança e. Operações de segurança produtos em seu ServiceNow AI Platform® instância.

Antes de Iniciar
Função necessária: ess_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribua uma função de usuário Analista de segurança (ess_analyst) no Splunk ES para executar todas as atividades relacionadas à integração no servidor Splunk.

Procedimento

1. Se você não instalou o. Splunk Enterprise Security Aplicação de ingestão de evento do ServiceNow Store para obter a integração, consulte Instale um Operações de segurança integração e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize Splunk Bloco Ingestões de evento.
3. Para configurar a aplicação, clique em **Novo** .



4. Como alternativa, se for um **Configurar** é exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestões de evento exibida, preencha os campos.

Campo	Descrição
Nome	Nome do Splunk Enterprise Security console ou Splunk Cloud instância usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `SplunkES2` .
URL base da API Splunk	URL do Splunk Enterprise Security console ou Splunk Cloud instância. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Autenticação básica	O padrão é desabilitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se você estiver usando o Nome de usuário da conta de API e a Senha da API para configuração, habilite a caixa de seleção.
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário da API no Splunk Enterprise Security console.
Senha da API	Senha que você criou para sua conta de usuário de API no Splunk Enterprise Security console.
Baseado em token (disponível a partir da versão 12,0.0)	Token que você criou para sua conta de usuário de API no console do Splunk Enterprise Security.
Token	Token que você criou para sua conta de usuário de API no Splunk Console do Enterprise Security.
Implantação no Local	O padrão é desabilitado. Se você estiver usando uma versão baseada no local de Splunk Enterprise Security verifique se esta caixa de seleção está marcada.
MID Server	Opção para escolher um MID Server específico para configurar em seu ambiente, que será usado por esta integração para extrair eventos notáveis ServiceNow. Você pode selecionar um MID Server específico na lista ou selecionar **Qualquer** Para habilitar uma seleção automática de um MID Server válido na lista para esta integração. **Nota:** ◦ O MID Server selecionado durante este tempo de configuração se aplica a toda esta integração. ◦ Somente MID Servers ativos e validados são exibidos nesta lista. Por padrão, o valor é definido como **Qualquer** . Por exemplo, há três MID Servers A, B e C. Se você selecionar **Qualquer** Um desses MID Servers é selecionado automaticamente e se aplica a toda esta integração. Se você selecionar um MID Server específico, digamos C, o MID Server C selecionado se aplicará a toda esta integração. Se você quiser mudar o MID Server, será necessário reconfigurá-lo no bloco Configuração da aplicação.

A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão no local de Splunk Enterprise Security Com um MID Server.

Tradução automática

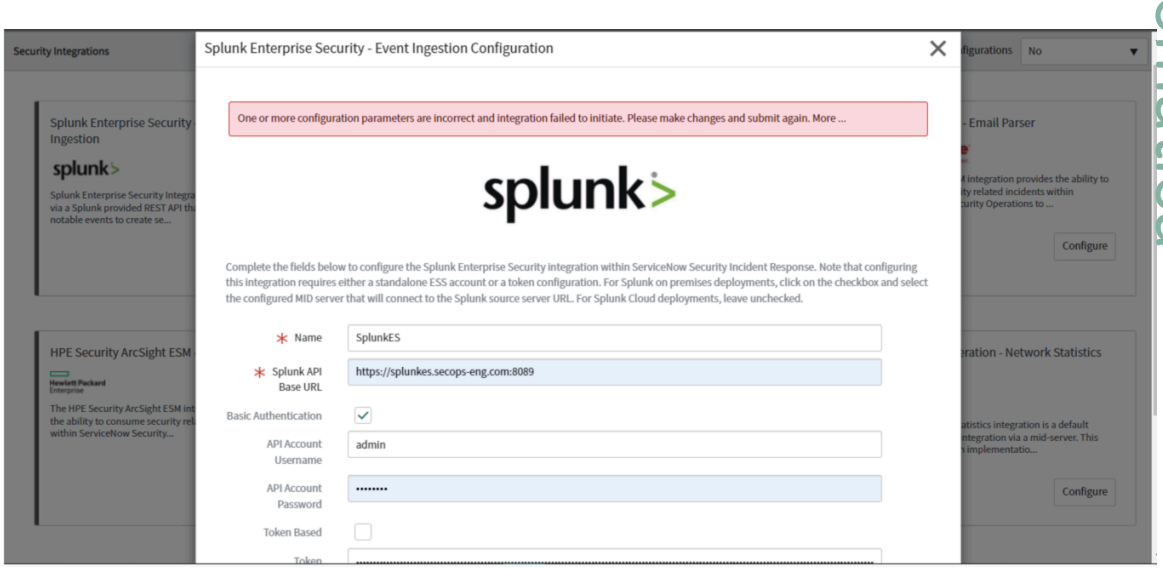
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada um Splunk Enterprise Security tipo de evento notável que você ingere do seu Splunk Enterprise Security o console de revisão de incidentes requer um perfil de evento exclusivo em seu ServiceNow AI Platform® instância. No entanto, a origem que você configura no formulário Configuração de ingestões de evento pode ser reutilizada para vários ServiceNow AI Platform® perfis, desde que cada perfil ingere tipos de evento notáveis exclusivos.

6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, **Atualização** e. **Excluir** os botões são exibidos conforme mostrado na figura a seguir.

Nota: Os usuários precisam usar autenticação básica ou autenticação baseada em token. Habilitar ambos resultará no seguinte erro.



Nota: Se os usuários preferirem atualizar os blocos de configuração existentes para baseados em token, eles precisarão habilitar a ativação desta configuração para atualizar o existente Splunk configurações de origem para configuração de suporte à autenticação baseada em token em Splunk Módulo Configurações empresariais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada evento é validado e enviado com sucesso Splunk A configuração do servidor é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, selecione **Sim** .

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Configurar Splunk Configurações do Enterprise Security

Use Splunk Configurações do Enterprise Security (ES) para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Navegar até **Tudo** > **Integração com Splunk ES** > **Configurações do Splunk ES**.
2. No formulário, preencha os campos.

Configurações do Splunk ES

Campo	Descrição
Impor um limite no número de eventos notáveis que podem ser agregados a um único incidente.	Opção para impor um limite no número de eventos notáveis que você deseja agregar a um único incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por padrão, o valor é definido como 100.
Impor um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas.	Opção para impor um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. Por padrão, o valor é definido como 1000.
Impor um limite no número de valores a serem analisados em cada campo recebido Splunk.	Opção para impor um limite no número de valores que você deseja analisar para cada campo recebido Splunk. Por padrão, o valor é definido como 1000.
Número de regras de correlação das quais extrair Splunk.	Opção para definir o número de regras de correlação das quais recuperar Splunk. Por padrão, o valor é definido como 500.
O parâmetro Tempo de vida útil para Splunk trabalho de pesquisa em segundos.	Opção para definir o parâmetro Tempo de vida útil para Splunk pesquise na forma de segundos. Por padrão, o valor é definido como 600.
Número de tipos notáveis para lote em uma pesquisa.	Opção para definir o número total de tipos notáveis que você deseja em lote em uma única pesquisa. Por padrão, o valor é definido como 20.
Número de dias para reter o. Splunk pesquisar metadados do trabalho em ServiceNow	Opção para definir o número de dias em que você deseja reter os metadados do trabalho de pesquisa do Splunk ServiceNow. Por padrão, o valor é definido como 30.
O caractere delimitador para dividir os valores em mapeamentos de campo.	Opção para definir o caractere delimitador para dividir os valores em mapeamentos de campo. Por padrão, o valor é definido como (,).
Número de minutos de sobreposição a serem adicionados ao buscar os eventos de Splunk(Para superar o atraso de indexação do Splunk)	Opção para definir o número de minutos de sobreposição a serem adicionados ao recuperar os eventos de Splunk para superar o atraso de indexação de Splunk. Por padrão, o valor é definido como 30.
Extrair eventos notáveis atualizados	Opção para recuperar eventos notáveis atualizados. Por padrão, o valor é definido como Não
Ative esta configuração para atualizar o existente Splunk configurações de origem para suporte à autenticação baseada em token. Você deve atualizar a configuração de integração com os detalhes do token depois que essa configuração for habilitada.	Opção para atualizar o existente Splunk configuração de origem para suporte à autenticação baseada em token de uma versão existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Depois que você fizer upgrade para a nova versão, o campo de token ficará indisponível. Você deve habilitar esta configuração para obter a autenticação baseada em token, após a qual você deve atualizar a configuração de integração com detalhes do token. Por padrão, o valor é definido como Não
Habilite a caixa de seleção para extrair notables encerrados durante a ingestão.	Opção para extrair os eventos encerrados para a ServiceNow Splunk Instância ES. Se desmarcado, somente os eventos ativos serão extraídos para a instância. Por padrão, o valor é definido como Não

3. Clique em **Salvar**.

Erros de autenticação

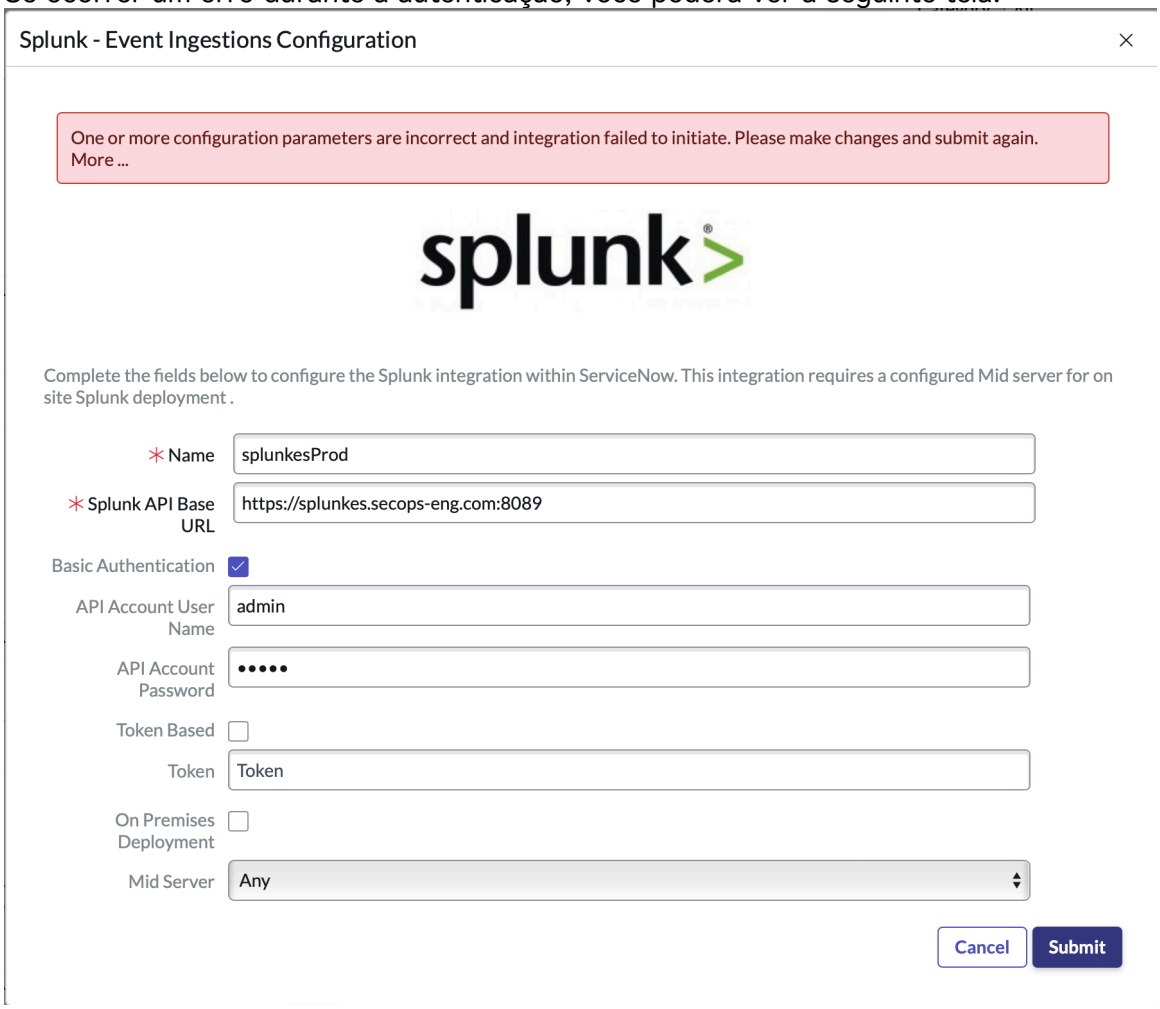
Esta seção descreve alguns erros de autenticação comuns e como eles podem ser resolvidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema de validação de certificado

Se ocorrer um erro durante a autenticação, você poderá ver a seguinte tela:



Se você verificou que as credenciais da conta da API e as informações da URL da base do Splunk estão corretas, esse erro pode ser devido a um problema com o certificado do Splunk para a comunicação da porta 8089. ServiceNow® a instância requer um certificado válido com um nome comum que corresponda ao nome do host do servidor para estabelecer conexões seguras. Para obter mais informações, consulte Certificados . Se você vir esse erro, poderá verificar se o problema se deve a um problema de certificado exibindo os logs do sistema.

Uma condição de erro semelhante à seguinte provavelmente aparecerá:



Created	Level	Message	Source
08-24 02:08 3m ago	Error	Splunk ES REST API error [1].org.apache.commons.httpclient.HttpException: javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated	sn_sec_splunkes

Para prosseguir com a autenticação, você deve substituir o certificado padrão do Splunk que é fornecido para acesso à API na porta 8089. Para obter instruções detalhadas sobre como substituir o certificado SSL, consulte KB0778285 .

Crie e nomeie um perfil de evento para Splunk Enterprise Security integração de ingestão de evento

Você cria um perfil de evento em seu ServiceNow AI Platform e determine qual Splunk eventos notáveis criam incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Antes ServiceNow AI Platform Resposta a incidentes de segurança(SIR os incidentes de segurança são criados a partir de eventos notáveis ingeridos, os valores de campo dos alertas são exibidos em um layout de um ServiceNow AI Platform incidente de segurança para que você possa visualizar como o incidente de segurança real será criado.

De uma perspectiva de integração usando as APIs disponíveis, Splunk ES eventos notáveis são encaminhados individualmente e manualmente como eventos notáveis discretos ou são automaticamente ingeridos em Operações de segurança do seu ServiceNow AI Platform instância dependendo do tipo de perfil definido.

Os fluxos de trabalho de integração ingerem diferentes tipos de eventos notáveis, como tentativas de acesso não autorizado e malware, por exemplo. Esses eventos notáveis são ingeridos com base nos perfis que você configura no Operações de segurança ambiente da sua instância.

Inicialmente, todos os notables são ingeridos para um tipo de pesquisa de correlação configurado em um perfil. Os notables ingeridos podem ser filtrados ainda mais para especificar quais notables criam incidentes de segurança. Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para eventos notáveis identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de eventos notáveis ingeridos, os valores de campos individuais nos eventos notáveis são mapeados para os campos correspondentes em um layout do incidente de segurança para uma visualização.

Procedimento

1. Nomes dos perfis de evento em seu ServiceNow AI Platform a instância deve ser exclusiva e só pode ser mapeada para um perfil de evento ativo a qualquer momento.
2. . ServiceNow AI Platform ingere notables específicos usando os fluxos de trabalho da integração.
   Todos os eventos notáveis que atendem aos critérios de seleção em seu Splunk ES inicialmente, o console é ingerido em seu ServiceNow AI Platform instância.
3. Um perfil em seu ServiceNow AI Platformé um encapsulamento de um evento notável em seu Splunk ES console.
   Há um relacionamento um para um entre eventos notáveis que são ingeridos com um perfil e conexões com seu Splunk ES console: um tipo de evento notável para uma conexão.
4. Para criar perfis para eventos notáveis agendados, consulte Configure um perfil para ingestão de eventos notáveis programados.
5. Para criar perfis para encaminhamento manual de eventos, consulte Configure um perfil para encaminhamento manual de eventos.

Configure um perfil para ingestão de eventos notáveis programados

Dependendo do perfil definido, Splunk ES eventos notáveis são ingeridos automaticamente em Operações de segurança do seu ServiceNow AI Platform instância.

A tabela a seguir mostra a lista de tarefas que você precisa seguir para configurar um perfil para ingestão programada de eventos notáveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Etapas para configurar um perfil para ingestão de eventos notáveis programados

Tarefa	Seção
Crie um perfil de evento	Veja Crie perfis para ingestão de eventos notáveis programados
Selecione eventos notáveis com base no nome da pesquisa de correlação	Veja Selecione eventos notáveis com base no nome da regra de correlação para o perfil para Splunk ES Integração de ingestão de evento
Mapear campos de evento notável	Veja Mapeamento de campos de evento notável para Splunk Enterprise Security integração
Crie mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada)
Visualize o incidente de segurança	Veja Visualize o incidente de segurança do Splunk Enterprise Security Integração de ingestão de evento
Programar e recuperar eventos notáveis novos e atualizados	Veja Programar e recuperar eventos notáveis novos e atualizados para Splunk Enterprise Security Integração de ingestão de evento
Automatize atualizações e fechamento de eventos notáveis com base no status do incidente SIR	Veja Automatize atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Crie perfis para ingestão de eventos notáveis programados

Você pode configurar um perfil para que eventos notáveis sejam ingeridos automaticamente.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Para criar um perfil de evento para um evento notável ou tipo de regra de correlação em seu ServiceNow AI Platform instância, navegue até **Splunk Integration** > **Perfil de evento do Splunk**.
2. . Splunk O formulário Perfil de evento não for exibido, clique em **Nome** Na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

Um exemplo de um formulário preenchido segue a tabela.

Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e os nomes de perfil duplicados não serão salvos. Nomes de perfil em seu ServiceNow AI Platform a instância deve ser exclusiva.

Tradução automática

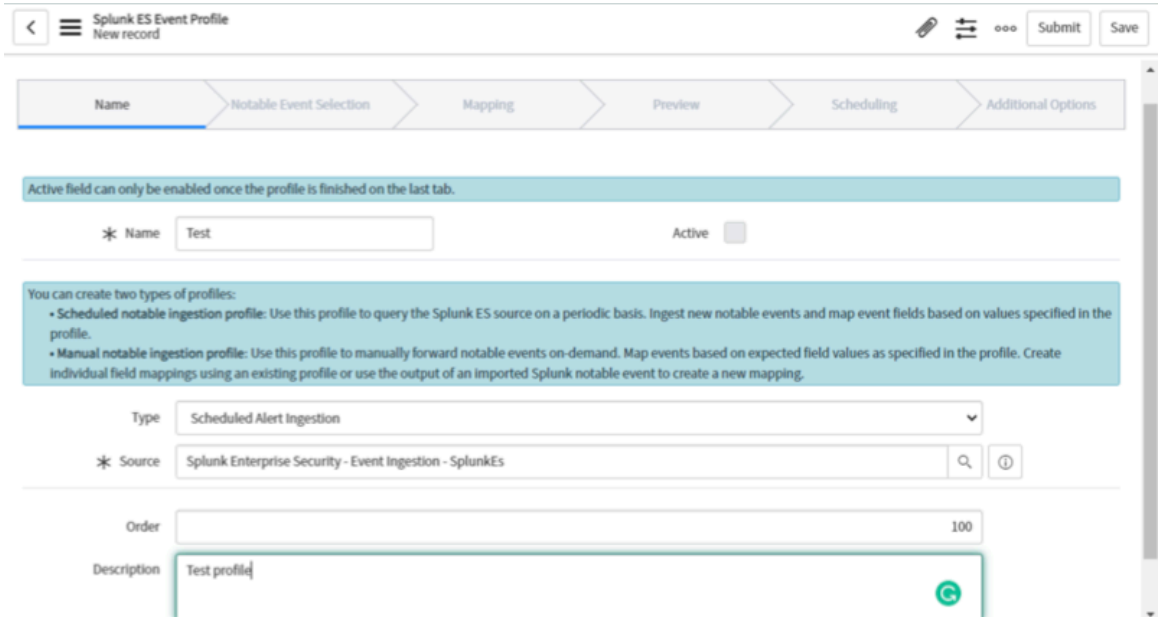
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	A caixa de seleção está desmarcada e desabilitada por padrão. Você deve concluir todas as seções no perfil antes de ativá-lo.
Tipo	Selecione o tipo de perfil na lista de seleção. ○ Ingestão de evento programado: Este tipo de perfil oferece suporte a eventos notáveis que são ingeridos em uma programação configurada. Preencha os campos. ○ Encaminhamento manual de eventos: Este tipo de perfil oferece suporte a eventos notáveis que são encaminhados manualmente do seu Splunk Enterprise Security Console de Revisão de incidentes sob demanda. Consulte as etapas a seguir para preencher o formulário para esses tipos de perfis.
Origem	Splunk fim do servidor ou da pesquisa que você configurou para ingerir eventos notáveis. Se você tiver vários Splunk servidores configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão ingeridos para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham as mesmas condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido para um tipo de evento notável programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para um perfil com um evento notável programado, escolha uma opção para continuar com a configuração do perfil.

Opção	Descrição
Continuar	Salve o perfil e o andamento na etapa Seleção de evento.
Atualizar	Salve as atualizações neste perfil e retorne ao Splunk Lista de perfis de evento.
Salvar	Salve este perfil e permaneça na página.
Excluir	Exclua este registro de perfil e retorne ao Splunk Lista de perfis de evento.

O que Fazer Depois

A próxima etapa é selecionar eventos notáveis para ingestão automática.

Selecione eventos notáveis com base no nome da regra de correlação para o perfil para Splunk ES Integração de ingestão de evento

Depois de criar um perfil para uma ingestão de tipo de evento notável programada, selecione um Splunk Enterprise Security nome da regra de correlação para este perfil para o qual você deseja mapear eventos notáveis correspondentes a um ServiceNow AI Platform Resposta a incidentes de segurança incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Exiba as regras de correlação disponíveis no seu ServiceNow AI Platform para que você conheça os tipos de evento notáveis para os quais deseja ingerir e criar incidentes de segurança. Selecione uma regra de correlação. Você pode selecionar um ou mais eventos notáveis na lista neste formulário.

Tradução automática

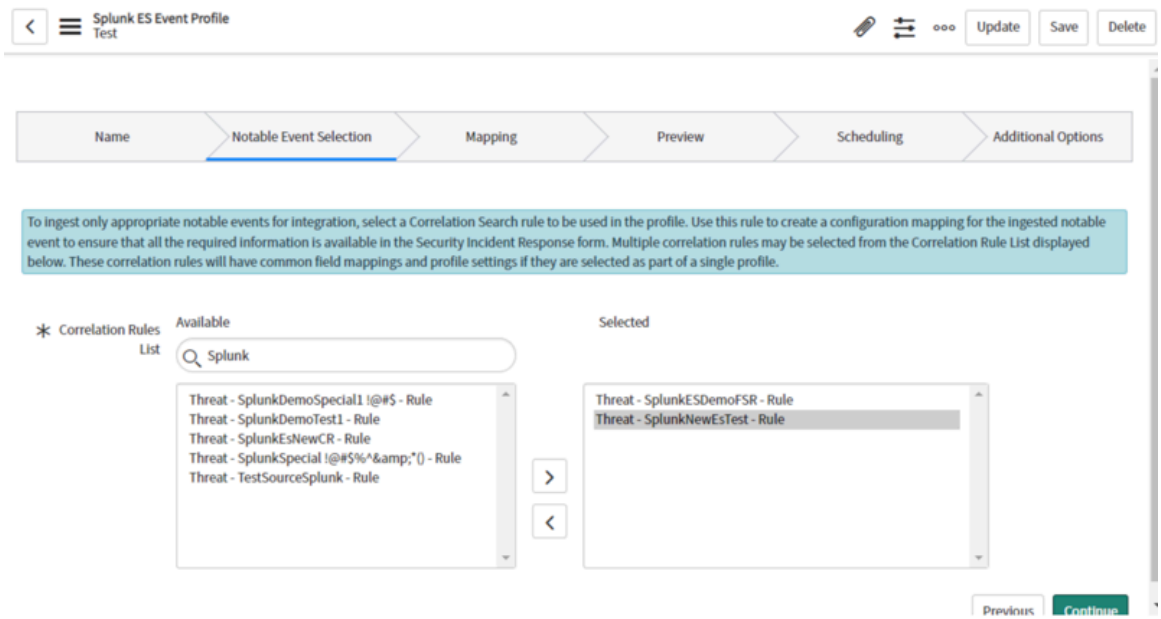
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a página Seleção de evento notável não for exibida, selecione-a na barra de andamento para exibi-la.
2. Na Lista de regras de correlação, escolha uma das seguintes opções para selecionar uma única regra de correlação ou várias regras de correlação e mova-as e mova-as para da coluna Disponível para a coluna Selecionado.

   A lista de regras de correlação neste formulário corresponde à lista de regras de correlação em seu Splunk ES Console de Revisão de incidentes. Até 500 regras de correlação são exibidas neste formulário. Se houver mais de 500 regras de correlação listadas em seu Splunk ES, somente os primeiros 500 eventos notáveis são exibidos neste formulário em seu ServiceNow AI Platform instância.

Opção	Descrição
No campo de pesquisa Lista de regras de correlação, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione uma regra de correlação e, com as teclas de seta, mova o alarme selecionado de **Disponível** . **Selecionado** .
Na Lista de regras de correlação, clique duas vezes em uma regra de correlação.	. **Selecionado** a coluna é preenchida com sua seleção.
Na Lista de regras de correlação, clique uma vez em uma regra de correlação.	A regra de correlação é selecionada. Com as teclas de seta, mova a regra de correlação selecionada de **Disponível** . **Selecionado** .



3. Escolha uma opção para continuar.

Opção	Descrição
Ou, como alternativa, clique em Mapeamento na barra de andamento	O formulário Mapeamento é exibido. **Mapeamento** está selecionado na barra de andamento. A próxima etapa é mapear

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	campos de evento notáveis para um SIR in–cidente de segurança.
Atualizar	Seus dados são salvos e a lista Perfis de eventos no-táveis do Splunk é exibida.
Anterior	. **Nome** a etapa é exibida.
Excluir	Exclua este perfil de evento e a lista Perfis de evento notáveis do Splunk será exibida.

O que Fazer Depois

Você selecionou com sucesso uma regra de correlação para um programado Splunk Enterprise Security perfil. A próxima etapa é mapear valores de evento notáveis para campos em um incidente de segurança.

Mapeamento de campos de evento notável para Splunk Enterprise Security integração

Depois de identificar a regra de correlação específica e o tipo de evento notável para o perfil, a próxima etapa é mapear campos de evento notável individuais para os campos em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Visão geral do mapeamento

Para a etapa de mapeamento, você pode ingerir eventos notáveis de amostra para a regra de correlação selecionada ou exportar dados de eventos notáveis para eventos notáveis encaminhados manualmente. O processo de mapeamento de eventos é idêntico, independentemente do tipo de perfil que você está criando.

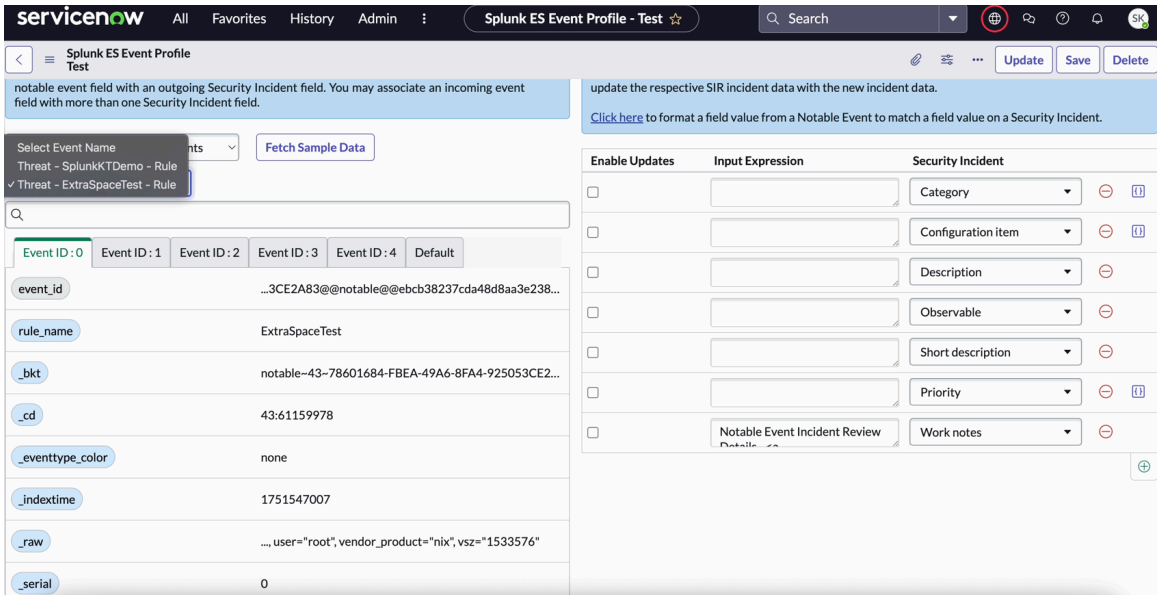
As figuras a seguir são exemplos das configurações de mapeamento padrão fornecidas para cada tipo de perfil de evento. Você pode personalizar os campos que preenchem o incidente de segurança. Durante esta fase de mapeamento, você pode garantir que todos os dados de campo de evento notável relevantes sejam mapeados para o local apropriado no formulário de incidente de SIR e, em seguida, visualizar o incidente de SIR na seção de visualização.

Se várias correlações forem usadas, eventos notáveis poderão ser obtidos selecionando Evento necessário. Usar **Nome do alerta** para escolher seu alerta se você tiver configurado vários alertas para ingestão.

Depois de clicar para buscar dados, o Splunk nomes de campos de evento notáveis e valores correspondentes são preenchidos no lado esquerdo do formulário. . Splunk campos de evento notáveis que estão disponíveis para mapear para SIR campos de incidente de segurança. Alguns campos podem ser mapeados várias vezes para os campos de incidente de segurança SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode preferir revisar alguns exemplos de eventos notáveis em seu Splunk console para ingerir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos notáveis de amostra de Splunk Enterprise Security para ajudar no processo de mapeamento de campo de evento notável. Há opções para ingerir os cinco eventos notáveis mais recentes para a regra de correlação selecionada ou ingerir até cinco eventos notáveis específicos com base nos IDs de evento notáveis.

Abaixo está um resumo das etapas necessárias para mapear eventos notáveis:

- Ingestão de dados de amostra de evento notável programado: Para dados de amostra que são usados para perfis de evento notável ingeridos automaticamente, os campos de evento notável disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento depois que os dados de amostra são recuperados. As guias são exibidas para que você exiba os valores de um ID de evento notável específico que você extraiu. Verifique se todos os campos críticos da seção Ingestão de amostra de evento notável à esquerda do formulário estão mapeados para ServiceNow campos de incidente de segurança à direita do formulário.
- Mapeamento de campo: Edite a configuração de mapeamento arrastando campos de evento notáveis do lado esquerdo e soltando-os no ServiceNow Seção de mapeamento de incidentes SIR à direita. O mapeamento à direita associa o campo Evento notável de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: Personalize a grade de mapeamento adicionando ou removendo campos usando o ícone de adição na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida (os campos mapeados ficam esmaecidos, os campos azuis não estão mapeados).
- Condições de geração de incidente: Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais eventos notáveis devem criar incidentes de segurança versus quais eventos notáveis devem ser filtrados, por exemplo, eventos notáveis de baixa prioridade. Isso é feito na seção Condições de geração de incidentes, localizada abaixo da seção Mapeamento de eventos notáveis.
- Critérios de agregação de evento: Defina critérios de agregação de evento adicionais que agreguem um evento notável de entrada a um existente SIR incidente de segurança em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

valor de correspondência de campo para cada perfil, esse recurso de agregação adicional pode reduzir o número de incidentes de segurança ativos sobrepostos, colocando todos os dados de eventos notáveis de segurança relacionados em um único incidente de segurança.

- Tradução de campo de formato: Em determinados casos, valores de campo de evento no Splunk Eventos notáveis da empresa podem não ser traduzidos diretamente para os campos no SIR incidente de segurança. Para esses valores, você pode usar um editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de scripts se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria Alerta de malware e infecção por vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser traduzidos em uma Atividade de código mal-intencionado comum no campo Categoria no SIR Incidente de segurança usando a funcionalidade Formatar tradução de campo.

A próxima etapa é ingerir eventos notáveis e mapear valores para SIR campos de incidente de segurança.

Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada)

Durante a etapa de mapeamento de campo de evento notável, você mapeia campos de evento individuais de eventos notáveis para campos em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa
A grade de mapeamento pode ser personalizada para o tipo de evento notável selecionado na seleção de regra de correlação. A codificação por cores dos campos de evento ajuda a acompanhar os valores de evento que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de evento importante restante permanece não mapeada.

Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de evento notável à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Campos padrão que normalmente são importantes para preencher no formulário de resposta a incidentes de segurança são exibidos. Esses campos podem ser removidos e todos os campos adicionais podem ser exibidos usando os botões mais e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no SIR incidente de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

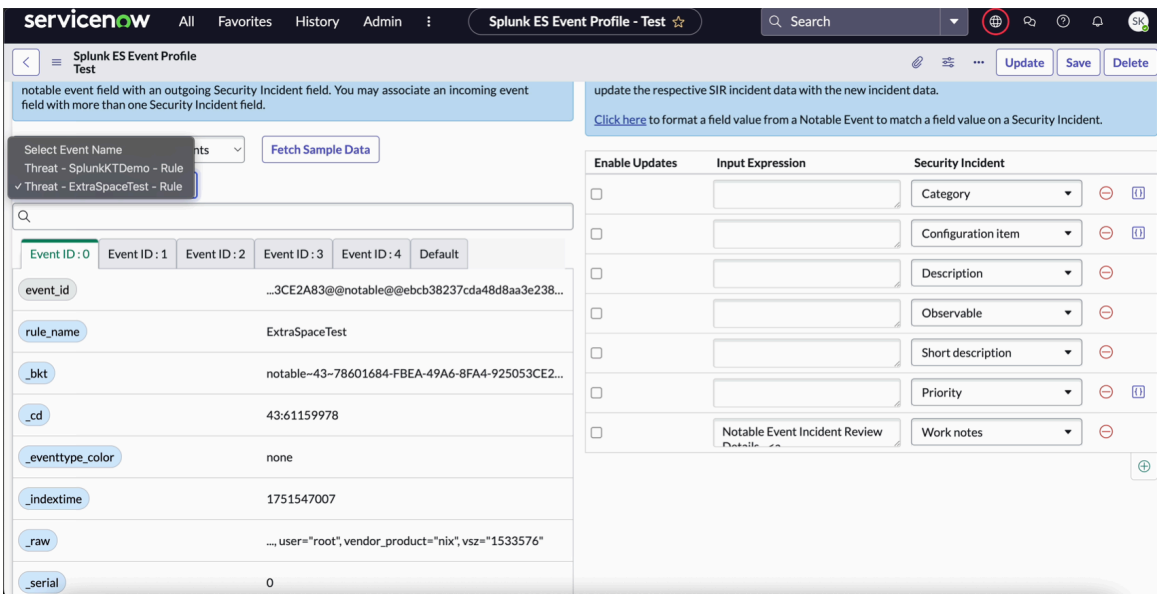
1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para obter um perfil com uma ingestão programada, abaixo de Ingestão de amostra de evento notável, clique em **Buscar dados de amostra** para extrair os eventos notáveis de amostra mais recentes do Splunk Enterprise console para a regra de correlação selecionada.

   Nota: Você pode extrair os eventos notáveis de amostra mais recentes ou fornecer os IDs de eventos notáveis exclusivos para os eventos notáveis específicos que você deseja usar para sua experiência de mapeamento de eventos notáveis.

   Os campos de evento notáveis e resultados de valores são exibidos como guias individuais. Você pode ingerir até cinco eventos notáveis.

   A extração de eventos notáveis de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

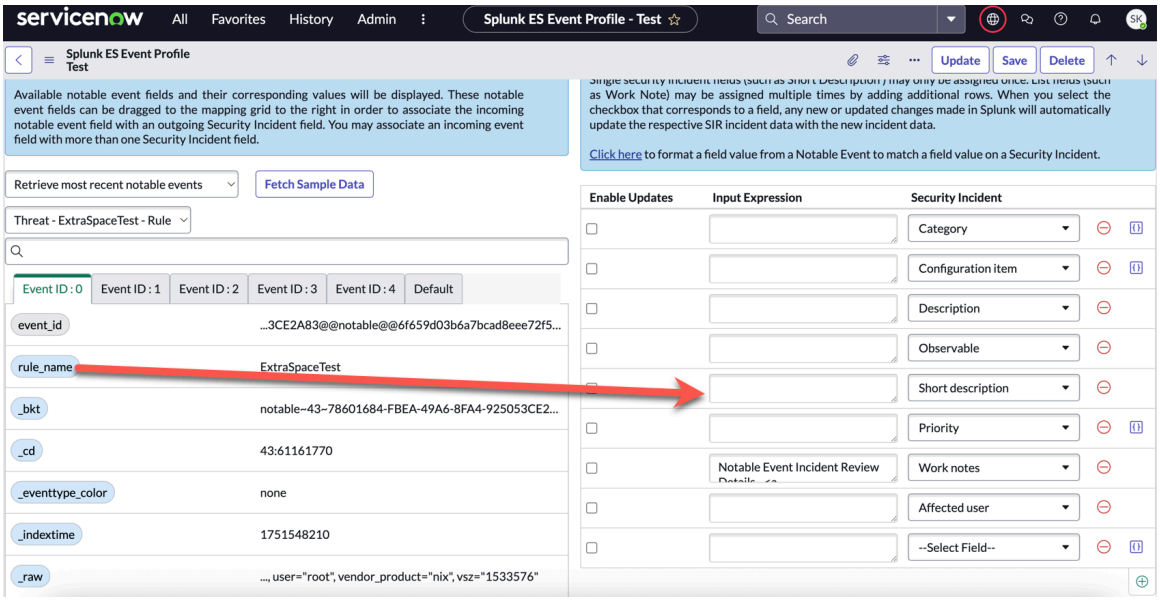
   Na figura a seguir, os pares de valor de nome de campo para o evento notável ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário depois que a extração de ingestão é concluída. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



3. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e segure um nome de campo azul no lado esquerdo do formulário.
4. Arraste o nome do campo, por exemplo, rule_name E solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

Tradução automática

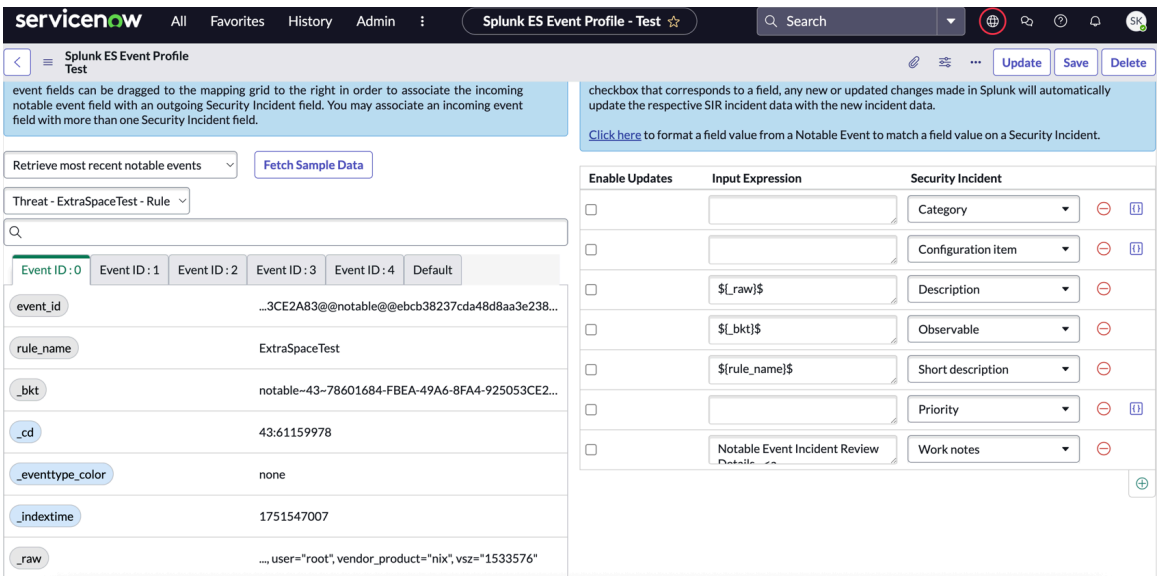
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, rule_name está mapeado para Descrição resumida campo no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar você a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Campos azuis claros à esquerda indicam que um campo de evento notável ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo notável de entrada a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Esta codificação por cores ajuda você a rastrear o mapeamento.



5. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

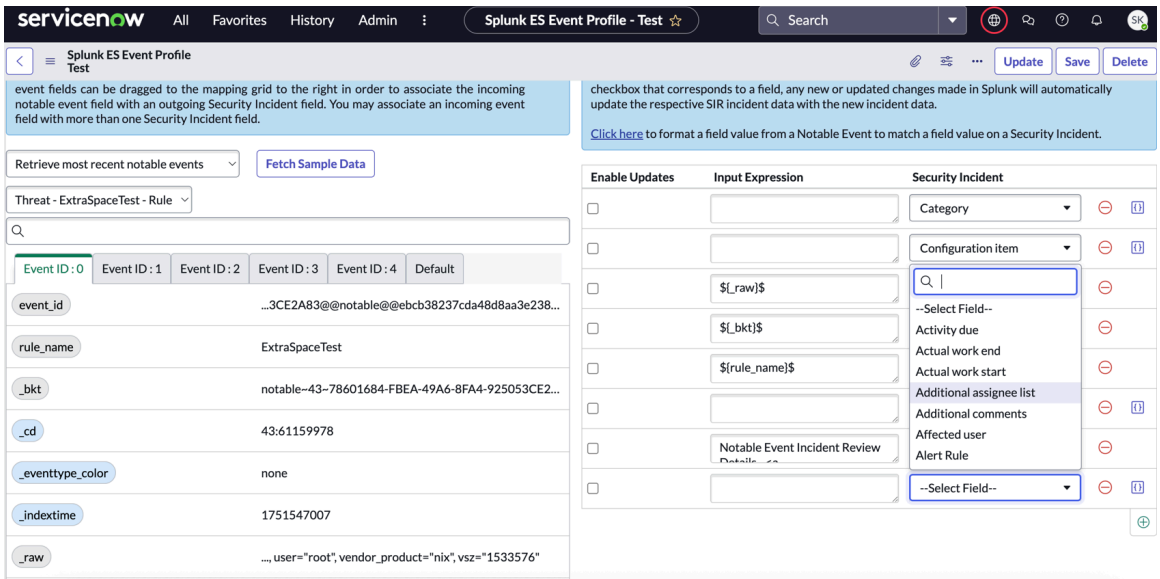
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Na lista expandida do novo campo, alguns campos são sombreados. Na figura a seguir, rule_name tem um fundo cinza, porque foi mapeado no incidente de segurança. Semelhante à codificação por cores dos campos de eventos notáveis no lado esquerdo do formulário, essa codificação por cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente DE SIR já mapeados.



Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho são compatíveis com vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, uma mensagem de erro será exibida informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista da qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não seja exibida na lista, o campo não será preenchido no incidente de segurança.

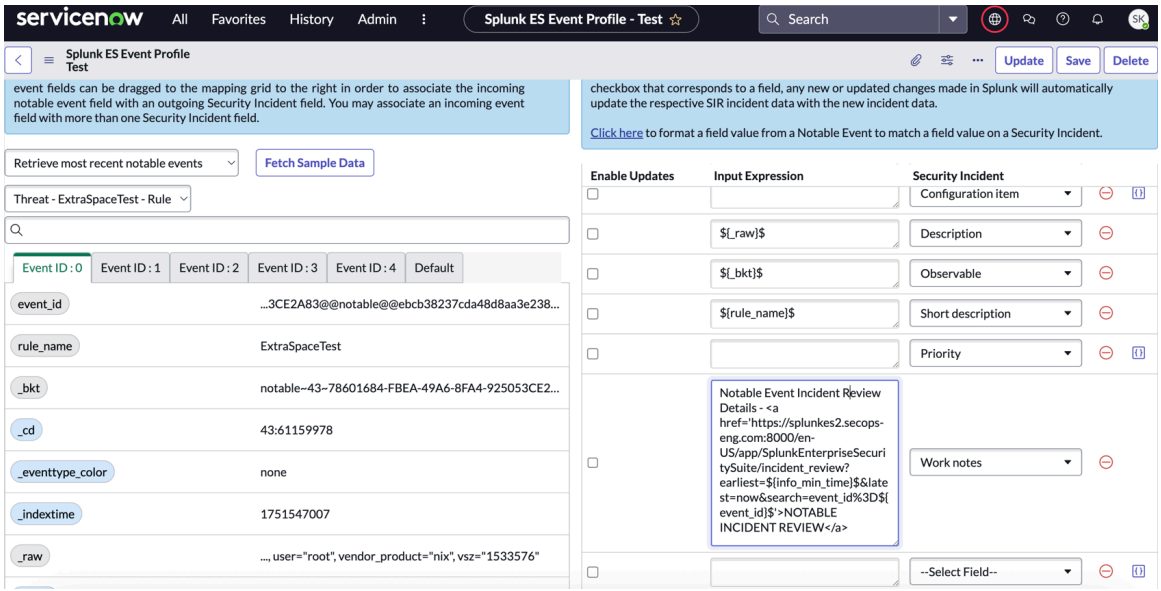
c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar **ID do evento** Que você deseja no campo Expressão de entrada.

6. Continue o mapeamento adicionando ou removendo valores de campo ao mapeamento.
A figura a seguir é um exemplo de um mapeamento editado. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Para o campo de cadeia de caracteres de texto longa, você pode expandir o campo de mapeamento para ver a cadeia de caracteres completa e redimensioná-la conforme necessário, puxando o canto inferior direito do campo, conforme indicado na captura de tela abaixo com o campo Anotações de trabalho adicionado:

Tradução automática

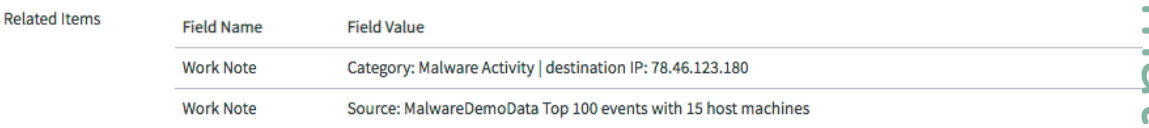
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Aviso: Observe que em **Mapeamento de campo de incidente DO SIR** A URL e o número da porta mencionados em **Expressão de entrada** O campo é apenas um exemplo e não o URL ou o número da porta fornecidos prontos para uso.

Na visualização, esses valores são exibidos nas anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à seção de mapeamento e há vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e os sinais de pontuação inseridos no campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

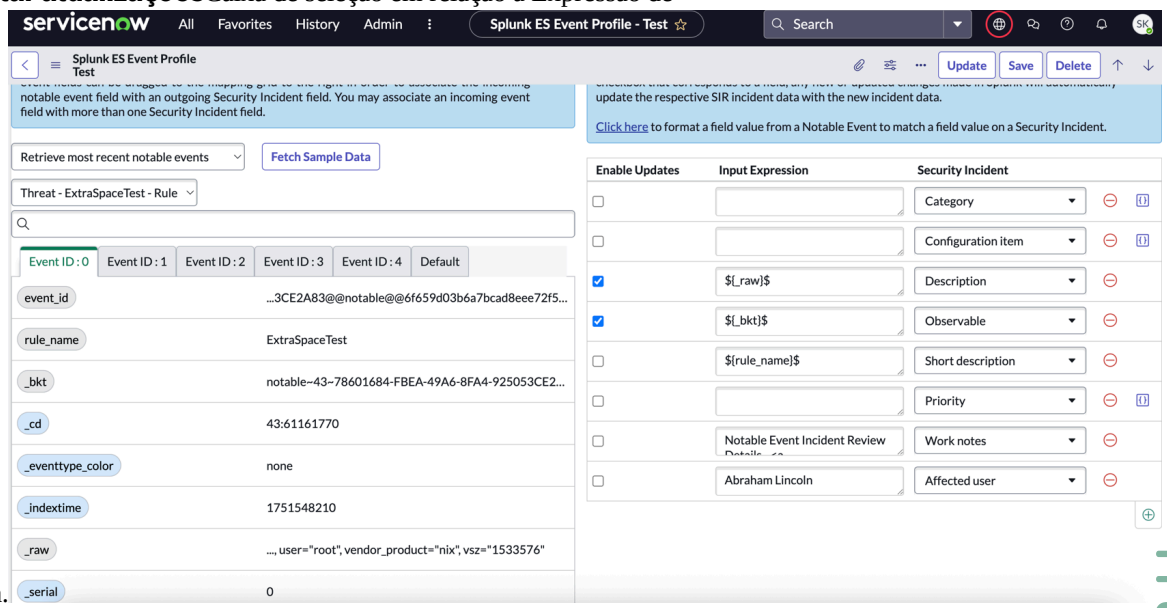
A imagem a seguir é um exemplo de como os valores na imagem anterior são exibidos no incidente de segurança.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Para receber atualizações para os campos mapeados no SIR, selecione **Habilitar atualizações**Caixa de seleção em relação à Expressão de entrada.



8. **Opcional:** Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um evento notável de entrada deve satisfazer para criar um SIR incidente de segurança.
Para definir condições de geração de incidentes, siga estas etapas.

   a. Role até a seção Condições de geração de incidentes no formulário e selecione **Filtro com base em condições** marque a caixa para habilitar a opção.

   (Optional) O construtor Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas do primeiro campo no construtor Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de evento notável para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo de Splunk eventos notáveis que você ingerir ou o evento selecionado para as amostras de evento notável encaminhadas manualmente. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores de Splunk Enterprise Security evento notável. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao Splunk Enterprise Security console e revise seus eventos notáveis para as palavras-chave.



   b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Para adicionar mais condições, à direita dos campos, clique em **E.** ou **OU** .
Se **E.** selecionado, todas as condições devem ser correspondidas. Se **OU** está selecionado, qualquer condição pode ser correspondida.

d. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando as duas condições de filtragem inseridas forem correspondidas.

Este tipo de filtragem de condição de geração de incidentes ajuda a restringir os eventos de segurança e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou os filtros em Splunk. Se critérios de filtragem adicionais forem definidos, somente eventos notáveis que correspondem a todos os critérios serão mapeados para incidentes.

Nota: Se qualquer um dos nomes de campo de evento tiver caracteres especiais, como aspas ("), hifens ("), sublinhados (-), em (") ou ampersands (&), esses caracteres podem ser substituídos para fins de tradução de mapeamento e possivelmente criar um nome de evento duplicado. O mapeamento pode ser feito corretamente, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `alerts.alert` e o segundo campo de evento é `alertas em alertas` esses campos não podem ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `alertas em alerta (1)` .

(Optional) Critérios de agregação de eventos para lidar com notables semelhantes e evitar incidentes duplicados

9. Opcional: Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos notáveis de entrada sejam agregados a um incidente de segurança em aberto.
Para definir os critérios, siga estas etapas abaixo.

a. Role até a seção Critérios de agregação de eventos no formulário e selecione **Condições agregadas** marque a caixa para habilitar esta opção.

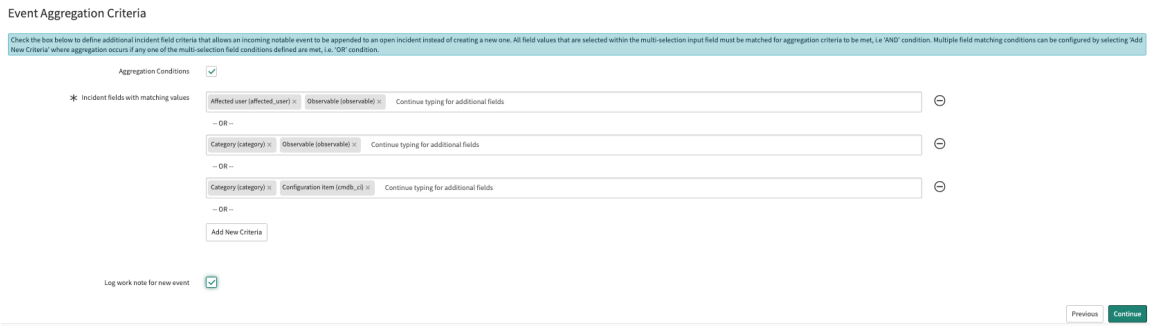
(Optional) Os campos Incidente com valores correspondentes são exibidos. Esses nomes de campos são os campos no incidente de segurança que incluem todos os campos personalizados configurados no SIR incidente de segurança.

Tradução automática

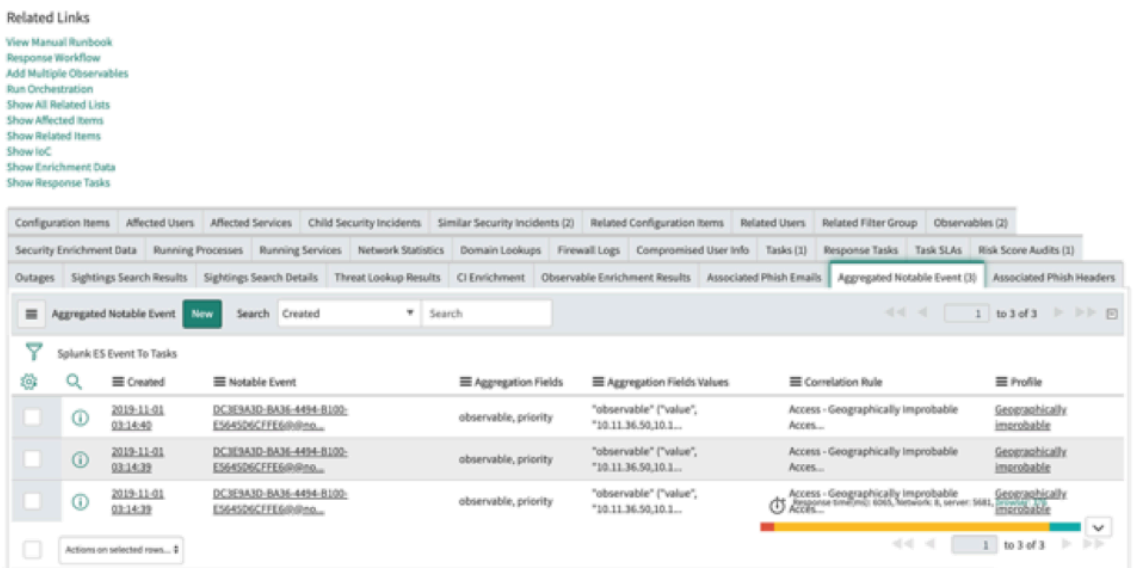
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. No campo de entrada de seleção múltipla, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes em seu ServiceNow AI Platform.

c. Use **Adicionar novos critérios** para selecionar várias condições de correspondência de campo. Todos os valores de campo selecionados no campo de entrada de seleção múltipla correspondem aos critérios de agregação usando a condição E. Clique em **Adicionar novos critérios** Para selecionar várias condições de correspondência de campo em que ocorre agregação se qualquer uma das condições de campo de várias seleções definidas for atendida usando a condição OU .



Se um novo evento notável corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo evento notável será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os eventos notáveis agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os eventos notáveis agregados em um incidente de segurança são exibidos no Splunk Evento para lista relacionada de tarefas. Esta lista detalha carimbos de data/hora associados e valores de campo agregados. Essas informações ajudam você a entender por que esses eventos notáveis estão sendo agregados aos incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique em **Mostrar todas as listas relacionadas** link.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Opcional: Para registrar em log uma anotação de trabalho para um novo evento notável que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra em log que um novo notável foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

Valores mapeados com sucesso de um Splunk evento notável para campos em um SIR incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexou eventos notáveis a existentes SIR incidentes de segurança quando os valores do campo de evento correspondem aos critérios de agregação configurados.

10. Escolha um para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido. **Visualização** está selecionado na barra de andamento. A próxima etapa é visualizar os campos mapeados em um SIR incidente de segurança.
Atualizar	Seus dados são salvos e a lista Perfis de evento do Splunk é exibida.
Anterior	O formulário Seleção de evento notável é exibido.
Excluir	Exclua este perfil de evento e a lista Perfis de evento do Splunk será exibida.

O que Fazer Depois

A próxima etapa é visualizar os valores mapeados no incidente de segurança.

Visualize o incidente de segurança do Splunk Enterprise Security Integração de ingestão de evento

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um ServiceNow AI Platform® Resposta a incidentes de segurança(SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos notáveis que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

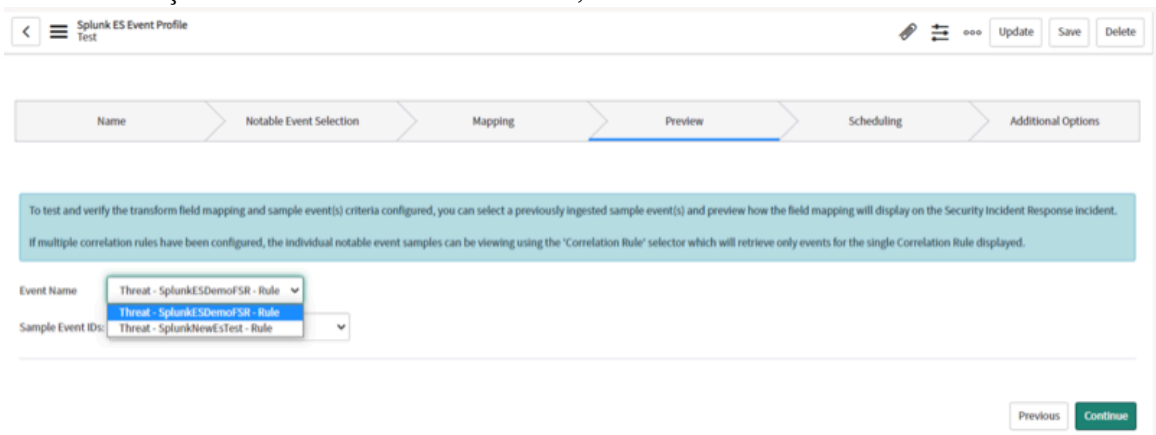
Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou preencher dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. Visualizações de SIR os incidentes de segurança não são salvos como incidentes reais no SIR produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualização** na barra de andamento.
2. Na lista de seleção Nome do evento, selecione um item se vários eventos tiverem sido usados.
3. Selecione IDs de evento na lista de seleção IDs de evento notáveis de amostra.
4. Na lista de seleção IDs de evento notáveis de amostra, selecione um item.



O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro desse incidente de segurança não é salvo.

5. Revise o mapeamento de campo dos valores de evento notáveis no incidente de segurança.



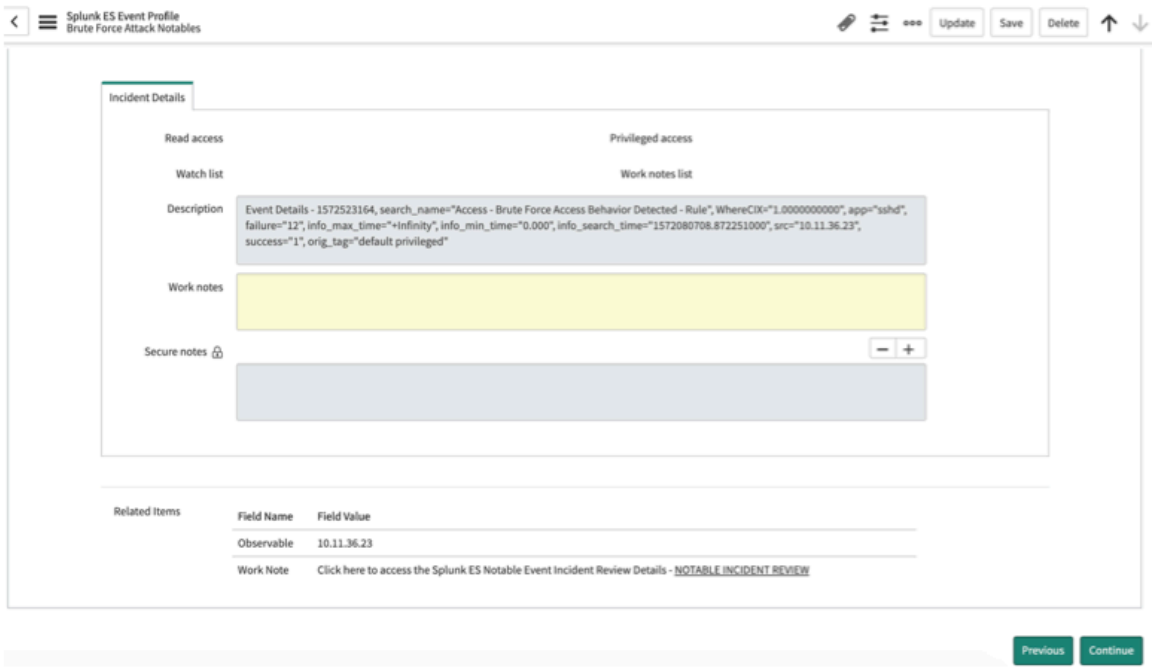
A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento Notable não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para Item de configuração . ServiceNow® Banco de dados de gestão de clientes (CMDB). Como resultado, este valor de campo mapeado não aparecerá no formulário de incidente de segurança SIR sem modificações adicionais.

6. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
7. Edite o mapeamento para corrigir valores incorretos ou preencher quaisquer dados ausentes.
8. Visualize o mapeamento novamente e continue a corrigir todos os erros descritos nas mensagens de erro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um SIR incidente de segurança após todas as mensagens de erro serem resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos do Splunk Enterprise Security amostras de eventos notáveis. O primeiro campo de anotações de trabalho não tem valor. Este campo foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotação de trabalho adicionais que têm valores foram adicionados à seção de mapeamento.



9. Depois de corrigir os erros e verificar se os campos estão do jeito desejado, escolha uma opção para continuar.

Opção	Descrição
Continuar	O formulário Programação é exibido para perfis com eventos notáveis programados. **Programação** está selecionado na barra de andamento.
Encerrar	Para perfis com configurados para encaminhamento manual de eventos, clique em **Concluir** . Não há etapa de programação para perfis com dados de evento que são exportados sob demanda diretamente do Splunk Enterprise Security console.
Atualizar	Seus dados são salvos e você retorna para Splunk Lista de perfis de evento.
Anterior	A etapa Mapeamento na barra de andamento é exibida.
Excluir	Exclua este perfil de evento e o. Splunk A lista Perfis de evento é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será Programar e recuperar alertas para Splunk Enterprise Event Ingestion integração.

Programar e recuperar eventos notáveis novos e atualizados para Splunk Enterprise Security Integração de ingestão de evento

Para perfis automatizados de ingestão de eventos notáveis, esta etapa é necessária na configuração do perfil de evento. Durante esta etapa, você pode verificar as configurações padrão para recuperação de evento notável ou modificar a programação conforme necessário. Esta etapa também permite recuperar eventos notáveis históricos usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Para perfis para ingestão automatizada de eventos notáveis, você escolhe se deseja ingerir eventos notáveis históricos durante a etapa Programação. Você também escolhe a frequência com que pesquisará novos eventos notáveis futuros e eventos notáveis atualizados que correspondam à configuração do perfil de alerta.

Para perfis automatizados de ingestão de eventos notáveis, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação de alertas. Esta é uma etapa obrigatória para todos os processos de configuração de perfil de evento para perfis de alerta programados.

Esses intervalos de pesquisa são configurados por perfil. O desempenho do Splunk a integração de ingestão de evento pode ser afetada pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no Splunk Enterprise Security servidor contra o desejo de ser notificado o mais rápido possível quando um evento notável é criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo eventos notáveis novos e atualizados

Quando a programação de pesquisa é definida, o trabalho agendado extrai eventos notáveis novos e atualizados que foram extraídos anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso fornece a flexibilidade para criar incidentes com base em critérios que podem não estar presentes quando um evento notável é criado pela primeira vez, mas se torna disponível após a ocorrência de uma atualização, por exemplo, durante a fase de investigação. Quando um incidente é criado para um evento notável específico, suas atualizações subsequentes são ignoradas, pois espera-se que o notável agora esteja sendo tratado como ativo ServiceNow® incidente de segurança. No entanto, todas as outras notables que foram ingeridas anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídas e verificadas em relação aos critérios de geração de incidentes até se tornarem parte de um incidente ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

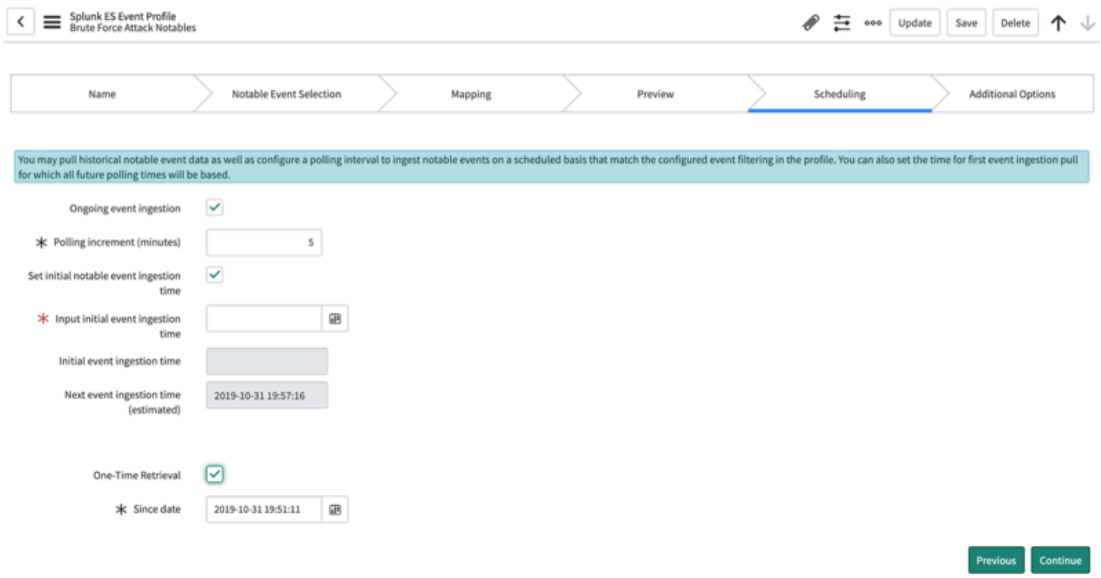
Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação** .
2. Escolha um para programar como e quando os eventos notáveis são extraídos do Splunk Enterprise Security console.

Opção	Descrição
◦ Campo Ingestão de evento em andamento selecionado ◦ Campo Recuperação única limpo	Evento em andamento Com base na configuração padrão, o. ServiceNow AI Platform a instância extrai do Splunk Enterprise Security servidor para eventos notáveis novos e atualizados a cada cinco minutos. Os incidentes de segurança serão criados se eventos notáveis forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar o desejo de sobrecarga de pesquisa de ingestão de obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, esse valor pode ser modificado para um minuto, se necessário.
◦ Campo de evento notável em andamento limpo ◦ Campo Recuperação única selecionado	Recuperação Única Use esta configuração se quiser uma extração única para ingerir eventos notáveis históricos. Quando esta configuração é definida, um perfil é usado uma vez para recuperar eventos notáveis de eventos históricos baseados em um intervalo de datas. À direita do campo Desde data, clique no ícone de calendário. No calendário exibido, selecione a data em que você deseja começar a extrair alertas. A partir do valor da data Desde, os eventos notáveis são recuperados até a data atual. Observe que você pode extrair até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de eventos históricos do Splunk Enterprise Security por motivos de arquivamento, mas sim uma quantidade mínima de eventos em andamento que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os eventos notáveis forem extraídos, esta configuração não recuperará eventos mais notáveis para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os eventos notáveis encontrados para o intervalo inserido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como exemplo para programar um horário de ingestão de evento notável inicial, se você tiver um diário Splunk Verificação de segurança que é executada uma vez por dia às 4 hora local, você pode configurar o perfil de evento notável correspondente em seu ServiceNow AI Platform Instância a ser executada às 4:05 hora local para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` No campo Ingestão de evento inicial. No campo Incremento (minutos), insira `1440` (24 horas) para programar a próxima ingestão de evento para 24 horas a partir da ingestão de evento inicial. A hora de ingestão do evento inicial e a hora de ingestão do próximo evento são exibidas nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

a. Com a página Programação exibida, selecione **Ingestão de eventos em andamento** marque a caixa para habilitar esta opção.

b. No campo Incremento (minutos), insira `1440` (24 horas).

c. Clique em **Selecione Ingestão de evento inicial** Caixa de seleção para habilitar a edição dos campos Ingestão de evento inicial e Ingestão de próximo evento.

d. No campo Ingestão de evento inicial, insira `04 05 00` .
No campo Próxima ingestão de evento (estimada), a hora da próxima ingestão de evento é exibida.

4. Clique em uma das opções a seguir para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Opções adicionais é exibido. **Opções adicionais** está selecionado na barra de andamento. A próxima etapa é atualizar os eventos notáveis quando o incidente SIR é criado e/ou encerrado.
Atualizar	Seus dados são salvos e Splunk A lista Perfis de segurança do evento é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Anterior	O formulário Programação é exibido.
Excluir	Exclua este perfil de evento e o. Splunk Enterprise Security A lista Perfis de evento é exibida.

Automatize atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Os incidentes de segurança podem ser criados e atualizados depois que são criados com uma interface bidirecional com o. Splunk Enterprise Security integração.

Antes de Iniciar

. Splunk Enterprise Security a integração tem uma interface bidirecional que permite que eventos notáveis criem incidentes de segurança, bem como atualizem os eventos notáveis depois que o incidente de segurança é criado e/ou encerrado.

Os detalhes relevantes do incidente incluem SIR número do incidente, grupo de atribuição, SIR URL do incidente. Esta seção é a parte final da configuração do perfil que fornece recursos opcionais para atualizar o. Splunk Enterprise Security eventos notáveis.

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais** .
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos notáveis com base nas atualizações de incidentes de segurança.

Opção ou Campo	Descrição
Atualizar eventos notáveis após a criação de incidente de SIR	Selecione esta opção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for criado a partir do evento notável. Isso pode ocorrer para os eventos notáveis iniciais que acionam o incidente de segurança, bem como eventos agregados.
Atualização inicial de status do evento notável	Você deve selecionar uma opção de status no menu que exibe todos os valores de status disponíveis recuperados do Splunk Enterprise Security servidor. Isso pode incluir um status criado personalizado, como ServiceNow- Atribuído conforme mostrado na captura de tela abaixo. Selecione o valor de status a ser definido para todos os eventos notáveis quando um incidente de segurança for criado para um evento notável ingerido. Notables que criam novos incidentes e notables que são ingeridos e agregados a um incidente em aberto existente.
Comentários iniciais retornados para o evento notável	Além de atualizar o valor de status notável, você também pode publicar comentários no histórico de revisão de incidente de evento notável. Conforme indicado nas instruções, você pode editar o texto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

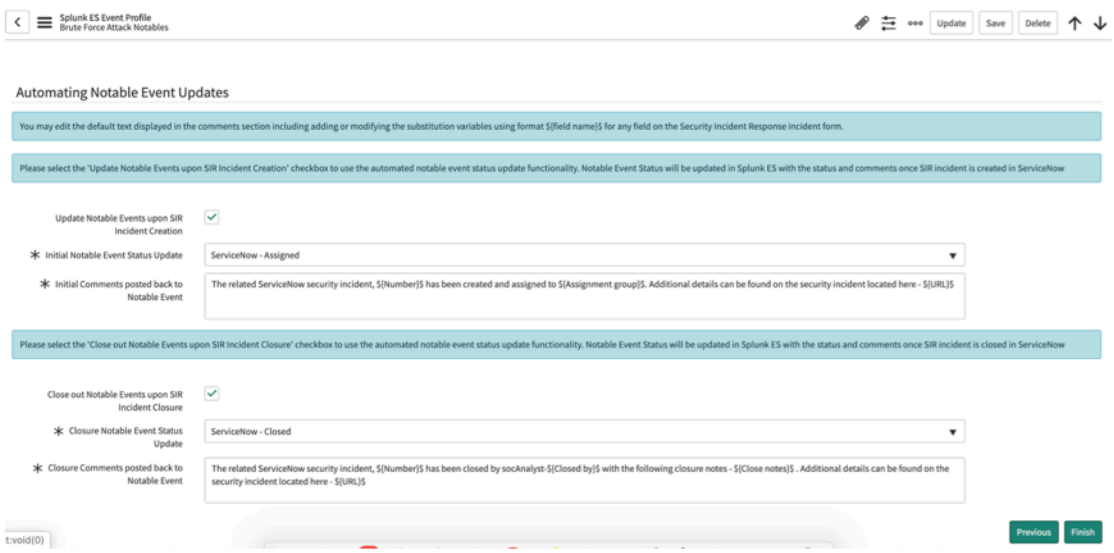
Opção ou Campo	Descrição
	padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato"nome do campo" para qualquer campo no Resposta a incidentes de segurança formulário incidente.
Fechar eventos notáveis após o fechamento do incidente de SIR	Selecione esta opção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for encerrado a partir do evento notável. Isso ocorrerá para os eventos notáveis de gatilho iniciais que criam o incidente de segurança, bem como eventos agregados.
Atualização de status do evento notável de fechamento	Você deve selecionar uma opção de status no menu de lista que exibe todos os valores de status disponíveis que são recuperados do Splunk Enterprise Security servidor. Isso pode incluir um status criado personalizado, como ServiceNow- Atribuído conforme mostrado na captura de tela abaixo. Selecione o valor de status a ser definido para todos os eventos notáveis quando um incidente de segurança for criado para um evento notável ingerido. Isso inclui notables que criam novos incidentes, bem como notables que são ingeridos e agregados a um incidente em aberto existente.
Comentários de fechamento retornados para o evento notável	Além de atualizar o valor de status notável, você também pode publicar comentários de fechamento no histórico de revisão de incidente de evento notável. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato"nome do campo" para qualquer campo no Resposta a incidentes de segurança formulário incidente.
Atualizar a atividade de automação da SIR com comentários do evento do Splunk	Opção para atualizar os comentários do evento Splunk no SIR Atividade de automação. O comentário em SIR A atividade de automação aparece com o prefixo `Comentário do Splunk` .
Atualizar comentários do Splunk com anotações de trabalho SIR	Opção para atualizar seu SIR Anotações de trabalho nos comentários do evento Splunk. O comentário no evento Splunk aparece com o prefixo `Comentário da ServiceNow` .

3. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair eventos notáveis do Splunk Enterprise Security console baseado em sua programação. Há um limite de 1 000 incidentes de segurança que podem ser criados em um período de 24 horas. Até 100 eventos notáveis são por alerta disparado. Eventos notáveis subsequentes serão ignorados depois que os limites forem atingidos.

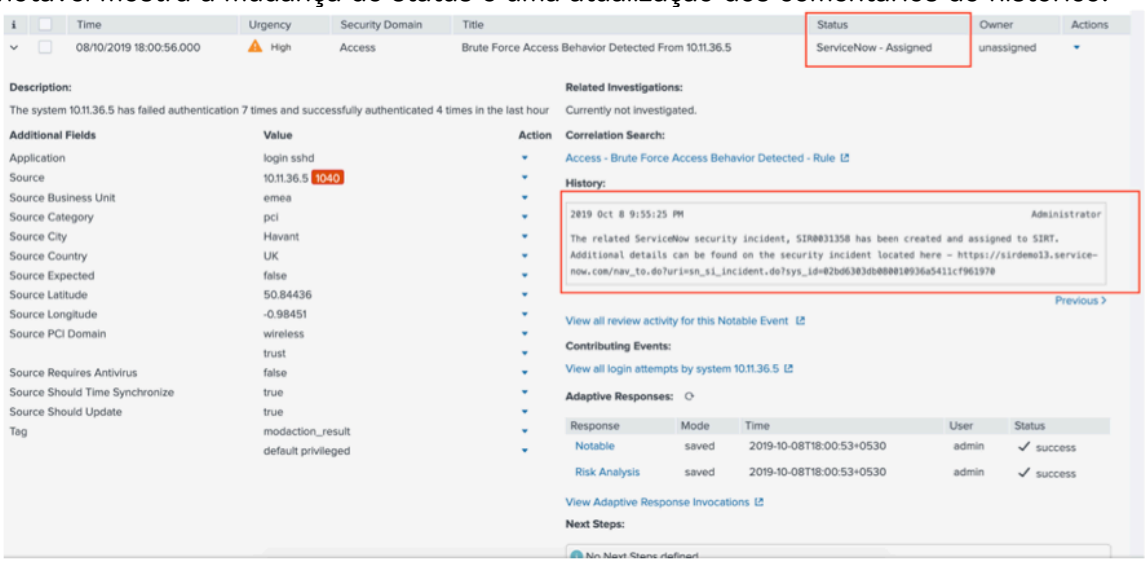
A imagem a seguir mostra a guia Opções adicionais com os valores padrão preenchidos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Com a configuração Opções adicionais habilitada, a revisão de incidente de evento notável mostra a mudança de status e uma atualização dos comentários do histórico:



Configure um perfil para encaminhamento manual de eventos

Dependendo do perfil definido, Splunk ES eventos notáveis são encaminhados manualmente como eventos notáveis discretos para Operações de segurança do seu ServiceNow AI Platform instância.

Para configurar um perfil para encaminhamento manual de eventos notáveis:

Tarefa	Seção
Crie um perfil de evento	Veja Crie perfis para eventos encaminhados manualmente
Mapear campos de evento notável	Veja Mapeamento de campos de evento notável para Splunk Enterprise Security integração
Crie mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (encaminhamento manual)

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Tarefa	Seção
Visualize o incidente de segurança	Veja Visualize o incidente de segurança do Splunk Enterprise Security Integração de ingestão de evento
Configure seu Splunk ambiente para ingestão manual	Veja Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise Security Integração de ingestão de evento notável
Automatize atualizações e fechamento de eventos notáveis com base no status do incidente SIR	Veja Automatize atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Crie perfis para eventos encaminhados manualmente

Você pode configurar um perfil para eventos encaminhados manualmente.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Procedimento

Para criar um perfil compatível com o encaminhamento manual de eventos, siga estas etapas.

Para eventos que você encaminha sob demanda do seu Splunk Enterprise Security console, você pode basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos que você encaminha manualmente não são programados no perfil de evento.

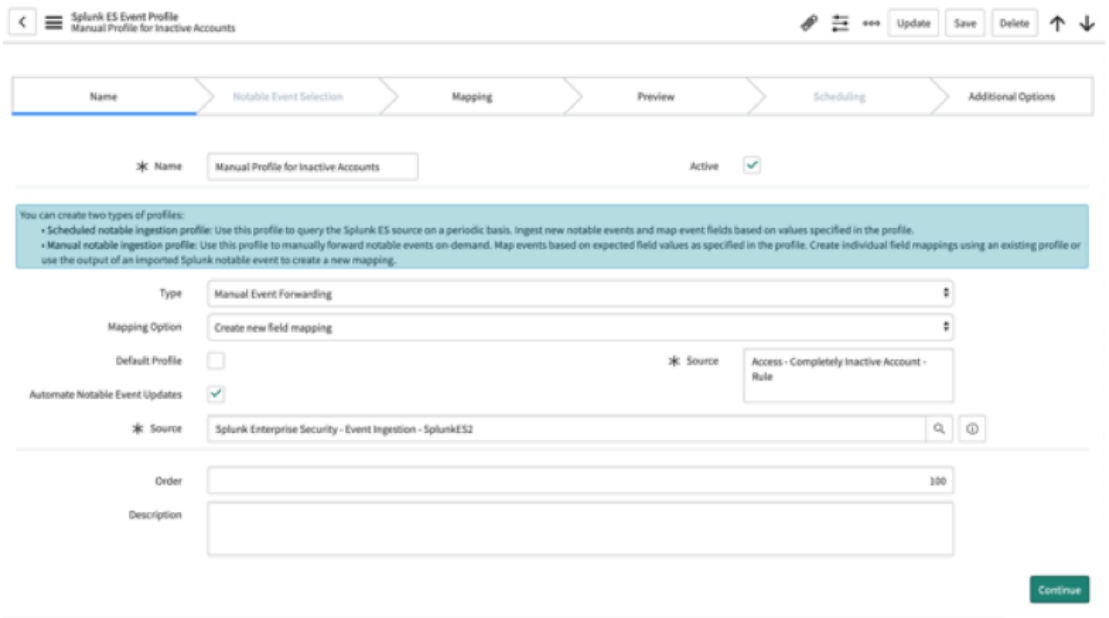
a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos** .

b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

Consulte as figuras e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para seu evento. Se você não tiver um mapeamento de campo existente semelhante ao perfil que está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos Splunk eventos. O padrão é limpo (desativado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este perfil é usado quando não há correspondência na origem do evento encaminhado manualmente. Ele se torna o perfil padrão para todos os eventos com origens desconhecidas. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo de evento notável)	Este é um campo que normalmente define a regra de correlação que acionou os notáveis, por exemplo, ataques de força bruta. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

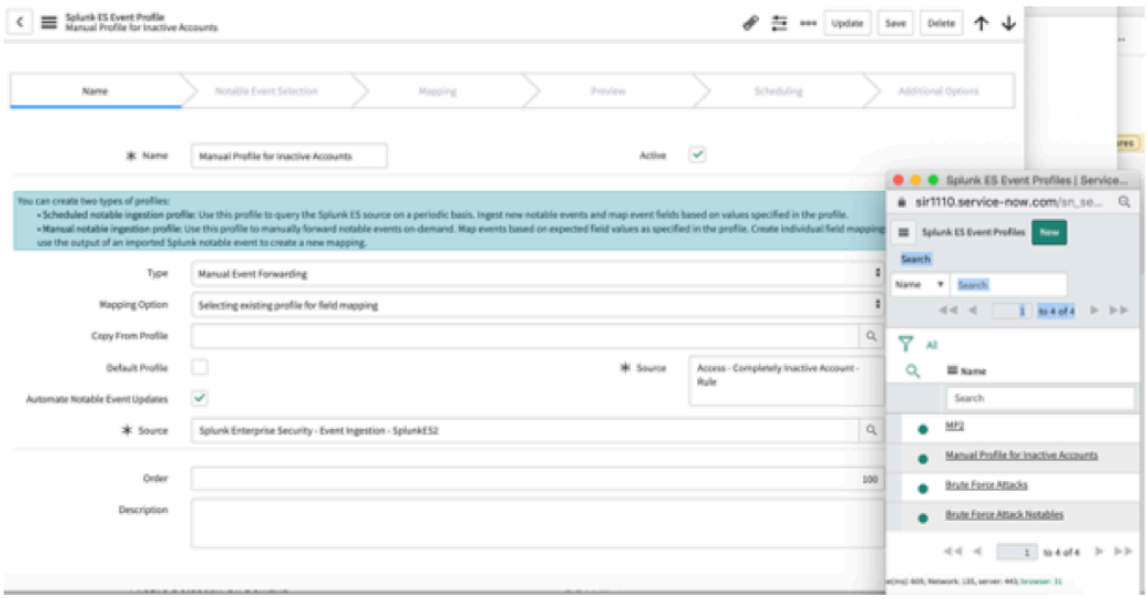
Opção ou campo	Descrição
	com base na regra de correlação do splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento de perfil com base na regra de correlação para atender a esse requisito.
Automatize atualizações de eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente SIR for criado a partir do evento notável e/ou quando o incidente SIR for encerrado. Tanto para os eventos notáveis de gatilho iniciais que criam o incidente SIR, bem como eventos agregados.
Origem (Splunk)	. Splunk servidor que você configurou como a origem de eventos notáveis. Se você tiver vários Splunk servidores configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você criou um grande número de perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para obter um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar o perfil existente para mapeamento de campo	Reutilize um mapeamento de campo existente para seu novo perfil de evento notável. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil. **i.** À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. **ii.** Em Splunk Lista Perfis de evento ES exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos Splunk eventos notáveis com origem incompatível. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo de evento notável)	Este é um campo que normalmente define a regra de correlação que acionou os notáveis, por exemplo, ataques de força bruta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base na regra de correlação do splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento de perfil com base na regra de correlação para atender a esse requisito.
Automatizar eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for criado a partir do evento notável ou quando o incidente de segurança for encerrado. Isso ocorre para os eventos notáveis de gatilho iniciais que criam o incidente de segurança, bem como eventos agregados.
Origem (Splunk)	Splunk servidor ou término de pesquisa que você configurou como a origem de eventos notáveis. Se você tiver vários Splunk servidores configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. Você deve inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você criou vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (encaminhamento manual)

Durante a etapa de mapeamento de campo de evento notável, você mapeia campos de evento individuais de eventos notáveis para campos em um ServiceNow AI Platform Resposta a incidentes de segurança(SIR incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa
Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de evento notável à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Campos padrão que normalmente são importantes para preencher no formulário de incidente SIR são exibidos. Esses campos podem ser removidos e todos os campos adicionais podem ser exibidos usando os botões mais e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no SIR incidente de segurança.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Siga estas etapas para carregar dados de anexo em seu ServiceNow AI Platform® instância.

   a. Se ainda não estiver conectado, faça login em Splunk Enterprise console.

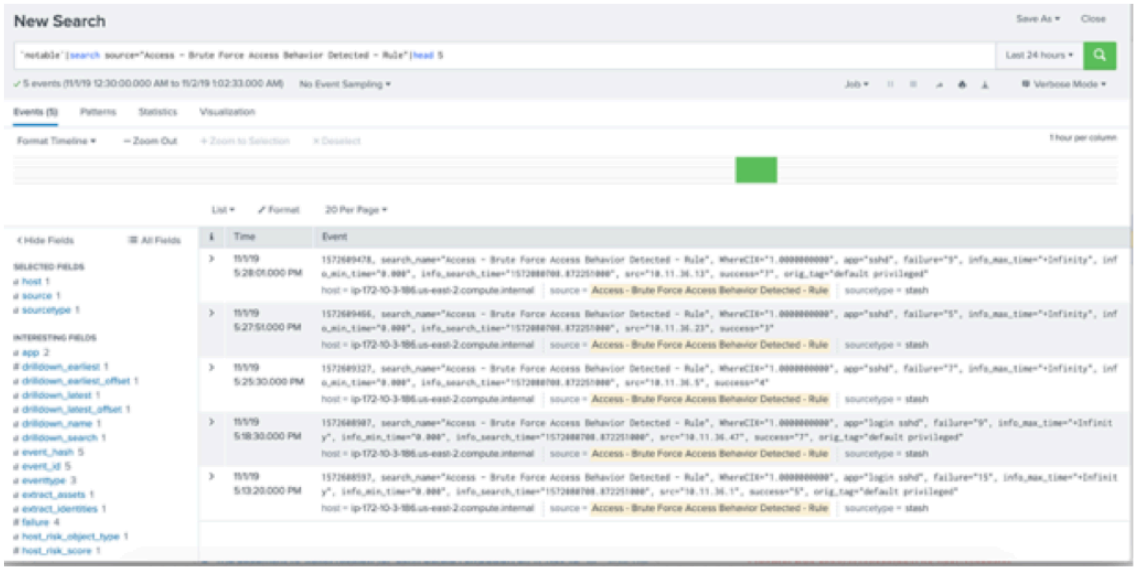
   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados de evento notáveis que você deseja exportar.
   Um exemplo de formato de pesquisa para recuperar eventos notáveis para a regra de correlação de comportamento de acesso de força bruta seria o seguinte: "Notable" | search source: "Access - comportamento de acesso de força bruta detectado - regra".

   c. Expanda o evento Notável e, na coluna Campo, selecione os campos que você deseja importar.

   Esses campos são os pares campo-valor que são exportados e exibidos na página Mapeamento do seu ServiceNow AI Platform® instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

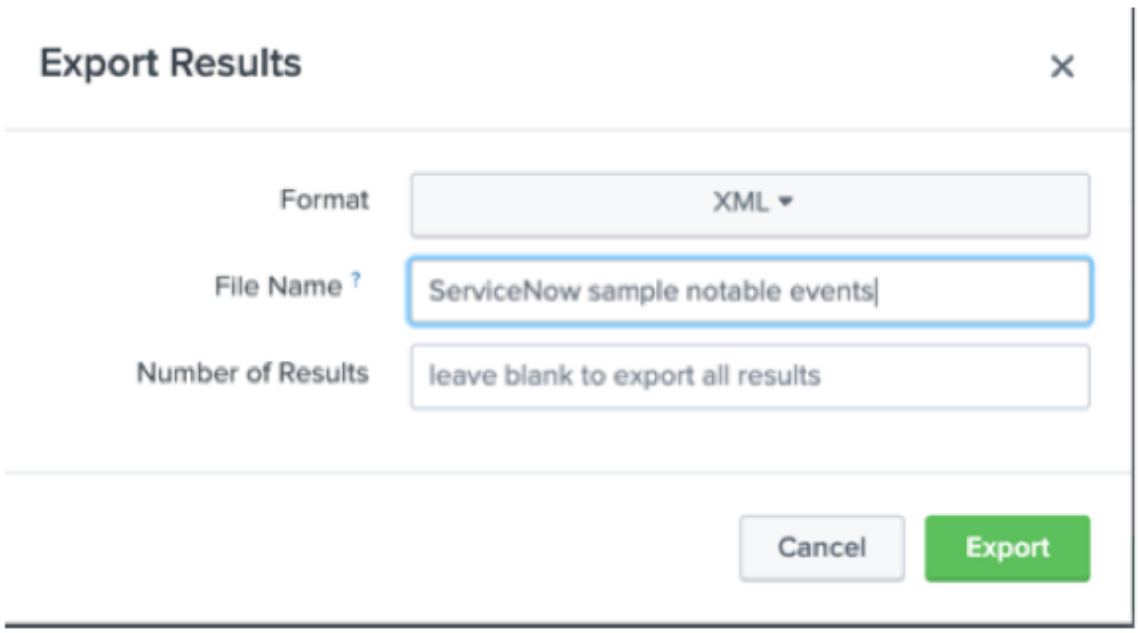


d. Em seu Splunk Enterprise No canto superior direito da página Pesquisar, clique em **Exportação** ícone.

e. Na lista de seleção do campo Formato na caixa de diálogo exibida, clique em **Formato XML** .

f. Opcional: Insira um novo nome de arquivo.

g. Clique em **Exportar**.



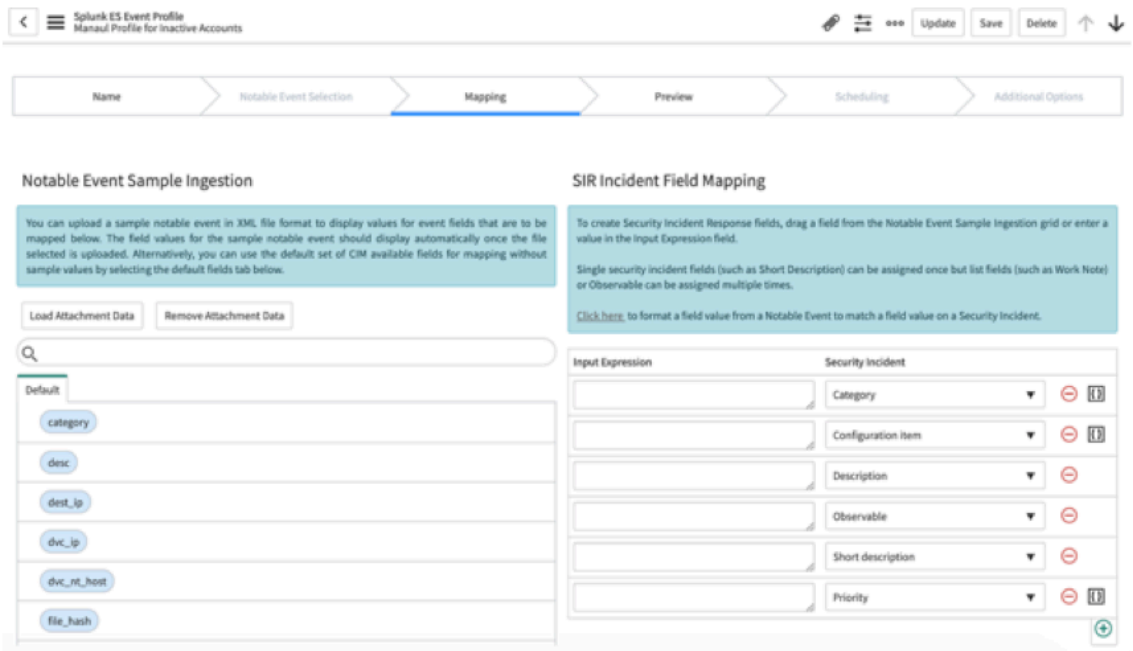
Exportado Splunk O arquivo XML de evento notável agora deve ser carregado em seu ServiceNow AI Platform® instância.

h. Se a página Mapeamento ainda não estiver exibida em seu ServiceNow AI Platform® instância, clique em **Mapeamento** na barra de andamento.

i. Na coluna Ingestão de amostra de evento notável, clique em **Carregar dados do anexo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



j. Na caixa de diálogo exibida, clique em **Escolha Arquivos** e navegue até .xml arquivo exportado e clicado **Aberto** .
Depois de clicar para carregar dados de anexo para eventos encaminhados manualmente, o Splunk ES os campos de evento notável são preenchidos no lado esquerdo do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

3. Siga as etapas 5 a 10 em Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada) seção.

Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise Security Integração de ingestão de evento notável

Instale e configure o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security aplicação em seu Splunk Console do enterprise ou instância do Splunk Cloud se você quiser exportar eventos manualmente e sob demanda do seu Splunk Enterprise Security console para esta integração.

Antes de Iniciar

Instalação e configuração do ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security aplicação em seu Splunk O console enterprise ou a instância do Splunk Cloud são opcionais.

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in de complemento do splunkbase que é necessário para ingestão manual de eventos. Se você não instalou a aplicação para a integração do ServiceNow Store, consulte Instalar e configurar Splunk Enterprise Security Integração de ingestão de evento notável e siga as instruções para instalá-lo.

Função necessária: Splunk Enterprise Security administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se você quiser exportar eventos manualmente e sob demanda do seu Splunk Enterprise console para integração, download, instalação e configuração do ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security do splunkbase em seu Splunk Enterprise Security console. Isso ServiceNow o complemento de extensão é necessário para que os incidentes de segurança possam ser criados a partir de eventos exportados manualmente em seu ServiceNow AI Platform instância. Isso ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security a aplicação está disponível em splunkbase .

Para encaminhamento manual de eventos, você pode identificar até dois diferentes ServiceNow AI Platform endpoints (instâncias) em seu Splunk Enterprise Security console. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. PESQUISE ServiceNow Operações de segurança Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security.

   > **Nota:** Verifique se você selecionou ServiceNow Operações de segurança Complemento de ingestão de evento para Splunk Enterprise Security. Há adicionais ServiceNow complementos exibidos nesta lista. Estes addons são para diferentes ServiceNow Splunk e elas não são necessárias para esta integração.

   c. Baixe a aplicação.

   d. Abra seu Splunk Enterprise Security conta.

   e. Na página Aplicativos, clique no ícone de engrenagem ou em **Gerenciar aplicações** atalho na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicativos exibida, clique em **Instale o app do arquivo** .

   g. Clique em **Escolha Arquivo** , selecione ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security e clique em **Upload** .

   h. Se solicitado, reinicie Splunk Enterprise.
   . ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security está instalado em seu Splunk Enterprise Security console. A próxima etapa para configurar o complemento.

2. Para configurar o complemento, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em Splunk Enterprise Security, clique em **Aplicações** ícone de engrenagem ou **Gerenciar aplicações** na lista suspensa do menu.

b. Na lista de aplicações exibida, em **Ações** , clique em **Configurar** para ServiceNow Operações de segurança Complemento de ingestão de evento para Splunk Enterprise Security.

c. Preencha o formulário.

A figura a seguir é um exemplo de um formulário preenchido em seu Splunk Enterprise Security console.



Campo na seção Especificar instância primária da ServiceNow	Descrição
Rótulo da ação do fluxo de trabalho	Nome do ServiceNow AI Platform fluxo de trabalho para sua instância de produção (primária). Este nome é o nome de um ServiceNow AI Platform instância que seus usuários que estão monitorando Splunk Os eventos são identificados como uma instância primária, por exemplo, Ingestão de eventos da ServiceNow (produção). O padrão para este campo é Ingestão de eventos da ServiceNow (produção).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	Em seu Splunk Enterprise Security Este nome de fluxo de trabalho é exibido para a instância de produção (primária) no expandido Ações de evento lista suspensa de uma pesquisa. Este nome é o nome da sua instância de produção. Você pode editar o nome.
URL	O URL do ServiceNow AI Platform Instância que você inseriu no campo Rótulo de ação de fluxo de trabalho anterior. Copie o URL no seu navegador e cole-o neste campo no formulário.
Endpoint	Caminho da API de base. Para obter mais informações, consulte a figura que segue a tabela. Se você não tiver um valor para o endpoint do seu ServiceNow AI Platform instância de produção, siga estas etapas. **a.** Faça login no seu ServiceNow AI Platform instância de produção como um usuário com a função de administrador do sistema (administrador). **b.** Insira REST APIs com script no painel de navegação. **c.** Depois que o painel de navegação for atualizado, selecione **REST APIs com script** módulo exibido. **d.** Se a ingestão de evento não estiver listada na coluna Nome do REST APIs com script lista exibida, no campo de pesquisa na parte superior, insira Ingestão de evento . **e.** Na coluna Caminho da API base na página atualizada, copie este valor e cole-o no campo Endpoint do formulário. Um exemplo de caminho de api base é, /api/sn_sec_splunk_v2/event_ingestion .
Nome do usuário	Nome de usuário do ServiceNow AI Platform instância. Este nome é o nome de usuário do ServiceNow AI Platform instância na qual você atribuiu a um usuário a função (sn_sec_splunk_v2.api_account_access) para encaminhamento manual de eventos. Para obter mais informações sobre como atribuir esta função, consulte Configure seu ServiceNow AI Platform instância do Splunk Enterprise Event Ingestion integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

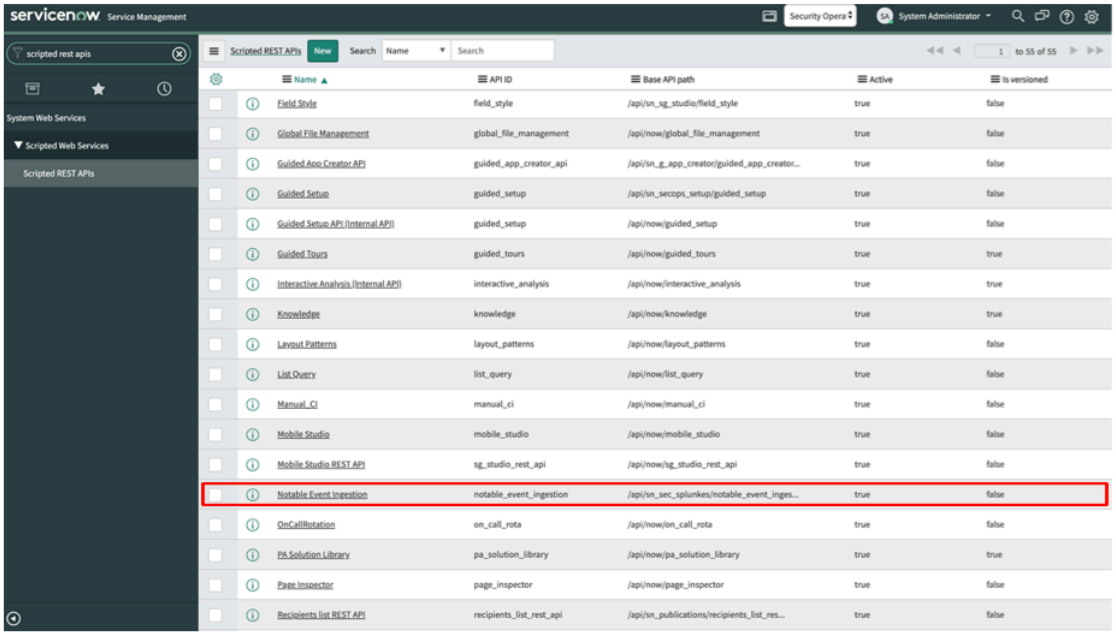
Campo na seção Especificar instância primária da ServiceNow	Descrição
Senha	Senha do ServiceNow AI Platform instância. Esta senha é a senha do ServiceNow AI Platform instância na qual você atribuiu a um usuário a função (sn_sec_splunk_v2.api_–account_access) para encaminhamento manual de eventos.
(Opcional) Campos na seção Especificar instância secundária da ServiceNow	Descrição Esses campos são opcionais. Você não precisa especificar uma instância secundária.
Rótulo da ação do fluxo de trabalho	Nome do ServiceNow AI Platform fluxo de trabalho para sua instância secundária (preparação). Este nome é o nome de um ServiceNow AI Platform instância que seus usuários que estão monitorando Splunk os eventos são identificados como uma instância secundária, por exemplo, ServiceNow Ingestão de evento (preparação). Em seu Splunk Enterprise Security Este nome de fluxo de trabalho é exibido para a instância de preparação (secundária) na lista suspensa Ações de evento expandidas de uma pesquisa. Isso ServiceNow AI Platform a instância é sua instância de preparação. Você pode editar o nome.
URL	O URL do ServiceNow AI Platform Instância que você inseriu no campo Rótulo de ação de fluxo de trabalho anterior para o secundário ServiceNow AI Platform instância. Copie o URL no seu navegador e cole-o neste campo no formulário.
Endpoint	Caminho da API de base. O valor do caminho da API base para sua instância secundária é o mesmo valor do caminho da API base para sua instância primária. Consulte a figura anterior do formulário para obter mais informações.
Nome do usuário	Nome de usuário do ServiceNow AI Platform instância de preparação. O usuário deve ter a função (sn_-sec_splunk_v2.api_account_access).
Senha	Senha do ServiceNow AI Platform instância de preparação. O usuário deve ter a função (sn_sec_splunkes.api_account_access).

A figura a seguir é um exemplo da lista REST APIs com script em seu ServiceNow AI Platform. A lista exibe o local do valor de endpoint de um ServiceNow AI Platform instância que você insere no formulário como parte da configuração para ServiceNow Complemento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de ingestão de evento de operações de segurança para Splunk Enterprise Security extensão em seu Splunk Enterprise Security console.



3. No formulário de configuração do seu Splunk Enterprise Security console, clique em **Salvar** para salvar suas edições.

   Após alguns momentos, na parte superior esquerda do formulário em seu Splunk Enterprise Security uma mensagem é exibida informando que o registro foi atualizado com sucesso.

   Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) do seu ServiceNow AI Platform As instâncias que você criou no formulário estão disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa em seu Splunk Enterprise Security console.

O que Fazer Depois

Se você ainda não salvou as pesquisas em seu Splunk Enterprise Security console, a próxima etapa é salvar pesquisas como alertas em seu Splunk Enterprise Security console.

Copie um perfil de evento para Splunk Enterprise Security Integração de ingestão de evento

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar perfis de alarme para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

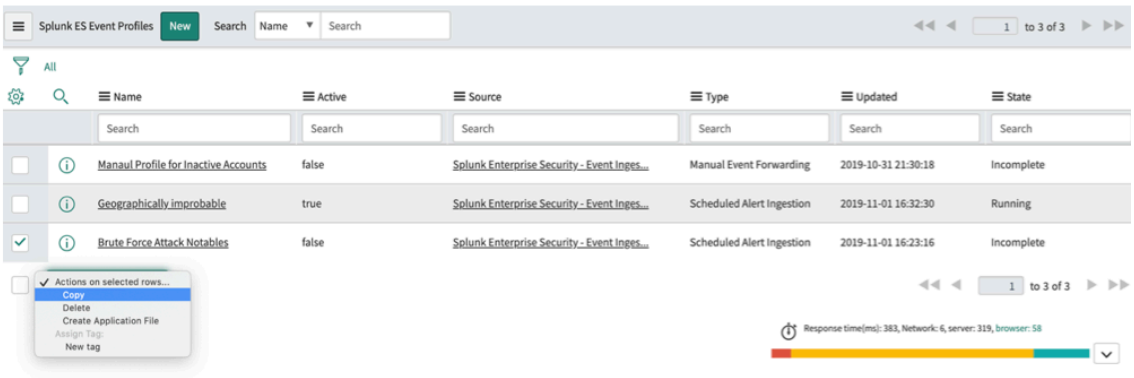
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desativado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

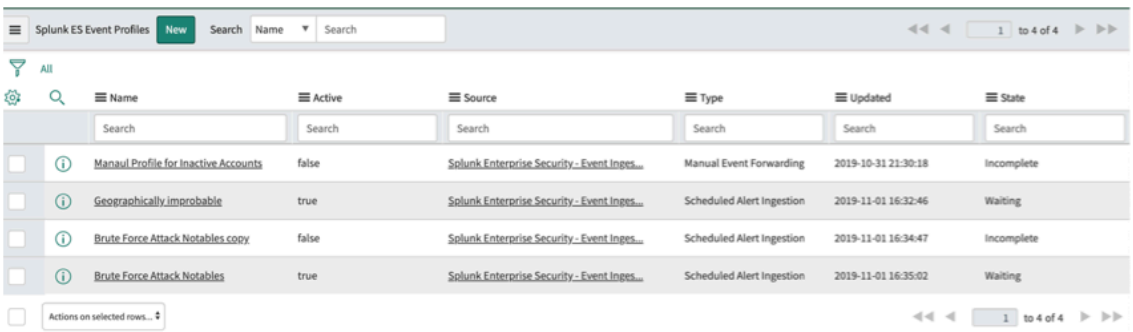
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Splunk Integration** > **Perfil de evento do Splunk**.
2. Em Splunk Lista Perfis de evento exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Cópia** .



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja ativado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode preferir editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir a etapa de configuração.

Use o editor de scripts para formatar valores de alerta para Splunk Enterprise Security Integração de ingestão de evento

Além dos campos mapeados diretamente a partir dos valores de eventos notáveis ingeridos e dos valores inseridos manualmente, use o editor de scripts para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Em determinados casos, Splunk Enterprise Security Valores de evento notáveis são mapeados para os campos Categoria, Item de configuração (IC) e Observável no SIR incidentes não

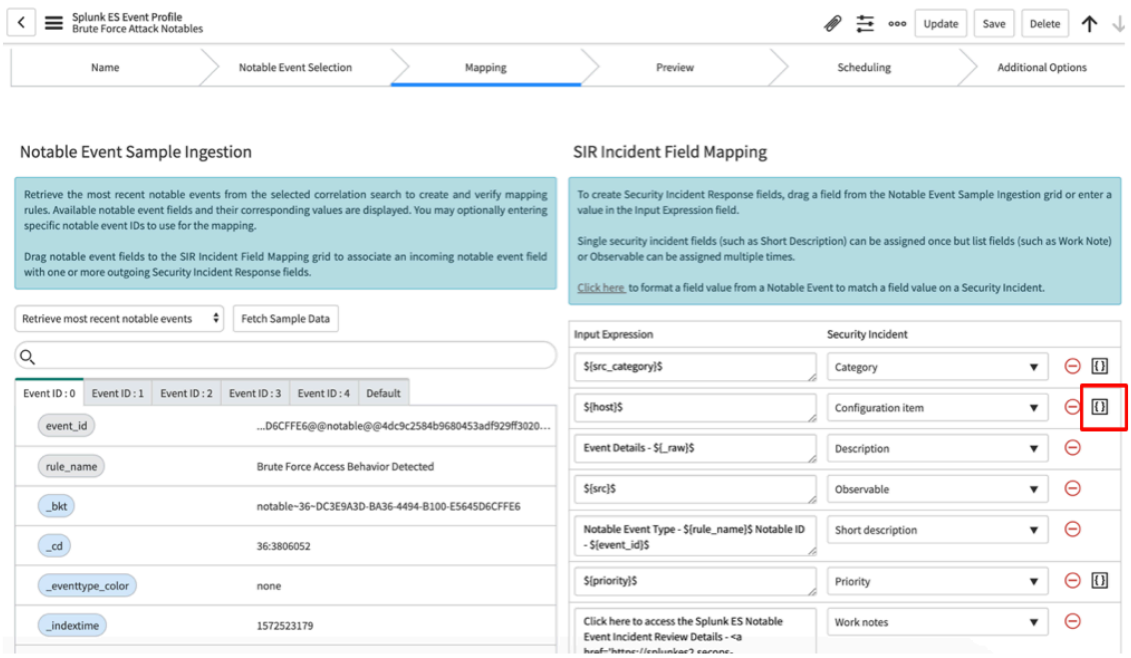
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são compatíveis. Você pode preferir editar os valores mapeados. Se você quiser traduzir o valor de um Splunk Enterprise Security evento notável para um valor que é compatível com esses campos no SIR incidente de segurança, use o editor de scripts.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de scripts.



2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete [] ao lado de um campo para abrir o editor de script desse campo.

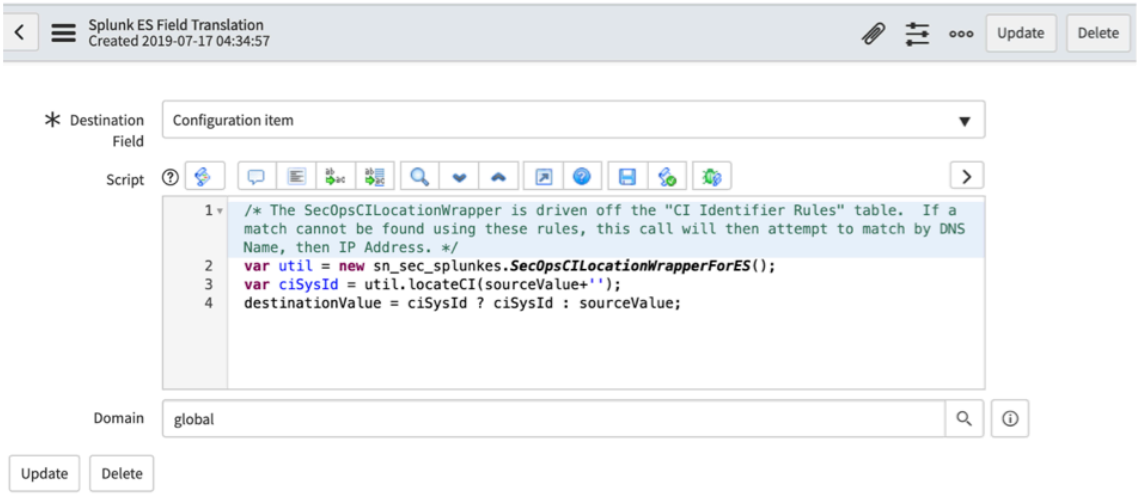
   Em determinados casos, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento notável, por exemplo, um valor para o item de configuração pode não ser correspondido.

   Se não for possível encontrar uma correspondência para um nome de host em ServiceNow AI Platform® CMDB Para o campo Item de configuração, você pode editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido em Campo de destino. A imagem a seguir mostra o editor com Item de configuração Campo como o Campo de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira as mudanças no script e clique em **Atualização** para salvar suas mudanças.
   . Splunk A tabela Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

Cópia Splunk Enterprise Security perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar Splunk Enterprise Security configurações de perfis de um ServiceNow AI Platform instância para um diferente ServiceNow AI Platform instância.

Antes de Iniciar

As configurações que você pode exportar e importar incluem nome de perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campo, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Função necessária: sn_si.ingestion_profile_admin

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Esta funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em um ServiceNow AI Platform instância, por exemplo, em não produção, para outra ServiceNow AI Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações exportadas e importadas incluem nome de perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campo, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Nota: Quando você exporta um tipo de perfil de encaminhamento de evento manual, os dados do anexo usados para o mapeamento de campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

Procedimento

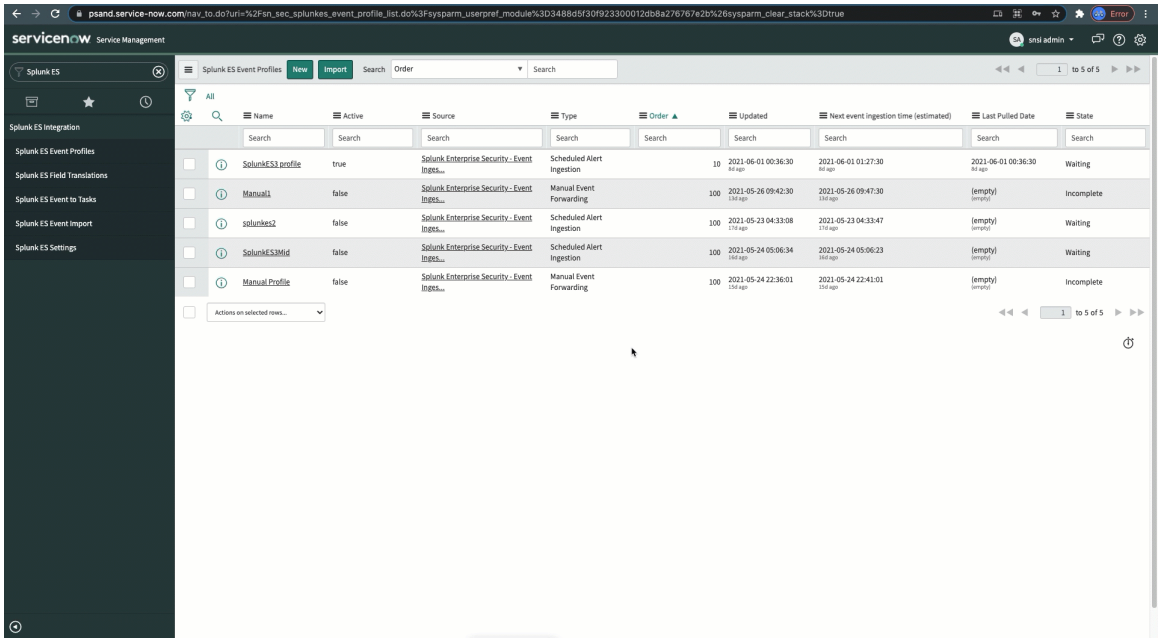
1. Navegar até **Tudo** > **Integração com Splunk ES** > **Perfis de eventos do Splunk ES**.
2. Selecione um perfil que você deseja exportar para outro ServiceNow AI Platform instância.
   Você pode selecionar vários perfis para exportação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No menu Ações, clique em **Exportação** .
4. Quando a mensagem de exportação concluída for exibida, clique em **Download** .

   A ilustração a seguir mostra como exportar um perfil (SplunkES3profile) do ServiceNow AI Platform instância (psand.service-now.com).



   O arquivo payload.xml exportado é baixado em seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campo, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

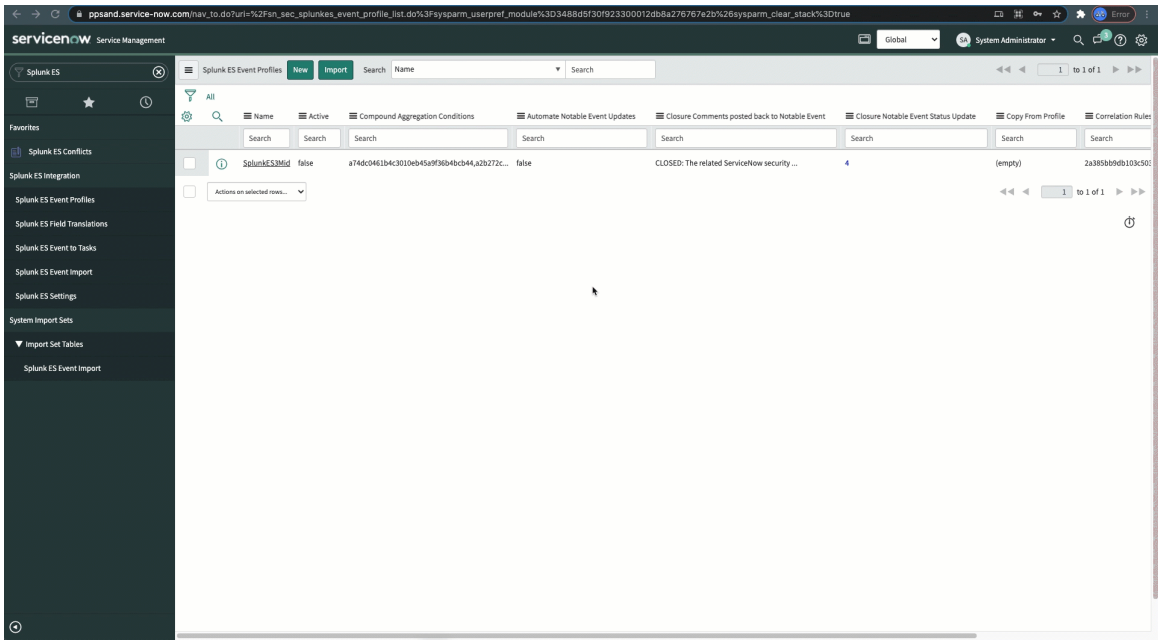
   Agora você pode prosseguir para importar o perfil em outro ServiceNow AI Platform instância.

5. Navegar até **Integração com Splunk ES** > **Perfis de eventos do Splunk ES**.
6. Clique em **Importar**.
7. Clique em **Escolha o arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Upload** (Carregar).
9. Clique em **Fechar e recarregar perfis** .

   A ilustração a seguir mostra como importar um perfil (SplunkES3profile) do ServiceNow AI Platform instância (psand.service-now.com) para ServiceNow AI Platform instância (ppsand.service-now.com).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outro ServiceNow AI Platform instância.

Verifique se a Origem exportada (Splunk Conta de API e. Splunk E as definições de configuração do MID Server são válidas e estão disponíveis no importado ServiceNow AI Platform instância. Atualize seu Splunk Enterprise Security configuração, se necessário.

10. **Opcional:** Verifique as configurações DO MID Server após importar um perfil.
11. **Opcional:** Navegar até **Operações de segurança** > **Configurações de Integração**.
12. **Opcional:** Selecione Splunk Enterprise Security bloco configuração e clique em **Atualização** .
13. **Opcional:** Revise e atualize os detalhes de origem e DO MID Server conforme necessário.

Check-list para Splunk Enterprise Security Integração de ingestão de evento notável

Use esta check-list para orientá-lo em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem resultados esperados para a integração.

Antes de Iniciar

Funções necessárias: sn_si.ingestion_profile_admin, admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrador

Nota: Usuários com a função sn_si.admin podem executar todas as operações disponíveis para um administrador de perfil, já que a função sn_si.admin herda as permissões necessárias por padrão.

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe seu andamento com a instalação, a instalação e a configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima etapa. Cada linha da tabela lista tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

As funções necessárias para cada tarefa são listadas com cada etapa na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Acompanhe seu andamento com a instalação, a instalação e a configuração da integração. Conclua todas as tarefas de uma etapa antes de passar para a próxima etapa.
2. Siga as etapas na tabela na ordem em que elas são apresentadas.

Check-list

☐	Como um usuário com ServiceNow AI Platform função de administrador, configure seu ServiceNow AI Platform instância. ○ Atribuir usuários com **sn_si.ingestion_profile_admin** (ou sn_si.admin) e sn_si.analyst conforme necessário. ○ Instale e configure um MID Server se o Splunk o servidor está implantado em sua rede corporativa. ○ Verifique se o ServiceNow Resposta a incidentes de segurança os plug-ins estão ativados para sua versão do ServiceNow AI Platform. ○ (Opcional) Se você quiser encaminhar eventos manualmente do seu Splunk Enterprise Security console em seu ServiceNow AI Platform, verifique se você atribuiu a função (sn_sec_splunkes.api_account_access) a um usuário com Splunk Enterprise Security permissão de administrador. Para obter mais informações, consulte Configure seu ServiceNow AI Platform instância do Splunk Enterprise Security integração.
☐	Como um usuário com ServiceNow AI Platform função de administrador, instale e configure o. Splunk Enterprise Security aplicação do ServiceNow Store. **a.** Baixe e instale o aplicativo em seu ServiceNow AI Platform instância. **b.** Configure a aplicação e conecte-se ao seu Splunk Enterprise Security console. Para obter mais informações, consulte Instalar e configurar Splunk Enterprise Security Integração de ingestão de evento notável.
☐	(Opcional) Se você pretende exportar eventos manualmente do seu Splunk Enterprise Security console para seu ServiceNow AI Platform execute as seguintes tarefas: ○ . Splunk Enterprise Security administrador, instale, configure e habilite o. ServiceNow Complemento de ingestão de evento de operações de segurança para Splunk Enterprise Security do splunkbase em seu Splunk Enterprise Security console. ○ . Splunk Enterprise Security se ainda não estiver configurado, salve as pesquisas como eventos notáveis em seu Splunk Enterprise Security console.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para obter mais informações, consulte Configure seu Splunk ambiente para ingestão manual de eventos para Splunk Enterprise Security Integração de ingestão de evento notável.
☐	Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** criar e nomear um perfil de evento. Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do seu Splunk Enterprise Security console. ○ Para um alerta programado, selecione um alerta disponível. ○ Para perfil para dados exportados manualmente, crie um novo mapa ou copie um mapa existente. Para obter mais informações, consulte Crie e nomeie um perfil de evento para Splunk Enterprise Security integração de ingestão de evento.
☐	Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** valores de função, mapa ingeridos ou dados de anexo que são exportados de Splunk Enterprise Security. ServiceNow AI Platform incidentes de segurança. **a.** Buscar dados de amostra para um alerta programado. **b.** (Opcional) Exporte dados de anexo manualmente de Splunk Enterprise Security para um evento. **c.** Edite a configuração de mapeamento padrão. **d.** Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de scripts. Para obter mais informações, consulte Mapeamento de campos de evento notável para Splunk Enterprise Security integração e Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada).
☐	○ Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** visualizar os dados de Splunk Enterprise exibido em um ServiceNow AI Platform incidente de segurança. ○ Corrija erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida. Para obter mais informações, consulte Visualize o incidente de segurança do Splunk Enterprise Security Integração de ingestão de evento.
☐	Como um usuário com ServiceNow AI Platform **sn_si.ingestion_profile_admin** programar recuperação de alerta para um perfil com um alerta programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para obter mais informações, consulte Programar e recuperar eventos notáveis novos e atualizados para Splunk Enterprise Security Integração de ingestão de evento.

Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.

Splunk - Integração de aprimoramento de incidentes

. Splunk- A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos incidentes de segurança.

Explorar	Configuração
Integrações do Security Incident Response	Comece a usar Splunk Integração de pesquisa para Operações de segurança
Usar	**Desenvolver**
• Execute uma Pesquisa de vistas • Integração de operações de segurança - Fluxo de pesquisa de vistas • Integração de operações de segurança - Fluxo de pesquisa de vistas do Splunk • Exibir detalhes da pesquisa de vistas • Exibir resultados da pesquisa de vistas	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação
Solução de problemas e Informações adicionais	
• Solução de problemas de integração • Ou responda perguntas na comunidade de Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Comece a usar Splunk Integração de pesquisa para Operações de segurança

Splunk o software pesquisa, monitora e analisa big data gerado por máquina e se integra facilmente ao Operações de segurança. Antes de poder usar Splunk- Integração de aprimoramento de incidentes, você deve baixá-la do ServiceNow Store E adicione a URL base da API apropriada e as credenciais de login.

Antes de Iniciar

Função necessária: sn_si.admin

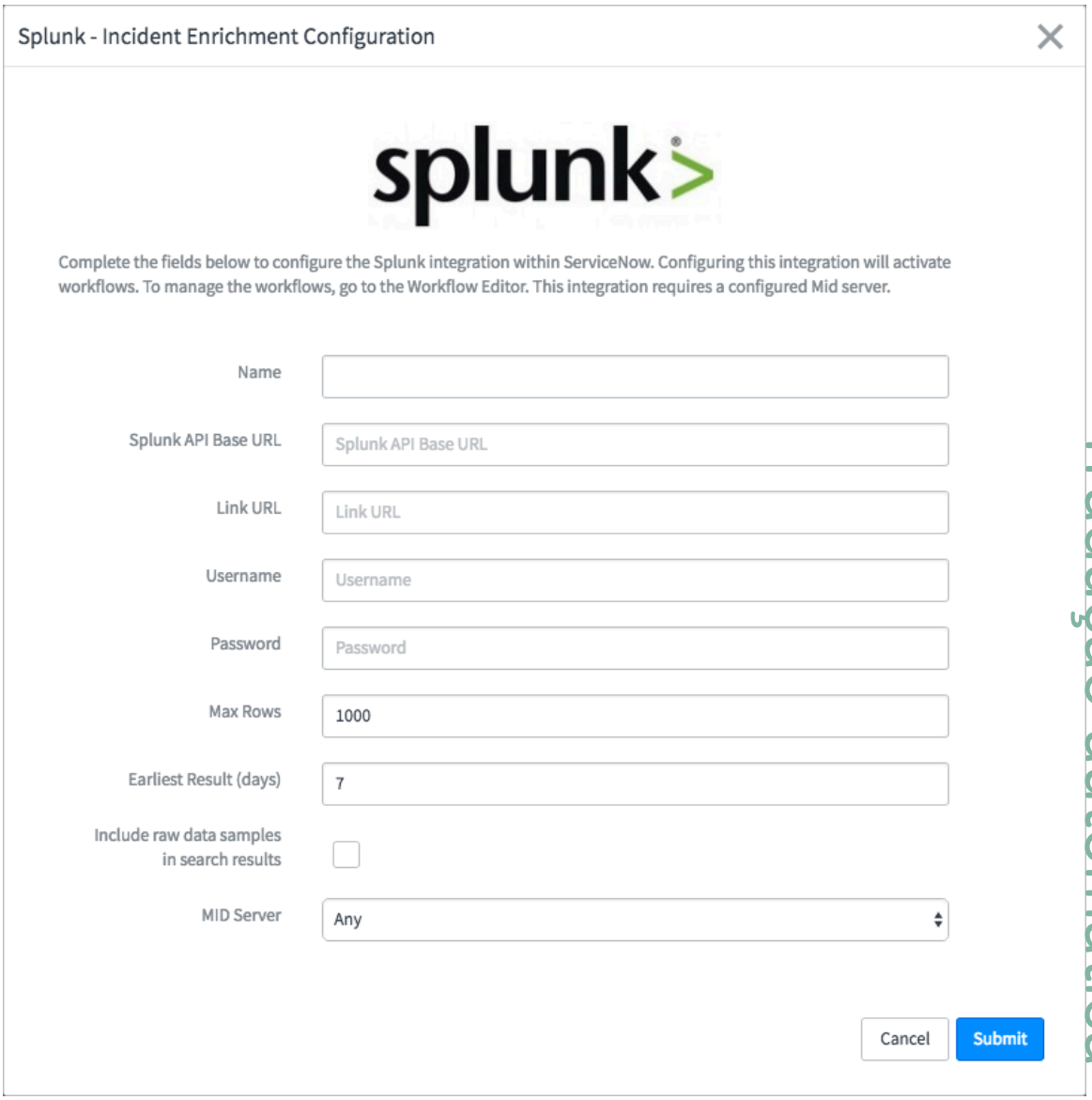
Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Splunk E obtenha a chave de API e o ID da API em seu perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Splunk - Aprimoramento de incidente, clique em **Novo** .



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL base da API Splunk	O URL base que você adquiriu do Splunk site.
URL do Link	[Opcional] O URL do link vinculado ao Splunk interface da web, quando disponível.
Nome do usuário	Seu nome de usuário do Splunk.
Senha	Sua senha do Splunk.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração no **número de linhas de dados brutos** propriedade em Propriedades de resposta do incidente de segurança .
MID Server	Selecione **Qualquer** Para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até **Editor de fluxo de trabalho** .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** em **Mostrar Configurações** lista suspensa.

Experiência móvel para Resposta a incidentes de segurança

Use seu Android ou iOS Dispositivo móvel para gerenciar suas tarefas do SOC (Security Operations Center, centro de operações de segurança).

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Resposta a incidentes de segurança

Se você não estiver familiarizado com os conceitos básicos do Resposta a incidentes de segurança(SIR) no seu ServiceNow AI Platform® instância, consulte Painel Visão geral do Resposta a incidentes de segurança para obter mais informações sobre inteligência contra ameaças e como este produto pode ajudar você a priorizar e resolver ameaças cibernéticas à sua organização.

Visão geral

Como gerente do SOC (Security Operations Center, centro de operações de segurança) ou um usuário com ServiceNow AI Platform função de analista de segurança (sn_si.analyst), você pode fazer login em um ServiceNow AI Platform instância diretamente do seu dispositivo móvel. Com Aplicação Resposta a incidentes de segurança para celular, você pode exibir, editar e atribuir seus mais atuais e críticos SIR incidentes de segurança e tarefas de resposta. As notificações informam quando incidentes de segurança críticos atribuídos a você chegam.

Com Aplicação Resposta a incidentes de segurança para celular, você pode executar o seguinte SIR-tarefas relacionadas do seu dispositivo móvel:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exiba uma lista de incidentes de segurança críticos e tarefas de resposta.
- Receba notificações detalhadas para incidentes de segurança e tarefas que atendam aos critérios de notificação predefinidos.
- Exiba agrupamentos de incidentes ou tarefas de segurança baseados em um conjunto predefinido de consultas ou filtros.
- Exiba as anotações de trabalho e as listas relacionadas de incidentes de segurança.
- Atualize incidentes de segurança e adicione anotações de trabalho ou anexos.
- Edite os campos em incidentes de segurança.
- Atribua incidentes de segurança a você mesmo ou a outros membros da sua equipe de segurança.

Quando eles são preenchidos, você pode exibir as seguintes listas relacionadas em SIR incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular:

- Item de configuração
- Usuário afetado
- Serviços afetados
- Incidentes de segurança secundários
- Incidentes de segurança semelhantes (não compatíveis com ServiceNow AI Platform)
- Observáveis
- Tarefas de resposta
- Tarefas
- ANS de tarefa
- Anexos (não compatíveis com ServiceNow AI Platform)

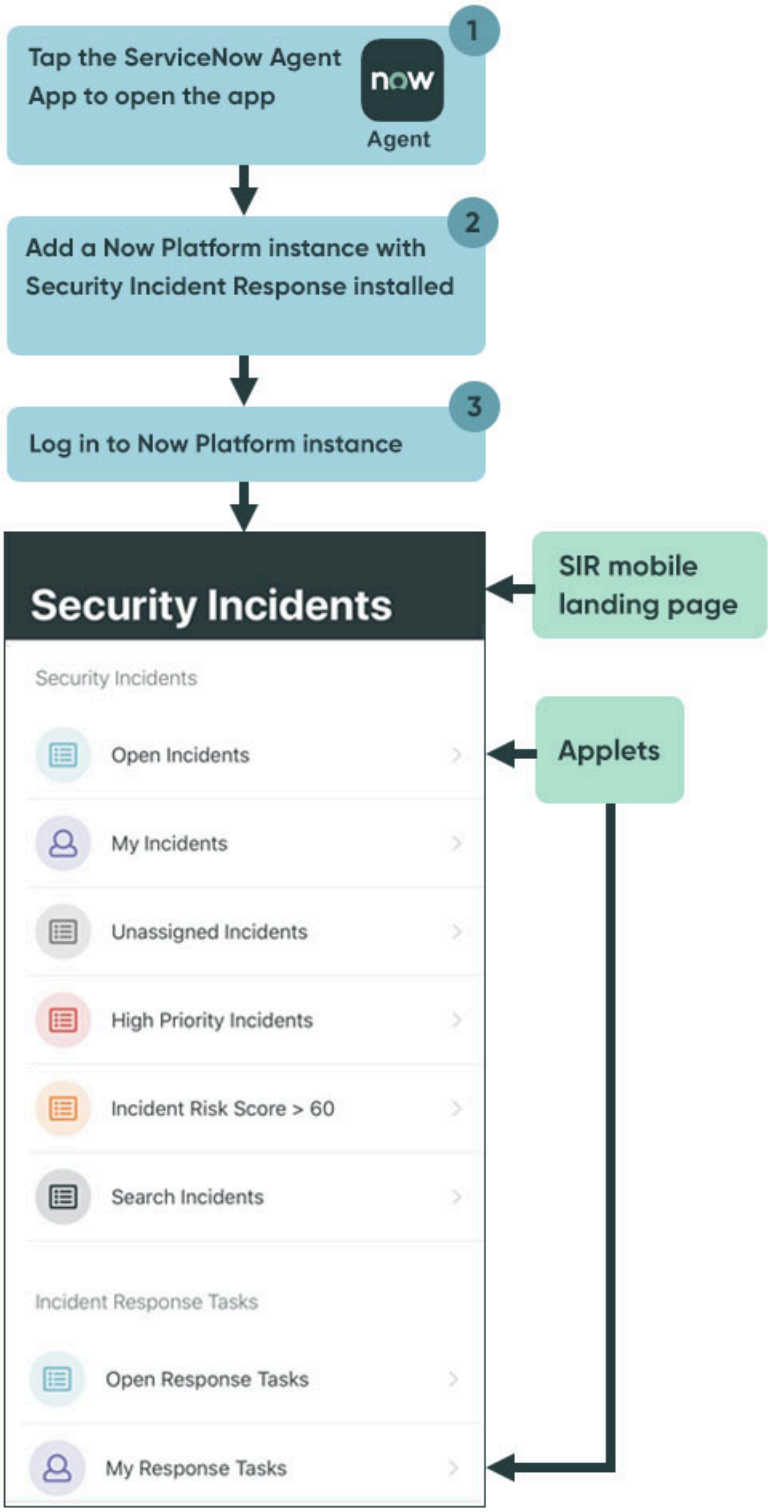
A figura a seguir ilustra como você faz login em ServiceNow AI Platform do seu dispositivo móvel e a estrutura da tela principal do Aplicação Resposta a incidentes de segurança para celular que é reproduzido depois que você faz login.

Para obter instruções passo a passo sobre como configurar seu ServiceNow AI Platform e instale o. Aplicação Resposta a incidentes de segurança para celular, consulte Configurar check-list para Aplicação Resposta a incidentes de segurança para celular. Para obter instruções sobre como fazer login, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação Resposta a incidentes de segurança para celular



Aplicações

As aplicações são ServiceNow® componentes de software, como Resposta a incidentes de segurança(SIR), Resposta a vulnerabilidades(VR), Governança, risco e conformidade(GRC) que fornecem recursos e funcionalidades específicos em seu ServiceNow AI Platform instância. Depois de instalar o. Resposta a incidentes de segurança aplicação principal e Aplicação Resposta a incidentes de segurança para celular em seu ServiceNow AI Platform, o ícone da aplicação principal é exibido na parte inferior do seu Android ou iOS dispositivo móvel depois de fazer login.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação Resposta a incidentes de segurança para celular Ícone (incidentes de segurança)

Pastas

Cada um ServiceNow® Mobile a aplicação contém pastas que separam os applets por categoria. Na imagem anterior da página principal, **Incidentes de segurança** e. **Tarefas de resposta do incidente** são pastas.

Applets

Miniaplicativos são as diferentes opções na aplicação. Os ícones em **Incidentes de segurança** e. **Tarefas de resposta do incidente** as seções são os miniaplicativos disponíveis do Aplicação Resposta a incidentes de segurança para celular.

Configurar check-list para Aplicação Resposta a incidentes de segurança para celular

A check-list a seguir inclui as tarefas de configuração que você deve concluir em ServiceNow AI Platform® e no seu dispositivo móvel antes de usar o. Aplicação Resposta a incidentes de segurança para celular.

Antes de Iniciar

Como opção, imprima esta check-list e use-a para orientá-lo nas tarefas de configuração necessárias para Aplicação Resposta a incidentes de segurança para celular. Verifique se cada item na lista está concluído para que você possa exibir e editar SIR incidentes de segurança em seu dispositivo móvel.

Os itens da lista de verificação são exibidos em texto realçado. Cada item na coluna à direita é acompanhado por mais informações. Tempo estimado para concluir esta tarefa: 15-20 minutos.

Funções necessárias: administrador, sn_si.analyst

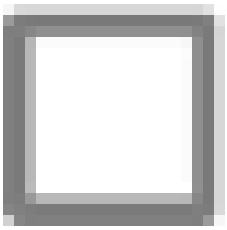
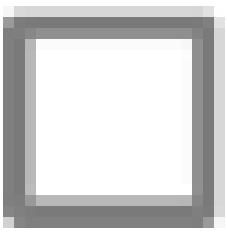
Check-list para dispositivos móveis

Item	Descrição
	Como um usuário com a função de administrador, verifique se você tem Resposta a incidentes de segurança aplicação principal instalada em um ServiceNow AI Platform instância. . ServiceNow AI Platform instância que você exibe em seu dispositivo móvel. **Nota:** . Resposta a incidentes de segurança aplicação principal e ServiceNow AI Platform a instância deve ser da mesma versão da família. 1. Para verificar se a aplicação principal está instalada em sua instância, navegue até **Plug-ins** E pesquise Resposta a incidentes de segurança. 2. . Resposta a incidentes de segurança a aplicação principal ainda não está instalada, clique em **Instalar** para instalá-lo. Para obter mais informações sobre como instalar o. Resposta a incidentes de segurança aplicação principal, consulte Instalar e configurar Resposta a incidentes de segurança. . Resposta a incidentes de segurança A aplicação principal não está visível em Plug-ins. Para obter mais informações sobre como instalar aplicações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
	principais e direitos a aplicações, consulte Operações de segurança e o ServiceNow Store.
	Como um usuário com a função de administrador, verifique se você tem Aplicação Resposta a incidentes de segurança para celular instalado no ServiceNow AI Platform instância que você deseja exibir em seu dispositivo móvel. **Nota:** . Aplicação Resposta a incidentes de segurança para celular e o. ServiceNow AI Platform a instância deve ser da mesma versão da família. Baixe e instale o. Aplicação Resposta a incidentes de segurança para celular em ServiceNow Store em seu ServiceNow AI Platform instância. Ao instalar o. Aplicação Resposta a incidentes de segurança para celular suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também estão instaladas. Para verificar se essas dependências estão instaladas: **1.** Navegue até **Plug-ins** . **2.** PESQUISE os IDs do plug-in (com.glide.sg e com.glide.sg.agent_native_client). **3.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para Aplicação Resposta a incidentes de segurança para celular. Para obter mais informações sobre como instalar aplicações e direitos a aplicações, consulte Operações de segurança e o ServiceNow Store.
	Como um usuário com ServiceNow AI Platform função de administrador, verifique se você atribuiu aos usuários móveis as funções necessárias em seu ServiceNow AI Platform instância. **1.** Para exibir as funções atribuídas a um usuário, navegue até **Usuários e Grupos** > **Usuários**. **2.** Selecione o nome de usuário seguido pela lista relacionada Funções. Todas as funções atribuídas a este usuário são exibidas. **3.** Verifique se um usuário foi atribuído ou atribua a um usuário a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar incidentes de segurança. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **4.** Verifique se um usuário foi atribuído ou atribua a um usuário a função de analista de segurança (sn_si.analyst). Usuários com a função sn_si.analyst podem ler e editar registros de incidentes de segurança. Esta função é adicionada automaticamente quando você atribui a função itil. **5.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
	Nota: Se você tiver um grande número de usuários para o aplicativo para celular, como alternativa, poderá atribuir a função sn_si.analyst a um grupo. Cada usuário adicionado ao grupo herda esta função. Para obter mais informações sobre analistas de segurança, consulte Atribuição de analistas de segurança. Para obter mais informações sobre usuários e como atribuir funções a usuários e grupos, consulte Administração de usuários .
☐	Como um usuário com a função sn_si.analyst, baixe o mais recente ServiceNow® Aplicativo Agent em seu dispositivo móvel. A versão mais atual do app Agent está disponível na Apple iOS App Store e Google Play Store. 
☐	Como um usuário com a função sn_si.analyst, verifique se as notificações estão habilitadas em seu dispositivo móvel e em seu ServiceNow AI Platform instância. As notificações informam quando incidentes de segurança críticos são atribuídos a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no Aplicação Resposta a incidentes de segurança para celular para navegar diretamente até o incidente de segurança. Para habilitar notificações no seu ServiceNow AI Platform para que eles sejam exibidos em seu dispositivo móvel, siga estas etapas. **1.** Verifique se você baixou e instalou o. Aplicação Resposta a incidentes de segurança para celular em seu ServiceNow AI Platform instância. **2.** Em Configurações do sistema em seu ServiceNow AI Platform Em Notificações, verifique se você habilitou **Aplicação para celular da ServiceNow** . Para obter mais informações sobre como configurar notificações, consulte Definir preferências de notificação do usuário na IU principal .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
	ServiceNow AI Platform as notificações também são exibidas na tela mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Você configurou com sucesso seu dispositivo móvel e o. ServiceNow AI Platform para Aplicação Resposta a incidentes de segurança para celular. A próxima etapa é fazer login em seu ServiceNow AI Platform instância com seu dispositivo móvel.

Faça login no Aplicação Resposta a incidentes de segurança para celular

Abra o aplicativo Security Incident Response Mobile e adicione um ServiceNow AI Platform® Instância com Resposta de incidente de segurança para seu dispositivo móvel.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

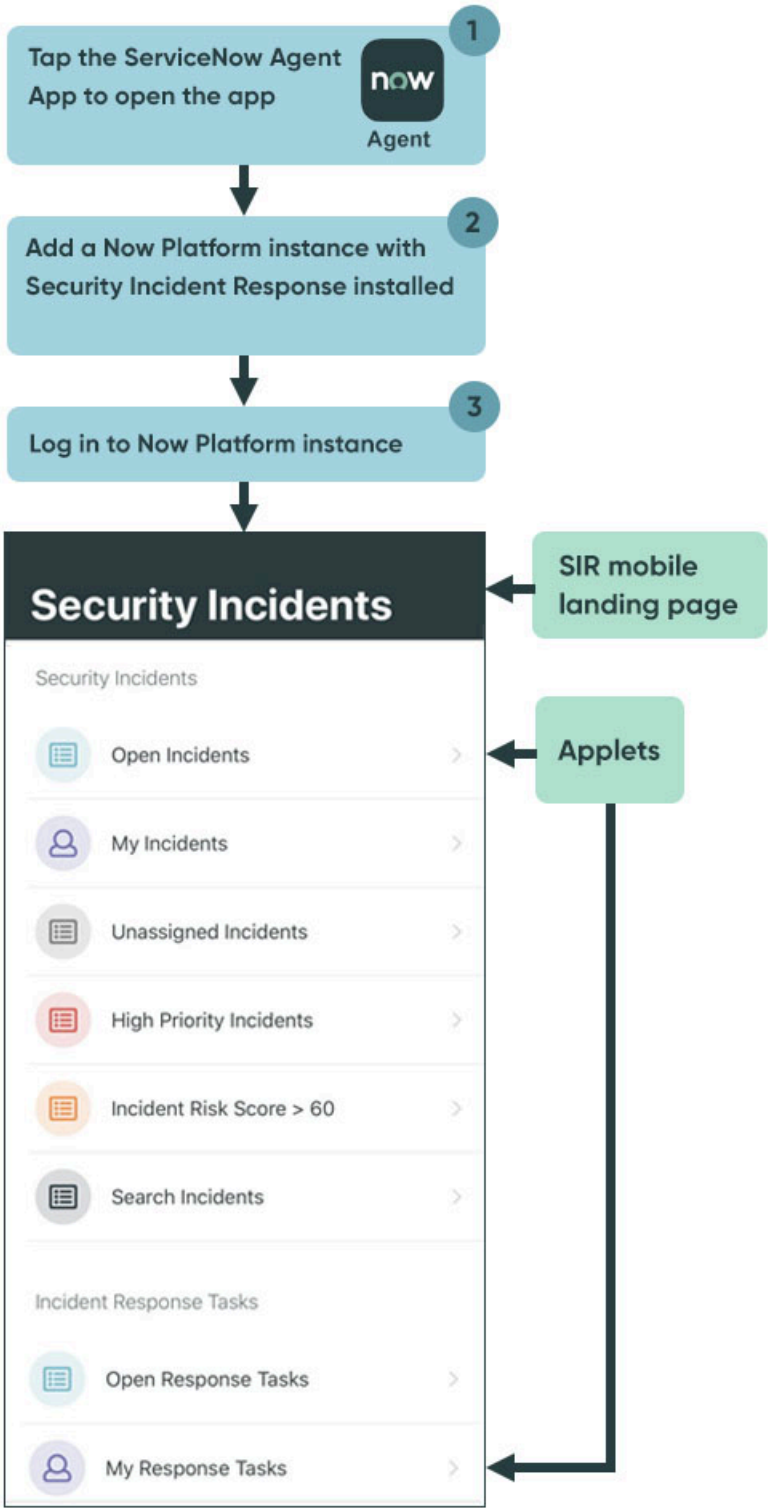
Tempo para concluir esta tarefa: 5-10 minutos.

Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para Aplicação Resposta a incidentes de segurança para celular.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

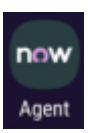
Aplicação Resposta a incidentes de segurança para celular



Tradução automática

Procedimento

1. Em seu dispositivo móvel, toque em **Agente da ServiceNow** para abri-lo.



© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você ainda não estiver conectado a um ServiceNow AI Platform, a tela Instâncias é exibida.

2. . ServiceNow AI Platform instância com Resposta a incidentes de segurança a aplicação principal ainda não foi adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

   a. Na tela Instâncias exibida, toque em  .
   É exibida uma tela solicitando que você insira e salve um endereço de um ServiceNow AI Platform instância.

   b. Preencha os campos.

Campo	Descrição
Insira o endereço da instância ou leia um código QR.	Escolha um para continuar: ▪ . .service-now.com insira o nome do seu ServiceNow AI Platform instância, por exemplo, sirmobileny . ▪ Insira um endereço. Este endereço é o URL do seu ServiceNow AI Platform instância que você deseja exibir em seu dispositivo móvel, por exemplo, https://sirmobileny.service-now.com. ▪ Digitalize um código QR.
(Opcional) Insira o apelido	Insira um apelido para esta instância. Se você tiver várias instâncias adicionadas ao dispositivo, os apelidos poderão ajudá-lo a localizar rapidamente um ServiceNow AI Platform instância.

   c. Toque em **Salvar e fazer login**.

3. Em ServiceNow Tela de login exibida, insira o Nome de usuário e a Senha do ServiceNow AI Platform instância que você deseja adicionar e tocar **Login** .
   A tela principal Incidentes de segurança é exibida. Você fez login com sucesso no Aplicação Resposta a incidentes de segurança para celular.

4. Depois de fazer login, verifique se as notificações estão habilitadas no Aplicação Resposta a incidentes de segurança para celular.

   a. Na tela principal na parte inferior, toque em **Notificação** .

   b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
   Notificações do ServiceNow AI Platform São exibidos na tela Notificações em Aplicação Resposta a incidentes de segurança para celular.

5. Depois de fazer login em uma instância no seu dispositivo móvel, ele será o padrão ServiceNow AI Platform instância no dispositivo.
   Se você quiser exibir outro ServiceNow AI Platform no dispositivo, você deve fazer logout da instância padrão. Para fazer logout:

   a. Toque no ícone de configurações.

   b. Toque em **Logout** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tela Instâncias é exibida com qualquer ServiceNow AI Platform instâncias que você adicionou ao dispositivo móvel.

c. **Opcional:** Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Se a tela Instâncias do Aplicação Resposta a incidentes de segurança para celular não é exibido depois que você toca em **Agente da ServiceNow** em seu dispositivo, verifique se **Agente da ServiceNow** é permitido como um app confiável no seu dispositivo. Para permitir o acesso como um app confiável, navegue até as configurações e gestão geral de dispositivos em seu dispositivo e toque na opção (Aplicativo de confiança etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois que você inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha do ServiceNow AI Platform a instância está correta.

Se você tiver problemas para exibir a tela principal, verifique sua conexão de rede.

Se você não puder exibir a tela Instâncias depois de tocar em **Agente da ServiceNow** , tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app da Apple iOS App Store ou Google Play Store e tente reinstalá-lo.

Exiba, edite e atribua incidentes de segurança em aberto com Aplicação Resposta a incidentes de segurança para celular

Como analista de incidentes de segurança, exiba, edite e atribua em aberto Resposta a incidentes de segurança(SIR incidentes de segurança do seu dispositivo móvel. Exiba listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança em aberto a si mesmo ou reatribua-o. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

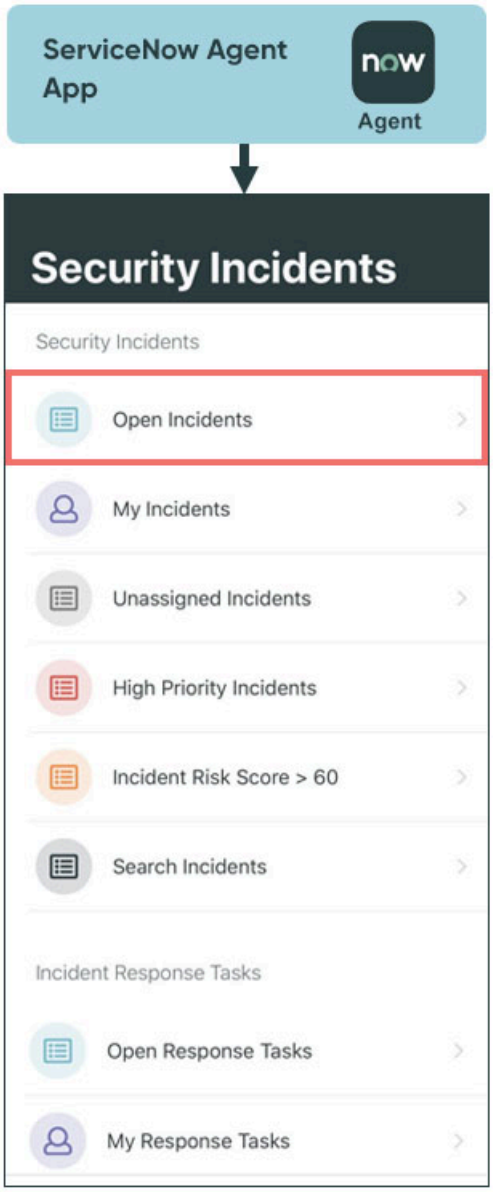
Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a página principal Incidentes de segurança exibida, toque em **Incidentes em aberto** .

Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

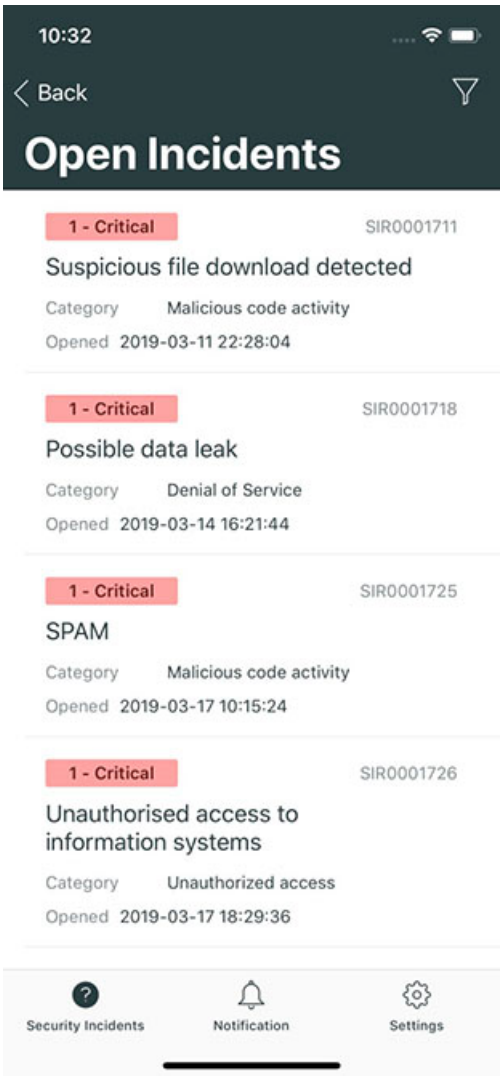
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes em aberto é exibida com uma lista de registros de incidentes de segurança em aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Para atribuir um incidente a si mesmo ou reatribuí-lo diretamente na lista de incidentes de segurança em aberto, deslize para a esquerda em um registro para abrir o menu.

5. Escolha um no menu exibido para continuar.

Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a você mesmo. Se o incidente de segurança já estiver atribuído a você, essa opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição:

Tradução automática

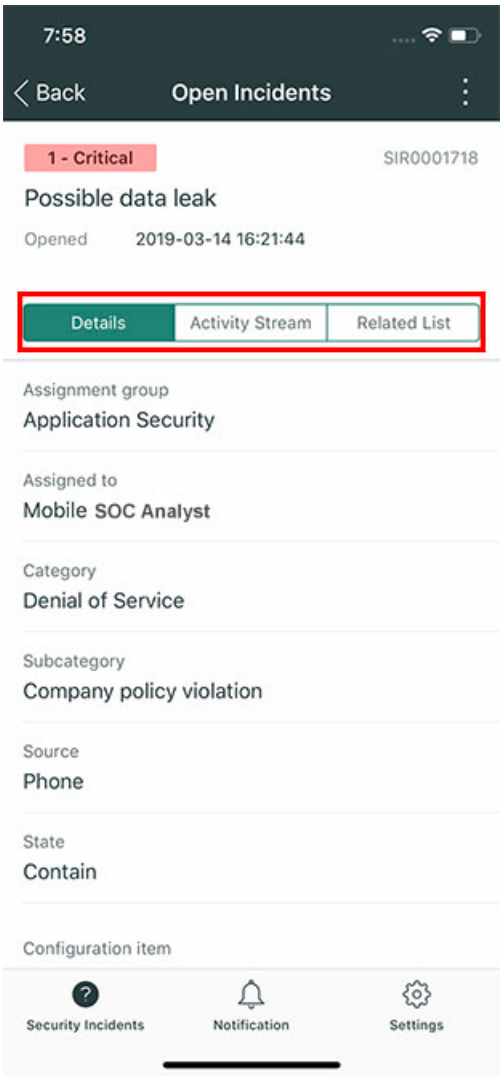
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Toque em **Grupo de atribuição**. **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança em aberto e ver mais registros associados e listas relacionadas, com a tela Incidentes em aberto exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar in–cidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como al–ternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir o incidente, toque em **Rea tribuir** ou **Atribuir a mim** . Siga as instru–ções descritas na tabela anterior. Depois de concluir suas edições, toque no ícone enviar (ou **Enviar** para salvar suas mudanças e atualizar o incidente de segu–rança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades seleciona–da, revise a trilha de auditoria de anota–ções de trabalho, atividades e comentários

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	adicionais do registro. Toque no ícone de adição ( para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens de todas as listas relacionadas do incidente de segurança que estão preenchidas. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidos, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Incidentes de segurança para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notificações do ServiceNow AI Platform e o. Aplicação Resposta a incidentes de segurança para celular. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Tradução automática

Exiba, edite e reatribua incidentes de segurança atribuídos a você com Aplicação Resposta a incidentes de segurança para celular

Como analista de incidentes de segurança, exiba, edite e reatribua Resposta a incidentes de segurança(SIR incidentes atribuídos a você. Exiba listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

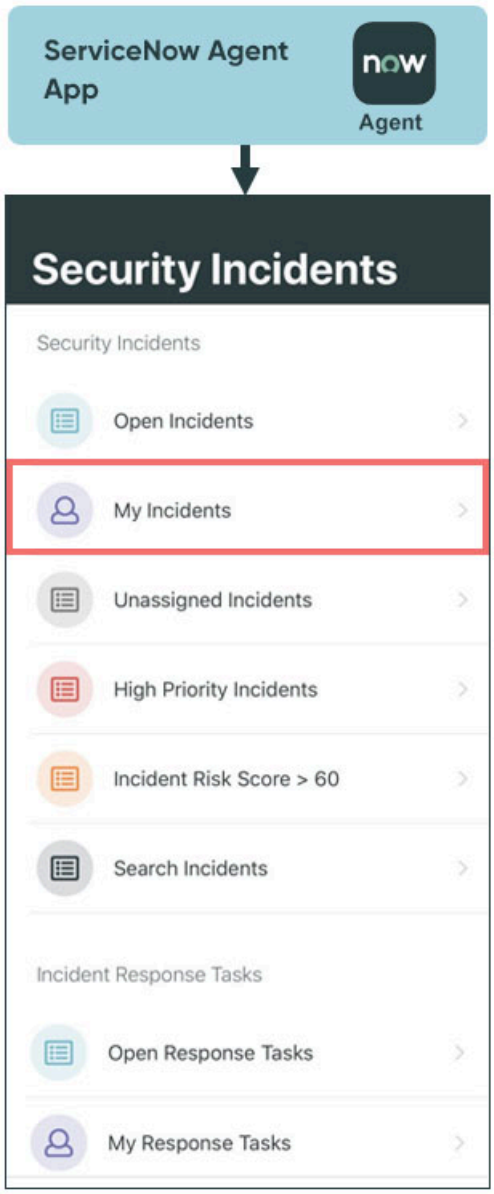
Reatribua um incidente de segurança em aberto para outro analista em seu grupo na lista de registros. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Meus incidentes** .

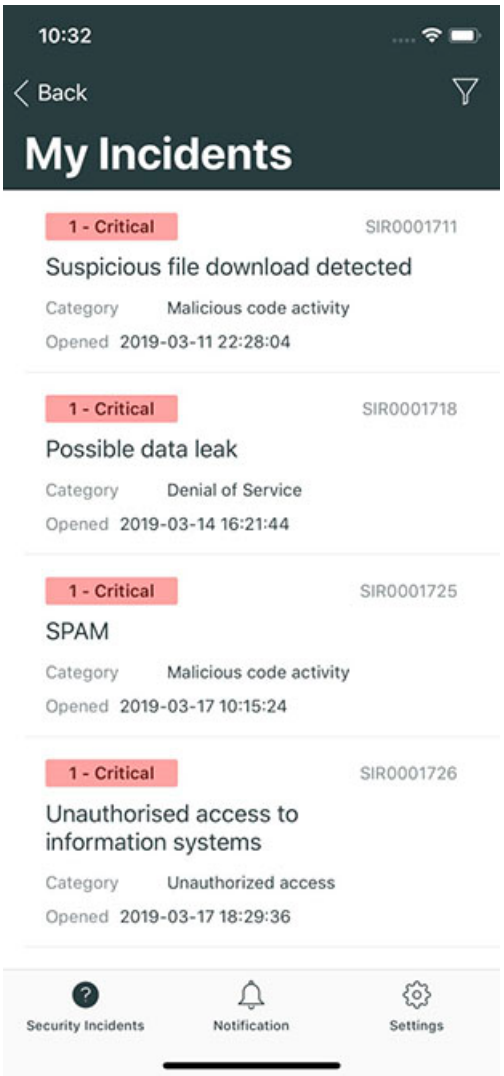
   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



   A tela Meus incidentes é exibida com uma lista de registros de incidentes de segurança em aberto atribuídos a você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



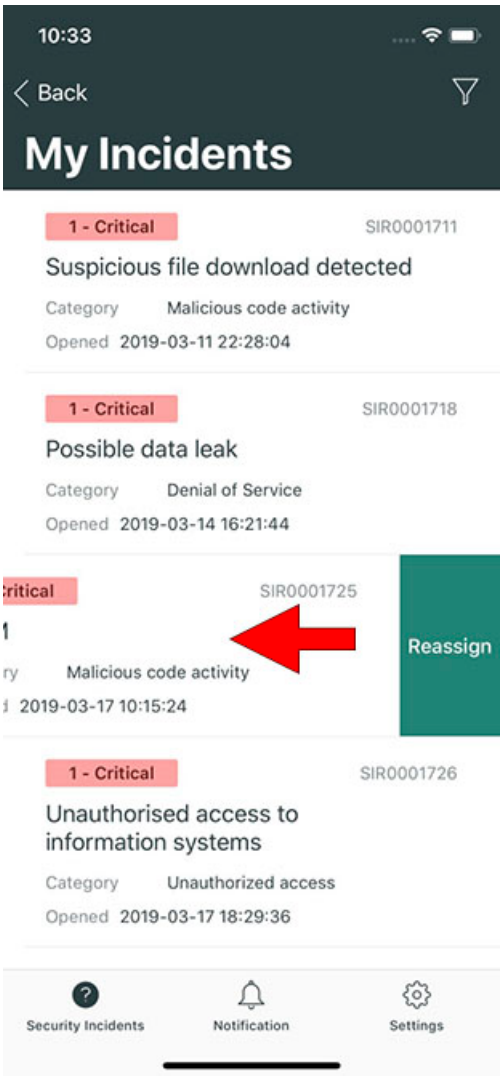
3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Para reatribuir um incidente diretamente da lista, com a lista de registros de incidentes de segurança em aberto exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

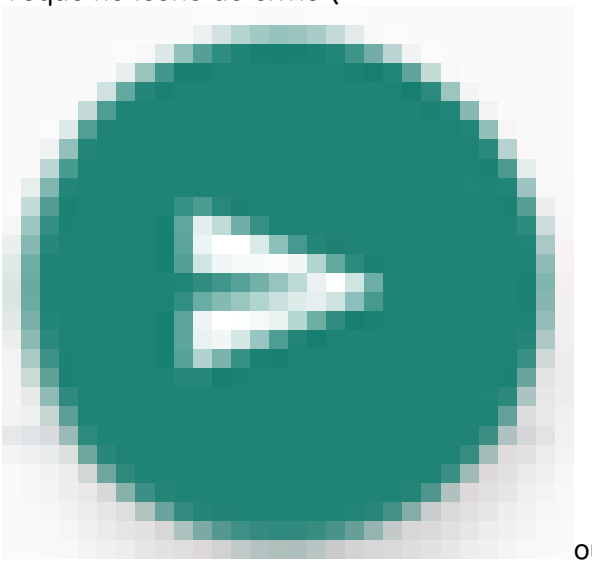


5. Edite os campos Grupo de atribuição ou Atribuído a no menu exibido.

Opção	Descrição
Reatribuir	Para reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa.

Tradução automática

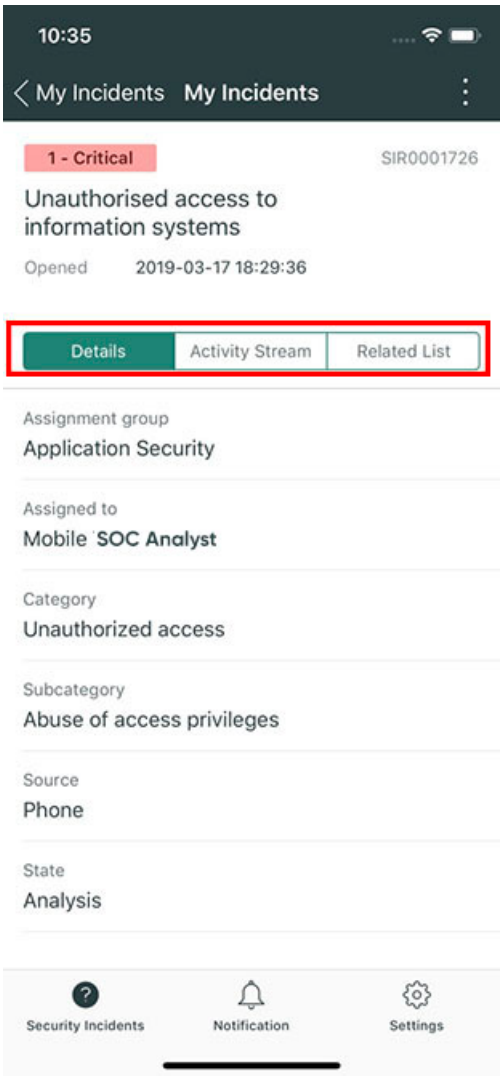
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Toque no ícone de envio () ou **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes do registro de incidente de segurança em aberto, com a tela Meus incidentes exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

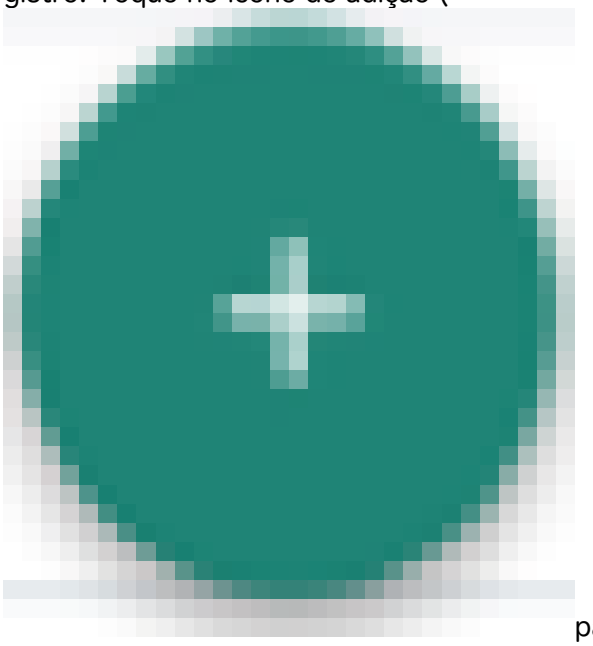
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir o incidente, toque em **Reatribuir** . Siga as instruções descritas na tabela anterior. Depois de concluir suas edições, toque no ícone enviar (

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	 ou **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição () para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em todas as listas relacionadas preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relaciona–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	da. Nas listas de itens exibidos, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas asso–ciadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Incidentes de segurança para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notifi–cações do ServiceNow AI Platform e o. Apli-cação Resposta a incidentes de segurança para ce-lular. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Exiba, edite e atribua incidentes de segurança não atribuídos com Aplicação Resposta a incidentes de segurança para celular

Em seu dispositivo móvel, exiba, edite e atribua não atribuídos Resposta a incidentes de segurança(SIR incidentes. Exiba listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança aberto e não atribuído a você ou a outro analista em seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

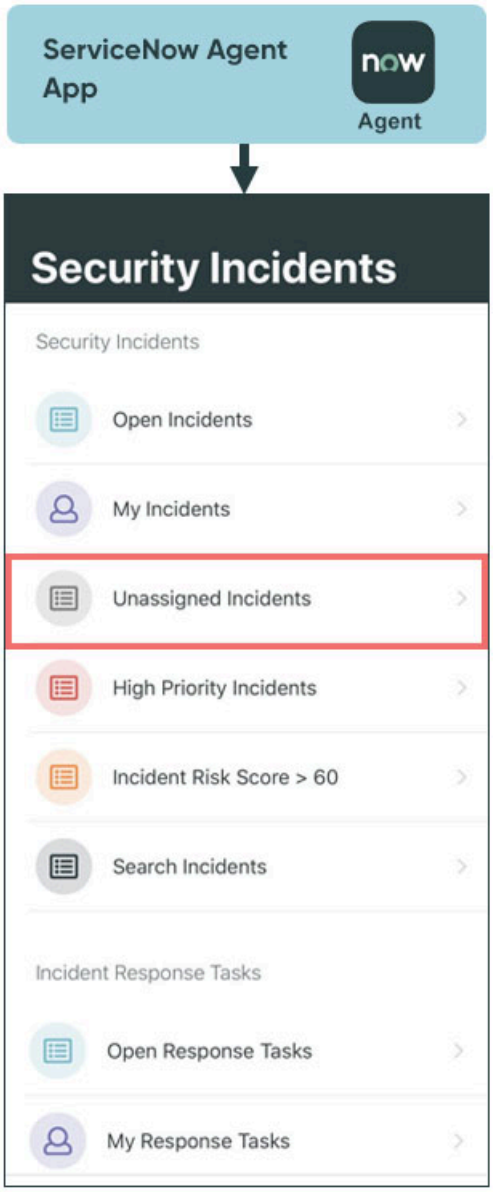
Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Incidentes não atribuídos** .

   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

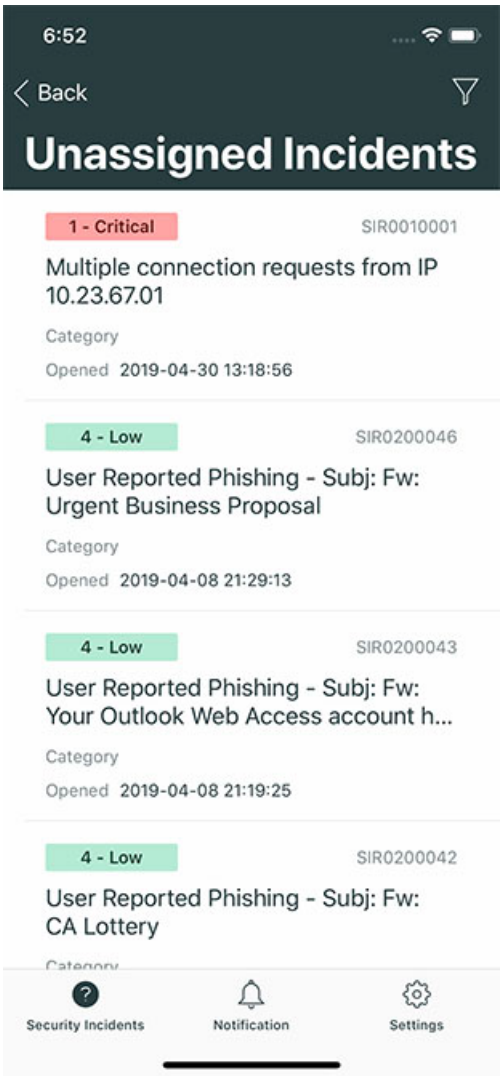
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes não atribuídos é exibida com uma lista de registros de incidentes de segurança não atribuídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



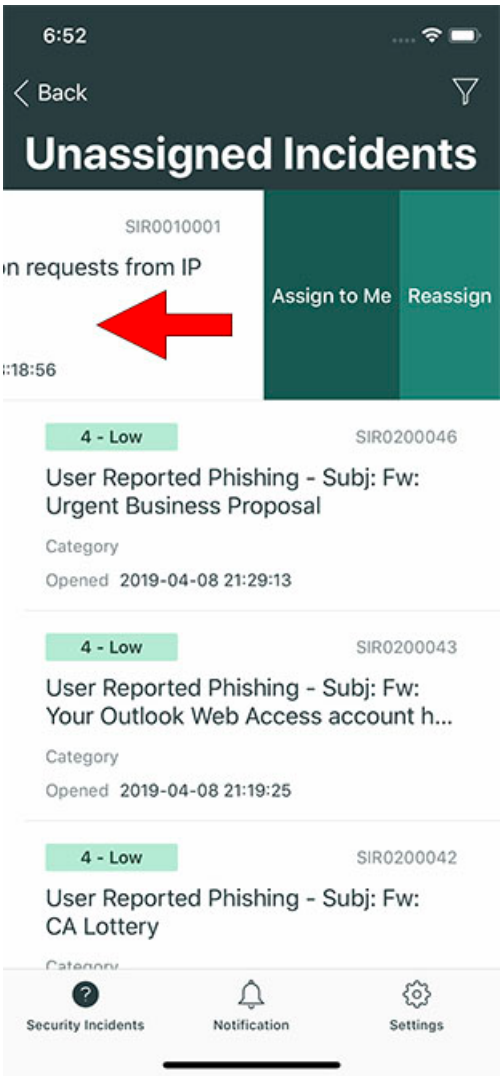
3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Para atribuir ou reatribuir um registro de incidente de segurança aberto diretamente na lista, com a lista de registros de incidentes de segurança não atribuídos em aberto exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um no menu para continuar.

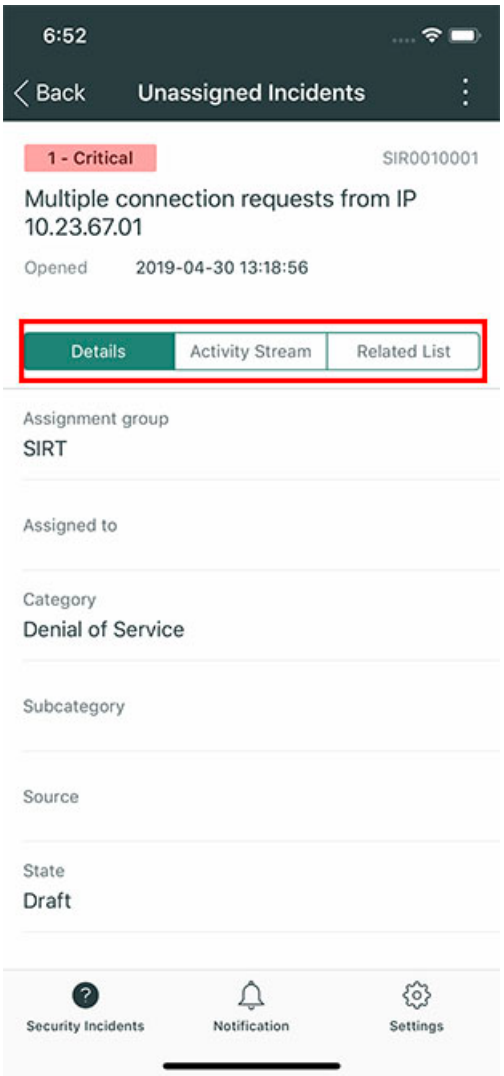
Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a você mesmo. Se o incidente de segurança já estiver atribuído a você, essa opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Toque no ícone de envio ( ) ou **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, com a tela Incidentes não atribuídos exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ○ Para atribuir ou reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim** . Siga as instruções descritas na tabela anterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Depois de concluir suas edições, toque no ícone enviar ( ou **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição ( para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em qualquer uma das listas relacionadas preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidos, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Incidentes de segurança para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notificações do ServiceNow AI Platform e o. Aplicação Resposta a incidentes de segurança para celular. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Tradução automática

Exiba, edite e atribua incidentes de alta prioridade com Aplicação Resposta a incidentes de segurança para celular

Em seu dispositivo móvel, exiba, edite e atribua alta prioridade Resposta a incidentes de segurança(SIR incidentes. Exiba listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

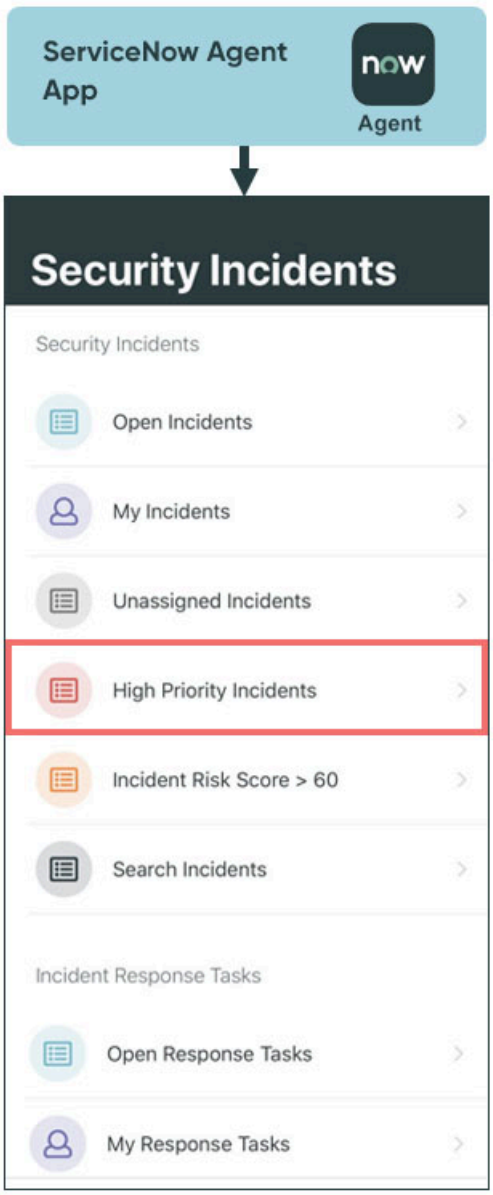
Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança crítico em aberto a você ou a outro analista em seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Incidentes de alta prioridade** .

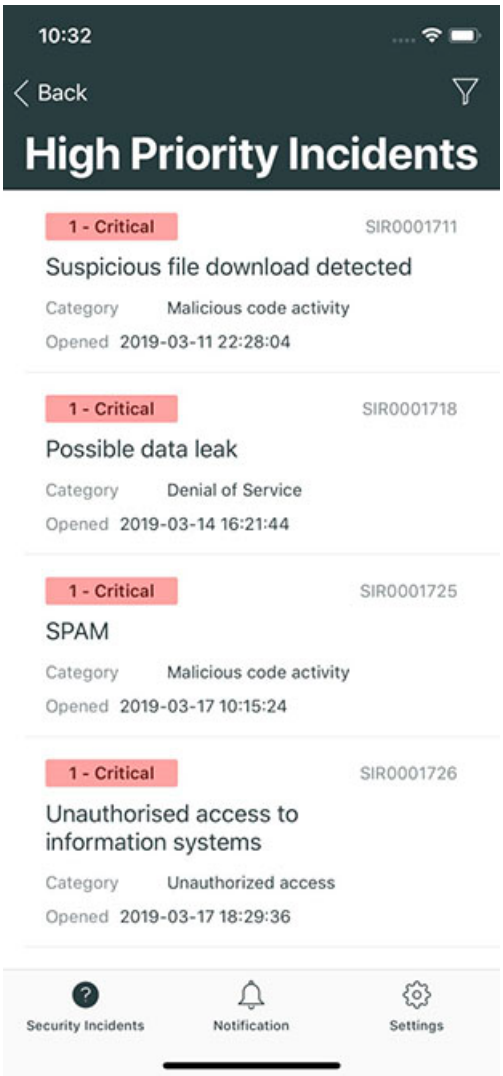
   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



   A tela Incidentes de alta prioridade é exibida com uma lista de incidentes de segurança críticos (alta prioridade).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



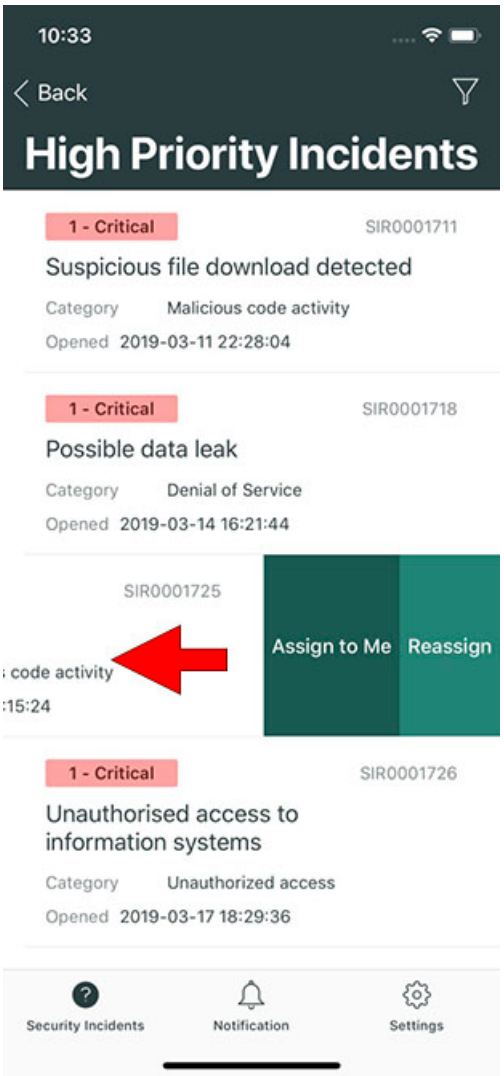
3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Com a lista de registros de incidentes de segurança de alta prioridade abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um para continuar.

Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a você mesmo. Se o incidente de segurança já estiver atribuído a você, essa opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição** **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** . **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa.

Tradução automática

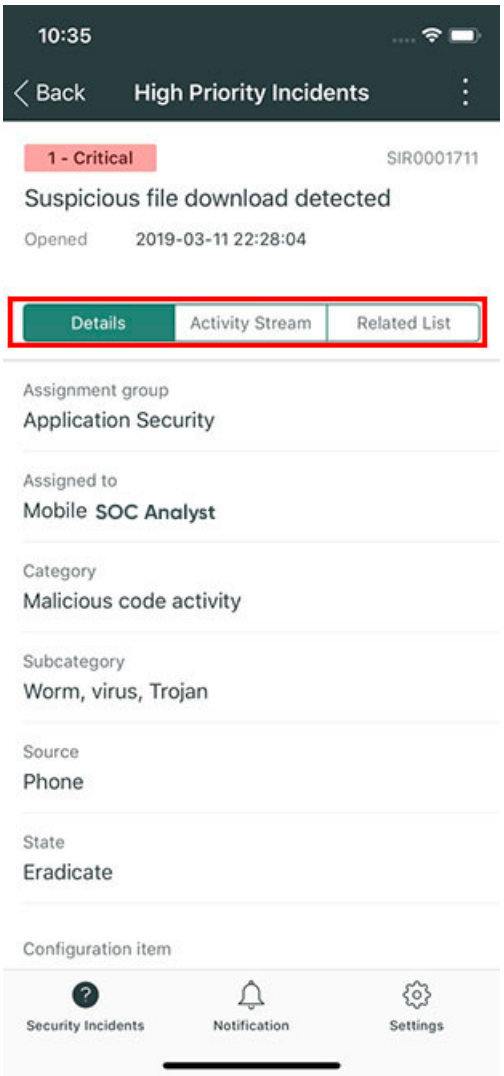
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Toque no ícone de envio () ou **Enviar** para salvar e enviar suas mudanças.

6. Para exibir os detalhes de um registro de incidente de segurança em aberto e ver mais registros associados e listas relacionadas, com a tela Incidentes de alta prioridade exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

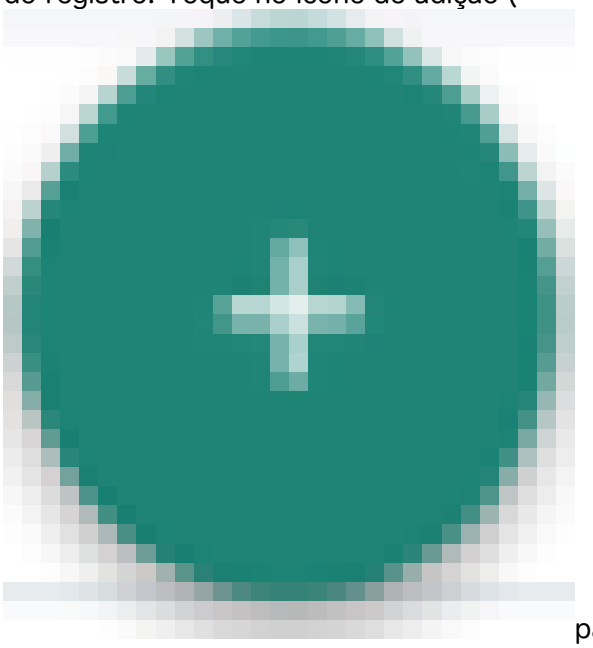
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim** . Siga as instruções descritas na tabela anterior. Depois de concluir suas edições, toque no ícone enviar (

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	 ou **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Atividade selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição () para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em qualquer uma das listas relacionadas preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidos, toque em um item para continuar a exibir os fluxos de atividades e as listas relacio-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	nadas associadas ao incidente de seguran–ça primário.
Toque em um ícone de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Incidentes de segurança para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notifi–cações do ServiceNow AI Platform e o. Apli-cação Resposta a incidentes de segurança para ce-lular. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Exiba, edite e atribua incidentes de segurança com pontuação de risco maior que 60 com Aplicação Resposta a incidentes de segurança para celular

No seu dispositivo móvel, exiba e edite Resposta a incidentes de segurança(SIR incidentes com um valor no campo pontuação de risco maior que 60. Exiba listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança em aberto que tenha uma pontuação de risco maior que 60 para você ou para outro analista em seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

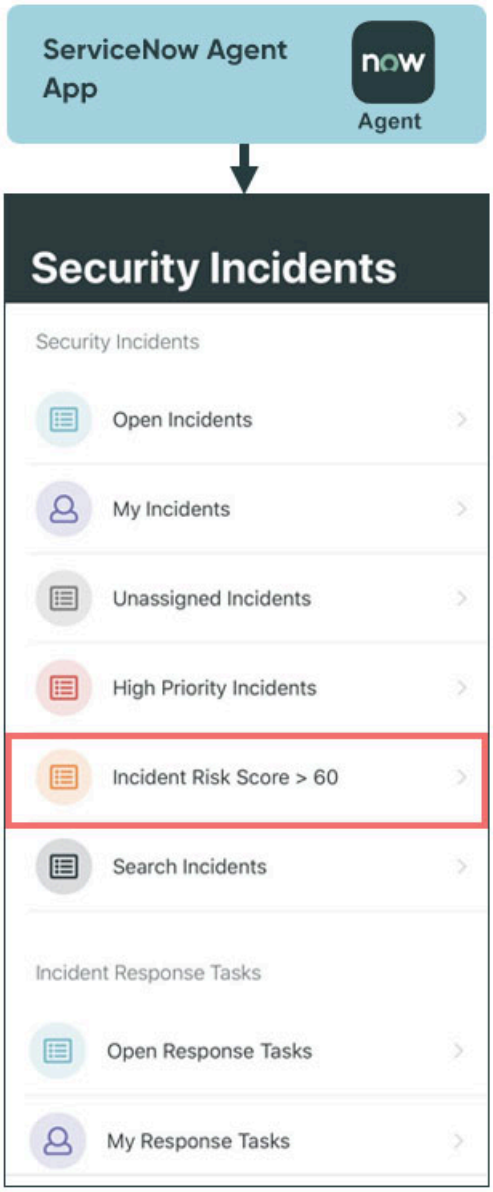
Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Pontuação de risco > 60** .

   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

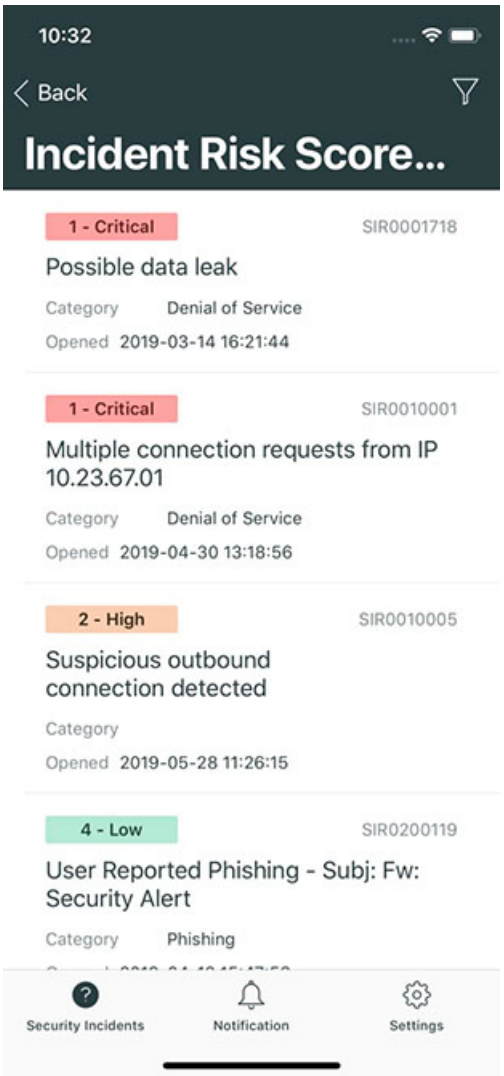
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Pontuação de risco do incidente é exibida com uma lista de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



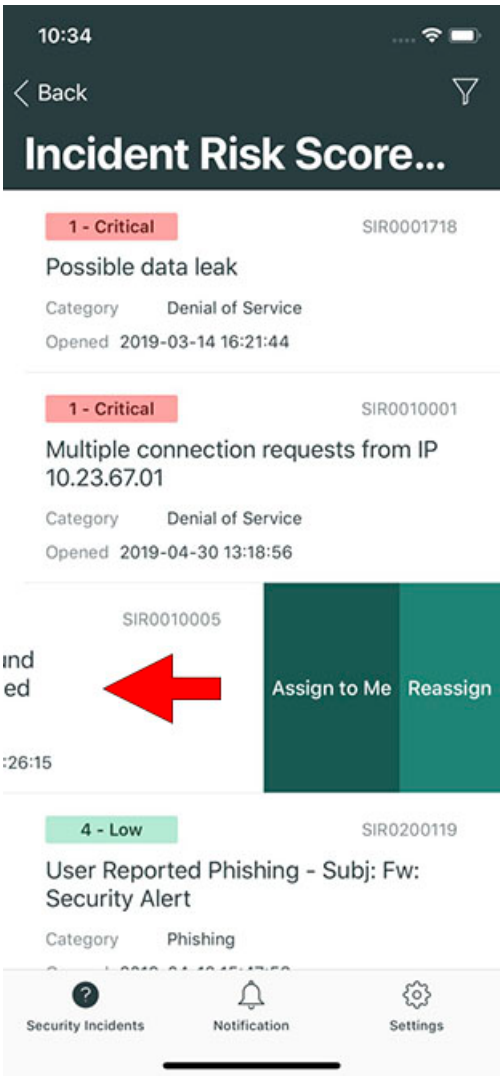
3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Para atribuir um incidente de segurança a si mesmo ou reatribuí-lo diretamente na lista de registros de incidentes de segurança abertos exibidos, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um para continuar.

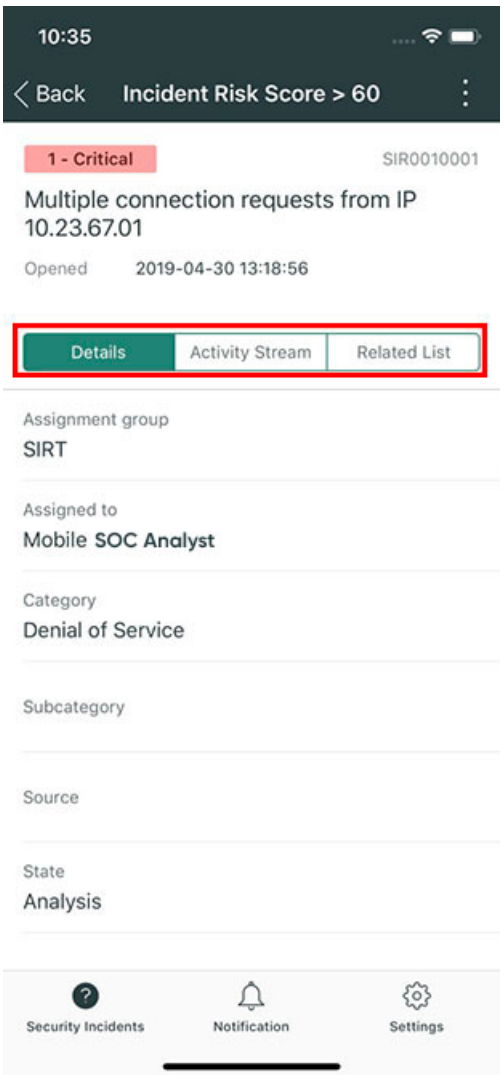
Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a você mesmo. Se o incidente de segurança já estiver atribuído a você, essa opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** e. **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança em aberto e ver mais registros associados e listas relacionadas, com a tela Pontuação de risco de incidente exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.



Opção	Descrição
Toque no ícone de menu no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como al–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir o incidente, toque em **Rea tribuir** ou **Atribuir a mim** . Siga as instru– ções descritas na tabela anterior. Depois de concluir suas edições, toque no ícone enviar (ou **Enviar** para salvar suas mudanças e atualizar o incidente de segu– rança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades seleciona– da, revise a trilha de auditoria de anota– ções de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição (para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada seleciona– da, exiba os itens em qualquer uma das lis– tas relacionadas preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lis– ta relacionada. Nas listas de itens exibidos, toque em um item para continuar a exibir os fluxos de atividades e as listas relacio– nadas associadas ao incidente de seguran– ça primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Toque no ícone Incidentes de segurança para retornar à tela principal. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notifi– cações do ServiceNow AI Platform e o. Apli- cação Resposta a incidentes de segurança para ce- lular. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform no seu dispositivo. ▪ Logout do atual ServiceNow AI Platform instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular

Pesquisar Resposta a incidentes de segurança(SIR incidentes de segurança em um ServiceNow AI Platform® instância. Somente incidentes que correspondem aos critérios de pesquisa específicos inseridos são exibidos.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5-10 minutos.

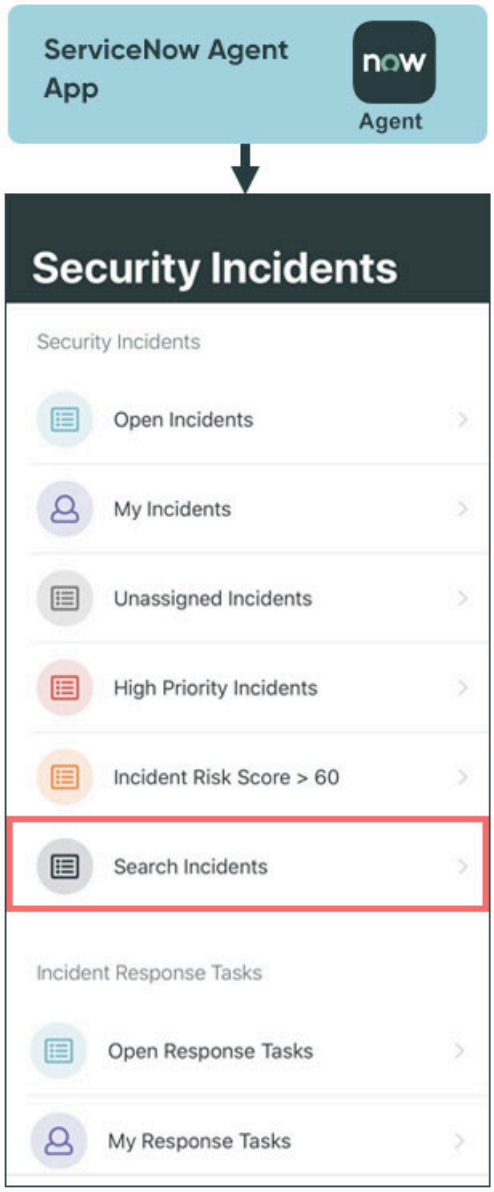
Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Incidentes de pesquisa** .

   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para limitar o número de resultados de pesquisa retornados, você pode preferir preencher o máximo de campos possíveis no formulário.
Para adicionar critérios de pesquisa, consulte a tabela a seguir. Siga as instruções após a tabela para editar os critérios de pesquisa existentes, limpar os critérios de pesquisa ou enviar uma pesquisa.

Toque neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e inserir em iOS dispositivos
Número	Insira um valor alfanumérico para um incidente de segurança, por exemplo, SIR0010004 . Este número é exibido no canto superior direito do incidente de segurança. O recurso pesquisa cadeias de caracteres numéricas e cadeias de caracteres	Insira um valor alfanumérico para um incidente de segurança, por exemplo, SIR0010004 . Este número é exibido no canto superior direito do incidente de segurança. O recurso pesquisa cadeias de caracteres numéricas e cadeias de caracteres

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Toque neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e inserir em iOS dispositivos
	numéricas parciais. Para pesquisas mais refinadas, insira mais dígitos. Curingas (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	numéricas parciais. Para pesquisas mais refinadas, insira mais dígitos. Curingas (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou **Pesquisa** para enviar uma pesquisa.
Descrição Resumida	Insira texto no campo, por exemplo, malware . O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres de texto parciais no campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Curingas (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	Insira texto no campo, por exemplo, malware . O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres de texto parciais no campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Curingas (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou **Pesquisa** para enviar uma pesquisa.
Prioridade	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar incidentes.
Categoria	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar incidentes.
Estado	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** Para retornar à tela Pesquisar incidentes.
Atribuição a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Toque neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e inserir em iOS dispositivos
	Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .	Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** .

Para Android Dispositivos, com a tela Pesquisar incidentes exibida e todos os seus critérios inseridos, escolha um para continuar.

Opção	Descrição
Limpe ou modifique os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios inseridos, com a tela Pesquisar incidentes exibida, toque na seta para voltar para limpar todos os campos e retornar à tela principal Incidentes de segurança. A pesquisa não é enviada e os critérios de pesquisa são limpos. Como alternativa, para editar um campo: ○ Com a tela Pesquisar incidentes exibida, toque em um campo com critérios de pesquisa para expandi-lo. ○ Toque em um item para desmarcá-lo. Toque em **Todos** para selecionar todos os itens. Toque em **Todos** novamente para limpar todos os itens. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** . ○ Toque no ícone de marca de seleção para salvar as mudanças e retornar à tela Pesquisar incidentes.
Envie uma pesquisa	Com a tela Pesquisar incidentes exibida com os critérios de pesquisa inseridos, toque no ícone enviar ( ). Os incidentes de segurança que correspondem aos seus critérios de pesquisa são exibidos. Após a conclusão da pesquisa, os critérios de pesquisa não são salvos.

4. Para iOS Dispositivos, com a tela Pesquisar incidentes exibida, escolha um para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Limpe ou modifique os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios e retornar à tela principal, toque no ícone Fechar (X). Os critérios de pesquisa inseridos não são salvos. Como alternativa, para editar um campo: ○ Com a tela Pesquisar incidentes exibida, toque em um campo com critérios de pesquisa para expandi-lo. ○ Toque em um item na lista para desmarcá-lo ou toque em **Limpar tudo** . Para limpar um valor para os campos Grupo de atribuição e Atribuído a, para nenhuma entrada, selecione **Nenhum** . ○ Toque em **Concluído** Para salvar as mudanças e retornar à tela Pesquisar incidentes.
Envie uma pesquisa	Com a tela Pesquisar incidentes exibida com os critérios de pesquisa inseridos, toque em **Pesquisa** . Os incidentes de segurança que correspondem aos seus critérios de pesquisa são exibidos. Após a conclusão da pesquisa, os critérios de pesquisa não são salvos.

5. **Opcional:** Se sua pesquisa retornar vários registros, você poderá Filtrar registros com Aplicação Resposta a incidentes de segurança para celular para refinar os resultados da pesquisa.

Exiba, edite e atribua tarefas de resposta em aberto com Aplicação Resposta a incidentes de segurança para celular

Exiba, edite e atribua tarefas de resposta em aberto. Suas mudanças são salvas na Tarefa de resposta do incidente de segurança do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua uma tarefa de resposta aberta e não atribuída a você ou a outro analista em seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5-10 minutos.

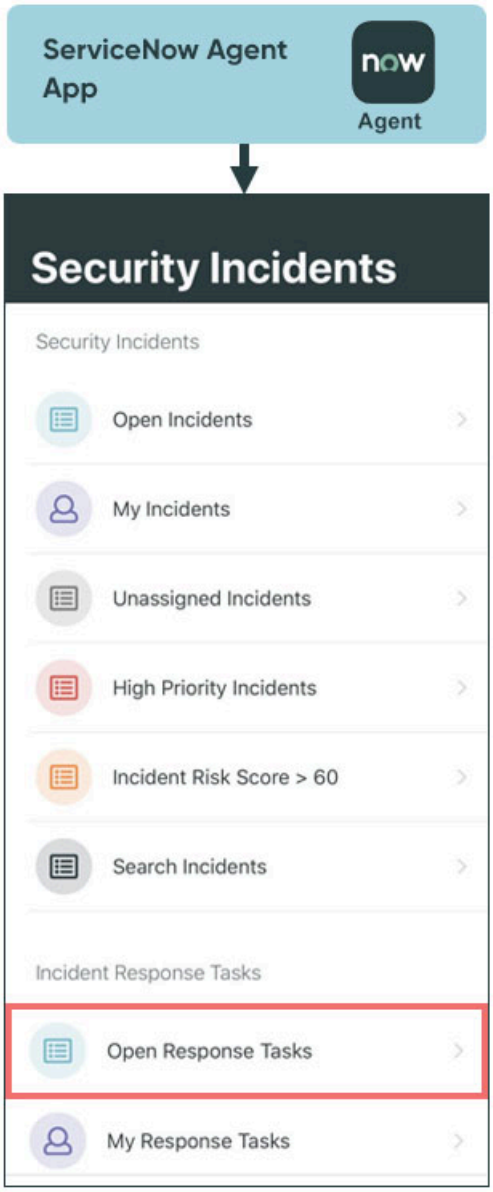
Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Tarefas de resposta em aberto** .

   Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

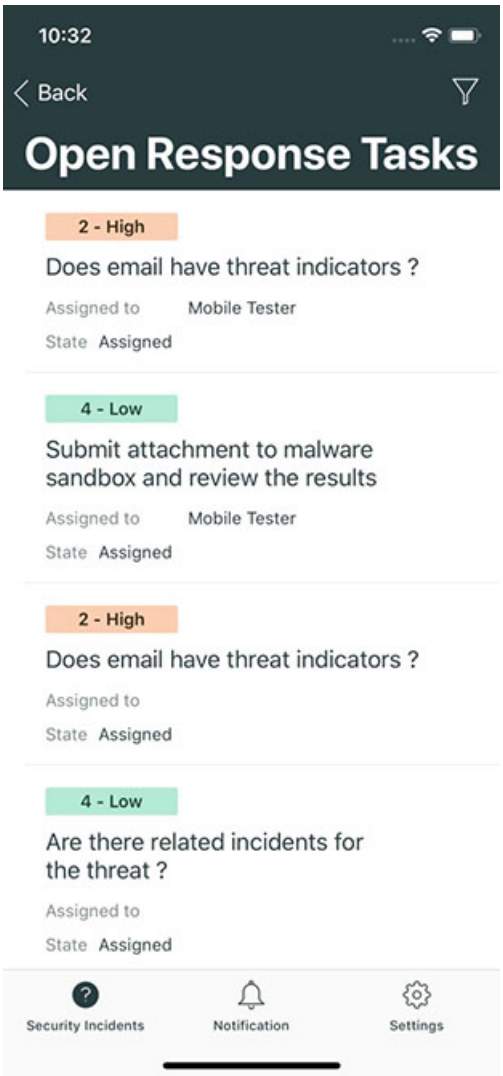
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Tarefas de resposta em aberto é exibida com uma lista de tarefas em aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

4. Com a lista de tarefas de resposta em aberto exibida, para atribuir ou reatribuir diretamente da lista, deslize para a esquerda em um registro para abrir o menu.

5. Escolha um para continuar.

Opção	Descrição
Atribuir a Mim	Atribua a tarefa de resposta a você mesmo. Se a tarefa já estiver atribuída a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição:

Tradução automática

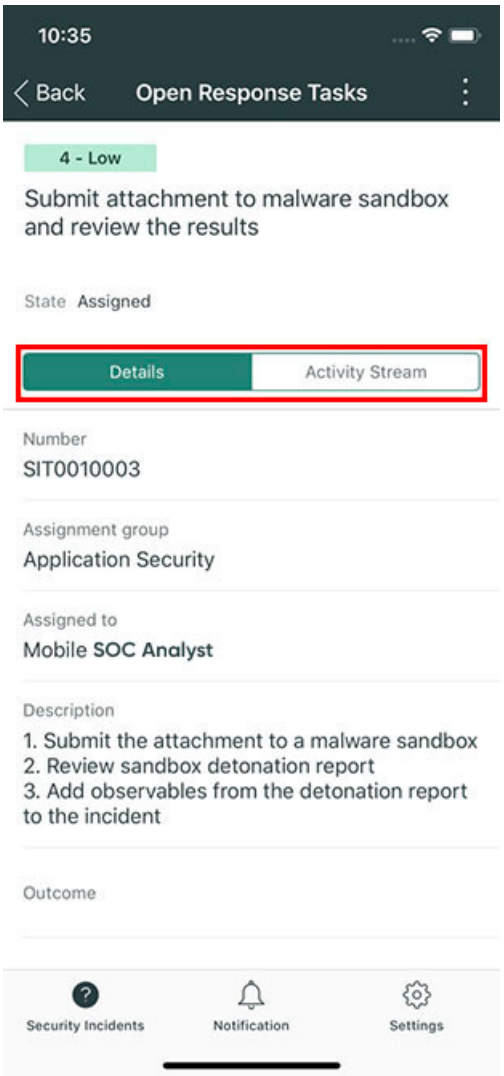
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Toque em **Grupo de atribuição** **b.** Toque em um grupo da lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir a tarefa a um membro do grupo de atribuição: **a.** Toque em **Atribuído a.** e. **b.** Toque em um nome da lista exibida ou insira o texto no campo de pesquisa. É exibida uma mensagem confirmando que o registro foi atualizado. A tarefa no incidente de segurança primário é atribuída a um novo usuário e atualizada em ServiceNow AI Platform instância. Toque no ícone de envio (ou **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de tarefa de resposta em aberto, com a tela Tarefas de resposta em aberto exibida, toque em um registro na lista.
7. Com as guias no registro da tarefa de resposta exibidas, escolha uma na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos na tarefa de resposta. Para editar campos ou atribuir a tarefa, toque no ícone de menu ( ). No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar tarefa de resposta exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir a tarefa, toque em **Reatribuir** ou **Atribuir a mim** . Depois de concluir suas edições, toque no ícone enviar (ou **Enviar** para salvar suas mudanças e atualizar o registro. A Tarefa de resposta do incidente de segurança no incidente de segurança primário em seu

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ServiceNow AI Platform a instância foi atualizada.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ○ Exiba a trilha de auditoria criada pelas anotações de trabalho no registro. Para adicionar uma anotação de trabalho ou anexar um arquivo, toque no ícone de adição ( ). ○ Toque no ícone de menu ( ) para editar ou reatribuir a tarefa.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ○ Toque em **Notificação** para exibir notificações de incidentes de segurança críticos atribuídos a você ou ao seu grupo de atribuição. ○ Toque em **Configurações** e escolha um para continuar. ▪ Exibir informações sobre ServiceNow AI Platform instância. ▪ Logout da instância atual. Para fazer logout de um ServiceNow AI Platform em seu dispositivo, com a página de detalhes exibida, toque em **Logout** .

Tradução automática

Exiba, edite e reatribua suas tarefas de resposta com Aplicação Resposta a incidentes de segurança para celular

Exiba, edite e reatribua tarefas de resposta atribuídas a você. Suas mudanças são salvas na Tarefa de resposta do incidente de segurança do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

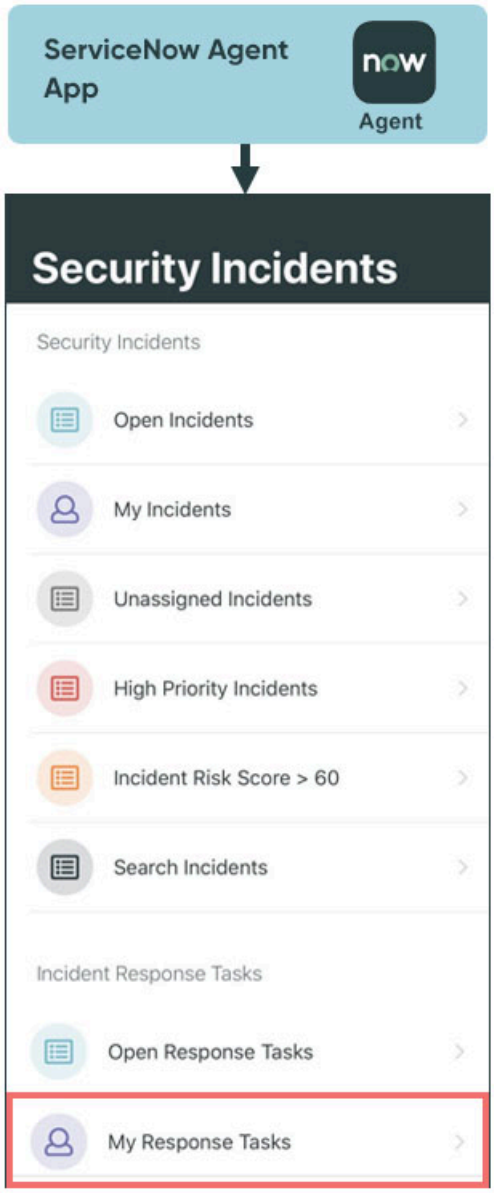
Na lista de registros, reatribua uma tarefa de resposta em aberto atribuída a você a outro analista em seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da reatribuição. Tempo para concluir esta tarefa: 5-10 minutos.

Procedimento

1. Se você não estiver conectado ao seu ServiceNow AI Platform em seu dispositivo móvel. para obter mais informações, consulte Faça login no Aplicação Resposta a incidentes de segurança para celular.
2. Com a tela principal Incidentes de segurança exibida, toque em **Minhas Tarefas de Resposta** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

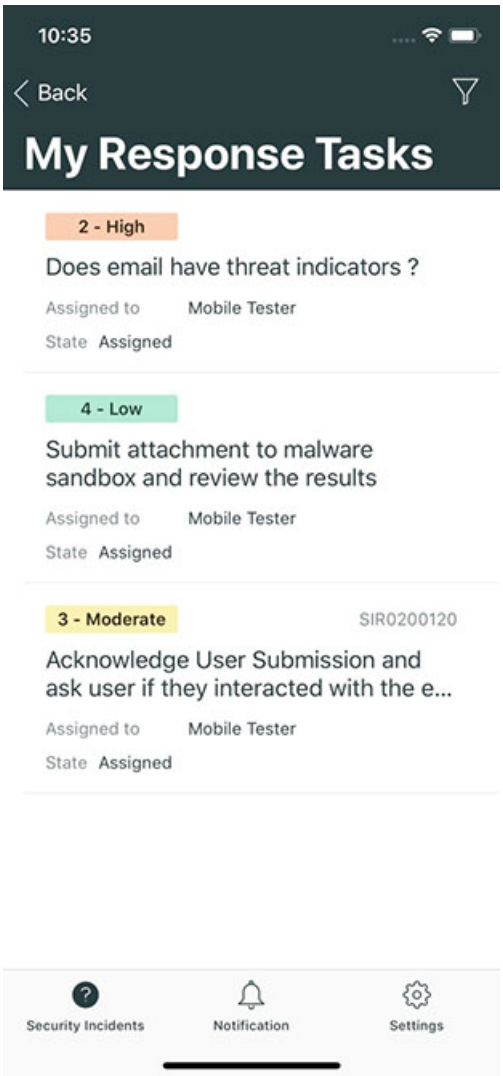
Se você sair do Aplicação Resposta a incidentes de segurança para celular Depois de fazer login, toque no aplicativo Now Agent (Executante) a qualquer momento para retornar à última tela exibida.



A tela Minhas tarefas de resposta é exibida com uma lista das tarefas de resposta atribuídas a você.

Tradução automática

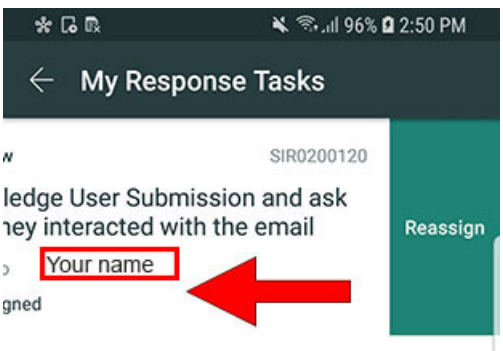
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte PESQUISE incidentes de segurança com Aplicação Resposta a incidentes de segurança para celular para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( exibido, Defina filtros para limitar o número de registros na lista. Filtrar registros em telas no aplicativo para celular funciona como filtrar com um construtor de condições no ServiceNow AI Platform.

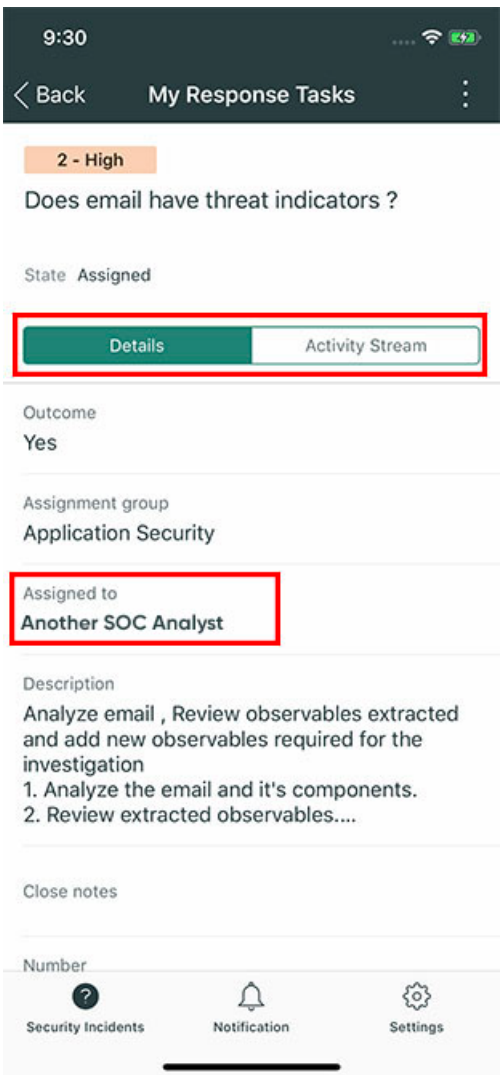
4. Para reatribuir uma tarefa diretamente da lista de registros de tarefa atribuídos a você, deslize para a esquerda em um registro para abrir o menu.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

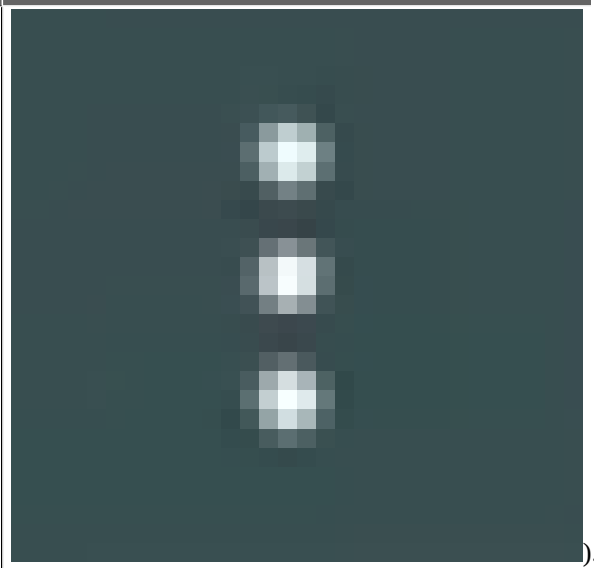
5. Toque em **Reatribuir** .
6. Na tela Atribuir tarefa de resposta a outra tela exibida, toque em um campo para expandi-lo e selecionar outro grupo ou usuário para a tarefa.
7. Toque no ícone de envio (ou **Enviar** para salvar suas mudanças e atualizar a tarefa de resposta.
É exibida uma mensagem confirmando que o registro foi atualizado. A tarefa é atribuída a um novo usuário no incidente de segurança primário e no ServiceNow AI Platform a instância foi atualizada.
8. Para exibir os detalhes de uma tarefa de resposta aberta e ver as anotações de trabalho, com a tela Minhas tarefas de resposta exibida, toque em um registro na lista.
9. Com os campos na tarefa de resposta exibidos, escolha um na tabela a seguir para continuar.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos na tarefa de resposta. Para editar campos ou reatribuir a tarefa, toque no ícone de menu (

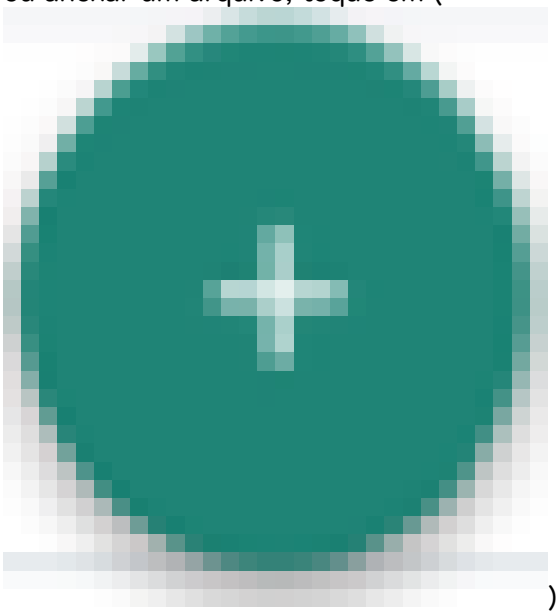
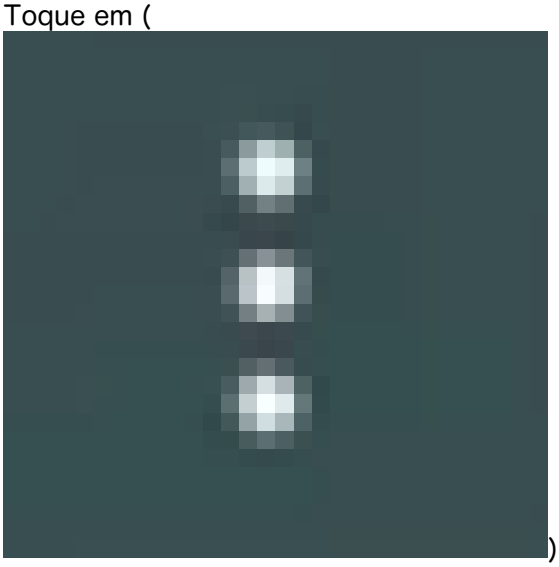
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	). No menu exibido, escolha uma das seguintes opções. ○ Toque em **Editar** . Com a tela Editar tarefa de resposta exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ○ Para reatribuir a tarefa, toque em **Atribuir a outro** . Depois de concluir suas edições, toque no ícone enviar ( ou **Enviar** para salvar suas mudanças e atualizar o registro. A Tarefa de resposta do incidente de segurança no incidente de segurança primário em seu ServiceNow AI Platform a instância foi atualizada.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Exiba a trilha de auditoria cria–da pelas anotações de trabalho no registro da tarefa. Para adi–cionar uma anotação de trabalho ou anexar um arquivo, toque em (). ○ Toque em () para editar ou reatribuir a tarefa.
Toque em um ícone de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ○ Se exibido, toque em outro ícone para abrir outro ServiceNow® aplicação princi–pal para abri-lo. ○ Toque em **Notificação** para exibir notifi–cações de incidentes de segurança críti–cos atribuídos a você ou ao seu grupo de atribuição. ○ Toque em **Configurações** e escolha um para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ Exibir informações sobre ServiceNow AI Platform instância. ▪ Logout da instância atual. Para fazer logout de um ServiceNow AI Platform em seu dispositivo, com a página de deta–lhes exibida, toque em **Logout** .

Filtrar registros com Aplicação Resposta a incidentes de segurança para celular

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na ServiceNow AI Platform.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro ( ).
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
3. Nas opções exibidas, toque na caixa de seleção ou toque em um item para o filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.
4. Toque na seta Voltar (Back ou **CONCLUÍDO** para salvar suas mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover todos os filtros e restaurar a configuração padrão.
5. **Opcional:** Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone Interseção Para criar condições E .
   Como alternativa, toque no ícone de interseção Para criar condições OR.
7. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **CONCLUÍDO** .
   Na tela, somente os registros que correspondem aos critérios de filtro são exibidos.

Orquestração de Resposta a incidentes de segurança

Orquestração de Resposta a incidentes de segurança As atividades permitem que os usuários interajam e recuperem dados de sistemas e ambientes baseados em Windows ou UNIX usando a orquestração de fluxo de trabalho.

Configurar

Antes de usar Orquestração de Resposta a incidentes de segurança Execute as etapas para configurar várias partes do sistema, incluindo o preenchimento do CMDB, a configuração do MID Server e a configuração de credenciais.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para usar Resposta a incidentes de segurança, Você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ativar Resposta a incidentes de segurança plug-in.
2. Configurar MID Servers .
3. Configure as credenciais de serviço do Windows MID Server .

Entenda fluxos de trabalho de Orquestração de resposta a incidentes de segurança e modelos de fluxo de trabalho

. Resposta a incidentes de segurança o sistema de base inclui uma série de fluxos de trabalho e modelos de fluxo de trabalho projetados para funcionar com registros de incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa
Você pode personalizar todos os fluxos de trabalho e modelos de fluxo de trabalho para atender melhor às suas necessidades, supondo que você tenha a função apropriada: sn_sec_cmn.admin. Os fluxos de trabalho são usados em todo o sistema de Operações de segurança para executar uma variedade de tarefas.
Modelos de fluxo de trabalho, no entanto, são acionados selecionando um valor em **Categoria** campo em um incidente de segurança. Quando isso ocorre, o modelo de fluxo de trabalho associado à seleção inicia um modelo de fluxo de trabalho que instrui os analistas de segurança a lidar com um tipo específico de ameaça.

Por exemplo, se você selecionar **Negação de serviço** em **Categoria** campo em um incidente de segurança, o. **Incidente de segurança - Negação de serviço - Modelo** É executado e o analista é direcionado para determinar se o destino do DOS é crítico para os negócios. Em caso afirmativo, a próxima tarefa fará com que a prioridade do incidente de segurança seja definida como **1 - Crítico** e executa a próxima tarefa. E assim por diante.

Então Resposta a incidentes de segurança os fluxos de trabalho e os modelos de fluxo de trabalho são essencialmente os mesmos, exceto que os modelos são usados para um conjunto específico de funções em um incidente de segurança.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Fluxos de trabalho** > **Exibir Fluxos de Trabalho de Segurança**.
2. Uma lista de fluxos de trabalho e modelos de fluxo de trabalho enviados no sistema de base é exibida. Novos fluxos de trabalho que você criou no Operações de segurança o pacote de aplicações também está incluído na lista.
3. Clique no nome do fluxo de trabalho ou modelo de fluxo de trabalho que você deseja exibir.

Nota: Os fluxos de trabalho podem ser acionados de várias maneiras diferentes. Associar um fluxo de trabalho a um gatilho de fluxo de trabalho não significa necessariamente que o fluxo de trabalho está ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração de Resposta a incidentes de segurança fluxos de trabalho e atividades

Vários fluxos de trabalho e atividades estão incluídos com Orquestração de Resposta a incidentes de segurança.

Somente usuários com a função sn_sec_cmn.admin podem Editor de fluxo de trabalho .

Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IOC

. **Resposta do incidente de segurança - Criar solicitação de pesquisa para mudanças de IOC**
O fluxo é acionado por uma regra de negócios para ser executada automaticamente quando um IOC é adicionado ou alterado. As verificações de malware são acionadas somente quando novos dados são inseridos e somente os novos dados são verificados.

Antes de Iniciar
Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa
Se o IOC estiver vazio, o fluxo de trabalho não será executado. Verificações históricas são mantidas e visíveis no **Solicitações de verificação de segurança** e anotações de trabalho do incidente de segurança. Os incidentes de segurança existentes são atualizados automaticamente.

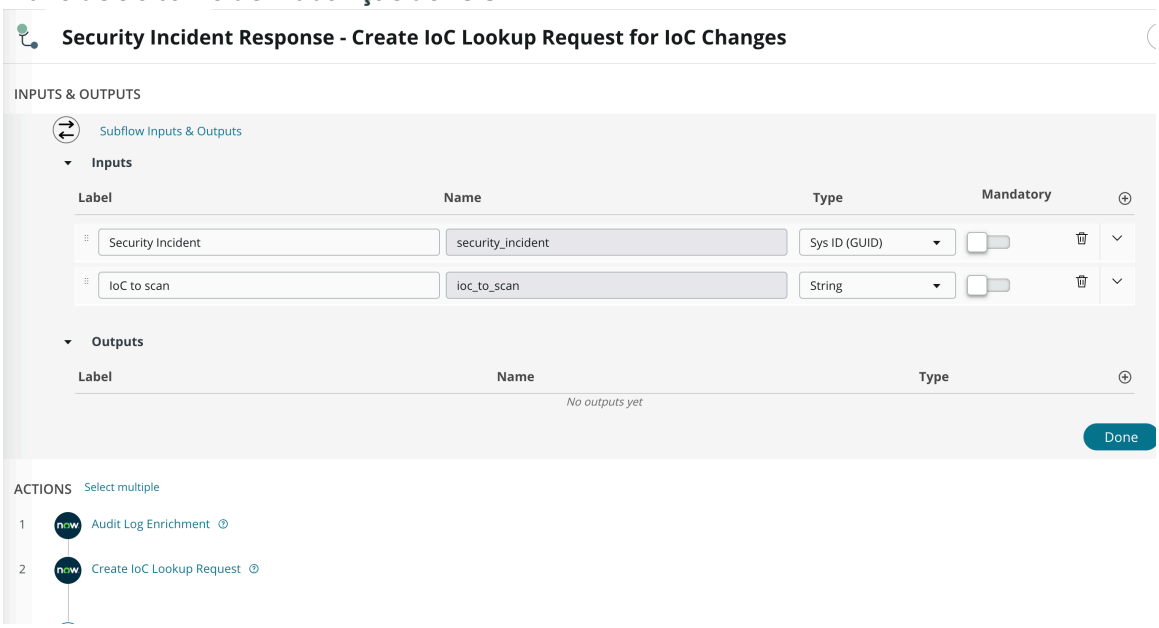
Importante:

. **Resposta do incidente de segurança - Criar solicitação de pesquisa para mudanças de IOC** O fluxo de trabalho é migrado para o Flow Designer. O fluxo é acionado somente quando o sn_ti_scanner tem pelo menos um registro.

As ações do Flow Designer incluem:

- Aprimoramento do registro de auditoria
- Atividade Criar solicitação de pesquisa de IOC

Fluxo de trabalho de mudanças do IOC



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Criar solicitação de pesquisa de IOC

. **Criar solicitação de pesquisa de IOC** A atividade pode ser usada com qualquer fluxo de trabalho para criar uma solicitação de pesquisa de malware para campos IOC adicionados ou modificados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Solicitação de pesquisa criada.
Falha	Solicitação de pesquisa não criada.

Variáveis de entrada

Variável	Descrição
IocString	Informações de IOC formatadas em JSON. IP, hash, url.
siId	Identificador do sistema de incidente de segurança

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ScnReqID	Identificador da solicitação de pesquisa

Resposta do incidente de segurança- Obter fluxo de estatísticas de rede

O **Resposta a incidentes de segurança** > **Obter estatísticas de rede** O fluxo recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no **Análise** estado.

Antes de Iniciar
Função necessária: sn_si.analyst

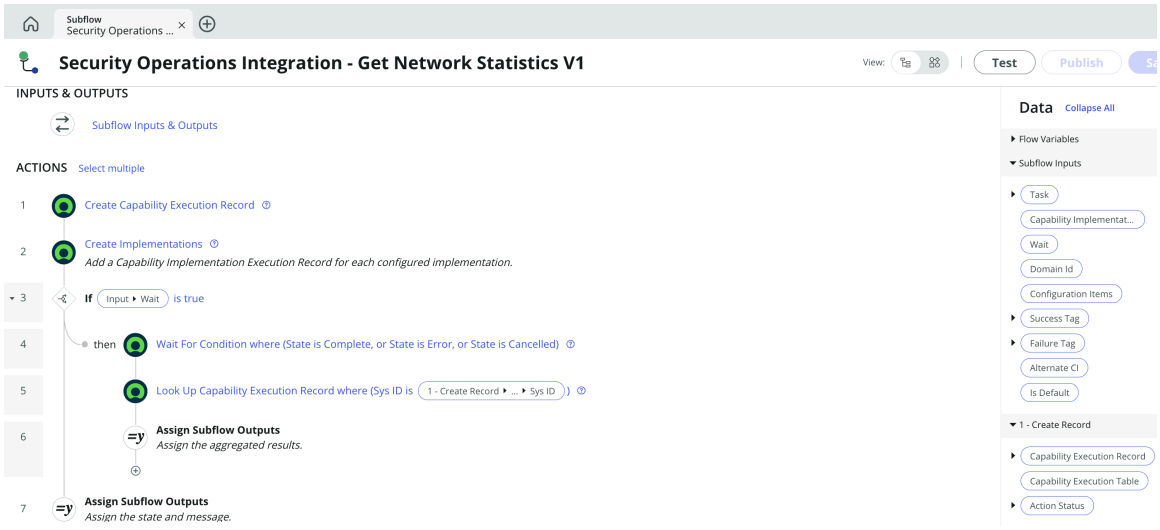
Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança que contêm itens de configuração, o fluxo é executado automaticamente quando o estado muda para **Análise** .

Os incidentes de segurança existentes são atualizados automaticamente quando você está em **Análise** e você adiciona um novo item de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter estatísticas de rede



As ações do processo de fluxo incluem:

Obter ação de fluxo de FQDN do item de configuração

Determinar Shell Script por SO

Se a instrução for executada pelo PowerShell

Acompanhamento da execução - Iniciar ação de fluxo

Obter estatísticas de rede por meio da ação de fluxo netstat

Acompanhamento da execução da capacidade - Ação de fluxo de falha

Ação de fluxo Criar registros de dados de aprimoramento

Acompanhamento da execução da capacidade - Ação de fluxo de falha - Retorna o ID de aprimoramento.

Acompanhamento da execução da capacidade - Ação de fluxo concluída

Procedimento

1. Abra um incidente de segurança.
2. Atualize o. **Estado** . **Análise** , se necessário.
3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração de Resposta a incidentes de segurança fornece informações de estatísticas de rede no **Links relacionados** > **Melhorias de incidentes de segurança** guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Resposta a incidentes de segurança - Obter fluxo de trabalho de serviços em execução

. **Resposta a incidentes de segurança - Obter fluxo de trabalho de serviços em execução**
Recupera uma lista de serviços em execução de baseados no Windows, ServiceNow Itens de configuração (ICs). Este fluxo de trabalho é usado para aprimoramento de incidentes durante investigações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

. **Resposta a incidentes de segurança - Obter fluxo de trabalho de serviços em execução** É executado automaticamente quando você adiciona um novo item de configuração a um incidente de segurança do Windows depois que o estado muda para **Análise** . As informações que este fluxo de trabalho obtém aparecem em **Mostrar Dados de Aprimoramento** guias do incidente de segurança.

Nota: Se o incidente de segurança permanecer em **Rascunho** estado, o. **Resposta a incidentes de segurança - Obter fluxo de trabalho de serviços em execução** o fluxo de trabalho não é executado.

As atividades de fluxo de trabalho incluem:

Atividade Script de aprimoramento do log de auditoria

Obter ação de fluxo de FQDN do item de configuração

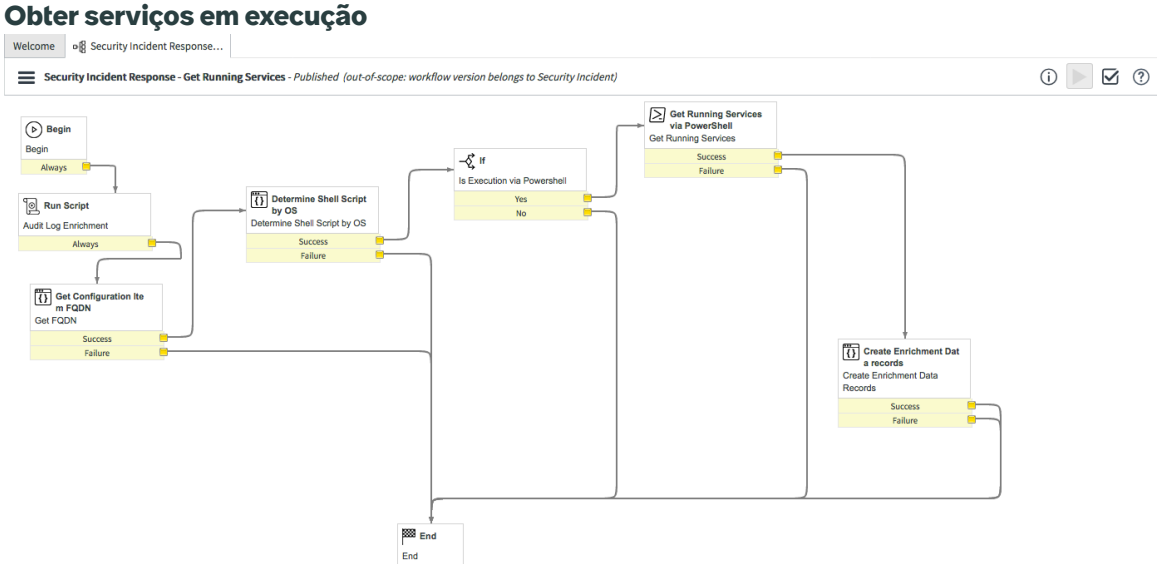
Atividade Determinar script do shell por SO

Atividade Execução via PowerShell

Obter serviços em execução - atividade de aprimoramento de WMI

Ação de fluxo Criar registros de dados de aprimoramento

Obter serviços em execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o. **Estado** . **Análise** , se necessário.
3. Adicione um item de configuração baseado no Windows (servidor, laptop ou semelhante).
4. Clique em **Atualizar**.
   Resposta a incidentes de segurança fornece informações de serviços em execução no **Links relacionados** > **Melhorias de incidentes de segurança**guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Determinar script do shell por SO

A atividade Determinar script de shell por fluxo de trabalho do SO determina qual sistema operacional usar no fluxo de trabalho

A atividade Determinar script de shell por SO pode ser usada com qualquer fluxo de trabalho para determinar qual script de shell executar com base no sistema operacional em execução no sistema que contém o item de configuração.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sistema operacional encontrado.
Falha	Nenhum sistema operacional encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ciSysId	Identificador do sistema do item de configuração.
processType	Identificador interno que define qual script extrair da tabela.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ProcessScript	Agente ECC que reúne o processo em execução.
ExecutitionTemplate	Determina se o script é executado por meio de uma probe ou usando o PowerShell.
EncripmentMappingId	Identificador do sistema do mapeamento de aprimoramento usado para transformar os dados de resposta.

Obter serviços em execução - Aprimoramento de WMI

. **Resposta a incidentes de segurança - Obter serviços em execução** o fluxo de trabalho reúne serviços em execução em um item de configuração adicionado a um incidente de segurança.

. **Obter serviços em execução - Aprimoramento de WMI** A atividade é iniciada automaticamente para recuperar informações de serviços em execução para um host Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os serviços em execução atuais no sistema de destino. Os dados JSON incluem: **nome** O nome do serviço **PID** O identificador do processo do serviço em execução **service_type** (Opcional) O tipo de serviço em execução. **start_name** O nome do sistema do serviço **caminho** O caminho do arquivo do executável do serviço em execução **start_mode** O modo de início do serviço em execução. **display_name** O nome do serviço em execução conforme ele aparece para o usuário

Restrições

O MID Server deve oferecer suporte a **PowerShell** .

O hash SHA-256 requer o PowerShell V4.

Execute o procdump fluxo

. **Execute o procdump** o flow executa um despejo de processo em um processo especificado e o salva em um arquivo que pode ser visado por analistas de segurança.

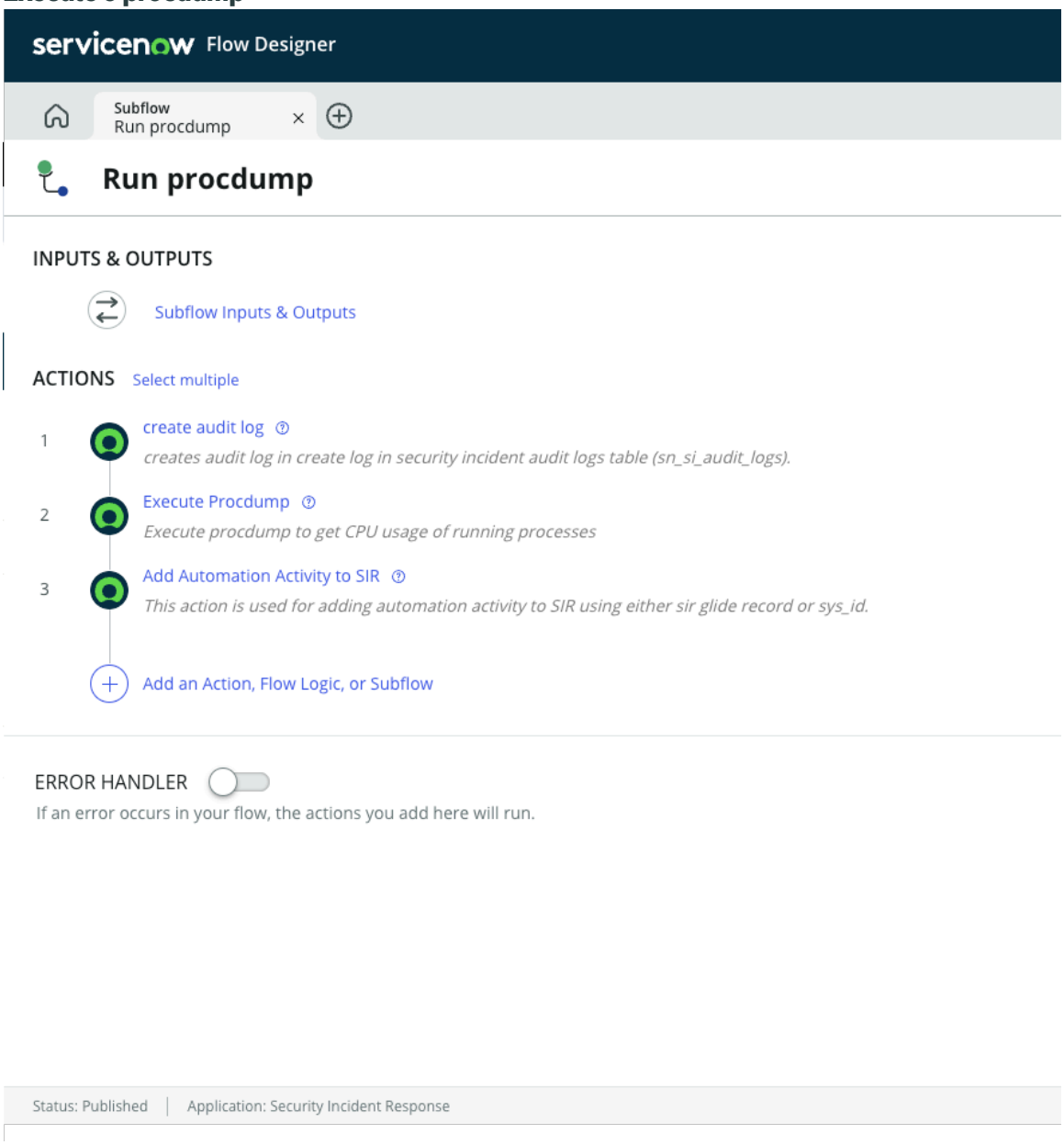
Função necessária: sn_si.analyst

Este fluxo é acionado quando processos aprimorados são selecionados e um **Execute o procdump** A ação de IU foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execute o procdump



Tradução automática

Os motivos pelos quais o procdump pode falhar incluem:

- Caminho de despejo inválido
- Caminho de compartilhamento de arquivo inválido
- Não é possível obter o nome de domínio totalmente qualificado da máquina Windows em que o procdump está sendo executado
- O nome do processo não foi especificado
- A variável de ambiente PROCDUMP não foi encontrada
- Uma cópia do arquivo de despejo falha ao copiar do caminho de despejo para o caminho de compartilhamento de arquivos

Execute procdump ação

Execute procdump é uma ação do powershell que executa o procdump nos processos selecionados, despeja os dados em um arquivo e os publica em um site compartilhado em

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

uma rede interna. Um analista pode exibir um processo listado de proibições, realçado em vermelho em um incidente de segurança e executar uma análise adicional no arquivo.

Resultados

Os resultados possíveis para esta ação são:

Resultados

Resultado	Descrição
Êxito	O procdump foi executado com sucesso em process_name e os detalhes estão disponíveis em actionOutput.response.
Falha	O procdump não foi executado no procdump em process_name e os detalhes estão disponíveis em actionOutput.response.

Variáveis de entrada

As variáveis de entrada são usadas para criar as saídas solicitadas.

Variáveis de entrada

Variável	Descrição
targetId	ID de destino para executar o procdump.
process_name	[Obrigatório] O nome do processo do procdump.
dump_path	[Obrigatório] O caminho do arquivo local no qual o arquivo de despejo gerado será salvo.
dump_filename	O nome do arquivo gerado pelo procdump. Todos os caracteres especiais serão substituídos por hifens (-) do nome do arquivo de despejo quando o arquivo for gerado.
file_share_path	[Obrigatório] O caminho de compartilhamento de arquivo para o qual o arquivo de despejo será copiado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
share_path	O caminho de compartilhamento de arquivo para o qual o arquivo de despejo foi copiado.
resposta	Uma representação JSON do resultado do procdump.
resultado	O resultado do procdump.

Incidente de segurança - Avalie o fluxo de trabalho do resultado da tarefa de resposta

Incidente de segurança - Avaliar o fluxo de trabalho de resultado da tarefa de resposta determina a tarefa a ser usada, invoca um fluxo de trabalho escolhido e um script de avaliação com base no registro do avaliador de resultado fornecido como entrada para o fluxo de trabalho escolhido.

Antes de Iniciar
Função necessária: sn_si.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho deve ser executado ao mesmo tempo que a atividade Criar tarefa a ser avaliada. O script de avaliação consulta os artefatos (como registros de pesquisa de vistas ou processos em execução) da capacidade configurada usando informações de contexto da tarefa de resposta (como incidente de segurança primário) para determinar o resultado apropriado para a tarefa de resposta. O resultado pode ser dependente da atividade do fluxo de trabalho, mas geralmente é **sim** ou **não** . Ao criar um avaliador de resultados, registre somente recursos que tenham um fluxo de trabalho configurado, com **É uma capacidade baseada em tarefa** e um conjunto de variáveis de entrada de tarefa está disponível para seleção.

As atividades do processo de fluxo de trabalho incluem:

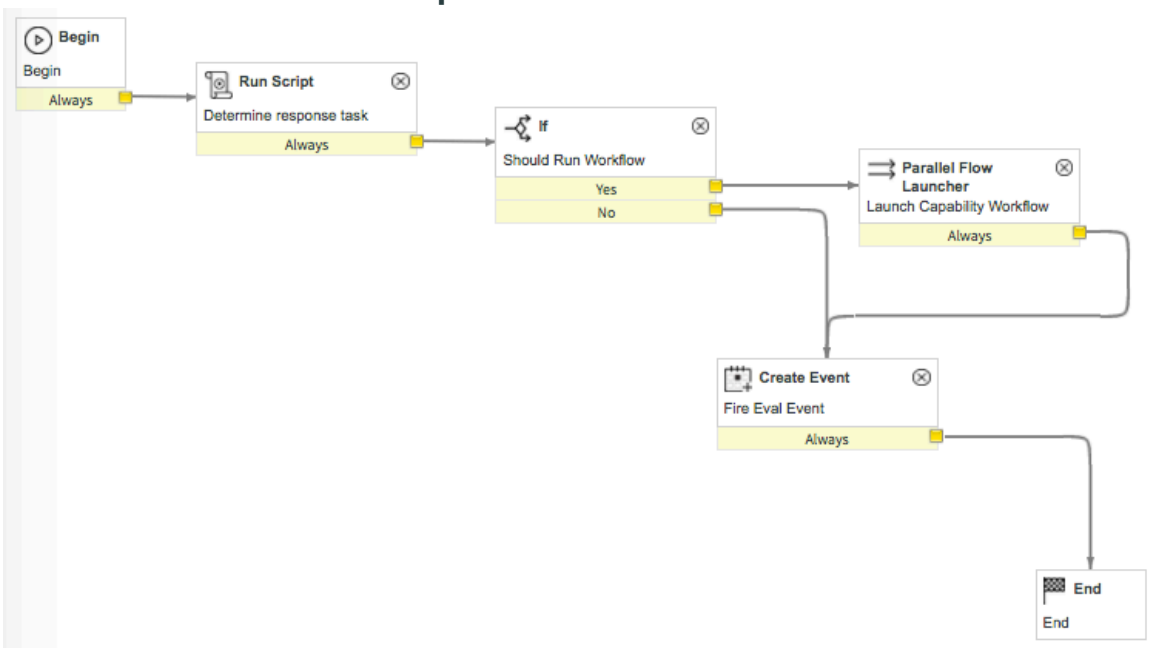
Execute o script para determinar a tarefa de resposta

Fluxo de trabalho deve ser executado

Fluxo de trabalho de capacidade de lançamento do inicializador de fluxo paralelo

Criar evento de avaliação

Avalie o resultado da tarefa de resposta



Tradução automática

Modelos de fluxo de trabalho de Resposta a incidentes de segurança

Os modelos de fluxo de trabalho são fornecidos com Orquestração de Resposta a incidentes de segurança para permitir que você execute procedimentos básicos de análise relacionados à operação de segurança. Os modelos podem ser usados como estão ou você pode personalizá-los para criar fluxos de trabalho que atendam melhor às suas necessidades específicas. Os modelos de fluxo de trabalho são desativados por padrão.

Somente usuários com a função sn_sec_cmn.admin podem Editor de fluxo de trabalho .

Modelo de fluxo de trabalho de exposição de dados confidenciais de incidente de segurança

O modelo Incidente de segurança - Exposição de dados confidenciais - permite que você execute uma série de tarefas projetadas para lidar com a exposição de dados confidenciais.

Antes de Iniciar

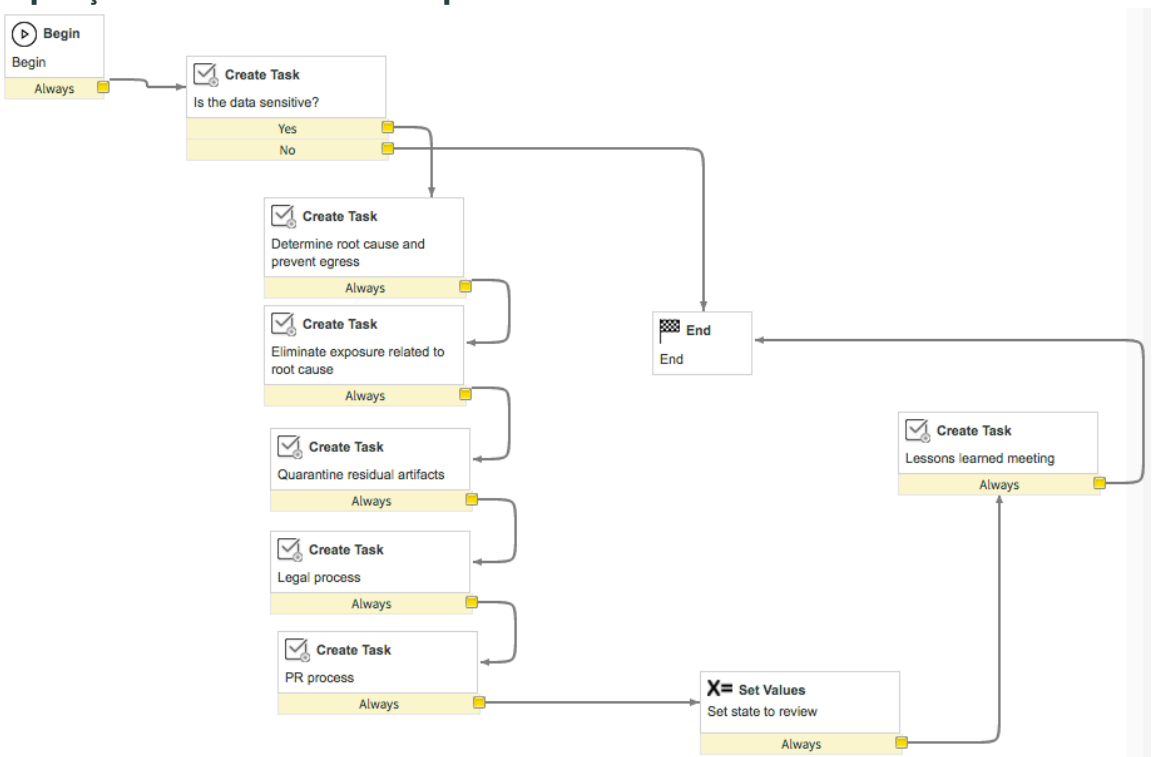
Função necessária: sn_si.write

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança é definido ou alterado para **Exposição confidencial de dados de identidade pessoal** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Exposição de dados de identidade pessoal confidencial



Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com a exposição a dados confidenciais, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Exposição confidencial de dados de identidade pessoal** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado

Tarefas de resposta no modelo de exposição de dados confidenciais

Tarefa de resposta	Descrição	Resultados
Os dados são confidenciais?	Determine se os dados associados a este incidente de segurança são confidenciais ou confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionou **Sim** , a próxima tarefa de resposta é executada. Se você selecionou **Não** , o fluxo termina.
Determine a causa raiz e evite a saída	Determine a causa raiz do ataque e adicione filtragem de saída para interromper a exfiltração, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Descrição	Resultados
Elimine a exposição relacionada à causa raiz	Com base na causa raiz, execute as etapas para eliminar a exposição, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Artefatos residuais em quarentena	Execute as etapas para colocar em quarentena todos os artefatos residuais, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Processo jurídico	Execute as etapas para atender aos requisitos legais desta análise, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Processo de PR	Execute as etapas para atender aos requisitos de PR desta análise, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** .
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado nesses dados confidenciais, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , o incidente de segurança permanece em **Revisão** estado até você fechá-lo.

Modelo de fluxo de trabalho de Negação de serviço de incidente de segurança

O modelo Incidente de segurança - Negação de serviço - permite que você execute uma série de tarefas projetadas para lidar com ataques de negação de serviço (DOS).

Antes de Iniciar

Função necessária: sn_si.write

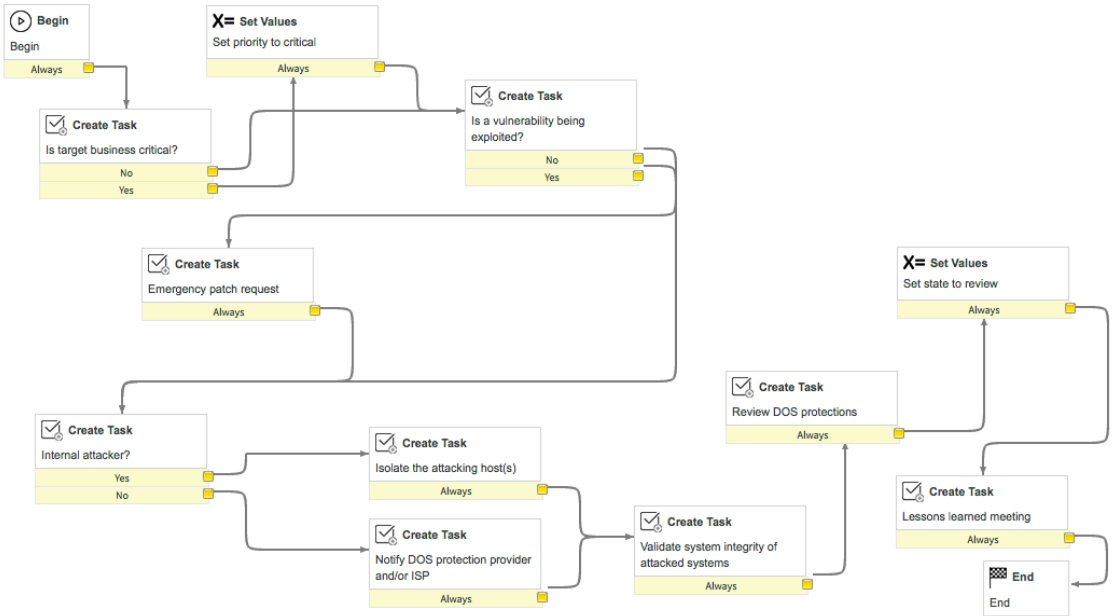
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Negação de serviço** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Negação de serviço (DOS)



Procedimento

1. Abra o incidente de segurança para esta ocorrência de negação de serviço, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Negação de serviço** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado

Tarefas de resposta no modelo de negação de serviço

Tarefa de resposta	Ação	Resultados
Os negócios de destino são críticos?	Determine se o destino desse ataque do DOS é crítico para os negócios. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Defina a prioridade como crítica** a tarefa foi executada. Se você selecionar **Não** . **Uma vulnerabilidade está sendo explorada?** a tarefa foi executada.
Defina a prioridade como crítica	Nenhuma ação necessária.	. **Prioridade** do incidente de segurança é alterado automaticamente para **Crítico** e **Uma vulnerabilidade está sendo explorada?** a tarefa foi executada.
Uma vulnerabilidade está sendo explorada?	Determine se este ataque do DOS explora uma vulnerabilidade de software.	Se você selecionar **Sim** . **Solicitação de patch de emergência** a tarefa foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Não** . **Invasor interno?** a tarefa foi executada.
Solicitação de patch de emergência	Emita uma solicitação de patch de emergência para os sistemas que estão sendo atacados. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Invasor interno?	Determine se a origem desse ataque do DOS é interna à sua organização. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Isolar host(s) atacante(s)** a tarefa foi executada. Se você selecionar **Não** . **Provedor de proteção do DOS e/ou ISP do notifique** a tarefa foi executada.
Isolar o(s) host(s) atacante(s)	Execute as etapas necessárias para isolar os hosts internos responsáveis pelo ataque. Atualize o. **Estado** campo na tarefa conforme apropriado.	Depois de concluir esta etapa, o **Validar a integridade do sistema dos sistemas atacados** a tarefa foi executada.
Provedor de proteção do DOS e/ou ISP do notifique	Execute as etapas necessárias para entrar em contato com o provedor de proteção contra negação de serviço e/ou com o provedor de serviços de Internet para notificá-los sobre o ataque. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Validar a integridade do sistema dos sistemas atacados	Execute as etapas necessárias para avaliar e validar a integridade dos computadores atacados. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Revise as proteções do DOS	Conduza uma revisão das proteções e procedimentos existentes do DOS. Faça as alterações necessárias. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** . . **Reunião de lições aprendidas** a tarefa foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de negação de serviço. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , o fluxo termina.

Modelo de fluxo de trabalho de equipamento perdido de incidente de segurança

O modelo Incidente de segurança - Equipamento perdido - permite que você execute uma série de tarefas projetadas para lidar com equipamentos perdidos.

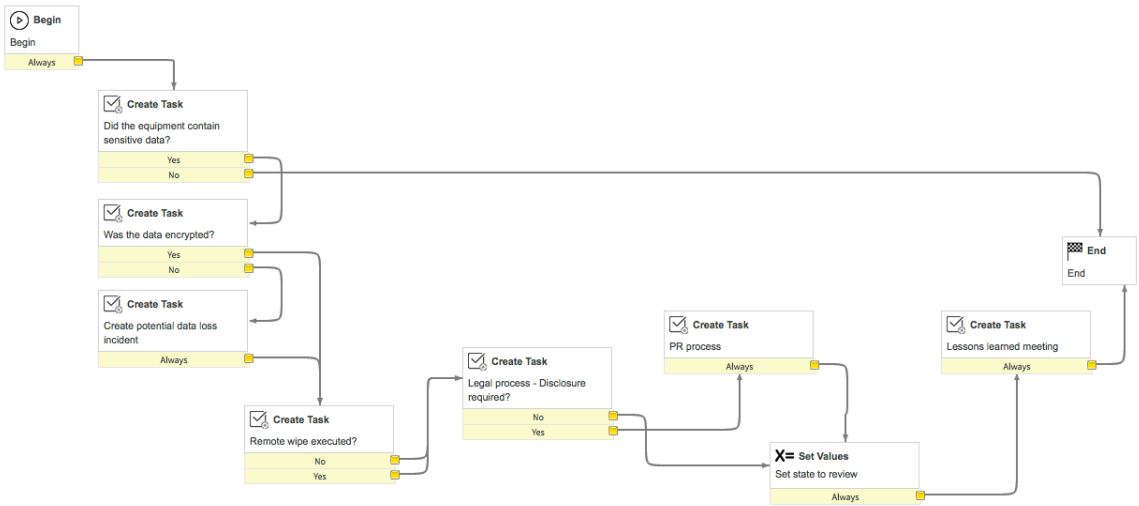
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Perda de equipamento** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Perda de equipamento



Procedimento

1. Abra o incidente de segurança da perda de equipamento, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Perda de equipamento** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de equipamento perdido

Tarefa de resposta	Ação	Resultados
O equipamento continha dados confidenciais?	Determine se o equipamento associado a este incidente de segurança continha informações confidenciais ou confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado** conforme apropriado.	Se você selecionar **Sim** . **Os dados foram criptografados?** a tarefa foi executada. Se você selecionar **Não** , o fluxo termina.
Os dados foram criptografados?	Determine se os dados confidenciais no dispositivo perdido foram criptografados. Na tarefa, selecione **Sim** ou **Não** em **Resultado** conforme apropriado.	Se você selecionar **Sim** . **Limpeza remota criada?** a tarefa de resposta foi executada. Se você selecionar **Não** . **Criar possível incidente de perda de dados** a tarefa de resposta foi executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um possível incidente de perda de dados. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	. **Limpeza remota criada?** a tarefa de resposta foi executada.
Limpeza remota criada?	Execute as etapas necessárias para executar uma limpeza remota do equipamento perdido. Na tarefa, selecione **Sim** ou **Não** em **Resultado** conforme apropriado.	. **Processo jurídico - Divulgação necessária** a tarefa é executada .
Processo jurídico - Divulgação necessária?	Execute as etapas para atender aos requisitos legais desta análise. Selecione **Sim** se uma divulgação jurídica for necessária, **Não** se não estiver.	. **Reunião de lições aprendidas** a tarefa foi executada.
Processo de PR	Execute as etapas necessárias para atender aos requisitos de PR desta análise. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	. **Defina o estado a ser revisado** a tarefa foi executada.
Defina o estado a ser revisado	Nenhuma ação é necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de equipamento perdido. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	O fluxo termina.

Modelo de fluxo de trabalho de software mal-intencionado de incidente de segurança

O Incidente de segurança - Software mal-intencionado - Modelo permite que você execute uma série de tarefas projetadas para lidar com software mal-intencionado em sua rede.

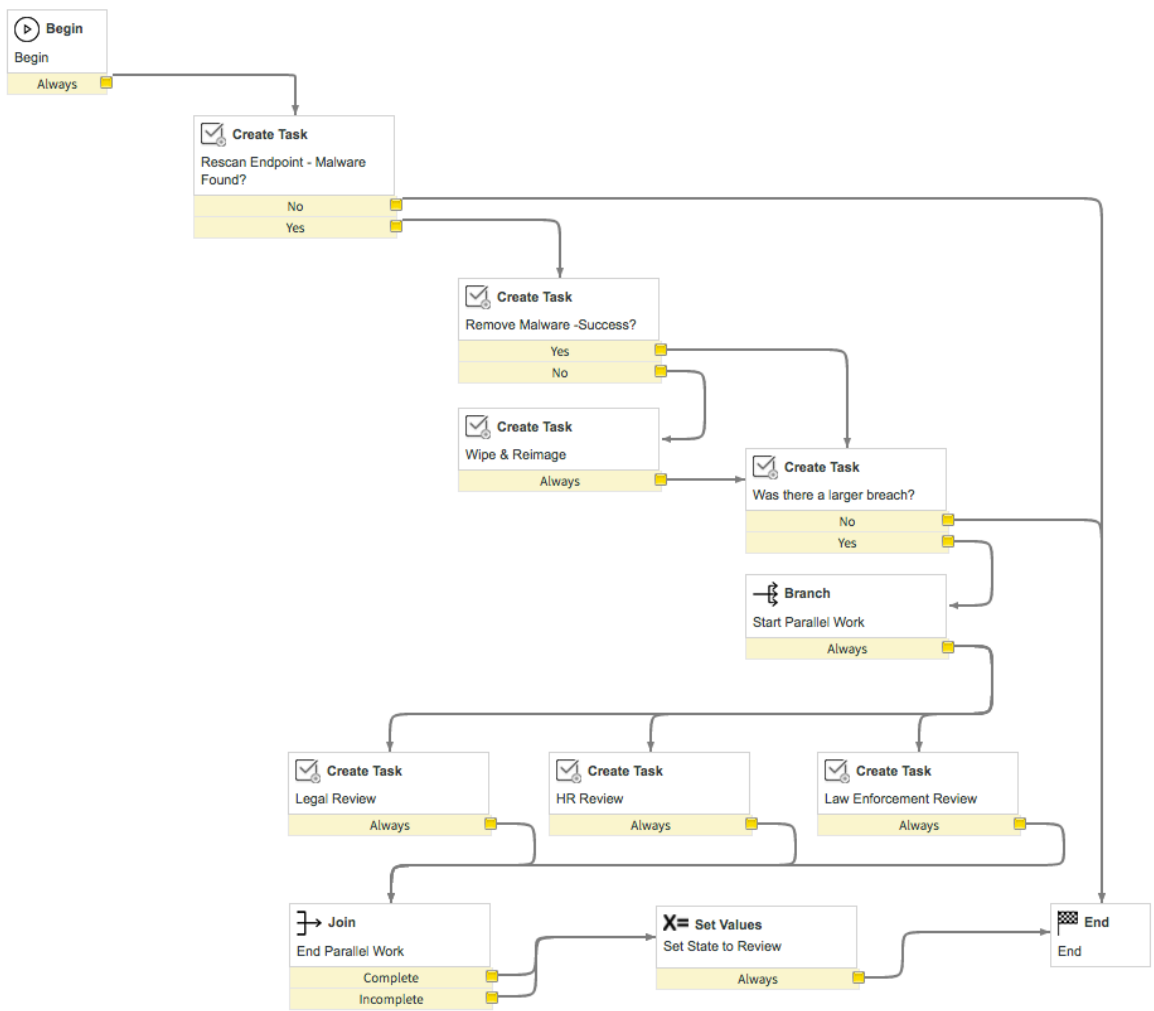
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Software mal-intencionado** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Software mal-intencionado



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para este possível ataque, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Atividade de código mal-intencionado** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta no modelo de software mal-intencionado

Tarefa de resposta	Ação	Resultados
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Remover malware - Sucesso?** a tarefa foi executada. Se você selecionar **Não** , o fluxo termina.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Houve uma violação maior?** a tarefa foi executada. Se você selecionar **Não** . **Limpar e recriar imagem** a tarefa foi executada.
Limpar e recriar imagem	Se você não conseguiu remover o malware encontrado, esta tarefa instruirá você a executar uma limpeza e recriação de imagem nos computadores infectados com o malware.	Após a conclusão da tarefa, o **Estado como Revisão** a tarefa foi executada.
Houve uma violação maior?	Determine se a violação causada pelo software mal-intencionado é maior do que se acreditava inicialmente. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** , as seguintes tarefas são executadas em paralelo: ○ Revisão jurídica ○ Revisão de RH ○ Revisão da aplicação da lei Se você selecionar **Não** , o fluxo termina.
Revisão jurídica Revisão de RH	Execute as etapas necessárias para que cada um desses departamentos revise o processo seguido para erradicar o software mal-intencionado.	Quando as tarefas são concluídas, o. **Estado como Revisão** a tarefa foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Revisão da aplicação da lei		
Estado como Revisão	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** e o fluxo termina.

Modelo de fluxo de trabalho de phishing de incidente de segurança

O modelo Incidente de segurança - Phishing - permite que você execute uma série de tarefas projetadas para lidar com e-mails de spear phishing em sua rede.

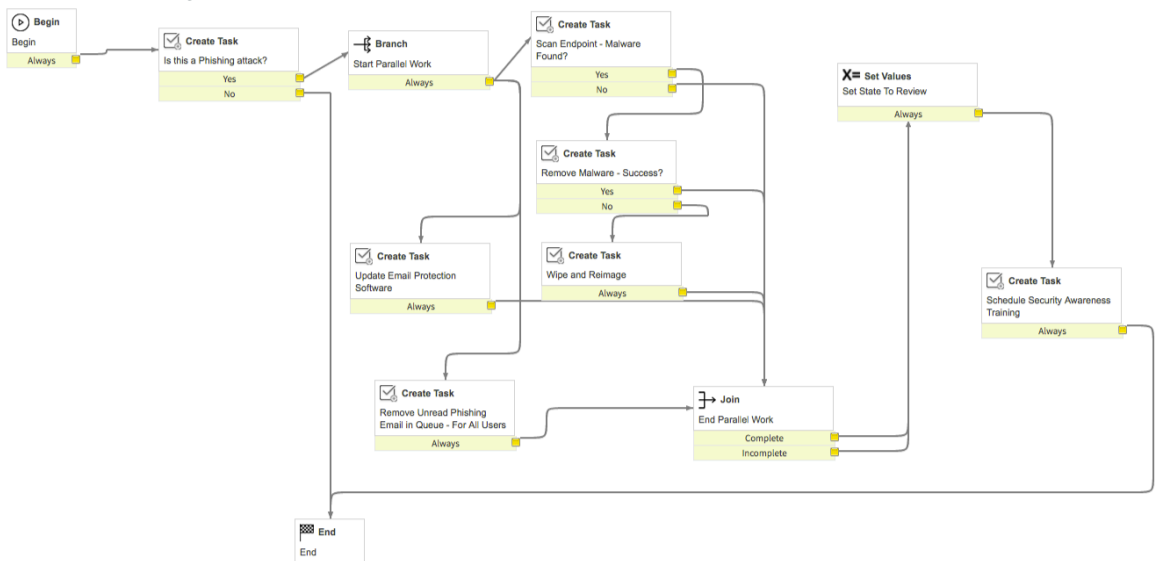
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Spear Phishing** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Spear Phishing



Procedimento

1. Abra o incidente de segurança para este possível ataque de spear phishing, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Spear Phishing** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de phishing Spear

Tarefa de resposta	Ação	Resultados
Este é um ataque de phishing?	Determine se este é um ataque de phishing. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** , as seguintes tarefas são executadas em paralelo: ○ Endpoint de verificação - Malware encontrado? ○ Atualizar o software de proteção de e-mail ○ Remover e-mail de phishing não lido na fila - para todos os usuários Se você selecionar **Não** , o fluxo termina.
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Remover malware - Sucesso?** a tarefa foi executada. Se você selecionar **Não** . **Estado como Revisão** a tarefa foi executada.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Estado como Revisão** a tarefa foi executada. Se você selecionar **Não** . **Limpe e crie uma nova imagem** a tarefa foi executada.
Limpe e crie uma nova imagem	Se você não conseguiu remover o malware encontrado, esta tarefa instruirá você a executar uma limpeza e recriação de imagem nos computadores infectados com o malware.	Após a conclusão da tarefa, o **Estado como Revisão** a tarefa foi executada.
Atualizar o software de proteção de e-mail	Se for determinado que este é um ataque de phishing, você será solicitado a atualizar seu software de proteção de e-mail adequadamente.	Quando a tarefa é concluída, o. **Estado como Revisão** a tarefa foi executada.
Remover e-mail de phishing não lido na fila - para todos os usuários	Execute as etapas necessárias para remover o e-mail de phishing que ainda está na fila para todos os seus usuários.	Quando a tarefa é concluída, o. **Estado como Revisão** a tarefa foi executada.
Estado como Revisão	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
		. **Programar treinamento de conscientização de segurança** a tarefa foi executada.
Programar treinamento de conscientização de segurança	Programe treinamento para aumentar a conscientização de segurança por seus funcionários. Atualize o. **Estado** campo na tarefa conforme apropriado.	Quando a tarefa é concluída, o fluxo termina.

Modelo de fluxo de trabalho de violação da política de incidente de segurança

O Incidente de segurança - Violação de política - Modelo permite que você execute uma série de tarefas projetadas para lidar com violações de política de segurança.

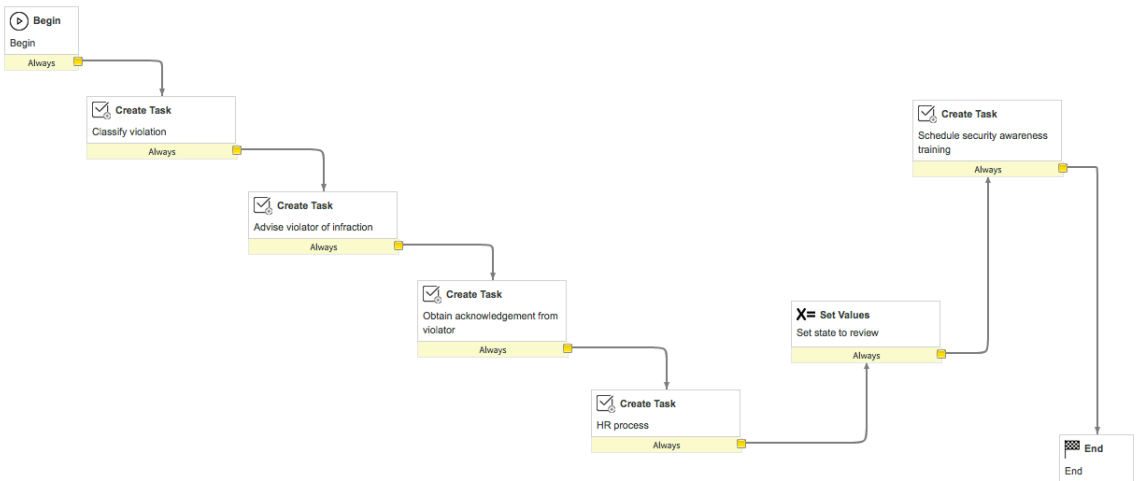
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Violação de política** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Violação de política



Procedimento

1. Abra o incidente de segurança da violação da política, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Violação de política** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de violação de política

Tarefa de resposta	Ação	Resultados
Classificar violação	Classifique como essa infração viola as políticas de segurança da sua organização. Atualize o. **Estado** na tarefa depois de concluí-la.	. **Aconselhar o infrator sobre infração** a tarefa de resposta foi executada.
Aconselhar o infrator sobre infração	Comunique a natureza da infração ao infrator. Atualize o. **Estado** campo na tarefa depois de comunicá-la.	. **Obter confirmação do violador** a tarefa de resposta foi executada.
Obter confirmação do violador	Obter uma confirmação do infrator da infração. Atualize o. **Estado** campo na tarefa conforme apropriado.	. **Processo de RH** a tarefa de resposta foi executada.
Processo de RH	Comunique todas as informações necessárias sobre esta violação ao RH. Atualize o. **Estado** campo na tarefa conforme apropriado.	. **Defina o estado a ser revisado** a tarefa de resposta foi executada.
Defina o estado a ser revisado	Nenhuma ação é necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** .
Programar treinamento de conscientização de segurança	Conduza um treinamento de conscientização de segurança para educar a equipe sobre como evitar violações de segurança semelhantes no futuro. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , o fluxo termina.

Modelo de fluxo de trabalho de reconhecimento de incidente de segurança

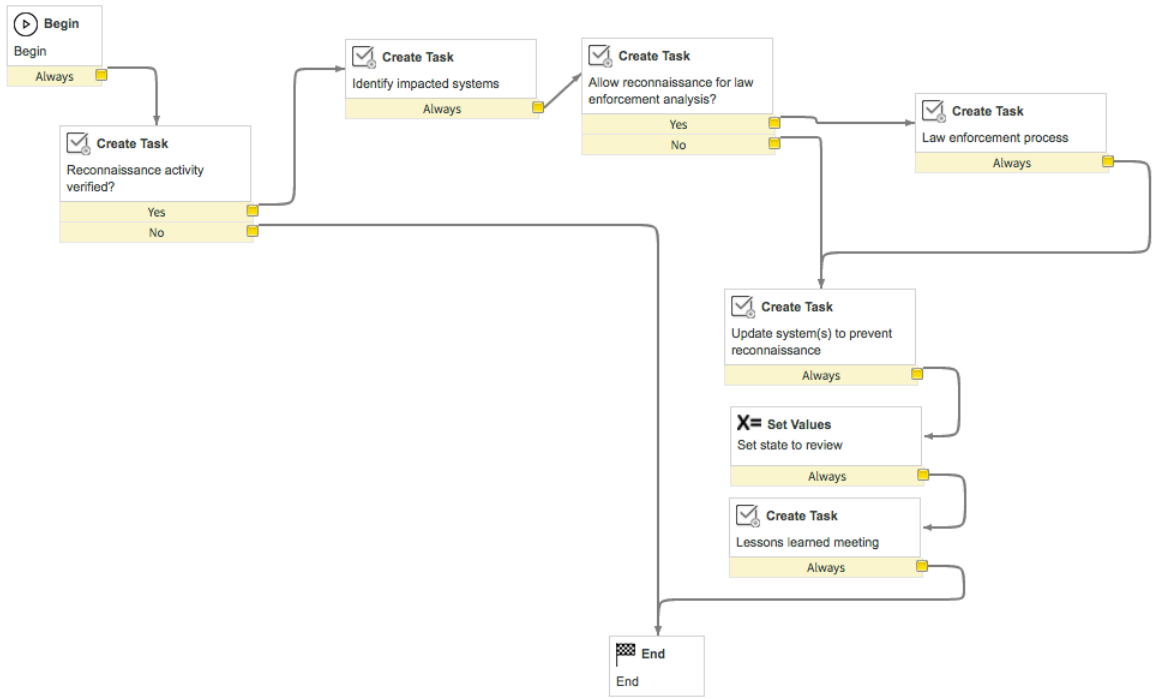
O reconhecimento é geralmente uma etapa preliminar para um ataque adicional que busca explorar um dispositivo ou sistema. O modelo Incidente de segurança - Reconhecimento - permite que você execute uma série de tarefas projetadas para lidar com o reconhecimento em sua rede.

Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Atividade de reconhecimento** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de reconhecimento



Procedimento

1. Abra o incidente de segurança para este possível ataque, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Atividade de reconhecimento** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta no modelo de reconhecimento

Tarefa de resposta	Ação	Resultados
Atividade de reconhecimento verificada?	Determine se algum reconhecimento observado foi verificado. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Identificar os sistemas afetados** a tarefa foi executada. Se você selecionar **Não** , o fluxo termina.
Identificar os sistemas afetados	Determine os sistemas afetados pelo reconhecimento.	Quando esta tarefa estiver concluída, o **Permitir reconhecimento para análise de aplicação da lei?** a tarefa foi executada.
Permitir reconhecimento para análise de aplicação da lei?	Determine se você deseja que o reconhecimento seja analisado pelas agências de aplicação da lei. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Processo de aplicação da lei** a tarefa foi executada. Se você selecionar **Não** . **Atualize o(s) sistema(s) para impedir o reconhecimento** a tarefa foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Processo de aplicação da lei	Execute o processo de aplicação da lei conforme definido pela sua empresa.	Quando esta tarefa estiver concluída, o **Atualize o(s) sistema(s) para impedir o reconhecimento** a tarefa foi executada.
Atualize o(s) sistema(s) para impedir o reconhecimento	Execute as etapas necessárias para atualizar os sistemas afetados pelo reconhecimento.	Quando esta tarefa estiver concluída, o **Defina o estado a ser revisado** a tarefa foi executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** e **Reunião de lições aprendidas** a tarefa foi executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de reconhecimento. Atualize o. **Estado** campo na tarefa conforme apropriado.	Quando esta tarefa é concluída, o fluxo termina.

Servidor invasor de incidente de segurança ou modelo de fluxo de trabalho de serviço

O Incidente de segurança - Servidor ou serviço invasor - Modelo permite que você execute uma série de tarefas projetadas para lidar com atividades de servidores ou serviços invasores que afetam sua rede.

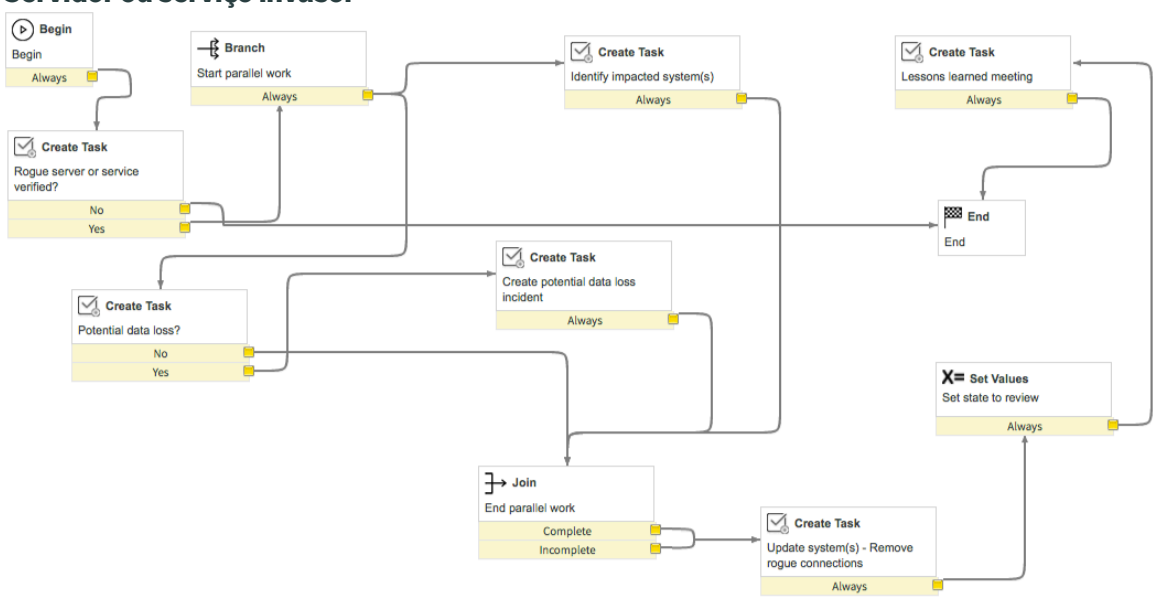
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Servidor ou serviço não autorizado** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Servidor ou serviço invasor



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para este possível ataque, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Servidor invasor ou atividade de serviço** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta em Servidor invasor ou Modelo de serviço

Tarefa de resposta	Ação	Resultados
Servidor ou serviço não autorizado verificado?	Determine se uma conexão com um servidor ou serviço não autorizado foi verificada em sua rede. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** , as duas tarefas a seguir são executadas em paralelo: ○ **Identificar sistema(s) afetado(s)** ○ **Possível perda de dados?** Se você selecionar **Não** , o fluxo termina.
Identificar sistema(s) afetado(s)	Determine os sistemas afetados pelo contato com o servidor ou serviço não autorizado.	Quando esta tarefa estiver concluída, o **Atualizar sistema(s) - Remover conexões não autorizadas** a tarefa foi executada.
Possível perda de dados?	Determine se a conexão com o servidor ou serviço invasor causou possível perda de dados. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Criar possível incidente de perda de dados** a tarefa foi executada. Se você selecionar **Não** . **Atualizar sistema(s) - Remover conexões não autorizadas** a tarefa foi executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um incidente de segurança para a possível perda de dados.	Quando esta tarefa estiver concluída, o **Atualizar sistema(s) - Remover conexões não autorizadas** a tarefa foi executada.
Atualizar sistema(s) - Remover conexões não autorizadas	Execute as etapas necessárias para remover as conexões não autorizadas.	Quando esta tarefa estiver concluída, o **Defina o estado a ser revisado** a tarefa foi executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** e **Reunião de lições aprendidas** a tarefa foi executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado	Quando esta tarefa é concluída, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	para este incidente de serviço ou servidor invasor. Atualize o. **Estado** campo na tarefa conforme apropriado.	

Modelo de fluxo de trabalho de spam de incidente de segurança

O modelo Incidente de segurança - Spam - permite que você execute uma série de tarefas projetadas para lidar com spam de e-mail em sua rede.

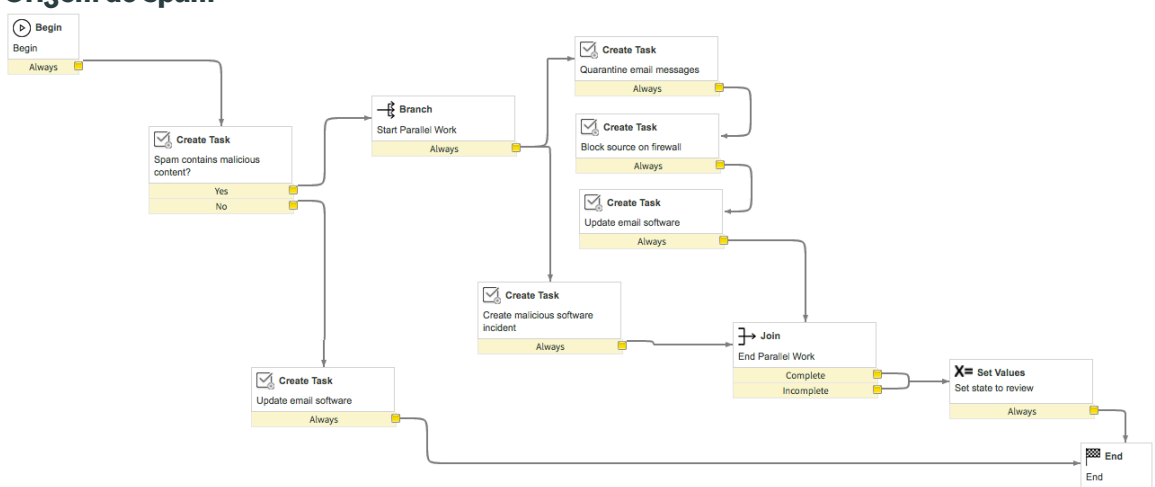
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança é definido ou alterado para **Origem do spam** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Origem do spam



Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com spam por e-mail ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Origem do spam** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta no modelo de spam

Tarefa de resposta	Ação	Resultados
O spam contém	Determine se o spam contém software mal-intencionado. Na	Se você selecionou **Sim** , as seguintes tarefas de resposta são executadas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
conteúdo mal-intencionado?	tarefa, selecione **Sim** ou **Não** em **Resultado** .	○ **Mensagem de e-mail em quarentena** ○ **Criar incidente de software mal-intencionado** Se você selecionou **Não** . **Atualizar software de e-mail** executado.
Criar incidente de software mal-intencionado	Execute as etapas para criar um incidente de segurança, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , esta tarefa de resposta aguarda até que as próximas três tarefas de resposta sejam concluídas. O estado do incidente de segurança muda para **Revisão** .
Mensagem de e-mail em quarentena	Execute as etapas para colocar o spam em quarentena, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Bloquear origem no firewall	Execute as etapas para bloquear o endereço de e-mail no firewall, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Atualizar software de e-mail	Adicione o endereço de e-mail à sua lista de bloqueios, atualizando o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada. **Nota:** Esta tarefa de resposta também será executada se você respondeu **Não** para **O spam contém conteúdo mal-intencionado?** tarefa de resposta.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** .

Tradução automática

Modelo de fluxo de trabalho de acesso não autorizado a incidentes de segurança

O modelo Incidente de segurança - Acesso não autorizado - permite que você execute uma série de tarefas projetadas para lidar com o acesso não autorizado à sua rede.

Antes de Iniciar

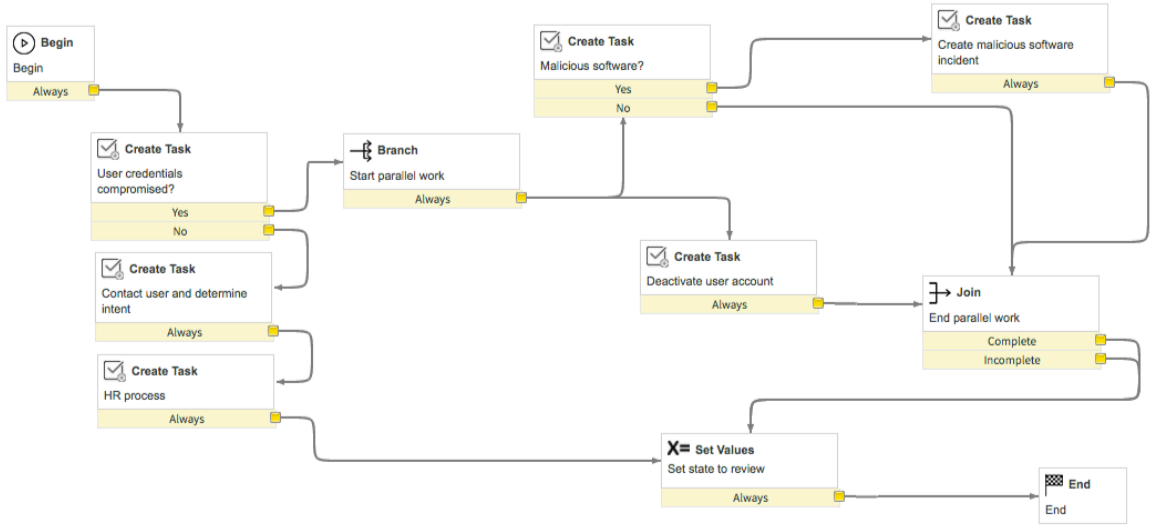
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Acesso não autorizado** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso não autorizado



Procedimento

1. Abra o incidente de segurança para este possível ataque, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Acesso não autorizado** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta no modelo de acesso não autorizado

Tarefa de resposta	Ação	Resultados
Credenciais do usuário comprometidas?	Determine se as credenciais do usuário foram comprometidas. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** , as duas tarefas a seguir são executadas em paralelo: ○ **Software mal-intencionado?** ○ **Desativar conta do usuário** Se você selecionar **Não** . **Entre em contato com o usuário e determine a intenção** a tarefa foi executada.
Software mal-intencionado?	Determine se o acesso não autorizado resultou na introdução de software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** . **Criar incidente de software mal-intencionado** a tarefa foi executada. Se você selecionar **Não** . **Defina o estado a ser revisado** a tarefa foi executada.
Criar incidente de	Execute as etapas necessárias para criar um incidente de segurança para o acesso não autorizado.	Quando esta tarefa estiver concluída, o **Defina o estado a ser revisado** a tarefa foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
software mal-intencionado		
Desativar conta do usuário	Execute as etapas necessárias para desativar a conta de usuário comprometida.	Quando esta tarefa estiver concluída, o **Defina o estado a ser revisado** a tarefa foi executada.
Entre em contato com o usuário e determine a intenção	Execute as etapas necessárias para entrar em contato com o usuário responsável pelo acesso não autorizado e determinar o motivo da tentativa de acesso.	Quando esta tarefa estiver concluída, o **Processo de RH** a tarefa foi executada.
Processo de RH	Execute as etapas necessárias para entrar em contato com os recursos humanos para implementar ações disciplinares, se necessário.	Quando esta tarefa estiver concluída, o **Defina o estado a ser revisado** a tarefa foi executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** e o fluxo termina.

Modelo de fluxo de trabalho de desfiguração da Web/BBS de incidente de segurança

O modelo Incidente de segurança - Desfiguração da Web/BBS - permite que você execute uma série de tarefas projetadas para lidar com o vandalismo direcionado contra um dos BBS ou sites da sua organização.

Antes de Iniciar

Função necessária: sn_si.write

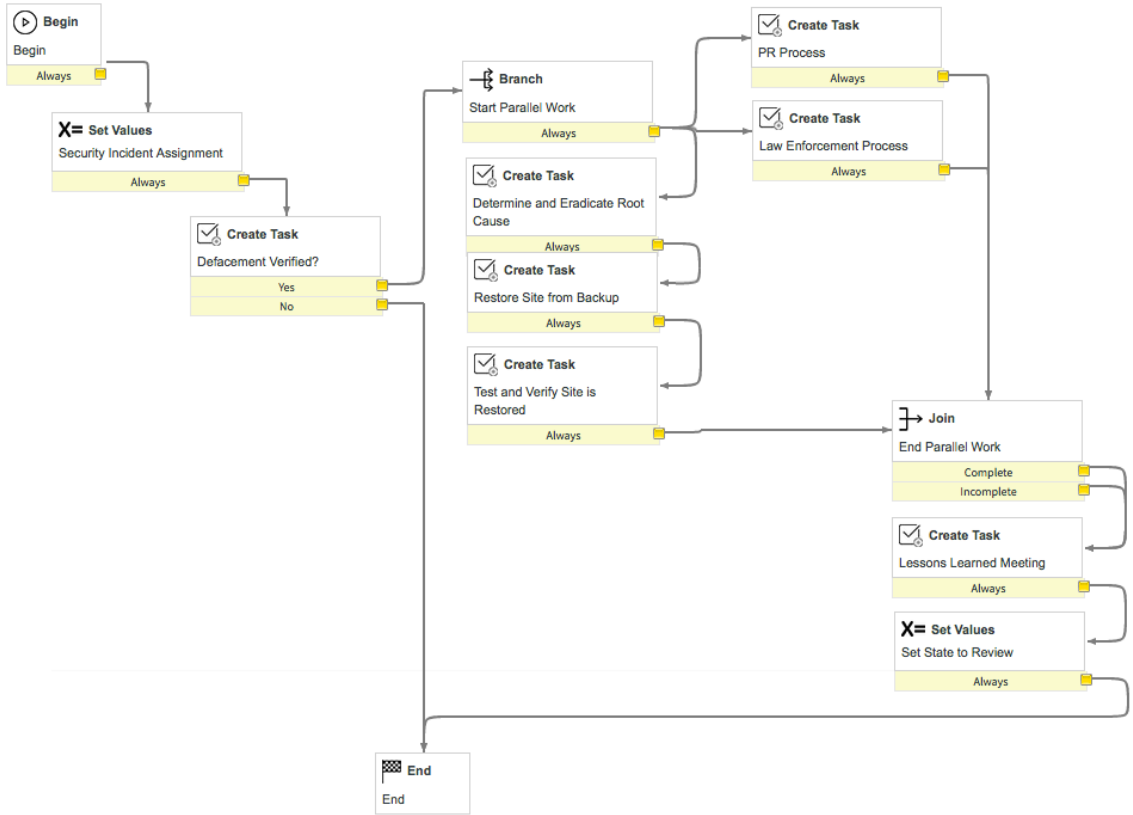
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando **Categoria** em um incidente de segurança está definido como **Desfiguração da Web/BBS** . Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Destruição da web/BBS



Procedimento

1. Abra o incidente de segurança para esta ocorrência de desfiguração da web ou BBS, ou crie um novo incidente de segurança .
2. Em **Categoria** , selecione **Desfiguração da Web/BBS** .
3. Salve o registro.
4. Role para baixo e abra **Tarefas de resposta** lista relacionada.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado

Tarefas de resposta no modelo de desfiguração da Web/BBS

Tarefa de resposta	Ação	Resultados
Atribuição de incidente de segurança	Crie um incidente de segurança para cada incidente relatado de site ou desfiguração de BBS.	A próxima tarefa de resposta é executada.
Desfiguração verificada?	Determine se o site ou o BBS foi de fato desfigurado. Na tarefa, selecione **Sim** ou **Não** em **Resultado** .	Se você selecionar **Sim** , as seguintes tarefas de resposta são executadas: ○ **Processo de PR** ○ **Processo de aplicação da lei** ○ **Determinar e erradicar a causa raiz** Se você selecionar **Não** , o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Processo de PR	Execute as etapas necessárias para notificar o público de que o site ou o BBS foi desfigurado. Ao terminar o processo de PR, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	. **Reunião de lições aprendidas** a tarefa foi executada.
Processo de aplicação da lei	Execute as etapas necessárias para envolver as agências de aplicação da lei apropriadas em relação ao ataque. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	. **Reunião de lições aprendidas** a tarefa foi executada.
Determinar e erradicar a causa raiz	Execute as etapas necessárias para descobrir e eliminar a causa raiz da desfiguração. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Restaurar site do backup	Execute as etapas necessárias para fazer backup e restaurar o site ou o BBS. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudou o estado da tarefa para **Encerrado concluído** ou **Cancelado** , a próxima tarefa de resposta é executada.
Teste e verifique se o site foi restaurado	Verifique se o site foi restaurado. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto** conforme apropriado.	. **Reunião de lições aprendidas** a tarefa foi executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de desfiguração do site/ BBS. Atualize o. **Estado** campo na tarefa conforme apropriado.	Se você mudar o estado da tarefa para **Encerrado concluído** ou **Cancelado** . **Defina o estado a ser revisado** a tarefa foi executada.
Defina o estado a ser revisado	Nenhuma ação necessária.	. **Estado** do incidente de segurança é alterado automaticamente para **Revisão** . O fluxo termina.

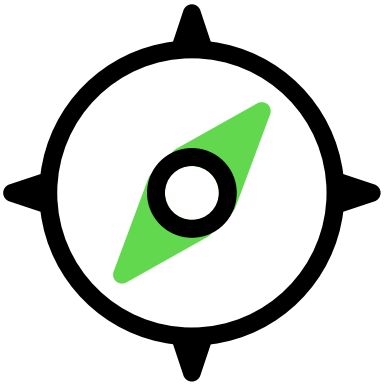
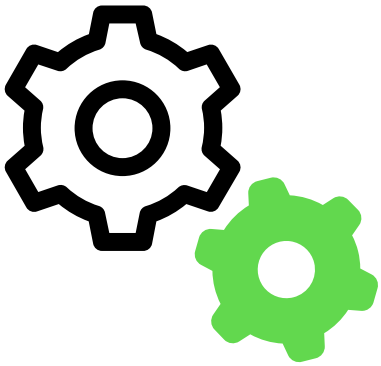
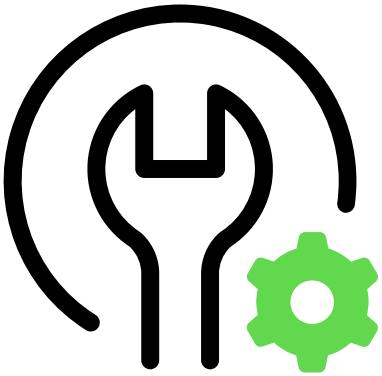
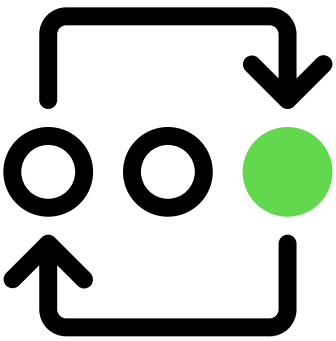
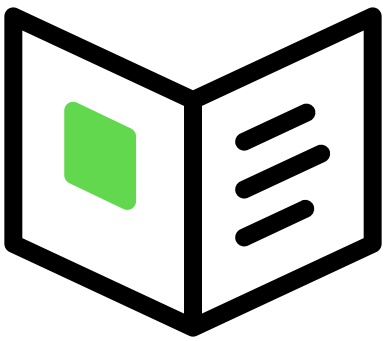
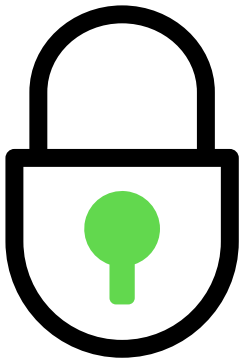
Inteligência contra ameaças

. ServiceNow® Inteligência contra ameaças A aplicação permite encontrar indicadores de comprometimento (IOC) e enriquecer incidentes de segurança com dados de inteligência contra ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar	Configurar	Administrar
		
Conheça os conceitos de Inteligência contra ameaças e seus principais recursos.	Configure, conheça os componentes instalados e as funções de usuário necessárias para atender às suas necessidades de negócios.	Defina as propriedades da Inteligência contra ameaças.
Integrar	Uso	Estrutura do MITRE ATT&CK
		
Estenda os recursos de Inteligência contra ameaças integrando com a ServiceNow e aplicações de terceiros.	Gerencie indicadores de comprometimento (IOC) e vários artefatos.	Estrutura MITRE-ATT&CK Identifique rapidamente ameaças e coordene respostas a ataques cibernéticos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Case Management



Gerencie a Gestão de casos de segurança reunindo informações sobre atividades suspeitas.

Recursos de aprendizado

- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Faça perguntas e explore outros recursos para Inteligência contra ameaças em Comunidade ServiceNow
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente
- Biblioteca de recursos de operações de segurança
- Comunidade de Operações de segurança

Noções básicas do Inteligência contra ameaças

. Inteligência contra ameaças A aplicação permite que você acesse e forneça um ponto de referência para a expressão estruturada de informações sobre ameaças da sua empresa (STIX ™) dados. Incluído em Inteligência contra ameaças. Gestão de casos de segurança aplicação, que fornece um meio para analisar ameaças à sua organização representadas por campanhas direcionadas ou agentes estatais.

STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. Usando dados do STIX e troca automatizada confiável de informações de indicador (TAXII ™), os profissionais de ameaças podem usar informações compartilhadas de ameaças cibernéticas para isolar ameaças que foram identificadas anteriormente por sua empresa e de outras fontes. O TAXII possibilita a troca automatizada generalizada de informações de ameaças cibernéticas.

Inteligência contra ameaças Compatível com STIX versões 1,1, 2,0 e 2,1.

STIX ™e. TAXII ™São marcas comerciais da MITRE Corporation.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Domain Separation e Inteligência contra ameaças

Domain Separation é compatível com Inteligência contra ameaças Módulo que está disponível como parte da Resposta a incidentes de segurança. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

No módulo Inteligência contra ameaças (como parte da aplicação Resposta a incidentes de segurança), a separação de domínio permite que os provedores de serviço (SPs) criem e gerenciem o repositório de inteligência contra ameaças das seguintes maneiras:

- Perfis de origens de ameaça e Trusted Automated Exchange of Indicator Information (TAXII)
- Observáveis
- Indicadores de comprometimento
- Modos/métodos de ataque a ameaças e gestão de casos em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço mais alta

Ter espaços de trabalho do cliente separados para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte ao Domain Separation em Inteligência contra ameaças por versão

Separação de domínios para o módulo Inteligência contra ameaças (como parte do Resposta a incidentes de segurança(aplicação) abrange as seguintes funcionalidades do produto:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os observáveis de incidentes de segurança são direcionados para o domínio apropriado do usuário cujo ID/Credencial/Escopo gera o incidente. Os observáveis extraídos do incidente são armazenados no domínio do incidente de segurança.
- Configuração de perfis de serviço do TAXII para baixar uma ou mais coleções do TAXII que oferecem feeds de informações de ameaças cibernéticas. A configuração é armazenada no domínio no qual o perfil está sendo configurado.
- Configuração do download de feeds de ameaças no repositório IOC no domínio no qual a configuração está sendo realizada.
- Criação de modos/métodos de ataque no domínio da origem de inteligência contra ameaças que fornece as informações automaticamente ou o domínio no qual um novo modo/método de ataque está sendo adicionado manualmente pelo usuário
- Criação de casos para investigação de longo prazo de incidentes, observáveis, ICs, usuários e indicadores de comprometimento (IOC) associados ao caso. O caso é armazenado no domínio criado pelo usuário.

Nota: Em todos os casos acima, os princípios abrangentes de visibilidade em domínios separados na NOW Platform se aplicam. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como o Domain Separation funciona no Inteligência contra ameaças(como parte de Resposta a incidentes de segurança)

A Inteligência contra ameaças faz parte da Resposta a incidentes de segurança nas camadas Professional e Enterprise, mas não na camada Standard. Um plug-in separado é necessário. O módulo Inteligência contra ameaças (como parte do Resposta a incidentes de segurança cria e gerencia as informações de inteligência contra ameaças associadas a incidentes de segurança em uma organização. Os seguintes casos de uso reconhecem a separação de domínios:

- Criação de observáveis de incidentes de segurança no momento da criação do incidente
  - De analisadores de e-mail (baseado em plataforma, phishing relatado pelo usuário, personalizado)
  - De aplicações em armazenamentos do Security Information and Event Management (SIEM) de terceiros
  - Inserido manualmente pelo analista do SOC
- Coleção de observáveis de origens do feed de ameaças - origens de inteligência contra ameaças de coleções TAXII
- Gerenciar observáveis de incidentes de segurança
  - Associe observáveis a indicadores relacionados
  - Associe observáveis a incidentes de segurança
  - Associe observáveis a observáveis secundários
  - Associe o observável à origem do feed de ameaças
  - Adicione anotações de segurança aos observáveis
- Gerenciar indicadores de comprometimento
  - Associe indicadores a observáveis relacionados
  - Associe indicadores ao modo/método de ataque

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Associe indicadores a tipos de indicador
- Associe indicadores à origem do feed de ameaças
- Adicione anotações de segurança aos indicadores

- Gerenciar casos
  - Criar caso (manualmente ou a partir de um incidente)
  - Editar um novo caso para adicionar detalhes (escolha o tipo de caso e a gravidade, adicionar incidentes, observáveis, itens de configuração, usuários, indicadores)
  - Exclua um caso

Configuração do Domain Separation

A configuração do Domain Separation para Inteligência contra ameaças não requer etapas adicionais. Todas as tabelas de Inteligência contra ameaças adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Observáveis de incidentes de segurança em um domínio não podem ser exibidos no escopo de outros domínios.
- Indicadores de comprometimento em um domínio não podem ser exibidos no escopo de outros domínios.
- Os modos/métodos de ataque associados a um domínio não podem ser exibidos no escopo de outros domínios.
- Os perfis de serviço TAXII associados a um domínio não podem ser exibidos no escopo de outros domínios.
- As origens de inteligência contra ameaças associadas a um domínio não podem ser exibidas no escopo de outros domínios.
- Os casos associados a um domínio não podem ser exibidos no escopo de outros domínios.

As propriedades da Inteligência contra ameaças são definidas no nível global e, portanto, não são separadas por domínio. As configurações incluem:

- O nome do domínio para recuperar informações adicionais para endereços IP/URLs
- A chave de API a ser usada para recuperação
- Pesquisa de tabelas IOC locais antes de enviar para o scanner remoto
- Número de dias em que observáveis locais são considerados
- Marcar um modo/método de ataque como inativo quando não recebido de fontes de informações de ameaça
- Marcando um indicador como inativo quando não recebido de nenhuma origem por um número especificado de dias

Configuração

Todos os aspectos da configuração da funcionalidade de inteligência contra ameaças são independentes em um ambiente separado por domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As seguintes tarefas podem ser configuradas por domínio:

1. Criação de perfis de serviço TAXII
   - Escolha uma configuração de serviço da Descoberta
   - Escolha uma configuração de serviço de coleção - Atribua funções a usuários e grupos de usuários
2. Criação de fontes de inteligência contra ameaças
   - Configure o serviço REST que fornece as informações de informações sobre ameaças
   - Programe o download de informações de informações sobre ameaças
   - Escolha as informações de detalhes da ameaça para atribuir à origem
3. Criação de modos/métodos de ataque (manual)
   - Origem, tipo de malware, mecanismo de ataque, tipo de agente de ameaça, descrição, efeito pretendido, visto pela primeira vez, visto pela última vez
   - Indicadores relacionados, modo/método de ataque secundário, incidentes de segurança associados

   Nota: Os modos/métodos de ataque também são criados automaticamente a partir das origens do feed de ameaças.

4. Definir listas padrão para as seguintes categorias de informações de ameaça:
   - Mecanismos de ataque
   - Métodos de descoberta
   - Feeds
   - Tipos de indicador
   - Efeitos pretendidos
   - Notificações
   - Tipos de observável
   - Definições de limite de taxa
   - Tipos de agente da ameaça
   - Motivações de ataque
   - Tipos de infraestrutura
   - Capacidades de malware
   - Tipos de malware
   - Tipos de relatório
   - Funções do agente de ameaça
   - Tipos de ferramenta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários do domínio do locatário podem criar seus próprios perfis de serviço TAXII.
- Os proprietários do domínio do locatário podem criar suas próprias fontes de inteligência contra ameaças.
- Os proprietários do domínio do locatário podem criar seus próprios modos/métodos de ataque.
- Os proprietários do domínio do locatário podem criar suas próprias listas padrão para categorias de informações de ameaça.

Nota: A lógica de negócios e os processos permitem que os cronogramas de download da fonte de inteligência contra ameaças sejam separados por domínio pelo proprietário da instância.

Tópicos relacionados

Domain Separation para provedores de serviço

Configurar Inteligência contra ameaças.

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store. Você também pode configurar propriedades e definir uma origem de ameaça.

Instalar Inteligência contra ameaças

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração suaves.

Tarefas de configuração	Descrição
Verifique se você tem o necessário ServiceNow funções para sua instância.	As seguintes funções são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá a função de Administrador de ameaças [sn_ti.admin]. • O administrador de ameaças [sn_ti.admin] supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

Siga as instruções para baixando uma aplicação do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Definido Inteligência contra ameaças propriedades.

Componentes instalados com Inteligência contra ameaças

Vários tipos de componentes são instalados com a ativação do plug-in Inteligência contra ameaças, incluindo tabelas e funções do usuário.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de ameaças [sn_ti.admin]	Tem controle total sobre todas as propriedades de ameaça, SLAs e notificações.	sn_ti.write
Leitor de ameaças [sn_ti.read]	Tem acesso de leitura a informações de ameaça.	sn.sec_cmn.int_read
Criador de ameaças [sn_ti.write]	Tem acesso de gravação a informações de ameaça. Não é possível excluir modos de ataque, indicadores ou observáveis. Apenas um administrador de ameaças pode excluí-los.	• sn_sec_cmn.int_write • sn_ti.read
Analista de MITRE [sn_ti.miter_analyst]	Esta função permite o acesso de leitura ao MITRE-ATT&CK módulos em Inteligência contra ameaças e para SIR módulo.	• sn_ti.read • sn_si.read

Tabelas instaladas

Tabela	Descrição
Mecanismo de ataque [sn_ti_attack_mechanism]	Organiza padrões de ataque hierarquicamente com base em mecanismos que são frequentemente empregados ao explorar uma vulnerabilidade. As categorias que são membros desta exibição representam as diferentes técnicas usadas para atacar um sistema.
Modo/método de ataque [sn_ti_attack_mode]	Modos e métodos de ataque são representações do comportamento de adversários cibernéticos. Caracterizam o que um adversário faz e como o faz em níveis crescentes de detalhe.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Método de descoberta [sn_ti_discovery_method]	Uma expressão de como um incidente foi descoberto.
Feed [sn_ti_feed]	Usado para configurar o Feed de ameaças (RSS) na Visão geral da ameaça.
Modo/método de ataque do indicador [sn_ti_m2m_indicator_attack_mode]	Usado para mapear modos/métodos de ataque para indicadores.
Indicador de comprometimento [sn_ti_indicator]	Usado para transmitir padrões observáveis específicos combinados com informações contextuais destinadas a representar artefatos e/ou comportamentos de interesse em um contexto de segurança cibernética.
Metadados do indicador de comprometimento [sn_ti_indicator_metadata]	Usado para preencher registros TAXII.
Origem do Indicador [sn_ti_m2m_indicator_source]	Usado para coletar todas as fontes que relatam o indicador específico.
Tipo de indicador [sn_ti_indicator_type]	Caracteriza um indicador de ameaça cibernética composto por um padrão que identifica determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões, como e quando eles são agidos e assim por diante.
Tipo de indicador associado [sn_ti_m2m_indicator_indicator_type]	Vincula indicadores com seus tipos aplicáveis
Contagem de incidentes [sn_ti_observable]	Número de incidentes de segurança associados a um observável.
Efeito pretendido [sn_ti_intend_effect]	Usado para expressar o efeito pretendido de um agente de ameaça.
Resultado da verificação de IP [sn_ti_ip_result]	Usado para mostrar os resultados de uma pesquisa de IP.
Limite de taxa de malware [sn_ti_rate_limit]	Define um limite de taxa a ser usado em uma origem de pesquisa.
Verificação de malware [sn_ti_scan]	Uma pesquisa. Contém o que pesquisar, com a origem da pesquisa e um resumo dos resultados da pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Entrada da fila de verificação de malware [sn_ti_scan_q_entry]	Um registro de pesquisa enfileirado para pesquisa ou processamento. Facilita as solicitações dentro dos limites de taxa estabelecidos.
Resultado da verificação de malware [sn_ti_scan_result]	Exibe o resultado de uma pesquisa.
Scanner de malware [sn_ti_scanner]	Define origens de pesquisa de terceiros a serem usadas na execução de pesquisas.
Limite de taxa do scanner de malware [sn_ti_scanner_rate_limit]	Associa uma origem de pesquisa a um limite de taxa.
Tipo de malware [sn_ti_malware_type]	Usado para expressar os tipos de instâncias de malware.
Observável [sn_ti_observable]	Observáveis no STIX representam propriedades com estado ou eventos mensuráveis pertinentes à operação de computadores e redes.
Tipo de contexto de observável [sn_ti_observable_context_type]	Armazena o contexto (origem, destino de um endereço IP e assim por diante) de um observável.
Indicador observável [sn_ti_m2m_observable_indicator]	Usado para relacionar observáveis a indicadores.
Origem de Observável [sn_ti_observable_source]	Usado para relacionar observáveis a origens de ameaça.
Tipo de Observável [sn_ti_observable_type]	Lista os vários tipos de observáveis, como endereços IP.
Categoria de Tipo de Observável [sn_ti_observable_type_category]	Armazena a primeira categorização de observáveis (por exemplo, endereços IP e URLs). É usado para determinar com mais precisão os tipos de observáveis.
Modo/método de ataque relacionado [sn_ti_m2m_attack_mode_attack_mode]	Usado para relacionar modos de ataque entre si.
Observáveis Relacionados [sn_ti_m2m_observables]	Usado para relacionar observáveis entre si.
Tipo de verificação [sn_ti_scan_type]	A definição de um tipo de pesquisa, com registros iniciais para Arquivo, URL e IP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Caso de segurança [sn_ti_case]	Armazena registros de casos de segurança criados usando a Gestão de casos.
IoC de caso de segurança [sn_ti_case_ioc]	Usado para gerenciar o relacionamento entre observáveis e casos.
Tarefa relacionada ao caso de segurança [sn_ti_m2m_case_task]	Usado para gerenciar o relacionamento entre tarefas (incidentes de segurança, solicitações de mudança e assim por diante) com casos de segurança.
Exclusão de relacionamento de caso de segurança [sn_ti_case_relationship_exclusion]	Fornece a definição de inclusão e exclusão de registros relacionados em casos de segurança.
Detecção [sn_ti_sighting]	O link m2m entre o observável e o resultado detalhado da Pesquisa de vistas usado na execução de uma solicitação de Pesquisa de vistas.
Itens de Configuração de detecções [sn_ti_m2m_sighting_ci]	Mapeia itens de configuração para uma Pesquisa de vistas.
Detalhe da pesquisa de vistas [sn_ti_sighting_search_detail]	Detalhes de uma Pesquisa de avistamento, por exemplo, o número de itens externos internos encontrados.
Resultado da pesquisa de vistas [sn_ti_sighting_search]	O cabeçalho de uma execução de Pesquisa de vistas.
Tipos de observáveis compatíveis [sn_ti_m2m_ind_type_obs_type]	Relaciona tipos de indicador a tipos de observáveis válidos.
Tipo de verificação compatível [sn_ti_supported_scan_type]	Mapeia o tipo de pesquisa para uma implementação específica de origem/ fornecedor de pesquisa. Indica que uma origem de pesquisa específica oferece suporte ao tipo .
Modo/método de ataque de tarefa [sn_ti_m2m_task_attack_mode]	Relaciona modos de ataque a tarefas.
Indicador de tarefa [sn_ti_m2m_task_indicator]	Relaciona indicadores a tarefas.
Observável de tarefa [sn_ti_m2m_task_observable]	Relaciona observáveis a tarefas.
Detecção de tarefa [sn_ti_m2m_task_sighting]	Armazena registros de tarefa (incidentes e casos de segurança) relacionados a um registro de avistamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Coleta TAXII [sn_ti_taxii_collection]	Define um feed de inteligência de risco cibernético que pode ser importado por um servidor TAXII.
Perfil TAXII [sn_ti_taxii_profile]	Define um repositório para compartilhar inteligência contra risco cibernético. Contém coleções TAXII.
Tipo de agente de ameaça [sn_ti_threat_actor_type]	Fornece caracterizações de agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo intenção presumida e comportamento observado historicamente.
Fonte da inteligência contra ameaças [sn_ti_source]	Define uma origem para importar dados de ameaça.
Motivação de ataque associada [sn_ti_stix2_m2m_object_attack_motivation]	Coleta todas as motivações de ataque associadas a um objeto STIX.
Tipo de infraestrutura associado [sn_ti_stix2_m2m_infra_type]	Vincula a infraestrutura aos seus tipos.
Fase da cadeia de eliminação associada [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Vincula fases da cadeia de inutilização a indicadores.
Fase da cadeia de eliminação associada [sn_ti_stix2_m2m_object_kill_chain_phase]	Vincula fases da cadeia de inutilização a objetos STIX.
Recurso de malware associado [sn_ti_stix2_m2m_malware_capability]	Vincula o malware com seus recursos.
Tipo de malware associado [sn_ti_stix2_m2m_malware_type]	Vincula malware aos seus tipos.
Observável associado [sn_ti_stix2_m2m_malware_observable]	Coleta todos os observáveis associados a um malware.
Observável associado [sn_ti_stix2_m2m_observed_data_observable]	Coleta todos os observáveis associados a dados observados.
Tipo de relatório associado [sn_ti_stix2_m2m_report_report_type]	Vincula relatórios de ameaças aos tipos.
Função do agente da ameaça associado [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Vincula os agentes de ameaça às suas funções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Tipo de agente da ameaça associado [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Vincula os agentes de ameaça aos seus tipos.
Tipo de ferramenta associado [sn_ti_stix2_m2m_tool_type]	Vincula ferramentas com seus tipos.
Motivação de ataque [sn_ti_stix2_attack_motivation]	A motivação do ataque molda a intensidade e a persistência de um ataque. Os agentes de ameaça e os conjuntos de invasão geralmente agem de uma maneira que reflete sua emoção ou situação subjacente, e isso informa os defensores da maneira de ataque.
Padrão de ataque [sn_ti_stix2_attack_pattern]	Um tipo de TTP que descreve métodos que os adversários usam para tentar comprometer metas.
Campanha [sn_ti_stix2_campanha]	Um agrupamento de comportamentos adversários que descrevem um conjunto de atividades ou ataques mal-intencionados (às vezes chamados de ondas) que ocorrem durante um período em relação a um conjunto específico de metas.
Linha de ação [sn_ti_stix2_course_of_action]	Uma recomendação de um produtor de inteligência para um consumidor sobre as ações que ele pode tomar em resposta à inteligência.
Referência externa [sn_ti_stix2_external_reference]	Ponteiros para informações representadas fora do STIX.
Detecção de identidade [sn_ti_stix2_m2m_sighting_identity]	Coleta todas as identidades associadas a um avistamento.
Identidade [sn_ti_stix2_identity]	Indivíduos, organizações ou grupos reais (por exemplo, ACME, Inc.), bem como classes de indivíduos, organizações, sistemas ou grupos (por exemplo, o setor financeiro).
Referência externa do indicador [sn_ti_stix2_indicator_external_reference]	Representa referências externas associadas a indicadores.
Detecção do indicador [sn_ti_stix2_indicator_sighting]	Representa vistas de indicadores.
Tipo de infraestrutura [sn_ti_stix2_infrastruction_type]	Representa os vários tipos de infraestrutura.
Infraestrutura	Um tipo de TTP que descreve todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_infrastructure]	destinados a oferecer suporte a alguma finalidade (por exemplo, servidores C2 usados como parte de um ataque, dispositivo ou servidor que fazem parte da defesa, servidores de banco de dados visados por um ataque e similares).
Software instalado [sn_ti_stix2_m2m_malware_analysis_sw]	Coleta todos os softwares (tipos de software SCO) associados a uma análise de malware.
Conjunto de intrusão [sn_ti_stix2_intrusão_set]	Um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns que se acredita serem orquestrados por uma única organização.
Fase da cadeia de eliminação [sn_ti_stix2_kill_chain_phase]	Representa fases da cadeia de destruição associadas a uma cadeia de destruição.
Cadeia de eliminação [sn_ti_stix2_kill_chain]	Representa várias cadeias de destruição.
Local [sn_ti_stix2_location]	Representa uma localização geográfica fornecida por meio do STIX.
Análise de malware [sn_ti_stix2_malware_analysis]	Os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.
Capacidade do malware [sn_ti_stix2_malware_capability]	Representa recursos comuns que uma família ou instância de malware exibe.
Sistema operacional de malware [sn_ti_stix2_m2m_malware_operating_system]	Coleta todos os sistemas operacionais (tipos de software SCO) associados ao malware.
Malware [sn_ti_stix2_malware]	Um tipo de TTP que representa código mal-intencionado.
Definição de marcação [sn_ti_stix2_marking_definition]	Representa requisitos de manipulação ou compartilhamento de objetos STIX.
Detecção de objeto [sn_ti_stix2_object_sighting]	Representa vistas de objetos STIX.
Relacionamento objeto-indicador [sn_ti_stix2_m2m_object_indicator]	Coleta todos os relacionamentos entre objetos STIX e indicadores STIX.
Relacionamento objeto-objeto	Coleta todos os relacionamentos entre objetos STIX e outros objetos STIX, excluindo os indicadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_m2m_object]	
Relacionamento objeto-observável [sn_ti_stix2_m2m_object_observable]	Coleta todos os relacionamentos entre observáveis STIX e objetos STIX.
Detecção de dados observados [sn_ti_stix2_m2m_sighting_observed_data]	Coleta todos os objetos de dados observados associados a um avistamento.
Dados observados [sn_ti_stix2_observed_data]	Transmite informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os objetos de observação cibernética (SCOs) do STIX.
Tipo de relatório [sn_ti_stix2_report_type]	Representa a finalidade primária ou o assunto dos relatórios de ameaças.
Observável relatado [sn_ti_stix2_m2m_malware_analysis_observable]	Coleta todos os observáveis associados à Análise de malware.
Objeto STIX V2 [sn_ti_stix2_object]	Tabela primária comum para objeto STIX.
Detecção de STIX V2 [sn_ti_stix2_sighting]	Tabela primária comum para tabelas de vistas STIX.
Função de agente da ameaça [sn_ti_stix2_threat_actor_role]	Representa funções que podem ser desempenhadas por agentes de ameaça.
Agente da ameaça [sn_ti_stix2_threat_actor]	Os agentes de ameaça são indivíduos, grupos ou organizações reais que se acredita estarem operando com intenção mal-intencionada.
Grupo de ameaça [sn_ti_stix2_threat_grouping]	Agrupa todos os objetos STIX que compartilham algum contexto comum.
Anotação de ameaça [sn_ti_stix2_threat_note]	Fornece contexto e análise adicional não contidos no objeto STIX correspondente.
Opinião sobre ameaças [sn_ti_stix2_threat_opinion]	Fornece avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente.
Relatório de ameaças [sn_ti_stix2_threat_report]	Relatórios são coleções de inteligência contra ameaças com foco em um ou mais tópicos, como uma descrição de um agente de ameaça, malware ou técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	relacionada a publicar como uma história abrangente de ameaças cibernéticas.
Tipo de Ferramenta [sn_ti_stix2_tool_type]	As categorias de ferramentas que podem ser usadas para executar ataques.
Ferramenta [sn_ti_stix2_tool]	Ferramentas são software legítimo que é usado por agentes de ameaça para executar ataques.
Vulnerabilidade [sn_ti_stix2_vulnerability]	Representa fraqueza ou defeito nos requisitos, projetos ou implementações da lógica computacional (código de exemplo) encontrados no software e em alguns componentes de hardware (firmware de exemplo). Eles podem ser explorados diretamente para afetar negativamente a confidencialidade, integridade ou disponibilidade desse sistema.

Definido Inteligência contra ameaças propriedades

Inteligência contra ameaças As propriedades permitem que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração** > **Propriedades**.
2. Defina as propriedades a seguir, conforme necessário.

Propriedades da Inteligência contra ameaças

Propriedade	Descrição
O nome do domínio para recuperar informações adicionais para endereços IP/URLs sn_ti.ip_lookup.web_site	O nome de domínio a ser usado para recuperar informações adicionais em seu banco de dados IOC. Esta propriedade é usada pelo `ThreatAdditionalInfo` Inclusão de script para preencher informações adicionais no formulário Observáveis. Valor padrão: http://api.ipinfodb.com/v3/ip-country/

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	Nota: A API de terceiros pinfodb.com está disponível sem custo extra e é usada em muitos programas de software comerciais. Se você substituí-lo por um nome de domínio diferente, também deverá fornecer a chave de API no próximo campo.
A chave de API a ser usada para o domínio, se houver sn_ti.ip_lookup.api_key	A chave de API a ser usada para recuperar informações adicionais em seu banco de dados IOC. Esta propriedade é usada (junto com a propriedade sn_ti.ip_lookup.web_site) pelo `ThreatAdditionalInfo` Inclusão de script para preencher informações adicionais no formulário Observáveis.
Não execute a pesquisa automatizada de ameaças em um observável quando o observável estiver associado a um IOC ou for considerado mal-intencionado. sn_ti.scan_ioc_before_sending **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.scan_ioc_num_days).	Opção para parar de executar a pesquisa automatizada de ameaças em um observável quando o observável for considerado mal-intencionado ou associado a um IOC pela duração configurada (em dias). Se você ainda precisar executar a ameaça, pesquise o observável, poderá fazê-lo manualmente. Valor padrão: sim
Duração (em dias) sn_ti.scan_ioc_num_days	Opção para definir a duração até a qual a pesquisa automatizada de ameaças do observável é ignorada. Valor padrão (em dias): 30
Não execute a pesquisa automatizada de ameaças em um observável se já estiver em execução. sn_ti.enable_threat_lookup_bypass **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.threat_lookup_bypass_times).	Se já houver um resultado de pesquisa de ameaça para um observável disponível, você terá a opção de ignorar a reexecução da pesquisa de ameaça automatizada para o mesmo observável até que a duração configurada tenha passado. Valor padrão: não **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.
Duração (em minutos) sn_ti.threat_lookup_bypass_time	Opção para definir a duração após a qual a pesquisa automatizada de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	ameaças do observável pode ser executada novamente. Valor padrão (em minutos): 0
Defina uma duração de validade para substituições do usuário na descoberta observável. sn_ti.enable_observable_finding_system_override **Nota:** Você precisa definir a validade na próxima propriedade (sn_ti.observable_finding_override_expiry).	Opção para definir uma duração de validade para substituições do usuário nas descobertas observáveis. A descoberta da pesquisa de ameaças do observável não será alterada pelo sistema de base durante essa duração de validade. Valor padrão: Não **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.
Validade (em minutos) sn_ti.observable_finding_override_expiry	Opção para definir o período de validade da descoberta observável. Valor padrão (em minutos): Nenhum
Quando um modo/método de ataque não tiver sido recebido de nenhuma fonte pelo número de dias especificado, marcá-lo como inativo sn_ti.attack_mode_inactivate_days	Número de dias a partir da última vez que um modo/método de ataque foi recebido para o registro ser marcado como inativo. Valor padrão: 360 **Nota:** . **Ativo** a caixa de seleção não está visível no **Modo/método de ataque** formulário por padrão. No entanto, você pode adicioná-lo. Quando os modos/métodos de ataque estão inativos, eles não podem ser selecionados em outros formulários.
Quando um indicador não tiver sido recebido de nenhuma fonte pelo número de dias especificado, marcá-lo como inativo sn_ti.indicator_inactivate_days	Número de dias a partir do momento em que um indicador foi recebido pela última vez para o registro ser marcado como inativo. Valor padrão: 180 **Nota:** . **Ativo** a caixa de seleção não está visível no **Indicador** formulário por padrão. No entanto, você pode adicioná-lo. Quando os indicadores estão inativos, eles não podem ser selecionados em outros formulários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
O tamanho máximo da carga (em MB) para um anexo STIX que pode ser analisado. sn_ti.stix.max_payload_size	Especifica o tamanho máximo da carga do anexo STIX que você pode analisar. Valor-padrão: nenhum Valor máximo permitido: Sem limite.
Tempo máximo em segundos que uma conexão HTTP de saída aguarda para obter dados de coleta de TAXII sn_ti.taxii.http.max_timeout	Especifica a quantidade máxima de tempo que uma conexão HTTP de saída espera antes de buscar o próximo pacote de dados de coleta TAXII. Valor padrão: 300
Número máximo de objetos recuperados em uma chamada REST de um servidor TAXII (aplicável somente para TAXII versões 2.0 e 2.1) sn_ti.taxii.max_page_size	Especifica o número máximo de objetos recuperados em uma chamada REST do servidor TAXII para uma página. Valor padrão: 5000 Valor máximo permitido: 50000
Número máximo de novas tentativas para uma chamada REST DO TAXII 2.X. sn_ti.taxii2.retry_count	Especifica o número máximo de novas tentativas para uma chamada REST DO TAXII com falha. Valor padrão: 3

3. Clique em **Salvar**.

Defina uma origem de ameaça

Você pode manter uma lista de Inteligência contra ameaças origens da ameaça. Cada origem inclui a capacidade de definir com que frequência uma origem é consultada. Você também pode executar uma origem de ameaça sob demanda para importar os dados do Stix (Structured Threat Information Expression) necessários.

Antes de Iniciar

Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

Inteligência contra ameaças Emprega duas tecnologias para importar informações relacionadas a ameaças: STIX e Trusted Automated Exchange of Indicator Information (TAXII).

O STIX fornece uma linguagem padronizada e estruturada para representar um amplo conjunto de informações de ameaças cibernéticas que inclui indicadores de atividade de comprometimento (IOC) (por exemplo, endereços IP e hashes de arquivo), bem como informações contextuais sobre ameaças, como modos/métodos de ataque, que, juntos, caracterizam mais completamente as motivações, capacidades e atividades de um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adversário cibernético. Como tal, os dados do STIX fornecem informações valiosas sobre como sua organização pode se defender melhor contra ameaças virtuais.

Trusted Automated Exchange of Indicator Information (TAXII) é usado para facilitar a troca automatizada de informações de ameaças virtuais. O TAXII define um conjunto de serviços e trocas de mensagens que permitem o compartilhamento de informações acionáveis de ameaças virtuais entre a organização e os limites de produto/serviço para a detecção, prevenção e mitigação de ameaças virtuais. Os perfis TAXII podem ser configurados como repositórios para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds do TAXII.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Origens** > **Origens de Ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da origem da ameaça.
Aplicação	A aplicação que contém este registro.
Ativo	Marque esta caixa de seleção para ativar a origem da ameaça.
Avançado	Marque esta caixa de seleção para exibir os scripts no **Script de fábrica de integração** e. **Processador de relatório** campos.
Descrição	Uma descrição desta origem de ameaça.

4. Preencha os campos em **Programação** , conforme apropriado.

Campo	Descrição
Executar	A frequência que você deseja que a integração execute, Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos com base na configuração desse campo.
Dia	O dia em que você deseja que a integração seja executada. ○ Se você selecionou **Semanalmente** em **Executar** este campo exibe os dias da semana. ○ Se você selecionou **Mensal** em **Executar** este campo exibe os dias do mês.
Hora	A hora em que você deseja que a integração comece.
Intervalo de repetição	Se você selecionou **Periodicamente** em **Executar** este campo exibe o número de dias e horas antes que a integração seja executada novamente.
Iniciando	Se você selecionou **Periodicamente** em **Executar** este campo exibe as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Se quiser adicionar parâmetros condicionais, selecione este campo.
Condição	Se você selecionou **Condicional** insira as condições aqui.

5. Preencha os campos em **Detalhes da ameaça** , conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Indicador	O indicador a ser usado quando os dados não fornecem um explicitamente. Para listas de bloqueios, se vazias, um novo indicador será criado para cada observável.
Tipo de indicador	O tipo de indicador a ser usado para indicadores criados e os dados não fornecem explicitamente um tipo de indicador.
Modo/método de ataque	O modo/método de ataque a ser usado quando os dados não fornecem um explicitamente.
Tipo de Observável	O tipo de observável a ser usado para observáveis criados e os dados não fornecem explicitamente um tipo de observável.[SI1]
Peso	Insira um valor de ponderação para esta origem a ser usada no cálculo de confiança.

Nota: O uso do **Indicador** , **Tipo de indicador** , **Modo/método de ataque** e **Tipo de observável** os campos são específicos da implementação. O processador padrão, SimpleBlocklistProcessor, se comporta como as dicas da ferramenta descrevem. No entanto, uma origem de ameaça TAXII é totalmente orientada por dados. Qualquer processador de origem de ameaça personalizado poderá usar sua própria estratégia. Basicamente, esses campos são itens a serem expostos à integração/processador e a implementação decide como usá-los.

6. Preencha os campos em **Detalhes da origem** , conforme apropriado.

Campo	Descrição
Endpoint	Insira o URL do endpoint do serviço web por onde a origem da ameaça é acessada Inteligência contra ameaças. Clique no ícone de cadeado para bloquear o URL.
Usar mensagem REST	Se você precisar de uma mensagem REST para acessar a origem da ameaça, marque esta caixa de seleção. . **Mensagem REST** e. **Método REST** os campos se tornam obrigatórios.
Mensagem REST	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** . Defina uma nova mensagem REST .
Método REST	Clique no ícone de pesquisa e selecione o método REST na lista ou clique em **Novo** Para definir um novo método REST.
Script de integração	O script de integração padrão é **SimpleRESSecurityDataIntegration** . Ele executa uma chamada REST simples, salva a resposta como um anexo e retorna o anexo para o processador. Este script atende às necessidades da maioria das organizações. Se quiser, clique no ícone de pesquisa e selecione um script de integração diferente ou defina um novo.
Script de fábrica de integração	. **Avançado** se a caixa de seleção estiver marcada, este campo exibirá o script real para criar o script de integração. Você pode editar o script conforme necessário. Esta capacidade é útil para implementações personalizadas. As integrações no sistema de base geralmente não precisam de lógica de construtor personalizada.
Processador de relatórios	O script de integração padrão é **SimpleBlocklistProcessor** . Este script é um processador simples que aceita uma lista de bloqueios simples (simples, ou seja, um documento de coluna única com observáveis, como URLs ou endereços IP) e cria observáveis. Ele usa os vários **Detalhes da ameaça** campos para determinar quais campos definir quando observáveis são criados.
Script de fábrica do processador	. **Avançado** se a caixa de seleção estiver marcada, este campo exibirá o script real para construir o processador. Você pode editar o script conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Geralmente, esse script é útil para implementações personalizadas. As integrações no sistema de base geralmente não precisam de lógica de construtor personalizada.

7. Clique em **Enviar**.

Nota: Para obter mais informações sobre como configurar a paginação da origem da ameaça, consulte KB1213825 artigo.

Crie um perfil TAXII

Você pode manter perfis TAXII para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds do TAXII.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Clique em **Nova**.
3. Preencha os seguintes campos conforme apropriado.

Campo	Descrição
Nome	O nome do perfil TAXII
Aplicação	A aplicação que contém este registro.
Usar mensagens de REST como modelo	Se você precisar de uma mensagem REST para acessar o perfil TAXII, marque esta caixa de seleção.
Versão de TAXII	Especifique a versão do TAXII. As versões compatíveis do STIX são 1,1, 2,0 e 2,1.
Descrição	Uma descrição deste perfil TAXII.

4. Preencha os campos em **Configuração do serviço da Descoberta** , conforme apropriado.

Campo	Descrição
Endpoint do serviço de descoberta	O endpoint da Descoberta autoriza os clientes a obter informações sobre um servidor TAXII e obter uma lista de raízes de API.
Usar Mensagem REST	Selecione esta opção se você precisar de uma mensagem REST para acessar o perfil TAXII. . **Mensagem REST do Serviço da Descoberta** e. **Método REST do Serviço de Descoberta** os campos se tornam obrigatórios.
Mensagem de REST do serviço de descoberta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** Para definir uma nova mensagem REST.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Método de REST do serviço de descoberta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** Para definir um novo método REST.

5. Preencha os campos em **Configuração do serviço de coleta** , conforme apropriado.

Campo	Descrição
Endpoint do serviço de informações de coleta	TAXII Collection é uma interface para um repositório lógico de objetos CTI fornecidos por um servidor TAXII e é usada por clientes TAXII para enviar informações para o servidor TAXII ou solicitar informações do servidor TAXII. Um servidor TAXII pode hospedar várias coleções por raiz de API, e as coleções são usadas para trocar informações de maneira de solicitação-resposta.
Usar Mensagem REST	Selecione esta opção se você precisar de uma mensagem REST para acessar o perfil TAXII. . **Mensagem REST do serviço de informações da coleção** e. **Método REST do serviço de informações da coleção** os campos se tornam obrigatórios.
Mensagem de REST do serviço de informações de coleta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** Para definir uma nova mensagem REST.
Método de REST do serviço de informações de coleta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** Para definir um novo método REST.

6. Clique em **Enviar**.

Repositório LOC

O repositório IOC contém objetos STIX, cada um desses objetos contém uma informação específica.

Ao combinar objetos STIX por meio de relacionamentos, você permite representações fáceis ou complexas da Inteligência contra ameaças cibernéticas (CTI).

Inteligência contra ameaças Compatível com STIX versões 1,1, 2,0 e 2,1.

Modos e métodos de ataque

Modos e métodos de ataque, às vezes chamados de táticas, técnicas e procedimentos (TTPs), são representações de como os adversários cibernéticos se comportam. Eles caraterizam o que esses adversários fazem e como o fazem, em níveis crescentes de detalhamento. Modos e métodos de ataque se aplicam STIX1,1.

Por exemplo, um modo/método de ataque pode ser usar malware para roubar credenciais de cartão de crédito. Ou outra tática relacionada (em um nível inferior de detalhe) pode ser enviar e-mails direcionados com anexos que contenham código malicioso, que é executado após a abertura, captura informações de cartão de crédito ao pressionar as

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

teclas e usa http para se comunicar com um servidor de comando e controle para transferir informações.

Modos e métodos de ataque se aplicam STIX1,1.

Defina um modo/método de ataque

Os modos e métodos de ataque são importados com dados do STIX, mas você pode adicionar novos modos/métodos, conforme necessário.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de classificação para adicionar metadados ao registro, você pode selecionar um ou mais marcadores para especificar o grau de sensibilidade do modo/método de ataque. Se você não configurou ou ativou marcadores de classificação, esta lista suspensa não será exibida.
Título	Insira um nome descritivo para este modo/método de ataque.
Tipo de malware	Selecione o tipo de malware para este modo/método de ataque. Os tipos de malware disponíveis são recuperados do servidor do fornecedor como dados STIX.
Origem	Selecione a fonte de dados da ameaça para este modo/método de ataque. Algumas fontes de dados estão incluídas com o sistema de base. Você pode criar novas fontes de dados conforme necessário.
Mecanismo de ataque	Selecione o mecanismo de ataque para este modo/método de ataque. Os mecanismos de ataque representam as diferentes técnicas usadas para atacar um sistema. Os mecanismos de ataque disponíveis são recuperados do servidor do fornecedor como dados STIX.
Visto pela primeira vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Visto pela última vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Tipo de Ator da Ameaça	Selecione o tipo de agente de ameaça para este modo/método de ataque. Os tipos de agente de ameaça caracterizam agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo intenção presumida e comportamento observado historicamente. Os tipos de agente de ameaça disponíveis são recuperados do servidor do fornecedor como dados do STIX.
Descrição	Insira uma descrição do modo/método de ataque.
Manipulação	Insira a instrução para lidar com este modo/método de ataque.
Efeito pretendido	Insira o efeito pretendido desse tipo de ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
   Você pode exibir qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça.
Modo/método de ataque secundário	Lista os modos/métodos de ataque que são secundários do modo/método de ataque primário.
Tarefas Associadas	Lista as mudanças associadas ao modo/método de ataque primário.

Adicione um IOC a um modo/método de ataque

Além de importar indicadores como dados STIX, você pode adicionar IOCs a um modo/método de ataque manualmente.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um IOC.
3. Clique em **Indicadores relacionados** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o IOC que você deseja adicionar.
6. Usando o slushbucket, adicione o IOC ao **Indicadores relacionados** lista.
7. Clique em **Salvar**.

Adicione um método de modo de ataque relacionado

Além de importar modos/métodos de ataque como dados do STIX, você pode adicionar modos/métodos de ataque relacionados manualmente.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um modo/método de ataque relacionado.
3. Clique em **Modo/método de ataque secundário** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar ao atual.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Usando o slushbucket, adicione o modo/método de ataque ao **Modo/método de ataque secundário** lista.
7. Clique em **Salvar**.

Adicione a tarefa associada a um modo/método de ataque

Além de importar tarefas associadas (como mudanças e incidentes) como dados do STIX, você pode adicioná-las a um modo/método de ataque manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar uma tarefa associada.
3. Clique em **Tarefas associadas** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao modo/método de ataque.
6. Usando o slushbucket, adicione a tarefa ao **Tarefas associadas** lista.
7. Clique em **Salvar**.

Indicadores de comprometimento

Indicadores de comprometimento (IOC) são artefatos observados em uma rede ou sistema operacional que provavelmente indicarão uma invasão. IOCs típicos são assinaturas de vírus e endereços IP, hashes MD5 de arquivos ou URLs de malware ou nomes de domínio. O IOC se aplica ao STIX1,1 e 2.x.

Um IOC pode ser um único observável ou uma coleção de observáveis (por exemplo, um único URL inválido conhecido ou a presença de um arquivo específico e alguns valores de chave de registro específicos).

Depois que os IOCs foram identificados em um processo de resposta a incidentes e perícia de computador, eles podem ser usados para detecção antecipada de futuras tentativas de ataque usando sistemas de detecção de invasão e software antivírus.

O IOC se aplica ao STIX1,1 e 2.x.

Exibir um IOC

IOCs, às vezes chamados de indicadores, são normalmente recuperados de uma fonte de dados de ameaça como dados STIX. Se necessário, você também pode criar IOCs.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Depois que o trabalho agendado recuperar os dados de IOC do fonte de dados definida , navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   Os IOCs recuperados são listados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Clique no IOC que você deseja exibir.
3. As informações a seguir são exibidas.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança Para adicionar metadados ao registro, você pode selecionar um ou mais marcadores para especificar o grau de sensibilidade do IOC. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Título	Um nome descritivo para este indicador.
Visto pela primeira vez	A primeira data em que este indicador foi observado no sistema.
Visto pela última vez	A data mais recente em que este indicador foi observado no sistema.
Contagem encontrada	O número de vezes que o indicador foi encontrado.
Contagem de itens originados	O número de vezes que o indicador foi importado de origens de ameaça definidas.
Anotações	Quaisquer anotações adicionais sobre o indicador. Este campo também pode conter pares de chave/valor JSON.

4. Você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Observáveis Relacionados	Lista observáveis vinculados ao indicador atual.
Modo/método de ataque relacionado	Lista os modos/métodos de ataque relacionados que foram identificados como relacionados a este indicador.
Tipo associado	Lista outros tipos de indicador associados a este IOC.
Fontes do Indicador	Lista as origens deste indicador, junto com o nível de confiança da origem.
Tarefas Associadas	Lista todas as tarefas, mudanças e incidentes associados ao IOC.
Metadados do indicador	. **Anotações** O campo contém pares de chave/valor JSON válidos, eles são analisados e exibidos. Se nenhum par de chave/valor JSON estiver presente ou se o JSON for inválido, esta lista relacionada não será exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Anotações de segurança	
Referências externas do indicador	
Fases da cadeia de eliminação associada	Lista as fases da cadeia de destruição associadas a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.

Adicione um observável relacionado a um IOC

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados a um IOC manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um observável relacionado.
3. Clique em **Observáveis relacionados** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar com o IOC.
6. Usando o slushbucket, adicione o observável ao **Observáveis relacionados** lista.
7. Clique em **Salvar**.

Adicione um modo/método de ataque relacionado a um IOC

Além de importar modos/métodos de ataque relacionados como dados do STIX, você pode adicionar modos/métodos de ataque relacionados a um IOC manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um modo/método de ataque relacionado.
3. Clique em **Modo/método de ataque relacionado** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar com o IOC.
6. Usando o slushbucket, adicione o modo/método de ataque ao **Modo/método de ataque relacionado** lista.
7. Clique em **Salvar**.

Identificar os tipos de indicador associados

Se um IOC não tiver tipos de indicador associados definidos, ele rastreará todos os tipos de observáveis. No entanto, se você associar um ou mais tipos de indicadores a um IOC, isso limitará os tipos de observáveis que podem ser associados ao IOC.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja associar um tipo de indicador.
3. Clique em **Tipo associado** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o tipo de indicador que você deseja associar ao IOC.
6. Usando o slushbucket, adicione o tipo de indicador ao **Tipo associado** lista.
7. Clique em **Salvar**.

Identificar as origens do indicador

Normalmente, as origens do indicador são rastreadas automaticamente como parte do processo de importação de ameaças, mas mais origens podem ser adicionadas manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar origens de indicador.
3. Clique em **Origens do indicador** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar a origem do indicador que você deseja associar ao IOC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Usando o slushbucket, adicione a origem do indicador ao **Origens do indicador** lista.
7. Clique em **Salvar**.

Adicione tarefas associadas a um IOC

Além de importar tarefas associadas (como mudanças e incidentes) como dados do STIX, você pode adicioná-las a um IOC manualmente.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no IOC ao qual você deseja adicionar uma tarefa associada.
3. Clique em **Tarefas associadas** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao IOC.
6. Usando o slushbucket, adicione a tarefa ao **Tarefas associadas** lista.
7. Clique em **Salvar**.

Observáveis

Observáveis representam propriedades com estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes. Observáveis se aplicam STIX1,1 e 2.x.

Conjuntos de observáveis cibernéticos são úteis para identificar indicadores de comprometimento quando combinados com informações contextuais que representam os comportamentos de ameaças cibernéticas.

Observáveis se aplicam STIX1,1 e 2.x.

Defina um observável

Observáveis são recuperados do servidor do fornecedor como dados STIX. No entanto, você pode criar observáveis, conforme necessário.

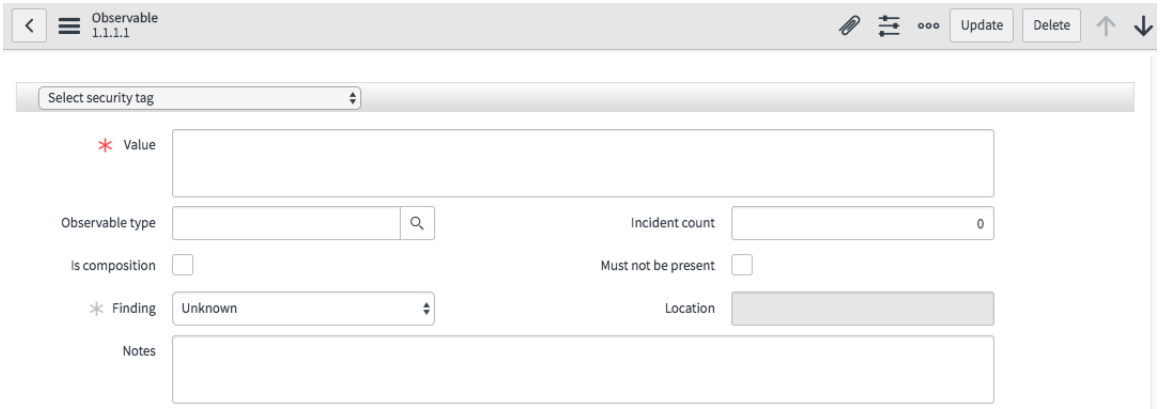
Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, você pode selecionar um ou mais marcadores para especificar o grau de sensibilidade do observável. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se for uma verificação de ameaça Em um endereço IP ou hash, malware retornado ou alguma outra falha, o endereço IP ou valor de hash é adicionado automaticamente à tabela observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação observável, como um endereço IP ou hash de arquivo. Esses tipos de observáveis são definidos em **Tipos de observáveis** módulo.
Contagem de incidentes	O número de vezes que o valor do observável foi encontrado.
É composição	Este campo é exibido somente depois que o registro do observável é salvo. . **Tipo de observável** está definido como qualquer coisa diferente disso **Composição do observável** e este novo observável é uma composição, marque esta caixa de seleção. . **Tipo de observável** já está definido como **Composição do observável** , a caixa de seleção é marcada e somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades: ○ **Mal-intencionado** : Indica que o observável é prejudicial para a organização. ○ **Suspeito** : Indica que o observável pode ser prejudicial para a organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Limpo** : Indica que o observável não é prejudicial para a organização. ○ **Desconhecido** Indica que ainda não determinamos a descoberta do observável. ○ Valor padrão: Desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como mal-intencionados.
Operador	Este campo aparece somente quando **É composição** a caixa de seleção está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente. Defina este campo como **E.** se todos os observáveis secundários precisarem estar presentes para que um indicador associado seja considerado presente. Defina como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.
Não deve estar presente	Este campo é exibido somente depois que o registro do observável é salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Local	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregue mais dados de IOC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** .
Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione um IOC relacionado a um observável

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados a um IOC manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um IOC relacionado.
3. Clique em **Indicadores relacionados** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o indicador que você deseja relacionar com o observável.
6. Usando o slushbucket, adicione o indicador ao **Indicadores relacionados** lista.
7. Clique em **Salvar**.

Adicione tarefas associadas a um observável

Além de importar tarefas associadas (como mudanças e incidentes) como dados do STIX, você pode adicioná-las a um observável manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar uma tarefa associada.
3. Clique em **Tarefas associadas** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao observável.
6. Usando o slushbucket, adicione a tarefa ao **Tarefas associadas** lista.
7. Clique em **Salvar**.

Adicione um observável relacionado

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um observável relacionado.
3. Clique em **Observáveis secundários** lista relacionada.
4. Clique em **Editar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar ao atual.
6. Usando o slushbucket, adicione o observável ao **Observáveis secundários** lista.
7. Clique em **Salvar**.

Carregue mais dados de IOC

Dependendo das configurações em duas propriedades e de uma definição de inclusão de script, você pode carregar informações de geolocalização para endereços IP e sites no formulário observáveis. Com personalização adicional, você também pode adicionar outras informações, como códigos de país, nomes de cidades.

Antes de Iniciar

As duas propriedades a seguir devem ser definidas:

- **O nome do domínio para recuperar informações adicionais para endereços IP/URLs** [sn_ti.ip_lookup.web_site]
- **A chave de API a ser usada para o domínio acima, se houver** [sn_ti.ip_lookup.api_key]

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no endereço IP ou URL do observável para o qual você deseja exibir mais dados de IOC.
   . **Local** O campo mostra a geolocalização do IOC.
3. Clique em **Enriquecer dados** Botão para carregar os dados IOC adicionais.
4. Você também pode configurar o formulário observável para adicionar outros campos relacionados ao local, como o código do país e o código da cidade.

> **Nota:** Para carregar mais informações relacionadas ao local, edite **ThreatAdditionalInfo** O script inclui e fornece a chave de API apropriada do site que fornece as informações adicionais.

Identificar fontes de observáveis

Se um observável não tiver origens definidas, ele usará todos os tipos de origens. No entanto, se você adicionar uma ou mais origens de ameaça a um observável, isso limitará as origens usadas.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar fontes do observável.
3. Clique em **Fontes observáveis** lista relacionada.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar a origem que você deseja associar ao observável.
6. Usando o slushbucket, adicione a origem do observável ao **Fontes observáveis** lista.
7. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Realizar pesquisas em observáveis

Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações de verificação executadas dependem das que você ativou.

Antes de Iniciar

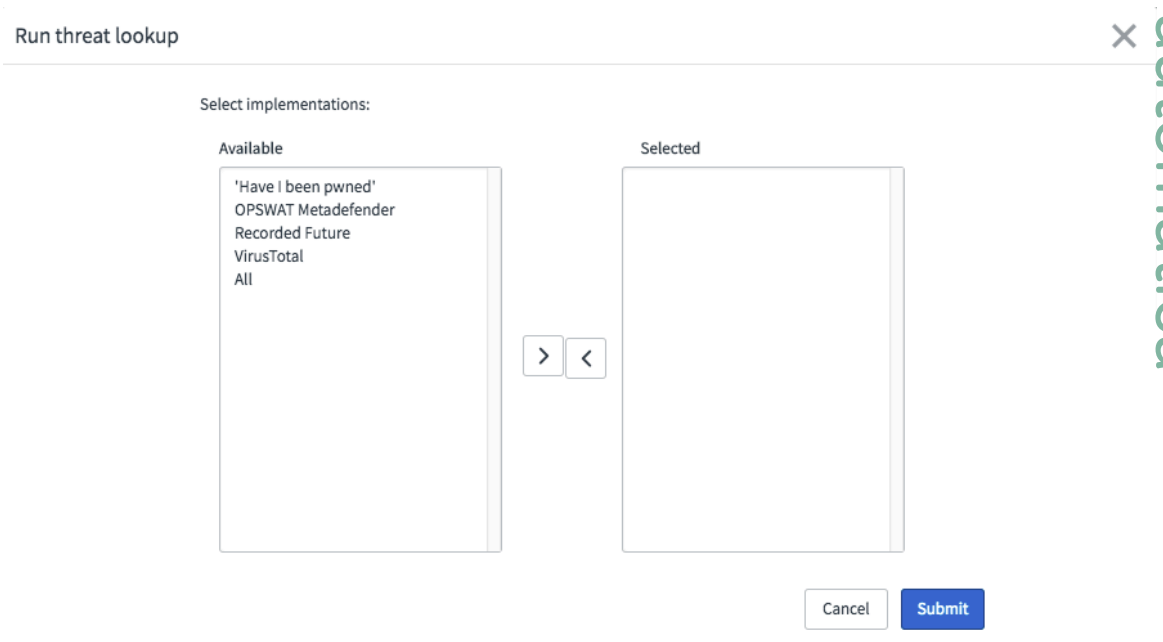
Antes de executar pesquisas, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais implementações de verificação:

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Operações de segurança Eu fui pwned?
- VirusTotal

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Execute uma das seguintes etapas:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis e clique em **Ações nas linhas selecionadas** e selecione **Executar pesquisa de ameaças** .
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique em **Executar pesquisa de ameaças** link relacionado.

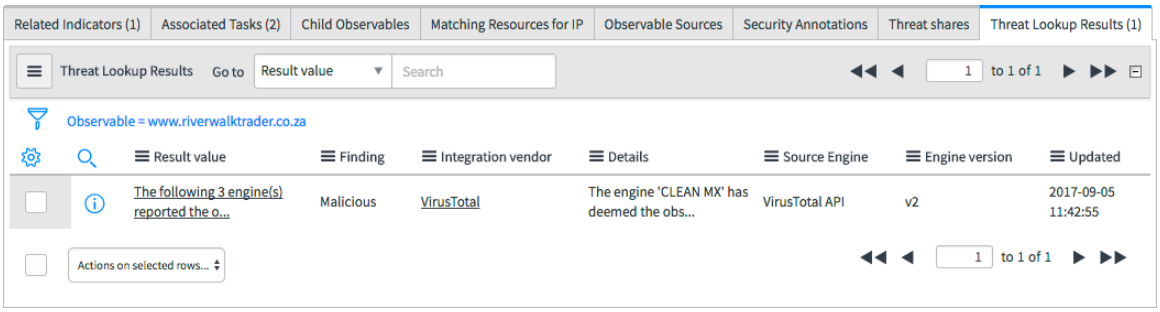


3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todos** para executar pesquisas usando todas as implementações ativas, clique em **Enviar** .
   Uma mensagem indica que as pesquisas de ameaça foram iniciadas. . Integração de operações de segurança - Fluxo de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação para as implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Quando as pesquisas forem concluídas, você poderá clicar em **Resultados da pesquisa de ameaças** para exibir os resultados.



Resultado recente da pesquisa de ameaças : Você também pode ver os resultados de pesquisa de ameaças mais recentes ou mais recentes de cada fornecedor de integração ao clicar em **Resultado recente da pesquisa de ameaças** guia.

Nota: . **Resultado recente da pesquisa de ameaças** a guia não faz parte do sistema de base.

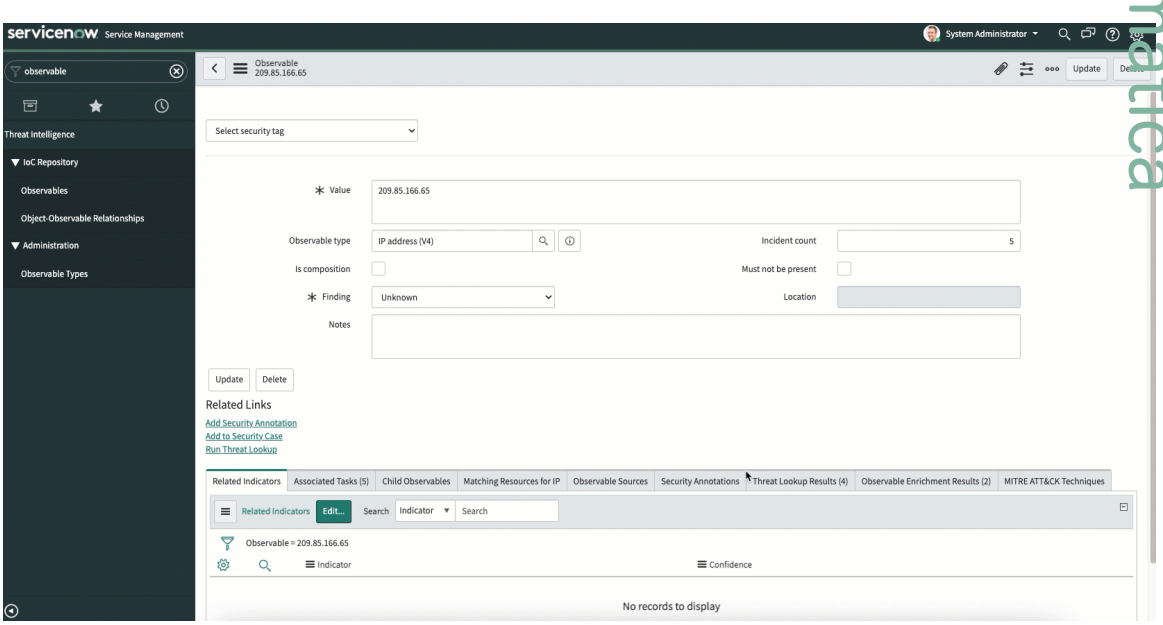
Para habilitar esta guia, faça o seguinte:

a. Clique com o botão direito do mouse no cabeçalho do formulário.

b. Navegar até **Configurar** > **Listas relacionadas**.

c. Localizar **Resultados recentes da pesquisa de ameaças** Na lista Disponível e mova-a para a lista Selecionado.

d. Clique em **Salvar**.
Agora você pode exibir os resultados recentes da pesquisa de ameaças de cada fornecedor de integração no **Resultado recente da pesquisa de ameaças** guia.

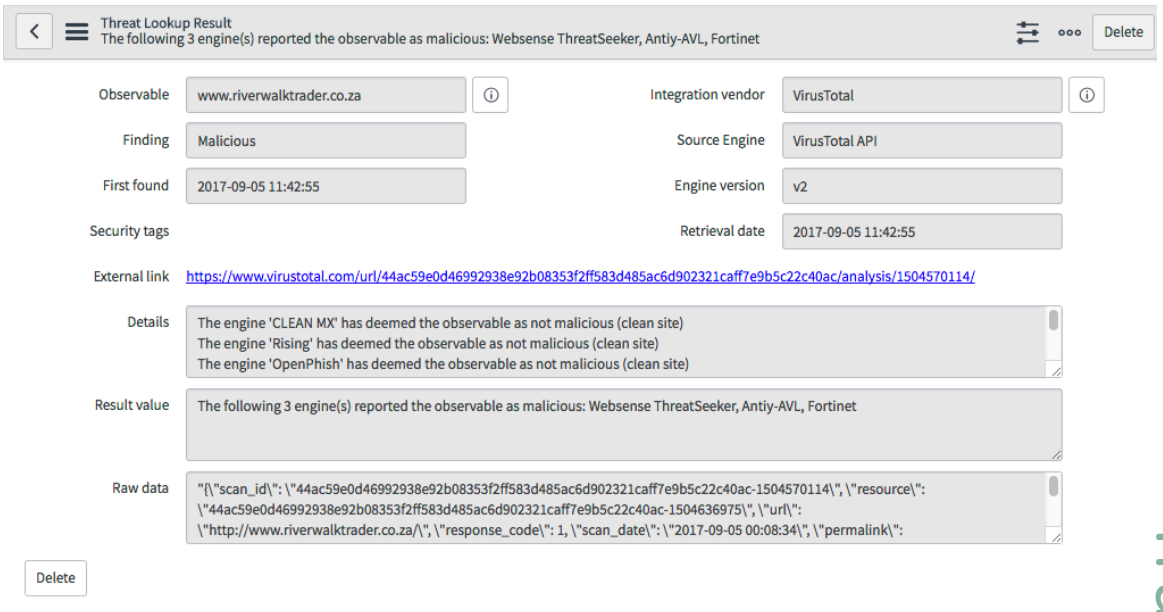


5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique em **Valor do resultado** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando as implementações VirusTotal ou OPSWAT Metadender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Aprimorar ameaças em observáveis

Você pode executar o aprimoramento da inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações executadas dependem das que você ativou.

Antes de Iniciar

Antes de executar o aprimoramento, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais das implementações de aprimoramento:

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Operações de segurança Eu fui pwned?
- VirusTotal
- WHOIS?

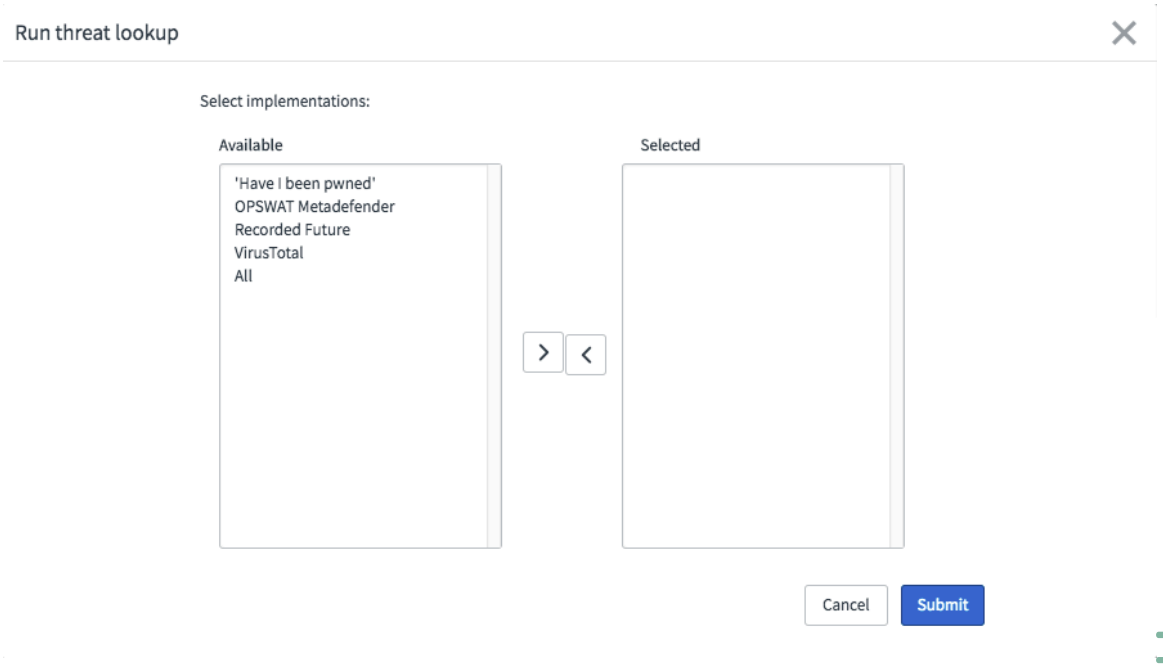
Função necessária: sn_ti.admin

Procedimento

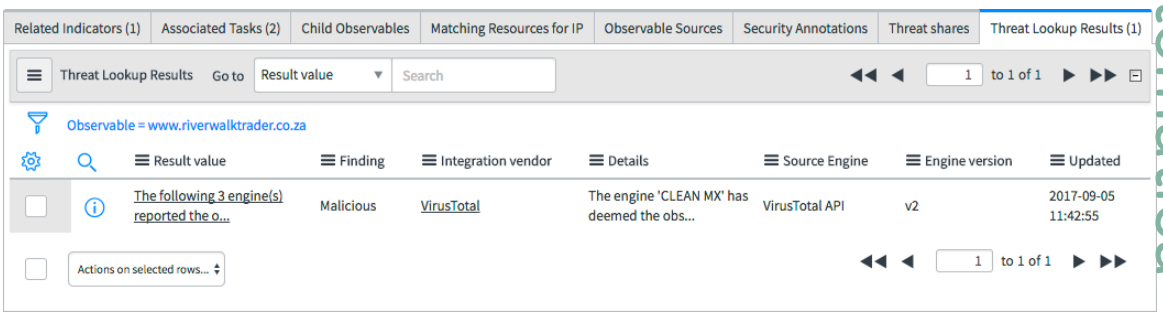
1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Execute uma das seguintes etapas:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis e clique em **Ações nas linhas selecionadas** e selecione **Executar pesquisa de ameaças** .
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique em **Executar pesquisa de ameaças** link relacionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todos** para executar pesquisas usando todas as implementações ativas, clique em **Enviar** .
   Uma mensagem indica que as pesquisas de ameaça foram iniciadas. . Integração de operações de segurança - Fluxo de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação para as implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.
4. Quando as pesquisas forem concluídas, você poderá clicar em **Resultados da pesquisa de ameaças** para exibir os resultados.

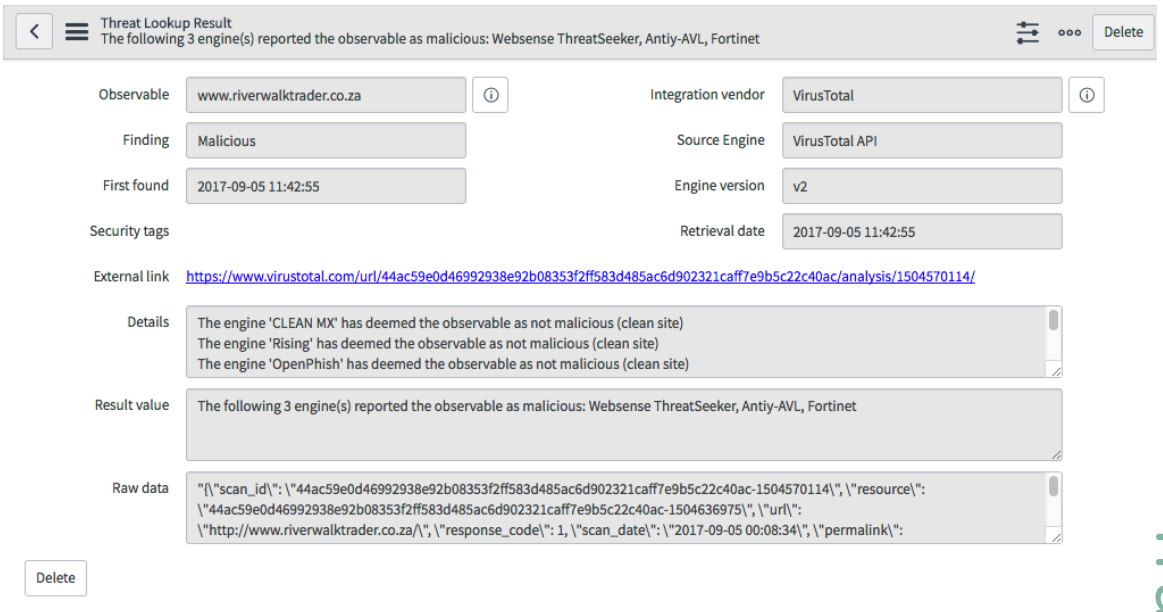


5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique em **Valor do resultado** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando as implementações VirusTotal ou OPSWAT Metadender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Padrões de ataque

Padrões de ataque são um tipo de táticas, técnicas e procedimentos (TTPs) que descrevem os métodos que os adversários tentam comprometer os alvos. Os padrões de ataque se aplicam ao STIX 2.x.

Os padrões de ataque são usados para ajudar a categorizar os ataques. Eles generalizam ataques específicos para os padrões que seguem e fornecem informações detalhadas sobre como os ataques são realizados.

Por exemplo, spear phishing é um tipo comum de ataque em que um invasor envia uma mensagem de e-mail cuidadosamente criada para uma parte com a intenção de fazer com que ela clique em um link ou abra um anexo para entregar malware. Os padrões de ataque são mais específicos, como spear phishing por um agente de ameaça específico (exemplo - que o alvo ganhou um concurso) também pode ser um padrão de ataque.

Defina um padrão de ataque

Defina um padrão de ataque para ajudar a categorizar os ataques.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Padrões de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para este padrão de ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Insira uma descrição do padrão de ataque.
Aliases	Nomes alternativos para identificar este padrão de ataque.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao padrão de ataque.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de destruição associadas a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linhas de ação	Lista o curso associado de ações a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para evitar um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Campanhas

Uma campanha é um agrupamento de comportamentos adversários. Esses comportamentos descrevem um conjunto de atividades ou ataques mal-intencionados que ocorrem ao longo do tempo contra um conjunto específico de destinos. As campanhas se aplicam ao STIX 2.x.

As campanhas geralmente têm objetivos bem definidos e podem fazer parte de um conjunto de Intrusão.

As campanhas geralmente são atribuídas a um conjunto de invasão e agentes de ameaça. Os agentes de ameaça podem reutilizar a infraestrutura conhecida do conjunto de invasão ou configurar uma nova infraestrutura específica para conduzir essa campanha.

As campanhas têm um objetivo comum nos incidentes que causam, nas pessoas ou nos recursos que visam e nos recursos que usam.

Por exemplo, um sindicato do crime ataca os executivos do ACME Bank. Eles atacam usando uma variante específica de malware e novos servidores para obter informações secretas sobre uma futura fusão com outro banco.

Defina uma campanha

Defina uma campanha para agrupar comportamentos adversários.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Campanhas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome descritivo para esta campanha.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a campanha. Isso inclui sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta campanha.
Objetivo	O objetivo primário, o objetivo, o resultado desejado ou o efeito pretendido da campanha. O que o agente de ameaça ou o conjunto de intrusão espera realizar com esta campanha.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à campanha.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Identidades	Lista de identidades associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Curso das ações

Um curso de ação é uma ação realizada para impedir um ataque ou para responder a um ataque que está em andamento. O curso das ações se aplica ao STIX 2.x.

O curso de ações descreve respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls). Também pode descrever ações de nível superior, como treinamento de funcionários ou mudanças na política.

Por exemplo, um curso de ação para mitigar uma vulnerabilidade pode descrever a aplicação do patch que a corrige.

Defina um curso de ação

Defina um curso de ação para evitar um ataque ou responder a um ataque em andamento.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Linhas de ação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para este curso de ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ação	Para capturar cursos de ação estruturados ou automatizados.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o curso da ação, potencialmente incluindo sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao curso da ação.

Links relacionados	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identidades

As identidades representam indivíduos, organizações ou grupos reais (ACME, Inc.) e classes de indivíduos, sistemas ou grupos (o setor financeiro). As identidades se aplicam ao STIX 2.x.

O SDO de identidade pode capturar informações básicas de identificação, informações de contato e os setores aos quais a identidade pertence. A identidade representa alvos de ataques, fontes de informação, criadores de objetos e identidades de agentes de ameaça.

Defina identidades

Defina identidades que representam indivíduos, organizações ou grupos reais.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Identidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para esta identidade. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Classe da identidade	O tipo de entidade que esta identidade descreve. Por exemplo, indivíduo ou organização.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a identidade, potencialmente incluindo sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Infraestrutura

A infraestrutura SDO representa um tipo de táticas, técnicas e procedimentos (TTPs). Eles descrevem todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque. A infraestrutura se aplica ao STIX 2.x.

Os elementos de um ataque são representados por outros SDOs ou SCOs. No entanto, o SDO de infraestrutura representa um grupo nomeado de dados que constitui a infraestrutura.

Os exemplos de infraestrutura incluem servidores C2 usados em um ataque, um dispositivo ou um servidor que faz parte de uma defesa ou servidores de banco de dados visados por um ataque.

Definir infraestrutura

Defina uma infraestrutura que sejam todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque.

Antes de Iniciar
Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Infraestrutura**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a infraestrutura.
Visto pela primeira vez	A hora em que esta infraestrutura foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta infraestrutura foi vista pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a infraestrutura, incluindo potencialmente sua finalidade, como ela está sendo usada, como ela se relaciona com outras atividades de inteligência capturadas em objetos relacionados e suas principais características.
Aliases	Nomes alternativos para identificar esta infraestrutura.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais. Você também pode associar outros objetos à infraestrutura.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Fases da cadeia de eliminação associada	Lista as fases da cadeia de destruição associadas a este objeto.
Observáveis Associados	Lista observáveis associados a este objeto.
Infraestrutura associada	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Conjunto de intrusão

Um conjunto de invasão é um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns. Um conjunto de Intrusão geralmente envolve uma única organização. O conjunto de intrusão se aplica ao STIX 2.x.

Um conjunto de invasão pode capturar várias campanhas ou outras atividades. Essas atividades compartilham atributos que indicam um agente de ameaça comumente conhecido ou desconhecido.

Uma nova atividade pode ser atribuída a um conjunto de Intrusão, mesmo que os agentes de ameaça por trás do ataque não sejam conhecidos. Os agentes de ameaça podem passar do suporte a um conjunto de invasão para o suporte a outro, ou podem oferecer suporte a vários conjuntos de invasão.

Um Conjunto de Intrusão é o pacote de ataque inteiro e pode ser usado por um longo período em várias campanhas para alcançar possíveis finalidades múltiplas.

Defina um conjunto de intrusão

Defina um conjunto de intrusão que seja um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Conjunto de Intrusão**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o conjunto de intrusão.
Visto pela primeira vez	A hora em que este conjunto de invasão foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este conjunto de invasão foi visto pela última vez executando atividades mal-intencionadas.
Motivação primária	A principal razão, motivação ou finalidade por trás deste conjunto de intrusão. A motivação é a razão pela qual o Intrusion Set quer atingir o objetivo (o que eles estão tentando alcançar). Por exemplo, uma intrusão definida com o objetivo de perturbar o setor financeiro em um país pode ser motivada pelo ódio ideológico ao capitalismo.
Nível de recurso	Esta propriedade especifica o nível organizacional no qual esse conjunto de invasão normalmente funciona, o que, por sua vez, determina os recursos disponíveis para uso em um ataque.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar este conjunto de intrusão.
Objetivos	Os objetivos de alto nível desse conjunto de intrusão, ou seja, o que eles estão tentando fazer. Eles podem ser motivados por ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito. Para fazer isso, eles podem executar campanhas específicas que tenham objetivos detalhados, como comprometer sistemas de ponto de venda em um grande Varejista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao conjunto de invasão.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Motivações de ataque associadas	Lista todas as motivações secundárias pelas quais este conjunto de intrusão deseja alcançar.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Localizações

Um local representa uma localização geográfica. Os locais são usados principalmente para dar contexto a outros SDOs. Os locais se aplicam ao STIX 2.x.

O local pode conter alguns ou todos os seguintes: Região (América do Norte), endereço cívico (Nova York, EUA), latitude e longitude.

O SDO do local pode estar relacionado a um conjunto de identidade ou invasão para indicar que o conjunto de identidade ou invasão está nesse local. Ele também pode estar relacionado a um malware ou padrão de ataque para indicar que a vítima de destino está em um local específico.

Por exemplo, um Local poderia ser usado em um relacionamento para descrever que o conjunto de intrusão Bourgeois Swallow tem origem na Europa Oriental.

Pelo menos uma das seguintes propriedades ou conjuntos de propriedades deve ser fornecida:

- região
- país
- latitude e longitude

Definir local

Defina uma localização geográfica para fornecer mais contexto a outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Localizações**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o local.
Endereço	O endereço descrito por este local. Esta propriedade inclui todos os aspectos ou partes do endereço.
Cidade	A cidade em que este local está.
CEP	O CEP em que este local está.
Região	A região em que este local está.
País	O país em que este local está.
Latitude	A latitude do Local em graus decimais. Números positivos descrevem latitudes ao norte do equador, e números negativos descrevem latitudes ao sul do equador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser de -90,0 a 90,0, respectivamente.
Longitude	A longitude do local em graus decimais. Números positivos descrevem longitudines a leste do Meridiano Primário e números negativos descrevem longitudines a oeste do Meridiano Primário. O valor desta propriedade deve ser de -180,0 a 180,0, inclusive.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao local.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Malware

Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido de forma secreta em um sistema. O malware se aplica ao STIX 2.x.

A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

O SDO de malware caracteriza, identifica e categoriza instâncias e famílias de malware a partir de dados derivados da análise. Este SDO captura informações detalhadas sobre como o malware funciona e o que ele faz.

Defina um malware

Defina um malware que represente código mal-intencionado.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Malware**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar a instância ou a família de malware, conforme especificado pelo produtor da SDO. Para uma família de malware, o nome deve ser definido.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a instância ou família de malware, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta instância ou família de malware.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É família	Especifica se o objeto representa uma família de malware ou uma instância de malware.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Capacidades associadas	Lista os recursos identificados e associados a este objeto.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de destruição associadas a este objeto.
Observáveis Associados	Lista observáveis associados a este objeto.
Malware associado	Lista o malware associado identificado com este objeto.
Sistemas operacionais associados	Os sistemas operacionais nos quais o objeto é executável. Isso se aplica a sistemas operacionais virtualizados, bem como aqueles em execução em bare metal.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Campanhas	Lista as campanhas associadas a este objeto.
Linhas de ação	Lista o curso associado de ações a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para evitar um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Análise de malware	Lista registros de análise de malware associados a este objeto.
Observáveis relatados	Lista observáveis relatados como parte deste objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

Análise de malware

A Análise de malware captura os metadados e os resultados de um malware. A análise de malware se aplica ao STIX 2.x.

A Análise de malware inclui análise estática ou dinâmica realizada em uma instância ou família de malware.

Definir análise de malware

Defina a análise de malware que captura os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Análise de malware**.
2. Clique em **Nova**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o conjunto de intrusão.
Versão do mecanismo de análise	A versão do mecanismo de análise ou produto (incluindo mecanismos AV) que foi usada para executar a análise.
Versão da definição de análise	A versão das definições de análise usadas pela ferramenta de análise (incluindo ferramentas de AV).
Análise iniciada	A data e a hora em que a análise de malware foi iniciada.
Análise finalizada	A data e a hora em que a análise de malware foi encerrada.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Resultado	O resultado da classificação conforme determinado pelo processo de análise do scanner ou da ferramenta.
Nome do resultado	O resultado da classificação ou o nome atribuído à instância de malware pela ferramenta de verificação.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre os objetos associados à análise de malware.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Malware associado	Lista o malware associado identificado com este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Observáveis relatados	Lista observáveis relatados como parte deste objeto.
Software instalado	Lista qualquer software não padrão instalado no sistema operacional usado para a análise dinâmica da instância ou família de malware.

Dados observados

Os dados observados transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os objetos de observação cibernética (SCOs) do STIX. Os dados observados se aplicam ao STIX 2.x.

Os dados observados capturam uma única observação de uma única entidade (arquivo, conexão de rede), bem como a agregação de várias observações de uma entidade.

Você pode usar Dados observados por conta própria (sem relacionamentos) para transmitir dados brutos coletados de qualquer fonte. As origens incluem relatórios de analistas, áreas restritas e ferramentas de detecção baseadas em rede e host.

Por exemplo, Dados observados podem capturar informações sobre um endereço IP, uma conexão de rede, um arquivo ou uma chave de registro. Os dados observados não são uma asserção de inteligência, são simplesmente a informação bruta sem qualquer contexto para o que significam.

Definir dados observados

Defina dados observados que transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os objetos de observação cibernética (SCOs) do STIX.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Dados observados**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observado pela primeira vez	A hora inicial em que os dados foram vistos.
Última observação	A última vez em que os dados foram vistos.
Contagem de observações	O número de vezes que cada objeto Cyber-observável foi visto. O valor deve ser um número inteiro de 1 a 999,999,999.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos dados observados.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Observáveis Associados	Lista observáveis associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.

Agentes de ameaça

Os agentes de ameaça são indivíduos, grupos ou organizações que agem com intenção mal-intencionada. Os agentes de ameaça se aplicam ao STIX 2.x.

Um agente de ameaça não é um conjunto de invasão, mas pode oferecer suporte ou ser afiliado a vários conjuntos de invasão, grupos ou organizações ao longo do tempo.

Os agentes de ameaça usam seus recursos e os recursos de um conjunto de invasão para conduzir ataques e executar campanhas contra destinos.

Você pode identificar os agentes de ameaça por motivos, capacidades, objetivos, nível de sofisticação, atividades anteriores, recursos aos quais eles têm acesso e sua função na organização.

Definir agentes de ameaça

Defina agentes de ameaça que são indivíduos, grupos ou organizações que agem com intenção mal-intencionada.

Antes de Iniciar

Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Agentes da ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar a instância ou a família de malware, conforme especificado pelo produtor da SDO. Para uma família de malware, o nome deve ser definido.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste agente de ameaça. A motivação é o motivo pelo qual o agente da ameaça deseja atingir o objetivo (o que ele está tentando alcançar). Por exemplo, um agente de ameaça com o objetivo de perturbar o setor financeiro em um país pode ser motivado pelo ódio ideológico ao capitalismo.
Nível de recurso	O nível organizacional no qual esse agente de ameaça normalmente trabalha, que, por sua vez, determina os recursos disponíveis para esse agente de ameaça para uso em um ataque.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o agente da ameaça, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Uma lista de outros nomes para identificar este agente de ameaça.
Objetivos	Os objetivos de alto nível desse agente de ameaça, ou seja, o que ele está tentando fazer. Eles podem ser motivados por ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agente de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Funções associadas	Lista as funções associadas ao agente da ameaça.
Motivações de ataque associadas	Lista as motivações de ataque associadas ao agente da ameaça.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Agrupamentos de ameaças

Um objeto de agrupamentos de ameaças declara explicitamente que os objetos STIX referenciados têm um contexto compartilhado. Os agrupamentos de ameaças se aplicam ao STIX 2.x.

Um objeto de Agrupamentos de ameaças representa um conjunto de dados que, dada análise suficiente, amadurece para transmitir um incidente ou relatório de ameaça como um objeto de Relatório STIX. Por exemplo, um agrupamento pode ser usado para caracterizar uma investigação em andamento em um evento ou incidente de segurança.

Um objeto de agrupamentos de ameaças também pode ser usado para declarar que os objetos STIX referenciados estão relacionados a um processo de análise em andamento. Por exemplo, um analista de ameaças pode colaborar com outras pessoas em sua comunidade de confiança para examinar uma série de campanhas e indicadores.

O SDO de agrupamento de ameaças contém uma lista de referências a SDOs, SCOs e SROs, junto com uma declaração explícita do contexto compartilhado pelo conteúdo, uma descrição textual e o nome do agrupamento.

Defina agrupamentos de ameaças

Defina agrupamentos de ameaças como objetos que têm um contexto compartilhado.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Grupos de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar o agrupamento de ameaças.
Contexto	Uma descrição do contexto específico compartilhado pelo conteúdo referenciado pelo agrupamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição resumida que fornece detalhes e contexto sobre o agrupamento. Isso inclui sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agrupamento de ameaças.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos agrupados	Lista objetos agrupados como parte do agrupamento de ameaças.
Indicadores agrupados	Lista indicadores agrupados como parte do agrupamento de ameaças.
Observáveis agrupados	Lista observáveis agrupados como parte do agrupamento de ameaças.

Definições de marcação

O objeto de definições de marcação representa uma marcação específica.

As marcações de dados representam restrições, permissões e outras orientações sobre como os dados podem ser usados e compartilhados.

Por exemplo, os dados podem ser compartilhados com a restrição de que eles não devem ser compartilhados novamente ou que devem ser criptografados em repouso.

No STIX, as marcações de dados são especificadas usando o objeto de definição de marcação. Essas definições são aplicadas a objetos STIX usando marcações de objeto e a propriedades individuais de objetos STIX por meio de marcações granulares.

Defina definições de marcação

Defina definições de marcação que representam uma marcação de dados específica.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Definições de marcação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Definição	Especifique o objeto de marcação (exemplo, TLP) ou alguma outra definição de marcação que foi definida.
Tipo de definição	Identifica o tipo de definição de marcação - declaração ou TLP (Protocolo de semáforo).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à definição de marcação.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos marcados	Listas de objetos marcados com a definição de marcação.
Indicadores marcados	Listas de indicadores marcados com a definição de marcação.

Tradução automática

Anotações de ameaças

Uma anotação de ameaça transmite texto informativo para fornecer análise adicional não contida nos objetos STIX, objetos de definição de marcação ou objetos de conteúdo de idioma aos quais a anotação está relacionada. As anotações de ameaças se aplicam ao STIX 2.x.

Por exemplo, um analista pode adicionar uma anotação a um objeto de campanha criado por outra organização. A anotação pode indicar que eles viram publicações relacionadas a essa campanha em um fórum de hackers.

As anotações geralmente são criadas por analistas humanos e são compostas de texto orientado para o ser humano, elas contêm uma propriedade extra para capturar o autor que criou a anotação.

Definir anotações de ameaça

Defina anotações de ameaça que transmitem informações para fornecer contexto ou análise adicional que não está disponível em objetos existentes.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Anotações de ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Resumo	Especifique um breve resumo do conteúdo da anotação.
Conteúdo	Especifica o conteúdo da anotação.
Autores	Especifica o nome do autor (exemplo, um analista).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados às anotações de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos associados	Listas de objetos aos quais as anotações de ameaça se aplicam.
Indicadores associados	Listas de indicadores aos quais as anotações de ameaça se aplicam.
Observáveis Associados	Lista observáveis associados a este objeto.

Opiniões sobre ameaças

Uma opinião é uma avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente. As opiniões sobre ameaças se aplicam ao STIX 2.x.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A propriedade de opinião captura o nível de acordo ou discordância usando uma escala fixa. A escala fixa também oferece suporte a um mapeamento numérico para permitir operações estatísticas consistentes em todas as opiniões.

Por exemplo, um analista de uma organização consumidora pode dizer que "discorda totalmente" de um objeto de campanha e fornecer uma explicação sobre o motivo.

As opiniões são subjetivas e a especificação não aborda a melhor forma de interpretá-las.

Os analistas humanos criam opiniões e são compostos de texto orientado para o ser humano, eles contêm uma propriedade extra para capturar o autor que criou a opinião.

Definir opiniões sobre ameaças

Defina opiniões de ameaça como uma avaliação da precisão das informações em um objeto STIX.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Opiniões sobre ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Opinião	A opinião do produtor sobre o objeto STIX.
Explicação	A explicação do produtor sobre a opinião.
Autores	Especifica o nome do autor (exemplo, um analista).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à opinião de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
	Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos associados	Lista de objetos aos quais a opinião de ameaça se aplica.
Indicadores associados	Lista de indicadores aos quais a opinião de ameaça se aplica.
Observáveis Associados	Lista observáveis associados a este objeto.

Relatórios de ameaças

Relatórios de ameaças são coleções de inteligência contra ameaças com foco em um ou mais tópicos. Os relatórios de ameaças se aplicam ao STIX 2.x.

Os relatórios de ameaças incluem a descrição de um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças relacionada a ameaças para que ela possa ser publicada como uma história abrangente de ameaças cibernéticas.

O relatório de ameaças SDO contém uma lista de referências a objetos STIX junto com uma descrição textual e o nome do relatório.

Definir relatórios de ameaças

Defina relatórios de ameaça que descrevem um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Relatórios de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Especifique um nome para identificar o relatório de ameaça.
Publicado	A data em que este relatório foi publicado oficialmente pelo autor do relatório.
Descrição	Uma descrição que fornece informações e contexto adicionais sobre o relatório.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos relatórios de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Objetos relatados	Lista de objetos relatados no relatório de ameaça.
Indicadores relatados	Listas de indicadores relatados no relatório de ameaça.
Observáveis relatados	Listas de observáveis relatados no relatório de ameaça.

Detecções

As vistas indicam que um indicador ou objeto foi visto. Os objetos podem ser malware, ferramenta, agente de ameaça e assim por diante.

As vistas rastreiam quem e o que é o alvo, como os ataques são realizados e para rastrear tendências no comportamento de ataque.

O objeto de relacionamento de vistas contém propriedades extras que não estão presentes nos objetos de relacionamento genéricos. Essas propriedades extras representam dados específicos dos relacionamentos de avistamento.

Por exemplo, uma contagem ou que representa quantas vezes algo foi visto.

Avistamento é capturado como um relacionamento porque você não pode ter um avistamento a menos que você tenha algo que foi avistado.

- O que foi avistado, como o malware, a campanha ou outro SDO
- Quem avistou e/ou onde foi avistado, representado como identidade
- O que foi visto em sistemas e redes, representado como dados observados

Defina vistas do indicador

Defina avistamentos que denotam que um indicador foi visto.

Antes de Iniciar

Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Avistamentos do indicador**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Indicador	Identifica o indicador. PESQUISE e selecione o indicador.
Contagem	O número de vezes que o objeto foi visto.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a detecção do indicador, potencialmente incluindo sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É resumo	
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vista do indicador.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina vistas de objetos

Defina a detecção de objeto que descreve que um objeto (malware, ferramenta, agente de ameaça e assim por diante) foi visto.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Detecções de objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto	Identifica o objeto. PESQUISE e selecione o objeto.
Contagem	O número de vezes que o objeto foi visto.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a visão do objeto, potencialmente incluindo sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É resumo	
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vista do objeto.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas relacionadas	Descrição
Dados observados	Lista os dados observados associados a este objeto.

Ferramentas

Ferramentas são software legítimo que são usados por agentes de ameaça para executar ataques. As ferramentas se aplicam ao STIX 2.x.

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Por exemplo, as ferramentas de acesso remoto (RDP) e as ferramentas de verificação de rede (Nmap) são ferramentas que um agente de ameaça usa durante um ataque.

Definir ferramentas

Defina ferramentas como software legítimo que é usado para executar ataques.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Ferramentas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a ferramenta.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a ferramenta, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta ferramenta.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto de ferramenta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de destruição associadas a este objeto.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linhas de ação	Lista o curso associado de ações a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para evitar um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Vulnerabilidades

Uma vulnerabilidade é um ponto fraco ou defeito em um componente de software ou hardware que os invasores exploram. As vulnerabilidades se aplicam ao STIX 2.x.

O ponto fraco ou defeito está nos requisitos, designs ou implementações do código encontrado em um componente de software ou hardware. Essa fraqueza é diretamente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

explorada para afetar negativamente a confidencialidade, integridade ou disponibilidade desse sistema.

CVE é uma lista de vulnerabilidades e exposições de segurança da informação que fornece nomes comuns para problemas conhecidos publicamente [CVE].

Por exemplo, se um malware explorar CVE-2015-12345, um objeto de malware poderá ser vinculado a um objeto de vulnerabilidade que faça referência a CVE-2015-12345.

Definir vulnerabilidades

Defina a vulnerabilidade como uma fraqueza ou defeito em um componente de software ou hardware que os invasores exploram.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Vulnerabilidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a vulnerabilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta ferramenta.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto de vulnerabilidade.

Links relacionados e listas relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
	Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linhas de ação	Lista o curso associado de ações a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para evitar um ataque.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Relacionamentos

Use os objetos de relacionamento para vincular dois SDOs ou SCOs (Cyber-observable Objects, objetos de observação cibernética) do STIX para descrever como eles se relacionam entre si.

SROs (STIX Relationship Objects, objetos de relacionamento do STIX) representam tipos de relacionamentos entre vários objetos do STIX. Os seguintes objetos de relacionamento estão disponíveis:

- **Relacionamento objeto-objeto** : Este objeto define relacionamentos entre SDOs, exceto o objeto indicador. Um exemplo de um relacionamento definido objeto-objeto é que um padrão de ataque entrega um malware.
- **Relacionamento Objeto-Indicador** : Este objeto define relacionamentos entre o objeto indicador e outros SDOs. Um exemplo de um relacionamento definido por objeto-indicador é que um indicador detecta evidências de uma campanha.
- **Relacionamento objeto-observável** : Este objeto define relacionamentos entre SDOs e o objeto observável (SCO). Um exemplo de um relacionamento definido objeto observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto STIX

Objeto de relacionamento	Origem de exemplo	Destino de exemplo	Descrição de exemplo
Relacionamentos objeto-objeto	Padrão de ataque	Malware	Este relacionamento descreve que este padrão de ataque é usado para entregar esta instância (ou família) de malware.
Relacionamentos objeto-indicador	Indicador	Ataque-padrão, Campanha, Infraestrutura, Conjunto de Intrusão, Malware, agente de ameaças, ferramenta	Este relacionamento descreve que o indicador pode detectar evidências do padrão de ataque relacionado, campanha, infraestrutura, conjunto de invasão, malware, agente ou ferramenta de ameaça. As evidências podem não ser diretas. Por exemplo, o indicador pode detectar evidências secundárias da campanha, como malware que é comumente usado por essa campanha específica.
Relacionamentos objeto-observável	Infraestrutura	Dados observados	Este relacionamento descreve que o indicador é criado com base nas informações de um objeto de dados observado. Um exemplo de um relacionamento definido objeto observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Defina relacionamentos objeto-objeto

Defina relacionamentos entre SDOs, exceto o objeto indicador.

Antes de Iniciar

Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Object-Object-Relacionamentos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto de origem	Selecione e defina o objeto de origem.
Tipo de objeto de origem	Define o tipo de objeto de origem.
Objeto de destino	Selecione e defina o objeto de destino.
Tipo de objeto de destino	Define o tipo de objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

Defina relacionamentos objeto-indicador

Defina relacionamentos entre o objeto indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Object-Indicator-Relacionamentos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto	Selecione e defina o objeto.
Tipo	Especifica o tipo de objeto com base no objeto selecionado.
Indicador	Selecione os indicadores de comprometimento.
Direção do relacionamento	Defina a direção do relacionamento, seja direta ou inversa.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

Defina relacionamentos objeto-observável

Defina relacionamentos entre SDOs e o objeto observável (SCO).

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório LOC** > **Object-observable-Relationships**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto	Selecione e defina o objeto de origem.
Tipo	Insira um nome descritivo para identificar o tipo de objeto.
Observável	Selecione e defina o observável.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

STIX Visualizador

O Visualizador STIX representa visualmente a estrutura do objeto STIX e seu relacionamento.

Você pode obter mais informações sobre o objeto ou relacionamento selecionado no painel de detalhes.

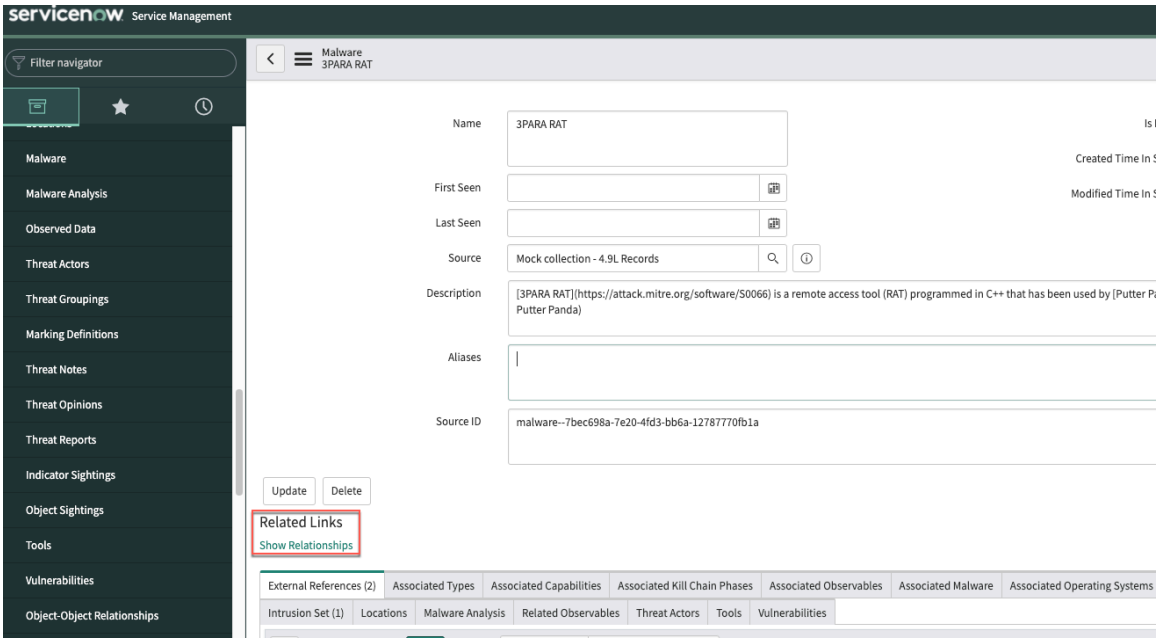
O gráfico de relacionamento mostra os relacionamentos de um objeto e fornece contexto para você investigar. Você pode clicar em qualquer nó no gráfico para ver mais detalhes.

Nota: O Visualizador STIX está disponível para todos os SDOs, exceto os objetos Relatório e Dados observados.

Tradução automática

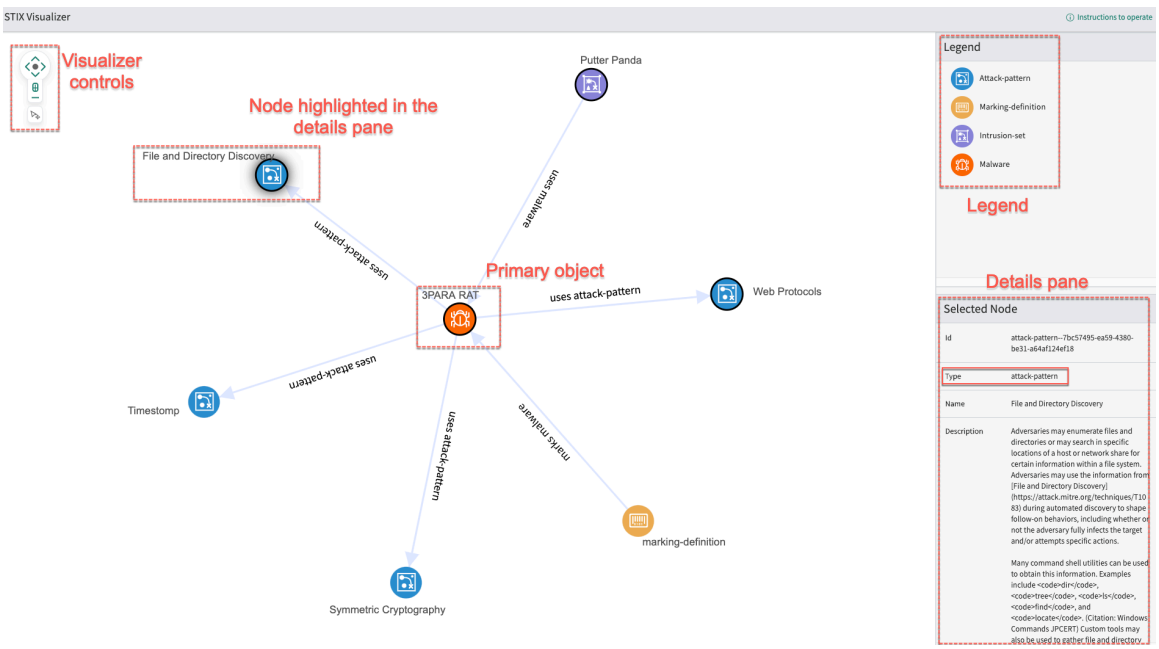
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesse o Visualizador do STIX



Clique em Mostrar relacionamentos Na seção Links relacionados para qualquer um dos SDOs exibir o Visualizador STIX.

Exiba detalhes no Visualizador STIX



No Visualizador, você pode exibir o objeto e seu relacionamento, o que fornece contexto para você investigar mais. O Visualizador usa cores e ícones para ilustrar várias informações sobre os objetos.

Você pode ampliar um objeto, arrastar os nós ou fixá-los para se concentrar em um relacionamento específico.

Clique em qualquer objeto para abrir o painel de detalhes. No painel de detalhes, você pode obter mais informações associadas ao objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE-ATT&CK™ visão geral da estrutura

. MITRE-ATT&CK A estrutura é uma base de conhecimento de táticas, técnicas e procedimentos (TTP) comuns que sua organização pode acessar para desenvolver modelos e metodologias de ameaça específicos contra ataques cibernéticos.

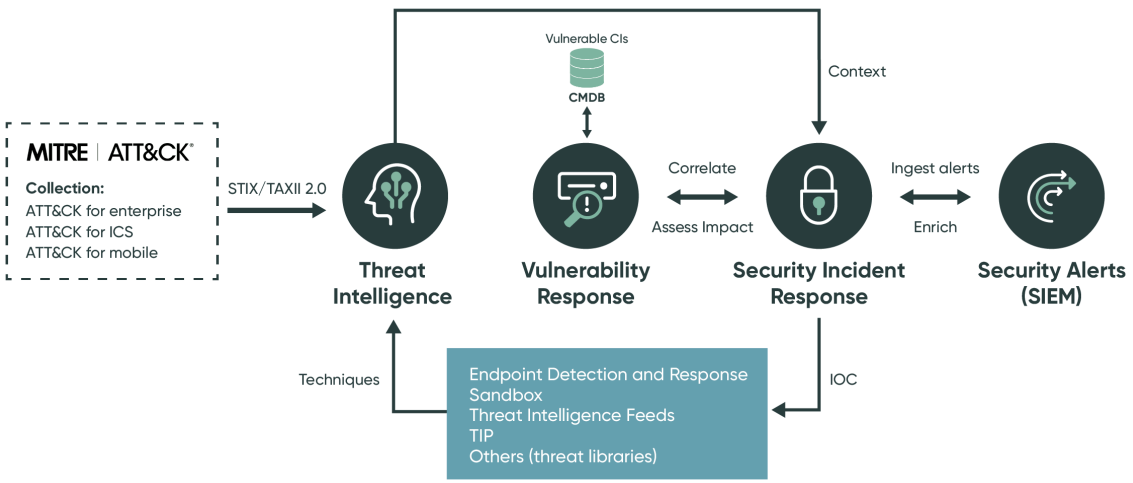
Visão geral

. MITRE A estrutura de táticas, técnicas e conhecimento comum (ATT&CK) documenta e rastreia várias técnicas adversas que são usadas durante diferentes fases de um ataque cibernético.

Usando o. MITRE-ATT&CK base de conhecimento da framework, a comunidade de inteligência contra ameaças cibernéticas pode identificar rapidamente ameaças e coordenar respostas a ataques cibernéticos.

MITRE-ATT&CK E Operações de segurança

Consulte o diagrama a seguir para saber como MITRE-ATT&CK as informações fluem com Operações de segurança aplicações.



- O pré-carregado TAXII cliente conecta-se ao TAXII servidor para ingerir o. coletas de dados . Inteligência contra ameaças.
- Existente Integrações do Security Information and Event Manager (SIEM) Ingerir os dados de ameaças (alertas e eventos), com TTPs relevantes e são associado a incidentes de segurança .
- . O IOC está associado a um incidente de segurança , Inteligência contra ameaças Pesquisa automaticamente feeds de ameaças em busca de informações relevantes e envia IOCs para fontes de terceiros, como EDR, Sandbox ou TIP para análise adicional.
- Se alguma origem de terceiros contiver MITRE-ATT&CK informações, então Inteligência contra ameaças extrai as informações da técnica e enriquece os dados em Inteligência contra ameaças repositório para correlação e análise.
- MITRE-ATT&CK também compartilha Informações de contexto CVE para cada técnica. Sua equipe de segurança pode revisar as técnicas exploradas em Resposta a vulnerabilidades determinar se seus ativos críticos para os negócios estão ameaçados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE-ATT&CK matrizes, táticas e técnicas

O núcleo do MITRE-ATT&CK a estrutura é uma matriz de táticas e técnicas do adversário. A sequência das táticas representa o que um adversário está tentando realizar na fase de um incidente. Quando sua equipe de segurança entende essa sequência, você tem a oportunidade de antecipar o próximo movimento de um adversário e quebrar a cadeia de destruição. O ATT&CK consiste nas seguintes matrizes:

- Enterprise ATT&CK: Descreve os comportamentos e as ações que um adversário toma para comprometer e operar em uma rede corporativa e na nuvem.

  Nota: A matriz Pré-ATT&CK foi descontinuada por MITRE E são mesclados com a matriz Enterprise.

- ICS ATT&CK: Descreve as ações que um adversário executa ao operar em uma rede de ICS (Industrial Control Systems, sistemas de controle industrial).
- Mobile ATT&CK: Descreve os comportamentos e ações do adversário que se concentram em dispositivos móveis.

As táticas representam o motivo de uma técnica ATT&CK. É o objetivo tático do adversário para realizar uma ação.

As técnicas representam como um adversário atinge um objetivo tático executando uma ação.

As técnicas podem estar associadas a mais de uma tática. Por exemplo, a manipulação de token de acesso é usada por um adversário para alcançar a tática de escalação de privilégio ou evasão de defesa.

Usando uma abordagem baseada em intenção para respostas a incidentes

Uma resposta baseada em intenção usa uma estrutura de cadeia de destruição dinâmica e contextual que pode ajudar sua organização a correlacionar incidentes de segurança e identificar um grande escopo de ataques. Sua equipe de segurança pode usar uma resposta baseada em intenção para entender como a organização está sendo atacada e o que o invasor pode fazer em seguida. Este tipo de resposta permite prever o comportamento de um invasor para que você possa concentrar seus recursos com eficácia.

Usando Resposta a incidentes de segurança Sua equipe de segurança pode gerenciar o ciclo de vida de cada incidente de segurança, da análise à contenção, concentrando-se em indicadores de comprometimento (IOCs), como endereços IP, hashes de arquivo e domínios.

Integrando Resposta a incidentes de segurança com MITRE-ATT&CK incidentes de segurança são tratados como links em um ataque maior em toda a empresa.

Como sua organização pode se beneficiar MITRE-ATT&CK Em Operações de segurança



Usando o. MITRE-ATT&CK a estrutura pode ajudar sua organização a fazer o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Equipe os analistas de segurança com MITRE-ATT&CK TTPs (táticas, técnicas e procedimentos) para analisar e responder melhor a incidentes de segurança.
- Automatize os fluxos de trabalho de incidentes usando o playbook para detectar e conter ameaças no contexto do MITRE-ATT&CK estrutura.
- Priorize indicadores de comprometimento e busca de ameaças com MITRE-ATT&CK informações.
- Entenda a postura de segurança de alto nível da sua organização no contexto do MITRE-ATT&CK estrutura.

Administração do MITRE-ATT&CK

Você pode configurar, mapear fontes de dados, mapear cobertura geral de detecção de técnica e manter o. MITRE-ATT&CK repositório no ServiceNow AI Platform.

Comece com MITRE-ATT&CK estrutura

Revise as informações a seguir antes de começar a configurar seu MITRE-ATT&CK estrutura.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform, Inteligência contra ameaças e Resposta a incidentes de segurança funções.	Estas funções são usadas nos recursos do MITRE-ATT&CK: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.miter_analyst - A função de analista DO MITRE foi introduzida para permitir a navegação cruzada do MITRE recursos entre Resposta a incidentes de segurança E Suporte à Inteligência contra ameaças comum. Com esta função, você pode exibir ambos Inteligência contra ameaças MITRE e Resposta a incidentes de segurança modo somente leitura. • sn_si.read Para obter mais informações, consulte Configurar Inteligência contra ameaças .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se o ServiceNow aplicações principais que são necessárias para oferecer suporte ao MITRE-ATT&CK estão instalados e ativados.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. • Suporte de Inteligência contra ameaças Componentes comuns de IU (sn_ti_sismic) - Versão 1,0 ou superior • Suporte à Inteligência contra ameaças comum - Versão 12,0 ou superior • Inteligência contra ameaças - Versão 12,0 ou superior • Resposta a incidentes de segurança - Versão 12,0 ou superior Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um produto de Operações de segurança ou aplicação e. Ativar uma aplicação da ServiceNow Store .
Domain Separation	Verifique seção domain separation se você pretende separar dados, processos e tarefas administrativas.

Entenda MITRE. STIX modelo de dados

Revise a terminologia usada por MITRE e. STIX para usar e entender com eficiência MITRE-ATT&CK™ estrutura no ServiceNow AI Platform.

MITRE objetos para STIX mapeamento

STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. O modelo de dados primário no Inteligência contra ameaças. STIX objetos. . MITRE os objetos são um subconjunto do primário STIX modelo de dados. Em MITRE-ATT&CK estrutura, MITRE fornece semelhante STIX informações com determinados rótulos e objetos.

MITRE. STIX mapeamento de objetos

Terminologia MITRE	Terminologia STIX
Técnica	Padrão de ataque
Mitigação	Linha de ação
Grupos	Conjuntos de intrusão
Malware	Malware

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE. STIX mapeamento de objetos

Terminologia MITRE	Terminologia STIX
Ferramenta	Ferramenta

Estendendo dados no Inteligência contra ameaças módulo

Você pode manter uma lista de Inteligência contra ameaças origens da ameaça e importe o necessário STIX dados que incluem um amplo conjunto de informações de ameaças cibernéticas. Você também pode usar TAXII perfis para facilitar a troca automatizada de informações de ameaças cibernéticas.

Nota: Para obter mais informações, consulte defina uma origem de ameaça e. Crie um perfil TAXII .

Estendendo dados no MITRE-ATT&CK módulo

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no MITRE-ATT&CK repositório.

Você pode criar um objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo de repositório MITRE ATT&CK, mas não é possível definir o tipo de relacionamento neste módulo. Para definir um tipo de relacionamento, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no Repositório MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazer isso no Repositório IOC.

Nota: Para obter mais informações, consulte estender MITRE-ATT&CK dados e. Repositório IOC .

Domain Separation e MITRE-ATT&CK

Esta visão geral do Domain Separation pertence a. MITRE-ATT&CK. Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com MITRE-ATT&CK

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com as funções sn_ti.admin necessárias no respectivo domínio.
- Replique o seguinte para cada domínio:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- TAXII Coleções

Nota:

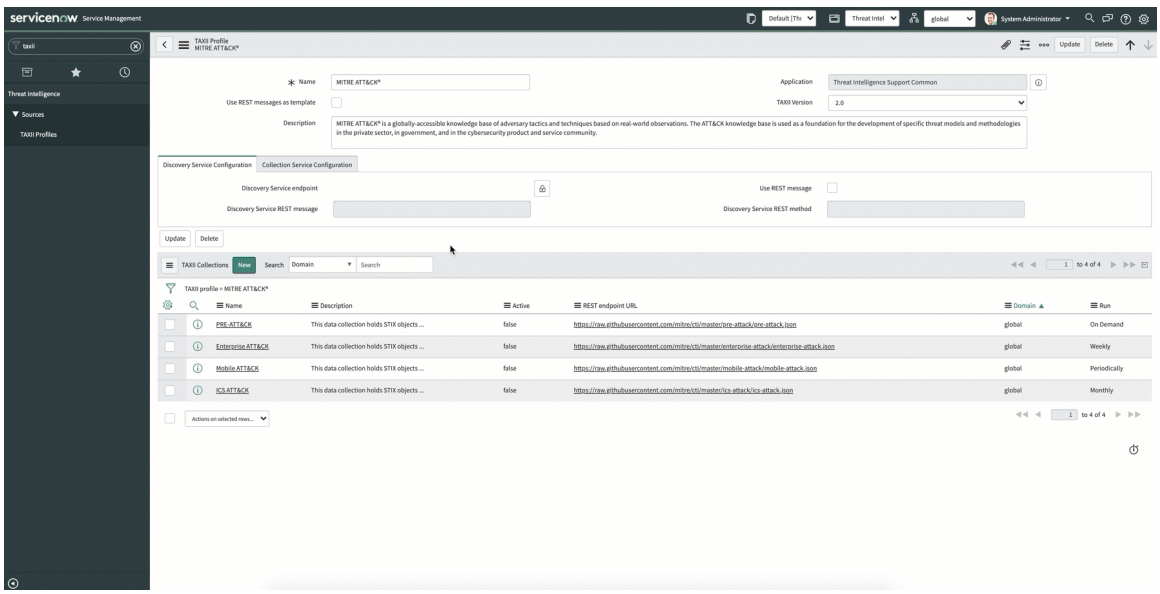
- Não ative as coleções no domínio global. Ative somente as coleções replicadas e disponíveis em seu domínio.
- Mude **Executar como** campo nas coleções para o usuário com a função sn_ti.admin no respectivo domínio.

- Definição de cobertura da técnica
- Regra de extração da técnica
- Regras de detecção - Mapeamentos MITRE ATT&CK
- Cobertura de mitigação
  - Copie todos os registros de definição de cobertura de mitigação.
  - Copie a calculadora de mitigação de cobertura ou crie uma nova calculadora para o respectivo domínio.
- Grupo de ameaças - Definições de mapa térmico da técnica

Replicar coleção de TAXII

1. Navegar até **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Na barra de cabeçalho, use o seletor de domínio para selecionar seu domínio.
3. Selecione a coleção TAXII relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).
4. Clique com o botão direito do mouse na barra de cabeçalho e selecione **Inserir e permanecer** . A coleção de TAXII duplicada é criada no domínio selecionado
5. Navegue de volta para o perfil MITRE ATT&CK TAXII para exibir a coleção de TAXII duplicada.

A ilustração a seguir mostra como selecionar o domínio TOP/Initech, replicar a coleção TAXII no domínio e verificar a coleção TAXII replicada.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o. MITRE-ATT&CK™ estrutura

Ative o. MITRE-ATT&CK e configure um trabalho agendado para que você possa configurar MITRE-ATT&CK coleções para detecção de ameaças em sua organização.

Antes de Iniciar

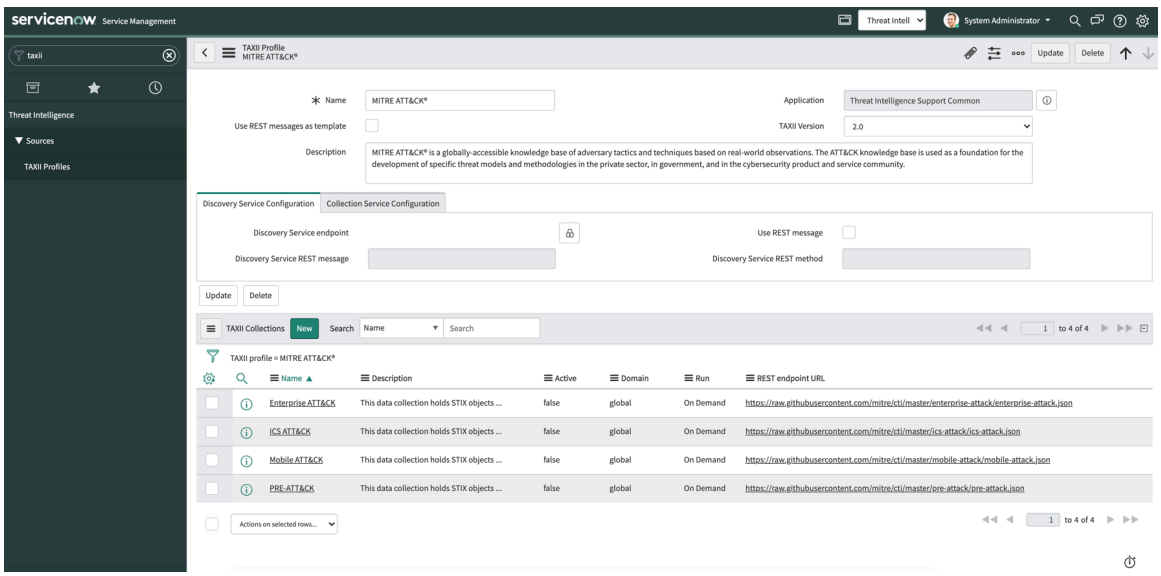
Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

Expressão de informações de ameaças estruturadas (STIX™) é uma linguagem para descrever informações de ameaças virtuais de maneira padronizada e estruturada. Usando dados do STIX e troca automatizada confiável de informações de indicador (TAXII™), as equipes de segurança podem usar informações compartilhadas de ameaças virtuais para isolar ameaças que foram identificadas anteriormente por sua empresa e de outras fontes.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
   Você vê o disponível TAXII perfis.
2. Clique em **MITRE ATT&CK** perfil fornecido com o sistema de base.



3. Para ativar o. TAXII coleção, defina **Ativo** opção como verdadeiro para TAXII Coleção relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).

Coleção TAXII	Descrição
Enterprise ATT&CK	Descreve os comportamentos e as ações que um adversário executa para comprometer e operar em uma rede corporativa e na nuvem. **Nota:** A matriz Pré-ATT&CK foi descontinuada por MITRE E são mesclados com a matriz Enterprise.
ATT&CK móvel	Descreve os comportamentos e as ações do adversário que se concentram em dispositivos móveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coleção TAXII	Descrição
ICS ATT&CK	Descreve as ações que um adversário executa ao operar em uma rede de Sistemas de controle industrial (ICS).

4. Para atualizar periodicamente a coleção, defina **Executar** conforme apropriado para sua organização. Por padrão, esta opção é definida como Sob demanda.

Nota:

a. As coleções são empacotadas como parte de Inteligência contra ameaças Plug-in principal. Instalar ou atualizar o Suporte de Inteligência contra ameaças Comum - Versão 12,0 ou superior e o Inteligência contra ameaças - Versão 12,0 ou superior garante que os dados de suas coleções sejam preenchidos automaticamente.

b. Ative o. TAXII coleção somente para a coleção que você pretende usar em sua organização e desabilitar as outras coleções. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, ative o Enterprise ATT&CK em TAXII nível de coleção e no Matrizes nível. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK no TAXII E no nível de matrizes.

c. Em TAXII Coleções relacionadas, se você selecionar a opção Executar como Diariamente, ocorrerá um erro e a opção será padronizada como Sob demanda. Este erro ocorre como programar o. MITRE-ATT&CK a atualização de dados diária é restrita para otimizar a carga no MITRE servidores. Além disso, MITRE Atualiza os dados do ATT&CK apenas duas vezes por ano.

d. . TAXII as coleções não são atualizadas a menos que você ative TAXII coleção.

e. As atualizações das coleções existentes podem ser recuperadas do MITRE programando a frequência de "execução" em cada coleção.

f. As personalizações que você faz no MITRE-ATT&CK Os dados do repositório (objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica) são salvos durante as atualizações programadas.

g. MITRE atualiza o. MITRE-ATT&CK base de conhecimento em que alguns objetos são identificados como revogados ou descontinuados, novos objetos são adicionados ou objetos existentes são modificados. Se MITRE revoga qualquer tática ou técnica e, em seguida, esses objetos são marcados como revogados em ServiceNow AI Platform. Os objetos revogados são mantidos no repositório, mas não estão disponíveis para uso no ServiceNow AI Platform.

O que Fazer Depois

Depois que a configuração do perfil TAXII estiver concluída, o. MITRE-ATT&CK os dados do repositório são importados em intervalos regulares para ServiceNow AI Platform®. Você pode ver esses dados navegando até **Repositório do MITRE ATT&CK** > **Matrizes** e **Repositório do MITRE ATT&CK** > **Técnicas**.

Gerenciar matrizes

Gerencie as matrizes que foram importadas do MITRE TAXII coleções. Matrizes são uma coleção de táticas e técnicas. Você pode exibir as matrizes para revisar se suas coleções estão disponíveis em MITRE-ATT&CK repositório.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Nota: Revise e verifique se somente a matriz que você pretende usar em sua organização está definida como ativa e desabilite as outras matrizes. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, a matriz Enterprise ATT&CK será ativada em Coleção TAXII E no nível Matrizes. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK no TAXII E no nível de matrizes.

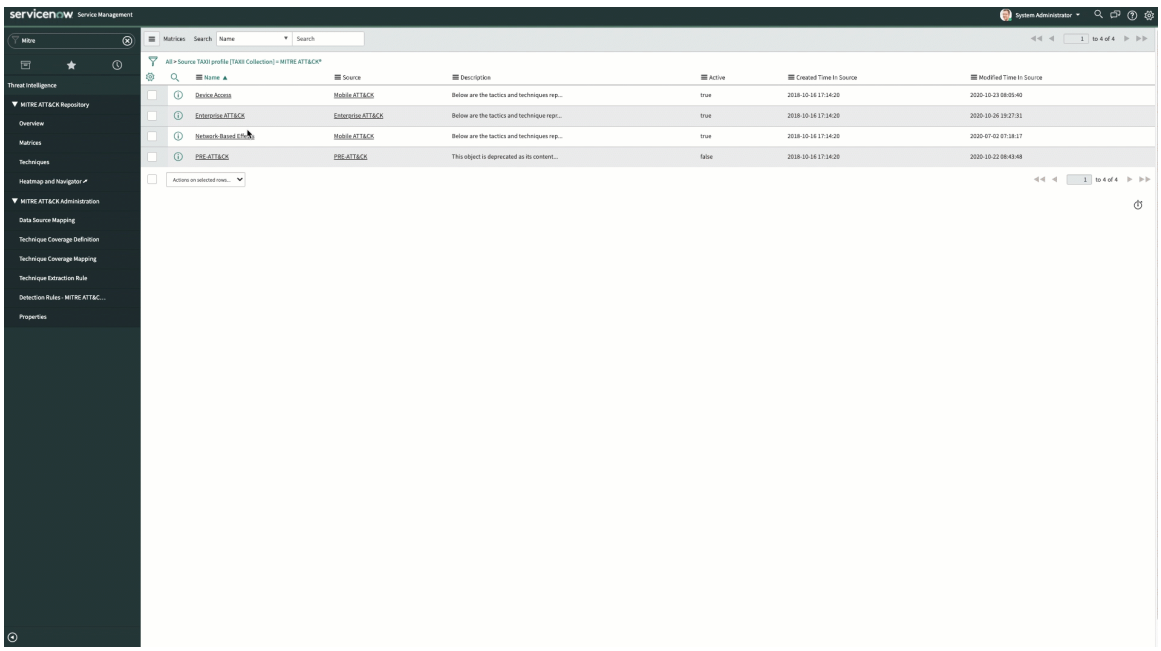
Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Matrizes**. Todas as matrizes estão desabilitadas por padrão.
2. Para ativar uma matriz, aponte para **Ativo** , clique duas vezes e selecione **verdadeiro** .
3. Para exibir todas as informações associadas, clique em uma matriz.
4. Para exibir todas as táticas associadas a esta coleção, clique em **MITRE táticas** guia.
5. Para exibir detalhes adicionais e as técnicas associadas a uma tática selecionada, clique em uma tática.
6. Em **TÉCNICAS MITRE ATT&CK** selecione uma técnica.
7. Nas Listas relacionadas, exiba as associações que estão disponíveis para a técnica selecionada.

Na ilustração a seguir, você pode ver o caminho de navegação da matriz Enterprise ATT&CK, para a tática Acesso inicial (TA0001) e, em seguida, para a técnica Phishing (T1566). Na página Padrão de ataque - Técnica de phishing, você pode exibir a lista relacionada - Tática, Subtécnica, Grupo, Mitigação, Referências externas, malware e ferramentas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você pode estenda as informações em alguns desses objetos de lista relacionados com base na técnica selecionada. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação, Referências externas, Malware e Ferramentas.

Gerenciar técnicas

Gerencie as técnicas que foram importadas do MITRE TAXII coleções. As técnicas contêm várias maneiras pelas quais os invasores desenvolveram para empregar uma determinada tática. Você pode revisar e desativar técnicas que não são relevantes para sua organização. Em STIX, as técnicas são conhecidas como padrões de ataque.

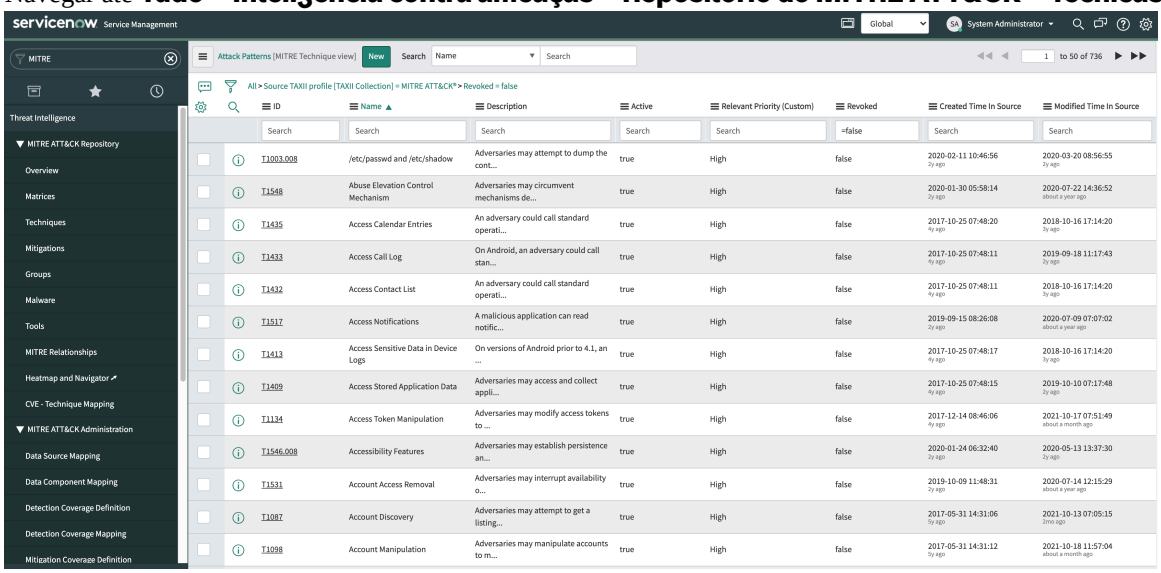
Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.



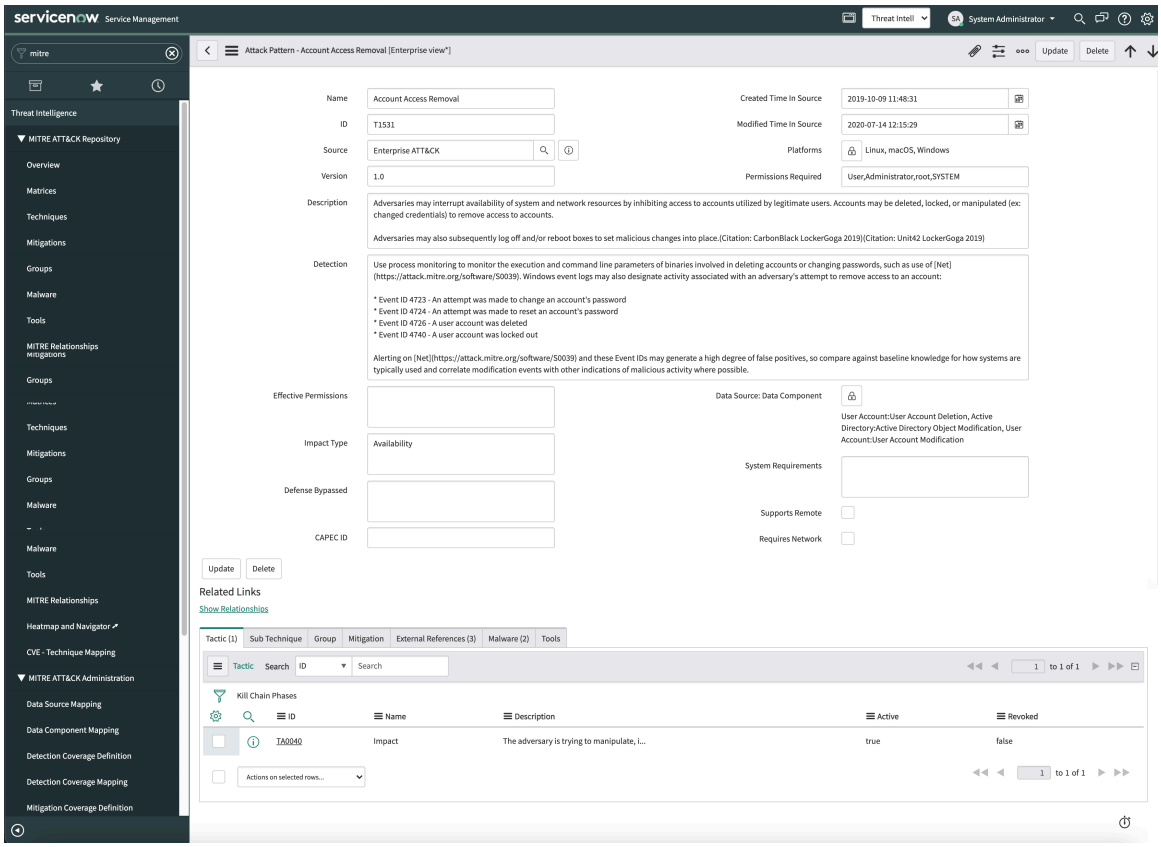
A lista de técnicas e subtécnicas agora está listada.

2. Para revisar e desativar técnicas que não são relevantes para sua organização, acesse a exibição de lista da técnica selecionada e, na coluna Ativo, atualize a configuração para **falso** e salve a configuração. Desative as técnicas que não são usadas pelos outros objetos no MITRE-ATT&CK repositório.
3. Para priorizar uma técnica, atribua uma prioridade no **Prioridade relevante (personalizada)** campo. A prioridade relevante do sistema de base está definida como nenhuma. . **Prioridade relevante (personalizada)** o campo não foi importado do MITRE-ATT&CK TAXII coleções, mas um campo personalizado introduzido em ServiceNow AI Platform. Você pode usar as informações de prioridade relevantes para filtrar e priorizar técnicas nos painéis, durante o mapeamento da fonte de dados ou ao analisar o mapa de calor.
4. Clique em uma técnica para exibir todas as informações associadas a esta técnica.

   Na ilustração a seguir, você pode exibir os detalhes de cada técnica de remoção de acesso à conta, seu ID, origem e outras informações relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Fonte de dados: Elemento de componente de dados introduzido por MITRE Substitui o campo Fonte de dados anterior. O componente de dados fornece uma subcamada extra de contexto para as fontes de dados. . MITRE-ATT&CK o repositório contém o antigo TAXII, em seguida, você pode exibir o campo Fonte de dados. Caso contrário, você pode exibir as fontes de dados com o contexto adicional de componentes de dados no campo Fonte de dados: Componente de dados. Você pode exibir o novo campo de componente de dados somente quando a origem for Enterprise ATT&CK. Para obter mais informações, consulte mapeamento de componente de dados .

5. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

O que Fazer Depois

Você pode estenda as informações em alguns desses objetos de lista relacionados. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação e Referências externas.

Gerenciar mitigações

Gerencie as mitigações que foram importadas do MITRE TAXII coleções. As mitigações permitem impedir que um adversário execute técnicas ou subtécnicas com sucesso em sua organização. Em STIX, as mitigações são conhecidas como curso de ações.

Antes de Iniciar

Função necessária:

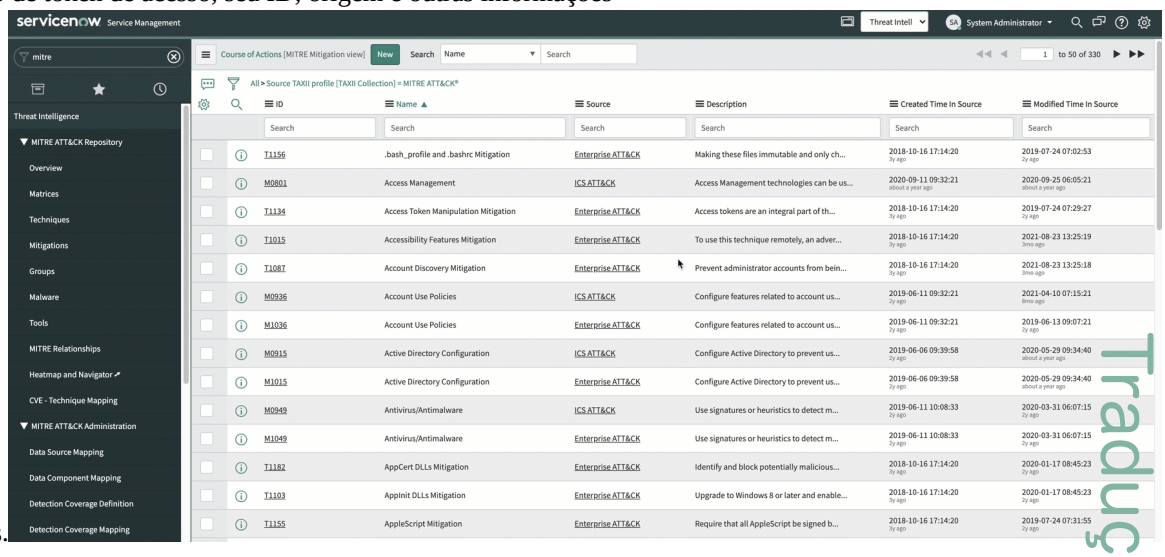
- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mitigações**.
   As mitigações agora estão listadas.
2. Clique em uma mitigação para exibir todas as informações associadas.
   Na ilustração a seguir, você pode exibir os detalhes da mitigação da manipulação de token de acesso, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

O que Fazer Depois

Use módulo de técnicas para adicionar ou modificar os dados de mitigação.

Gerenciar grupos

Gerencie os grupos que foram importados do MITRE TAXII coleções. Grupos são conjuntos de atividades de invasão relacionadas que são rastreados por um nome comum na comunidade de segurança. Os analistas rastreiam clusters de atividades usando vários termos, como grupos de ameaças, grupos de atividades, agentes de ameaças, conjuntos de invasão e campanhas. Em STIX grupos são conhecidos como conjuntos de intrusão.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

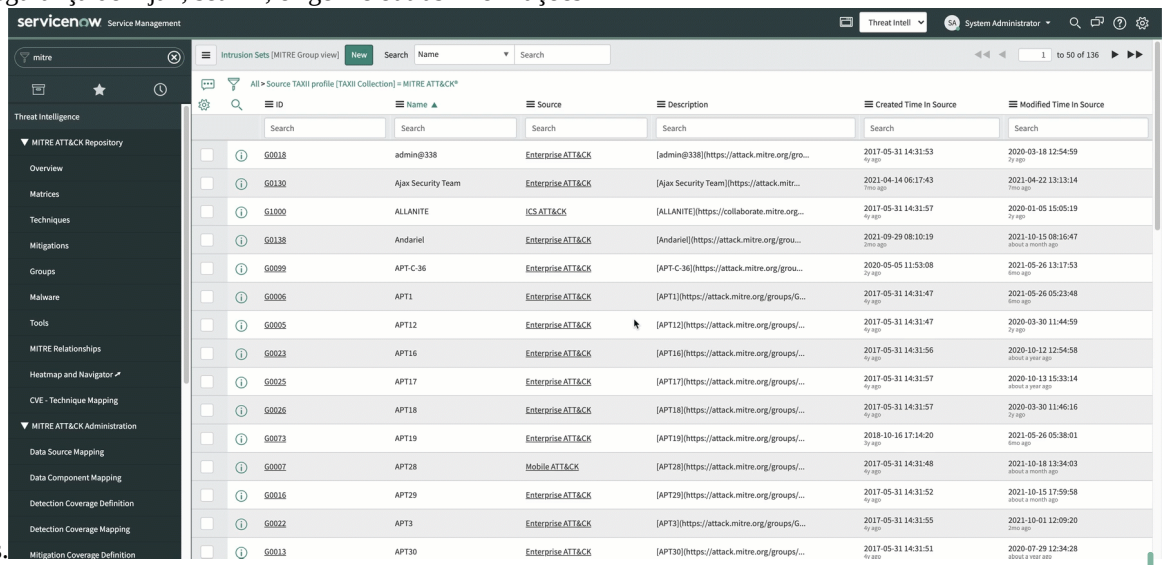
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Grupos**.
   Você pode exibir os grupos listados.
2. Clique em um grupo para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do grupo Equipe de segurança do Ajax, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

> **Nota:** Para associar os grupos de ameaça a um caso de segurança para investigação mais profunda, clique em **Adicionar ao Caso de segurança** .

O que Fazer Depois

Use módulo de técnicas para adicionar ou modificar os dados dos grupos.

Gerenciar malware

Gerencie as informações de malware que você importou do MITRE TAXII coleções. Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido de forma secreta em um sistema. A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

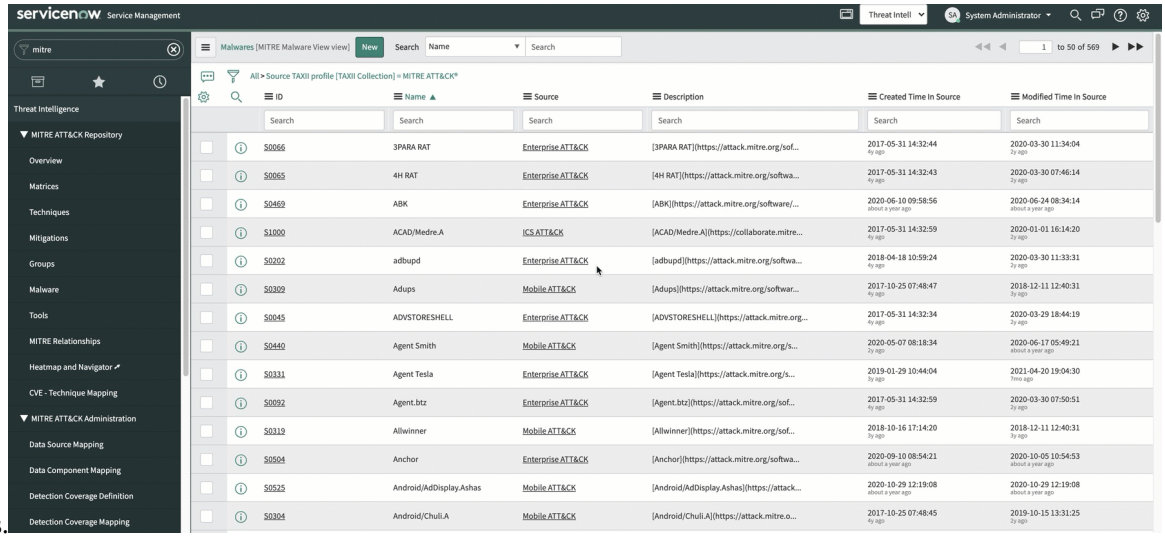
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Malware**. Você pode exibir o malware listado.
2. Clique em um malware para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do malware 3PARA RAT, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

O que Fazer Depois

Use módulo de técnicas para adicionar ou modificar os dados de malware.

Gerenciar ferramentas

Gerencie as informações de ferramentas que você importou do MITRE TAXII coleções. Ferramentas são software legítimo que são usados por agentes de ameaça para executar ataques.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Por Que e Quando Desempenhar Esta Tarefa

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

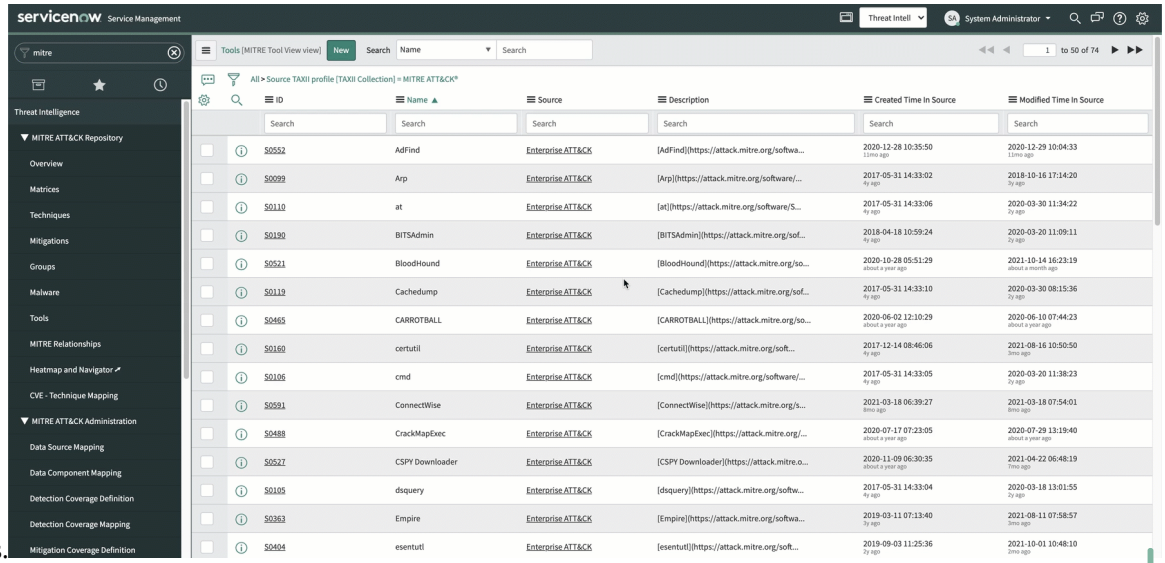
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Ferramentas**.
   Você pode exibir as ferramentas listadas.
2. Clique em uma ferramenta para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da ferramenta CARROTBALL, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

O que Fazer Depois

Use módulo de técnicas para adicionar ou modificar os dados das ferramentas.

Gerenciar MITRE relacionamentos

Gerencie o. MITRE informações de relacionamentos que você importou do MITRE TAXII coleções.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

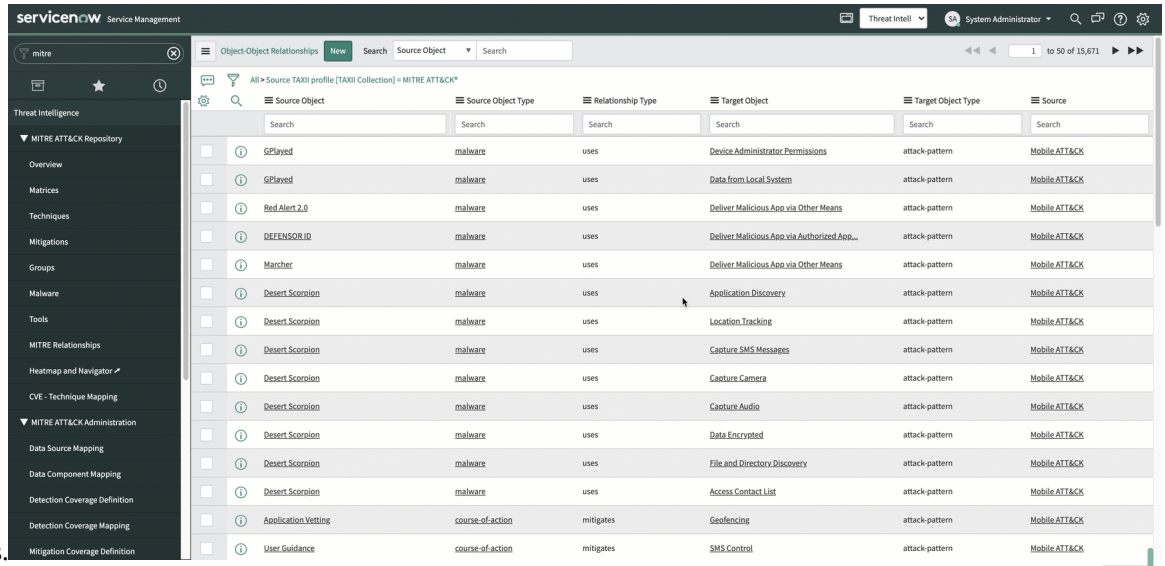
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Relações do MITRE**.
   Você pode exibir as ferramentas listadas.
2. Clique em um objeto de origem para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do objeto Red Alert 2,0, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos** .

O que Fazer Depois

Use módulo de técnicas Para adicionar ou modificar os dados de relacionamentos DO MITRE.

Gerenciar CVE e mapeamento de técnica

Gerencie o CVE e as informações de técnica mapeadas após a importação do MITRE TAXII coleções.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Nota: . **Mapeamento CVE-técnica** O módulo está disponível somente quando o produto Resposta a vulnerabilidades está instalado em seu ambiente.

Por Que e Quando Desempenhar Esta Tarefa

Depois de importar o. MITRE TAXII Coleções Você pode exibir os CVEs em seu ambiente e seu relacionamento com o associado MITRE-ATT&CK técnicas. Você também pode criar associações com CVEs e os padrões de ataque.

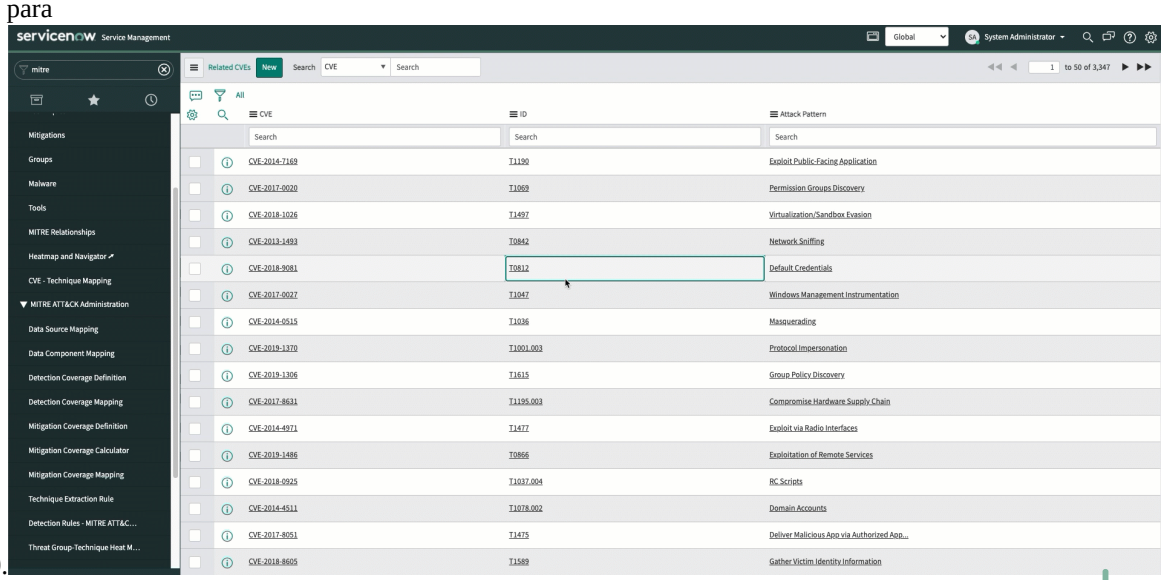
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **CVE - Mapeamento de técnica**.
   Você pode exibir os CVEs e as técnicas listadas.
2. Clique em um CVE para exibir a entrada do banco de dados de vulnerabilidades.

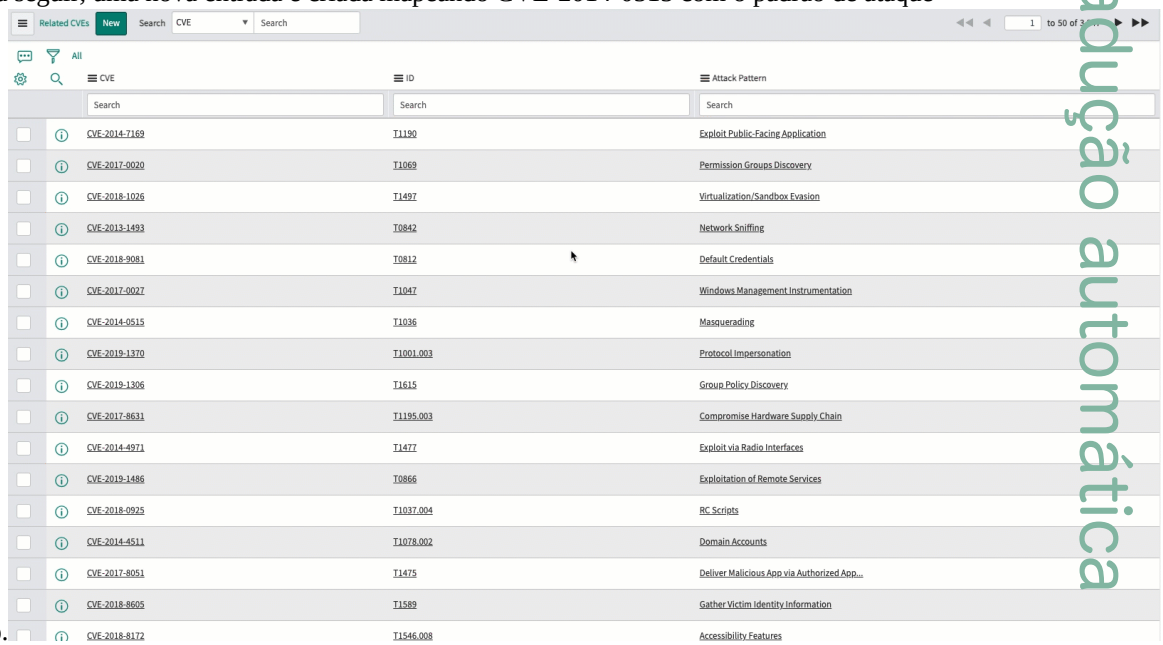
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da lista CVE e da entrada do banco de dados de vulnerabilidades para CVE-2014-7169.



3. Para adicionar uma entrada, clique em **Novo** Mapeie o CVE para um padrão de ataque e clique em **Enviar** . Na ilustração a seguir, uma nova entrada é criada mapeando CVE-2014-0515 com o padrão de ataque mascaramento.



Tradução automática

Estenda MITRE-ATT&CK dados

Estenda MITRE-ATT&CK dados do repositório no ServiceNow AI Platform enriquecendo-a.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: acesso de criação e gravação

Por Que e Quando Desempenhar Esta Tarefa

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no MITRE-ATT&CK repositório.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar um novo objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo de repositório MITRE ATT&CK, mas não é possível definir o tipo de relacionamento neste módulo. Para obter mais informações sobre como definir tipos de relacionamento, consulte relacionamentos objeto a objeto . Para definir um tipo de relacionamento, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

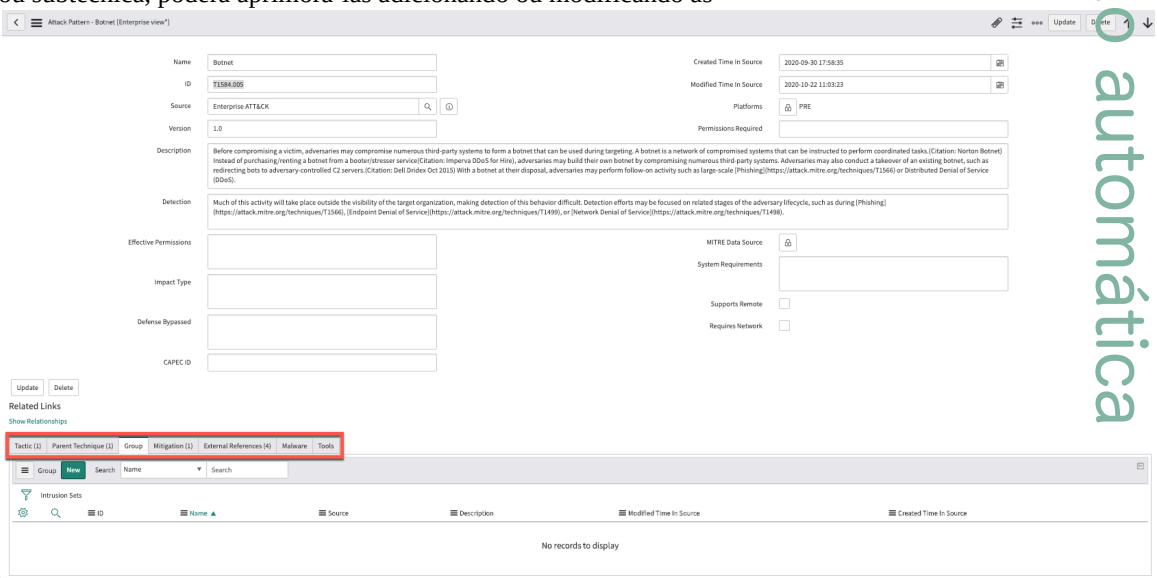
Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no Repositório MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazer isso no Repositório IOC.

Nota: Todas as personalizações feitas nos objetos são salvas durante as atualizações programadas.

Procedimento

1. Navegar até **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.
2. Clique em uma técnica ou subtécnica para exibir todas as informações associadas a esta técnica. Na ilustração a seguir, você pode ver que a técnica de Botnet (T1584.005) não está associada a nenhum grupo. Se você tiver informações adicionais sobre uma técnica ou subtécnica, poderá aprimorá-las adicionando ou modificando as informações.

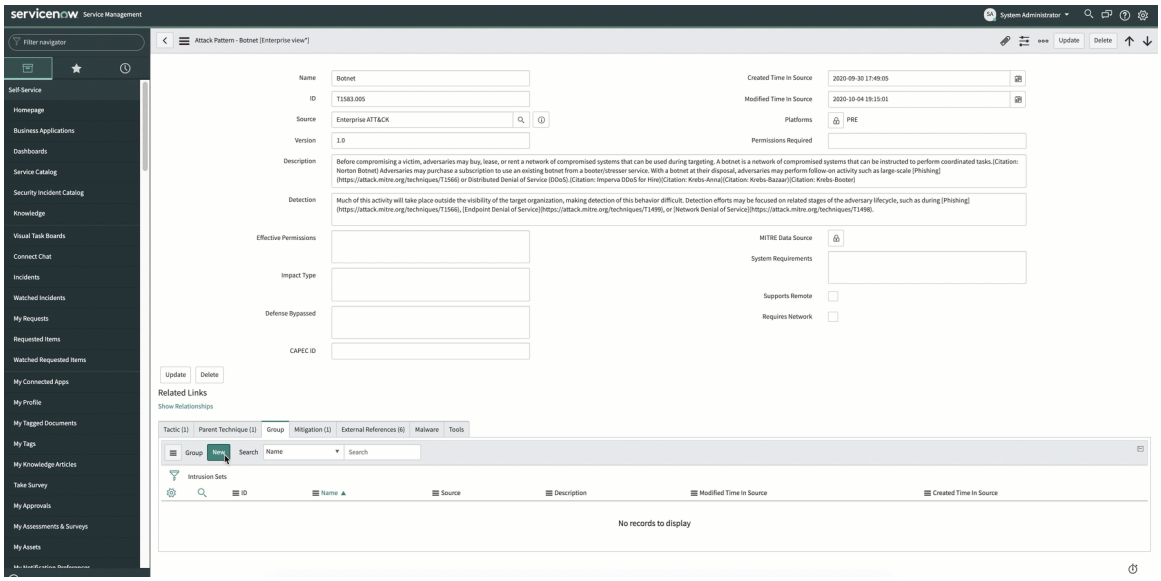


3. Clique em uma lista relacionada para enriquecer seus dados e associá-los a um novo grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, um grupo, Custom1, foi associado à subtécnica de Botnet.



Defina a fonte de dados e o mapeamento da ferramenta de detecção

Defina a fonte de dados e o mapeamento da ferramenta de detecção para MITRE-ATT&CK táticas e técnicas. O mapeamento da fonte de dados fornece informações sobre a relevância e a disponibilidade das fontes de dados e as ferramentas de detecção para monitorar as fontes de dados em seu ambiente.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação e exclusão
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar as fontes de dados e as ferramentas de detecção de que sua organização precisa para detectar as técnicas com eficácia.

Por exemplo, se sua organização se concentrar em 5 técnicas, talvez você precise de 10 fontes de dados e 10 ferramentas de detecção para monitorar essas fontes. Digamos que você identifique que sua organização não tem duas fontes de dados e cinco ferramentas de detecção. Este exercício fornece visibilidade das fontes de dados, sua relevância para sua organização e para identificar lacunas na cobertura. Você também pode se concentrar em aprimorar seu ambiente com as fontes de dados e ferramentas de detecção corretas.

Todas as táticas, técnicas, IDs e fontes de dados ativas são preenchidas automaticamente com base em TAXII perfil

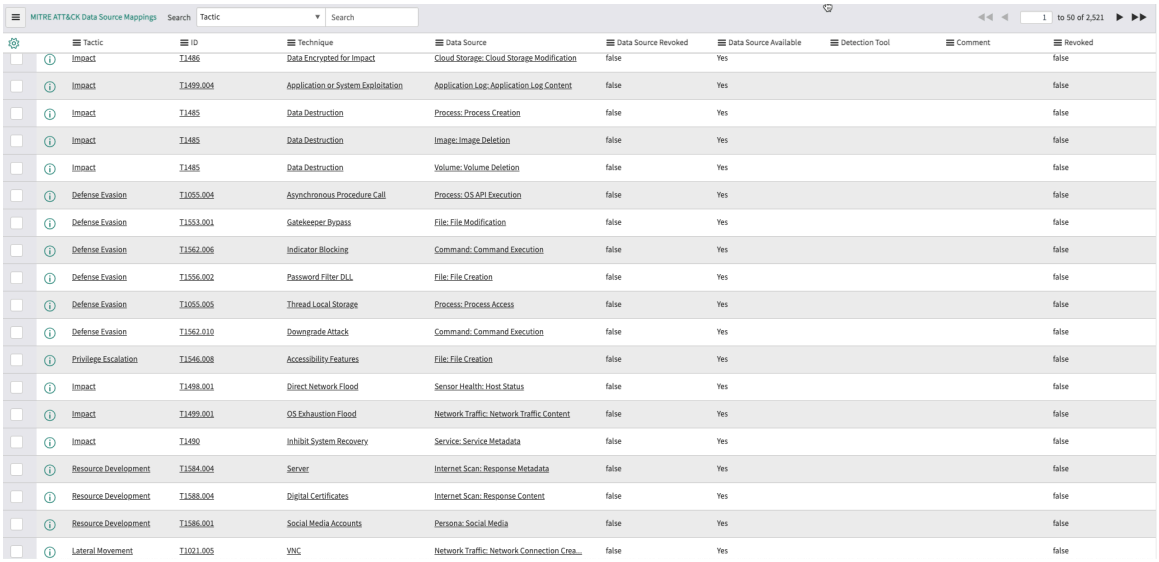
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de fonte de dados**.

   A ilustração a seguir mostra a lista de táticas, técnicas e seus IDs que foram preenchidos com base nas atualizações da sua coleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Campo	Descrição
Tática	Objetivo do adversário ou o motivo da execução de uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de dados	Fonte de dados associada à técnica.
Fonte de dados revogada	Se definida como verdadeira, a fonte de dados será revogada, no entanto, o mapeamento da fonte de dados ainda será mantido. Se o valor da fonte de dados não for encontrado em MITRE, Em seguida, o valor Fonte de dados revogada é marcado automaticamente como verdadeiro. O mapeamento da fonte de dados para um registro será revogado se os relacionamentos técnica e fonte de dados estiverem ausentes no atualizado MITRE dados. Padrão: falso
Fonte de dados disponível	Disponibilidade da fonte de dados.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção é mapeada com o sensor de alerta em SIR.
Revogado	O mapeamento da fonte de dados para um registro será revogado se os relacionamentos técnica e fonte de dados estiverem ausentes no atualizado MITRE dados. Padrão: falso

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Revise as fontes de dados listadas e modifique o valor em **Fonte de dados disponível** campo baseado em seu ambiente.

3. **Nota:** Não é possível editar esta entrada na exibição de lista.

   Em **Ferramenta de detecção** , execute as seguintes etapas:

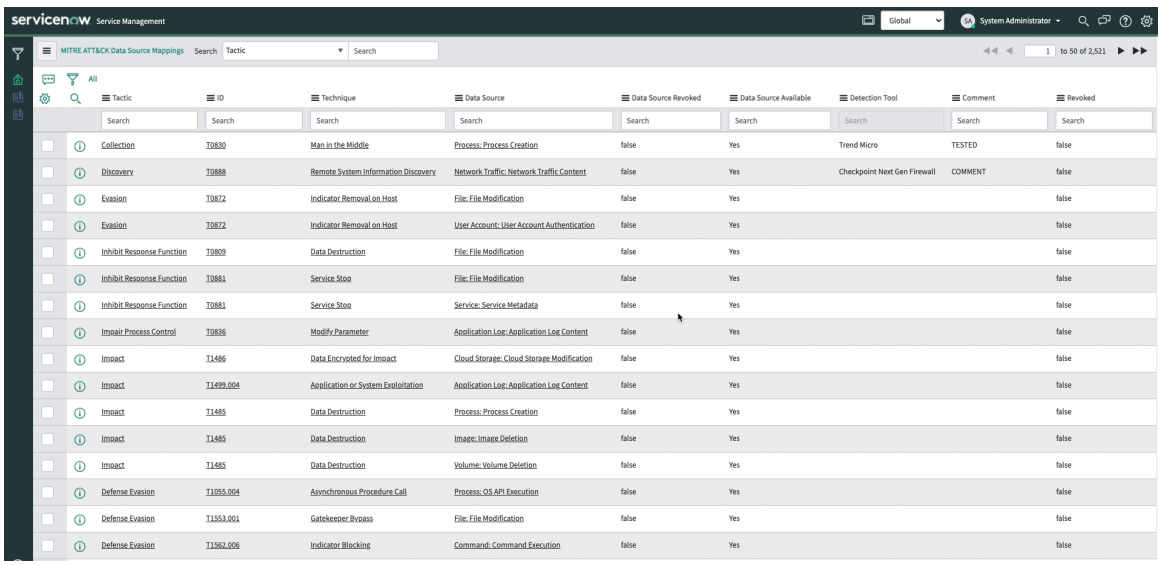
   a. Clique no ícone de informações e clique em **Registro em aberto** .

   b. Desbloquear **Ferramenta de detecção** entrada.

   c. Use a lista de pesquisa para selecionar uma ferramenta de detecção. Você pode selecionar várias ferramentas de detecção.

   d. Clique em **Atualizar**.

   Na ilustração a seguir, várias ferramentas de detecção são adicionadas para monitorar a fonte de dados.



Defina a fonte de dados e o mapeamento do componente de dados

Use o Mapeamento de componente de dados se estiver usando o mais recente TAXII e você deseja manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas. Mapeie as fontes de dados com o contexto adicional de componentes de dados que fornece uma subcamada extra de contexto para fontes de dados que permitem entender os comportamentos do adversário em MITRE-ATT&CK melhor.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação e exclusão
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Mapear as fontes de dados e os componentes de dados fornece visibilidade sobre as fontes de dados ou componentes e as técnicas relevantes para sua organização.

Por exemplo, se sua organização se concentrar em 7 técnicas, talvez você precise de 5 fontes de dados e 10 componentes de dados para monitorar essas fontes. Sua avaliação de ferramentas internas revela que sua organização não tem duas fontes de dados e

Tradução automática

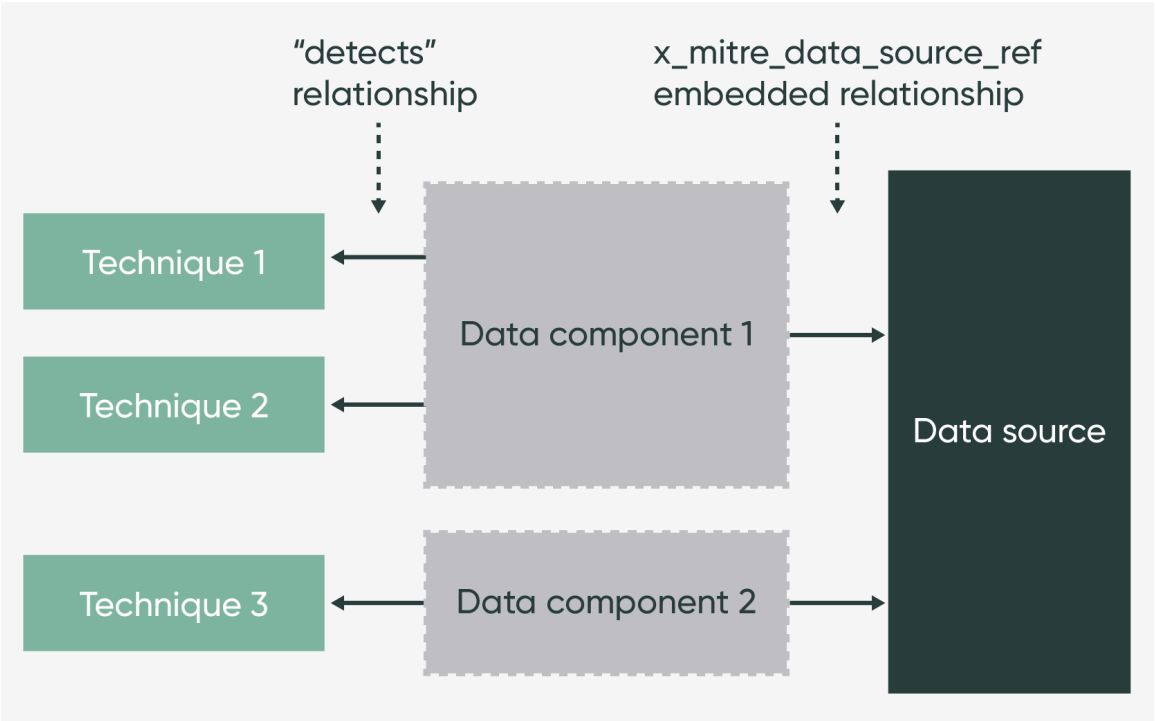
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quatro componentes de dados. Este exercício de mapeamento fornece visibilidade das fontes de dados, componentes e técnicas, sua relevância para sua organização e para identificar as lacunas na cobertura. Assim, você pode concentrar seu investimento nas fontes de dados corretas e nos sensores de alerta para detectar e mitigar as ameaças adversárias.

. MITRE-ATT&CK A estrutura contém uma estrutura atualizada para as fontes de dados - Fonte de dados: Componente de dados. Este novo formulário de fonte de dados fornece um contexto extra para as fontes de dados. O objeto da fonte de dados apresenta o nome da fonte de dados, bem como os principais detalhes sobre os dados coletados (arquivo, processo, tráfego de rede e assim por diante) e valores ou propriedades específicos necessários para detectar comportamentos adversários.

A ilustração a seguir mostra o. MITRE-ATT&CK STIX™ representação de estrutura para fontes de dados e componentes de dados. Você pode ver as fontes de dados e os componentes de dados capturados como personalizados STIX™ objetos. A ilustração mostra que cada fonte de dados contém um ou mais componentes de dados e cada componente de dados detecta uma ou mais técnicas.

Estrutura geral de fontes de dados e componentes de dados



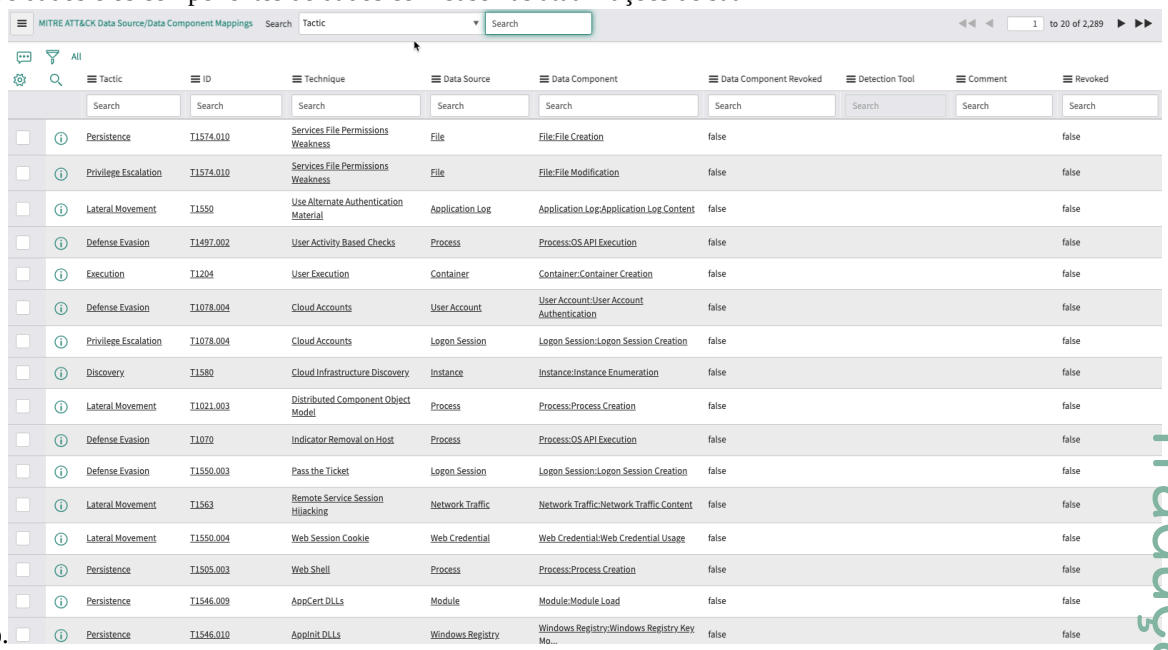
Você pode continuar usando Mapeamento da fonte de dados . MITRE-ATT&CK o repositório contém o antigo TAXII e você mapeou suas fontes de dados para várias técnicas. No entanto, use Mapeamento de componente de dados se você estiver usando o mais recente TAXII e você deseja manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de componente de dados**.
   A ilustração a seguir mostra a lista de táticas, IDs e técnicas junto com as fontes de dados e os componentes de dados com base nas atualizações de sua coleção.



Tactic	ID	Technique	Data Source	Data Component	Data Component Revoked	Detection Tool	Comment	Revoked
Persistence	T1574.010	Services File Permissions Weakness	File	File:File Creation	false			false
Privilege Escalation	T1574.010	Services File Permissions Weakness	File	File:File Modification	false			false
Lateral Movement	T1550	Use Alternate Authentication Material	Application Log	Application Log:Application Log Content	false			false
Defense Evasion	T1497.002	User Activity Based Checks	Process	Process:OS API Execution	false			false
Execution	T1204	User Execution	Container	Container:Container Creation	false			false
Defense Evasion	T1078.004	Cloud Accounts	User Account	User Account:User Account Authentication	false			false
Privilege Escalation	T1078.004	Cloud Accounts	Logon Session	Logon Session:Logon Session Creation	false			false
Discovery	T1580	Cloud Infrastructure Discovery	Instance	Instance:Instance Enumeration	false			false
Lateral Movement	T1021.003	Distributed Component Object Model	Process	Process:Process Creation	false			false
Defense Evasion	T1070	Indicator Removal on Host	Process	Process:OS API Execution	false			false
Defense Evasion	T1550.003	Pass the Ticket	Logon Session	Logon Session:Logon Session Creation	false			false
Lateral Movement	T1563	Remote Service Session Hijacking	Network Traffic	Network Traffic:Network Traffic Content	false			false
Lateral Movement	T1550.004	Web Session Cookie	Web Credential	Web Credential:Web Credential Usage	false			false
Persistence	T1505.003	Web Shell	Process	Process:Process Creation	false			false
Persistence	T1546.009	AppCert DLLs	Module	Module:Module Load	false			false
Persistence	T1546.010	AppInit DLLs	Windows Registry	Windows Registry:Windows Registry Key Mo...	false			false

Campo	Descrição
Tática	Objetivo do adversário ou o motivo da execução de uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de dados	Fonte de dados associada à técnica.
Componente de dados	Componente de dados associado à fonte de dados. Um componente de dados só pode ter uma fonte de dados primária.
Componente de dados revogado	Identifica se o componente de dados foi revogado no MITRE-ATT&CKbase de conhecimento.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção é mapeada com o sensor de alerta em SIR.
Comentário	Descrição sobre o mapeamento da fonte de dados e do componente de dados.
Revogado	Identifica se o componente de dados para mapeamento de técnica foi revogado por MITRE-ATT&CK.

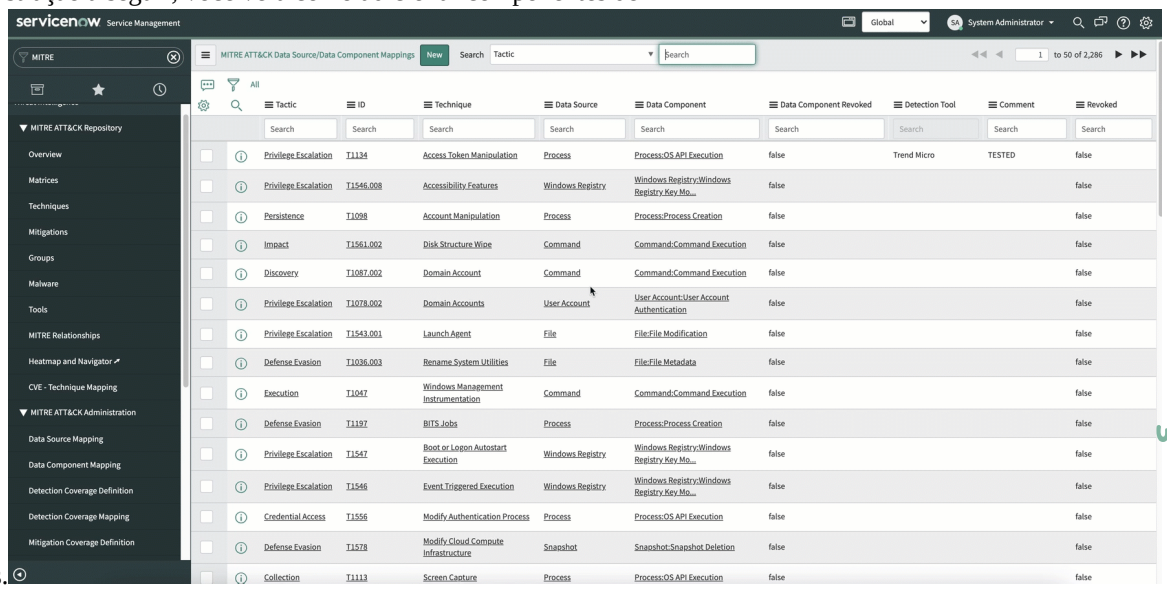
2. Revise as fontes de dados listadas e os componentes de dados e modifique os valores com base no seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Siga estas etapas para adicionar um componente de dados.
   a. Navegar até **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Técnicas**.
   b. Clique em uma técnica que você deseja modificar a fonte de dados: Informações do componente de dados.
   c. Desbloquear fonte de dados: Componente de dados.
   d. Use a lista de pesquisa para selecionar MITRE-ATT&CK componentes de dados.
   e. Bloquear fonte de dados: Componente de dados.
   f. Clique em **Atualizar**.

Na ilustração a seguir, você verá como adicionar componentes de dados.



Defina a cobertura de detecção da técnica

Defina a cobertura de detecção de técnica que sua organização deve medir e detectar técnicas específicas de adversários.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: Acesso de gravação
- Função necessária: sn_ti.read: Acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

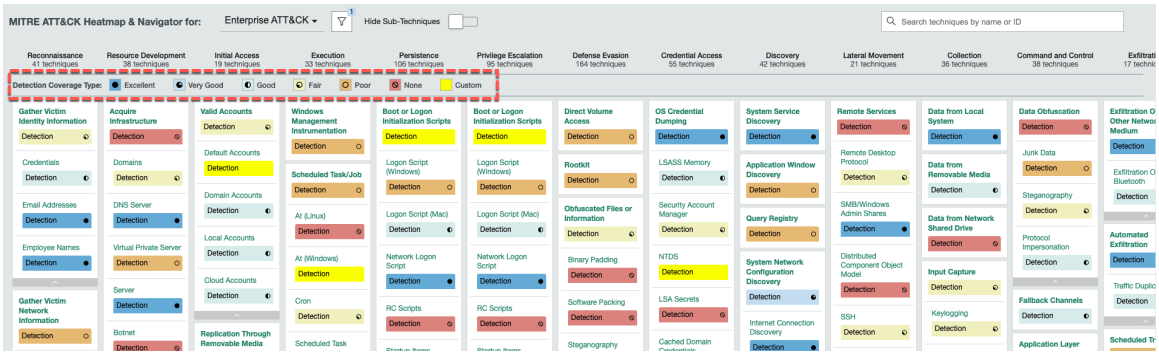
As definições de cobertura da técnica são usadas no mapeamento geral de detecção da técnica. Você pode usar a cobertura da técnica do sistema de base. . cobertura da técnica do sistema de base Consiste nos tipos de cobertura Nenhum, Ruim, Regular, Bom, Muito Bom, e excelente. A cobertura técnica do sistema de base também está associada a cores predefinidas. Você pode personalizar as entradas e as cores do tipo de cobertura ou criar suas próprias entradas. Por exemplo, você pode modificar os tipos de cobertura do sistema de base para Não aplicável, Cobertura parcial e Cobertura completa. Como alternativa, você também pode criar medidas numéricas para os tipos de cobertura, como 0-25%, 25 a 50% e 50 a 100%. Os tipos de modificações feitas na cobertura do sistema de base não se limitam aos exemplos compartilhados.

As personalizações que você faz no tipo de cobertura e na cor são usadas no mapeamento de detecção de técnica geral e também no mapa de calor .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você modificar a definição de cobertura do sistema de base, os ícones de Tipo de cobertura não serão exibidos com as técnicas no mapa de calor. O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que as cores de cobertura e cobertura de detecção de técnica definidas pelo sistema de base. No entanto, se você excluir campos existentes da cobertura de detecção de técnica geral, o mapa de calor não exibirá os ícones de tipo de cobertura.



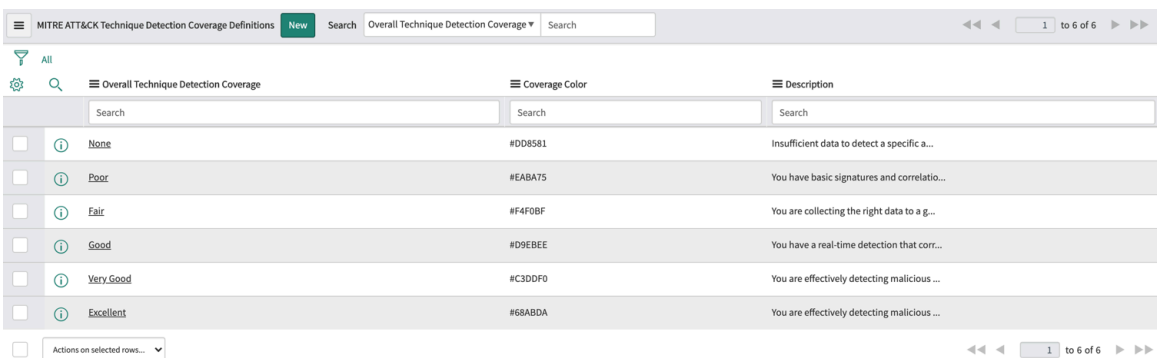
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de detecção**.
2. Revise as entradas gerais de detecção de técnica e personalize as entradas para o seu ambiente.

Definição de cobertura de detecção

Campo	Descrição
Cobertura da detecção de técnica geral	Nome da cobertura geral de detecção da técnica. . cobertura da técnica do sistema de base Consiste em Nenhum, Pobre, Regular, Bom, Muito Bom, ou excelente.
Cor da cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de detecção da técnica no mapa de calor. Você pode personalizar as cores usando códigos HEXADECIMAIS e valores RGB(A).
Descrição	Cobertura geral de detecção de técnica. Consulte a definição do sistema de base em Definição de pontuação .

A ilustração a seguir mostra a lista Definição de cobertura de detecção.



3. Para adicionar uma entrada, clique em **Novo** preencha as entradas e clique em **Enviar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE-ATT&CK Definição de pontuação

Defina o da sua organização MITRE-ATT&CK sistema de pontuação para que você possa medir a eficácia com que sua organização pode detectar técnicas específicas de adversários.

Definição de pontuação

Pontuação	Mapeamento de pontuação	Descrição
Nenhum(a)	0	Dados insuficientes para detectar uma técnica de adversário específica.
Ruim	1	Assinaturas básicas e regras de correlação estão em vigor para detectar técnicas específicas do adversário. A detecção de ameaças não ocorre em tempo real e abrange apenas um número mínimo de aspectos de uma técnica. Por exemplo, a caça ocorre somente em um endpoint de cada vez. Sua organização ainda pode ter milhares ou centenas de eventos que os caçadores devem revisar e correlacionar com outros eventos para encontrar exceções. O número de falsos positivos é alto.
Justo	2	Coletar os dados corretos em grande medida e a qualidade dos dados é justa. Por exemplo, sua organização pode estar começando a adicionar Logs do Sysmon, ETW, logs do PowerShell e similares. No entanto, a detecção de ameaças ainda não é em tempo real. Sua organização pode não ter todas as ferramentas certas para agregar e analisar os dados com eficácia. Os caçadores devem executar consultas manualmente e correlacionar para analisar os dados com precisão. O número de falsos positivos é alto.
Bom	3	Detecção em tempo real que correlaciona e integra vários dados em todos os endpoints. A detecção de ameaças abrange muitos aspectos dos procedimentos de uma técnica. Seus adversários podem ignorar a detecção com evasão e ofuscação. Sua organização pode identificar facilmente falsos positivos e filtrá-los. Sua organização usa técnicas básicas de ciência de dados para analisar os dados no repositório central.
Muito Bom	4	Detecte técnicas mal-intencionadas em tempo real e cubra a maioria dos aspectos dos procedimentos de uma técnica. A possibilidade de seus adversários contornarem a deteção com métodos de evasão e ofuscação é mais difícil do que no bom nível. Sua organização pode identificar facilmente falsos positivos e filtrá-los. Sua organização usa técnicas avançadas de ciência de dados para detectar as técnicas do adversário.
Excelente	5	Detecte técnicas mal-intencionadas em tempo real e cubra todos os aspectos dos procedimentos de uma técnica. Sua organização tem um bom entendimento do seu ambiente com a automação e a qualidade de dados corretas. A possibilidade de seus adversários ignorarem a detecção com métodos de evasão e ofuscação não é possível neste nível. O número de falsos negativos é baixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeie sua cobertura de detecção de técnica para uma técnica

Mapeie sua cobertura geral de detecção de técnica com a técnica que permite que sua organização detecte técnicas específicas de adversários.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: Acesso de gravação
- Função necessária: sn_ti.read: Acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar a cobertura de detecção de técnica para obter uma visão geral da cobertura de detecção de técnica geral da sua organização. Por exemplo, se um adversário estiver atacando sua organização, você verá o tipo de cobertura necessário para detectar as técnicas do invasor.

A técnica e o ID são preenchidos automaticamente para todos os coleções e. técnicas que você ativou. . tipo de cobertura e definição de pontuação que você definiu estão disponíveis para como uma opção que você pode selecionar na cobertura geral de detecção de técnica.

Você pode mapear a cobertura geral de detecção de técnica com a técnica para concluir o mapeamento. Você pode associar uma técnica a apenas uma cobertura geral de detecção de técnica.

O mapeamento de cobertura de detecção de técnica que você define é usado no visualização de cobertura no mapa térmico .

Nota: Você pode chegar à cobertura geral de detecção de técnica usando cálculos específicos da sua organização. Você pode usar qualquer produto de simulação de violação e ataque (BAS), o Repositório de análise cibernética (CAR) ou qualquer outro método conforme necessário para definir a definição de pontuação e usá-lo neste procedimento para o mapeamento de cobertura de detecção de técnica geral.

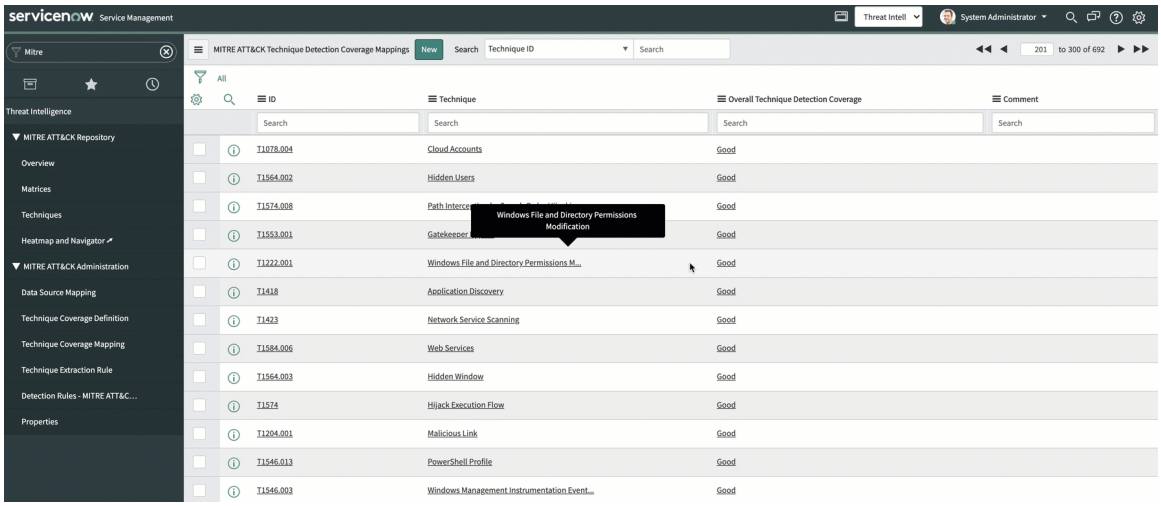
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de detecção**.

   Nesta ilustração, você vê que a subtécnica Contas de nuvem (T1078.004) tem uma cobertura excelente na organização e que a cobertura geral de detecção de técnica está mapeada para **Excelente** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Revise cada técnica e mapeie sua cobertura geral de detecção de técnica com base em definição de cobertura de detecção e a disponibilidade de cobertura da sua organização.

Defina a cobertura de mitigação

Defina a cobertura de mitigação para cada mitigação associada a uma técnica para que você obtenha visibilidade sobre o quão bem sua organização pode evitar os ataques que acontecem devido a uma técnica específica.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: Criar, gravar, excluir acesso
- Função necessária: sn_ti.read: Acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

As definições de cobertura de mitigação são usadas na mitigação geral e no mapeamento de cobertura de técnica. Você pode usar a cobertura de mitigação do sistema de base. A cobertura de mitigação do sistema de base consiste nos tipos de cobertura Nenhum, Ruim, Regular, Bom, Muito Bom, e excelente. A cobertura de mitigação do sistema de base também está associada a cores predefinidas e porcentagens de cobertura. Você pode personalizar os tipos de cobertura (adicionar ou remover tipos de cobertura), porcentagens de cobertura para limites inferiores e limites superiores e cores ou criar sua cobertura de mitigação personalizada.

As personalizações que você faz nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa de calor .

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de mitigação**.
2. Revise as entradas de detecção de mitigação e personalize as entradas para o seu ambiente.

Definição de cobertura de mitigação de técnica

Campo	Descrição
Cobertura da mitigação de técnica geral	Nome da cobertura de mitigação da técnica. . cobertura de mitigação do sistema de base Consiste em Nenhum, Pobre, Regular, Bom, Muito Bom, ou excelente.

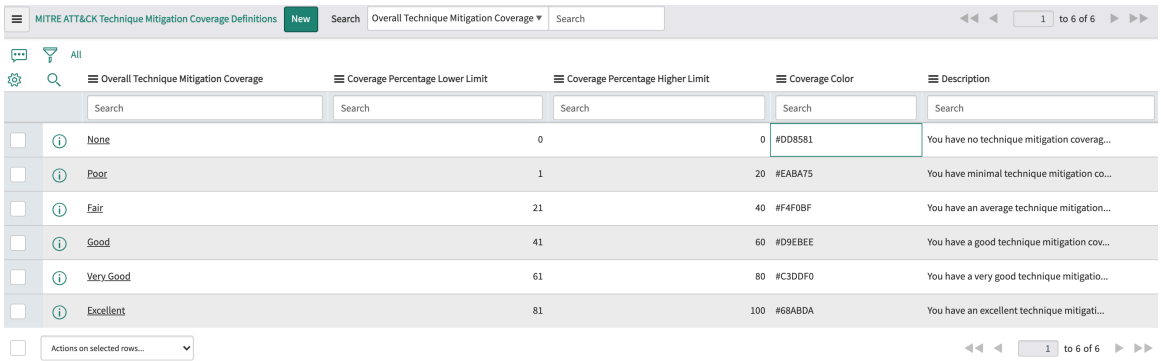
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Limite inferior do percentual de cobertura	O limite percentual inferior da cobertura de mitigação. Defina os valores numéricos entre 0 a 100.
Limite superior do percentual de cobertura	O limite percentual mais alto da cobertura de mitigação. Defina os valores numéricos entre 0 a 100.
Cor da cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de mitigação da técnica no mapa de calor. Você pode personalizar as cores usando códigos HEXADECIMAIS e valores RGB(A).
Descrição	Cobertura geral de detecção de mitigação. Consulte a definição do sistema de base em definição de cobertura de mitigação de técnica .

Nota: Não sobreponha os intervalos de porcentagem de cobertura se personalizar os limites de porcentagem (inferior ou superior). Por exemplo, se um registro de cobertura tiver os intervalos de 0 a 20, o próximo registro consecutivo deverá ter um intervalo de limite inferior de 21 ou superior para evitar sobreposição do intervalo de porcentagem de cobertura.

A ilustração a seguir mostra a lista de definição de cobertura de mitigação.



3. Para adicionar uma entrada, clique em **Novo** preencha as entradas e clique em **Enviar** .

Definições de cobertura de mitigação de técnica

Defina a cobertura de mitigação da sua organização para que você possa medir e detectar com eficácia técnicas específicas de adversários.

Definições de cobertura de mitigação de técnica de MITRE ATT&CK

Cobertura da mitigação de técnica geral	Limite inferior do percentual de cobertura	Limite superior do percentual de cobertura	Cor da cobertura	Descrição
Nenhum(a)	0	0	DD8581	Você não tem cobertura de mitigação de técnica e seus controles de defesa não têm capacidade de impedir um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação de técnica de MITRE ATT&CK

Cobertura da mitigação de técnica geral	Limite inferior do percentual de cobertura	Limite superior do percentual de cobertura	Cor da cobertura	Descrição
				ataque em qualquer cenário.
Ruim	1	20	EABA75	Você tem cobertura mínima de mitigação de técnica. As chances de um ataque são muito altas, e seus controles de defesa podem impedir um ataque em 0 a 20% dos cenários.
Justo	21	40	F4F0BF	Você tem uma cobertura média de mitigação de técnica. As chances de um ataque são altas, e seus controles de defesa podem impedir um ataque em 21 a 40% dos cenários.
Bom	41	60	DIEBEE	Você tem uma boa cobertura de mitigação de técnica. No entanto, as chances de um ataque são relativamente altas, e seus controles de defesa podem impedir um ataque em 41 a 60% dos cenários.
Muito Bom	61	80	C3DDF0	Você tem uma cobertura de mitigação de técnica muito boa. As chances de um ataque são baixas, e seus controles de defesa podem impedir um ataque em 61 a 80% dos cenários.
Excelente	81	100	68ABDA	Você tem uma excelente cobertura de mitigação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação de técnica de MITRE ATT&CK

Cobertura da mitigação de técnica geral	Limite inferior do percentual de cobertura	Limite superior do percentual de cobertura	Cor da cobertura	Descrição
				técnica e as chances de um ataque usando esta técnica são muito baixas e seus controles de defesa podem impedir um ataque em 81 a 100% dos cenários.

Mapeie sua cobertura de mitigação para uma técnica

Mapeie sua cobertura de mitigação com a técnica que permite detectar a estratégia de mitigação geral da sua organização.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: Acesso de gravação e exclusão
- Função necessária: sn_ti.read: Acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

As mitigações permitem impedir que um adversário execute técnicas ou subtécnicas com sucesso em sua organização. Cada um MITRE-ATT&CK a técnica contém mitigações que você pode implantar em sua organização para reduzir a chance de ser atacado. Você pode usar a cobertura de mitigação para obter uma visão geral da estratégia de mitigação geral da sua organização. Por exemplo, se um adversário estiver atacando sua organização, você verá o tipo de cobertura que precisa para mitigar as técnicas do invasor.

A técnica e as informações de mitigação são preenchidas automaticamente para todas as coleções e técnicas que você ativou. . definição de cobertura de mitigação que você definiu estão disponíveis para seleção na cobertura de mitigação de técnica.

Você pode identificar mitigações relevantes para sua organização. Se uma mitigação for relevante, você poderá definir se as estratégias de mitigação foram implantadas. Você pode especificar se as estratégias são aplicadas como parte da Política de SOC da sua organização. Você também pode identificar se sua organização tem ferramentas preventivas para mitigar as técnicas de um invasor e mapear todos os controles de segurança implantados por sua organização para minimizar os riscos de segurança. Preencha a cobertura de mitigação (porcentagem) para cada um dos registros.

Depois de mapear as informações de cada uma das técnicas, o calculadora de cobertura de mitigação Preenche automaticamente a Cobertura de mitigação de técnica calculada. Para calcular a cobertura geral de mitigação de qualquer técnica, os registros de mapeamento de mitigação da técnica devem estar ativos e relevantes para a organização. Os registros inativos e não relevantes não são considerados para calcular a cobertura geral de mitigação da técnica. Com base nos valores na Cobertura de mitigação de técnica calculada e no definição de cobertura de mitigação Sua Cobertura geral de mitigação de técnica (calculada) está preenchida.

As personalizações que você faz nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa de calor .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de mitigação**.
2. Revise cada técnica para mapeamento de mitigação e atualize o. **Cobertura de mitigação (porcentagem)** para calcular a disponibilidade de cobertura da sua organização.

Mapeamentos de cobertura de mitigação de técnica

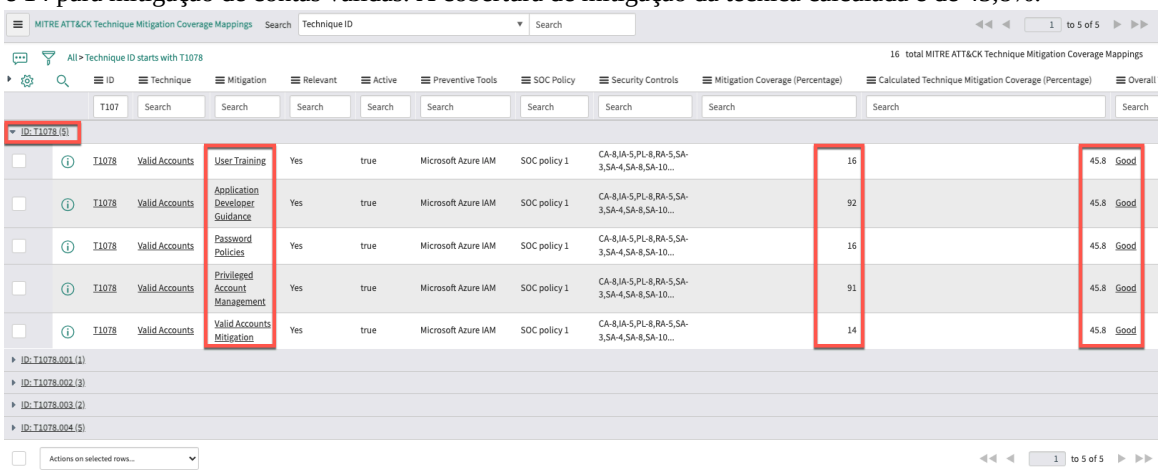
Campo	Descrição
ID	Identidade exclusiva da técnica. Os IDs são preenchidos automaticamente para todas as coleções e técnicas que você ativou.
Técnica	Como um adversário atinge um objetivo tático executando uma ação. As informações da técnica são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Mitigação	Mitigações que permitem impedir que um adversário execute técnicas ou subtécnicas com sucesso em sua organização. As informações de mitigação são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Relevante	Opção para especificar se a mitigação é relevante para sua organização.
Ativo	Opção para especificar se as estratégias de mitigação são implantadas em sua organização. Esta é uma opção necessária necessária para calcular a cobertura de mitigação da técnica.
Ferramentas preventivas	Opção para especificar se sua organização tem ferramentas preventivas para mitigar as técnicas de um invasor.
Política de SOC	As políticas de SOC que definem as estratégias de mitigação em sua organização.
Controles de segurança	Os controles de segurança da sua organização contêm as estratégias de mitigação para minimizar os riscos de segurança.
Cobertura de mitigação (percentual)	Um sistema de pontuação para calcular a cobertura de mitigação da técnica. Defina valores numéricos entre 0 a 100. Esta é uma opção necessária necessária para calcular a cobertura de mitigação da técnica.
Cobertura de mitigação da técnica calculada (percentual)	A cobertura de mitigação da técnica calculada em porcentagem. Este valor é determinado com base na fórmula definida em calculadora de cobertura de mitigação .
Cobertura da mitigação de técnica geral (calculada)	A cobertura geral de mitigação da técnica. Este valor é determinado com base em cobertura de mitigação definida para sua organização .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Comentário	Descrição sobre a técnica e o mapeamento de cobertura de mitigação.
Revogado	A técnica para mitigação do mapeamento de cobertura foi revogada.

Nesta ilustração, você vê que a técnica Contas válidas tem cinco mitigações associadas, cada uma com uma cobertura de mitigação de 16 para treinamento do usuário, 92 para orientação do desenvolvedor de aplicações e 16 para políticas de senha, 91 para gestão de contas privilegiadas e 14 para mitigação de contas válidas. A cobertura de mitigação da técnica calculada é de 45,8%.



Calculadora de cobertura de mitigação de técnica geral

A cobertura geral de mitigação da técnica é determinada com base na fórmula definida na calculadora de cobertura de mitigação.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: Criar, gravar, excluir acesso
- Função necessária: sn_ti.read: Acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

- Apenas uma calculadora de cobertura de mitigação pode ser definida como ativa por domínio.
- A calculadora de cobertura de mitigação do sistema de base é uma calculadora média.
- Todas as personalizações do script da calculadora devem garantir que a saída final seja um valor numérico entre 0 e 100.
- A definição de cobertura de mitigação é aplicada com base no intervalo da saída final.

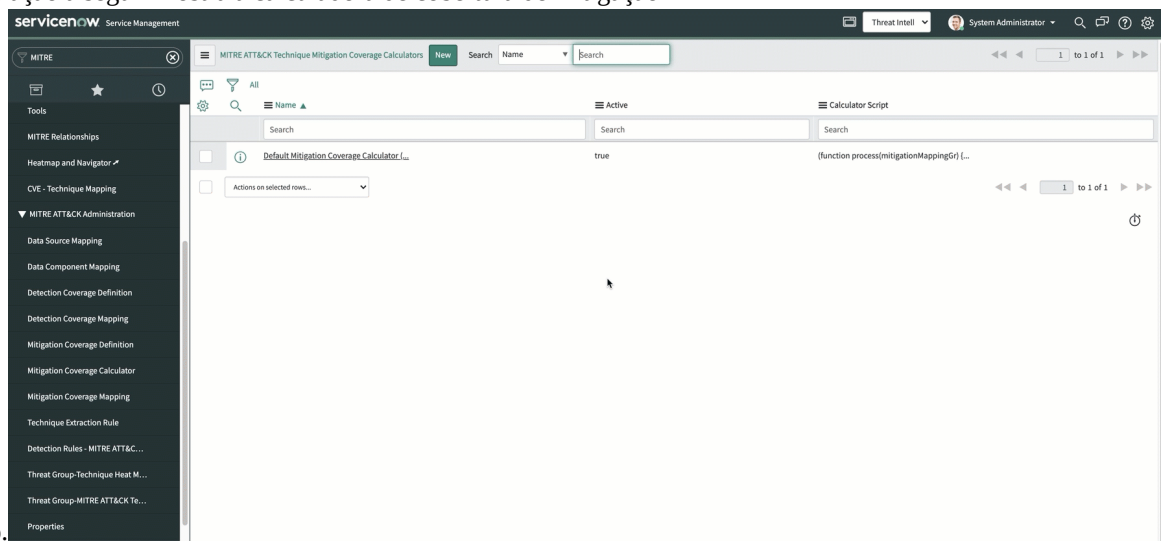
Procedimento

Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Calculadora de cobertura de mitigação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra a calculadora de cobertura de mitigação padrão.



Crie e mapeie regras de detecção

Crie regras de detecção e mapeie-as em relação às táticas e técnicas. Com este mapeamento, você pode ver a cobertura das regras de detecção em sua organização.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

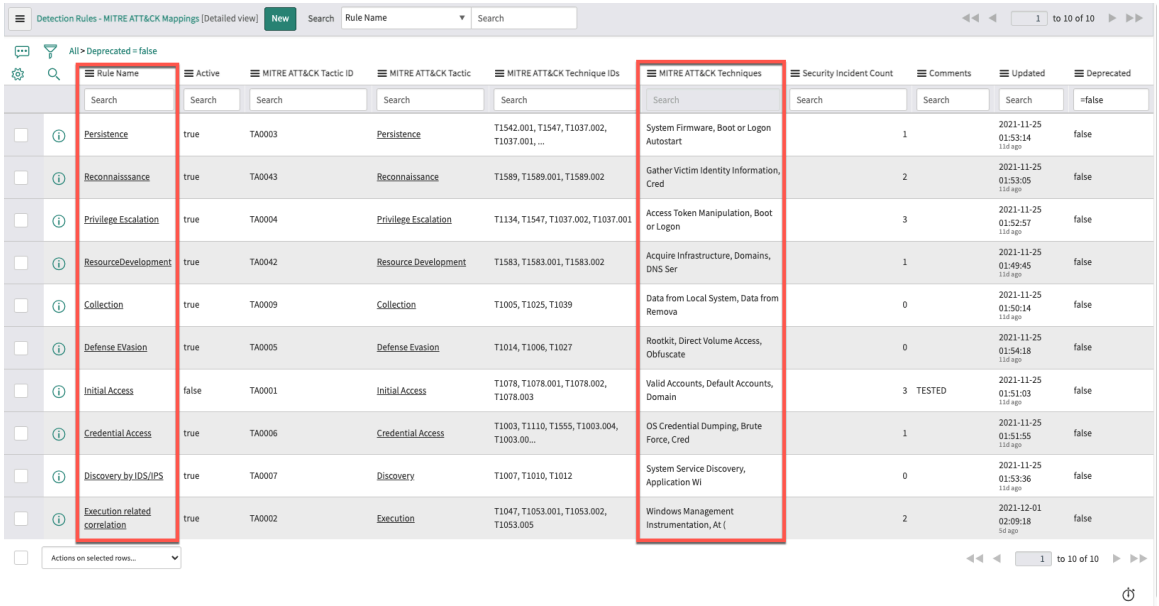
O mapeamento de regra de detecção permite que sua organização veja quais regras de detecção estão disponíveis para identificar técnicas específicas.

O objetivo principal do mapeamento é fornecer visibilidade se sua organização tiver as regras de detecção necessárias para identificar quando um alerta ou evento é acionado como resultado de um ataque de um adversário usando uma técnica específica.

Por exemplo, exiba a ilustração a seguir que mostra uma lista das regras de detecção mapeadas para várias técnicas. Você também pode exibir essas informações em o MITRE-ATT&CK navegador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você não pretende usar as regras de extração automática SIEM do sistema de base, habilite o rollup automático de MITRE-ATT&CK TTPs baseados no mapeamento de regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no Regra de alerta campo nome. Você também pode preencher Regra de alerta Campo Nome usando integração SIEM, análise de e-mail, criação manual etc. Para obter mais informações, consulte Acúmulo MITRE-ATT&CK informações das regras de detecção.

Nota:

O recurso de regras de detecção foi atualizado para incluir o mapeamento de uma única tática para várias técnicas. Anteriormente, você podia mapear uma única tática com uma única técnica. Se você estiver atualizando o. Inteligência contra ameaças plug-in da versão 12.0.4 para uma versão superior e, em seguida, revise os seguintes pontos antes de usar as regras de detecção em MITRE-ATT&CK módulo.

- Vários registros são mesclados em um único registro se os campos - nome da regra, sensor de alerta, origem, categoria, subcategoria, e. MITRE-ATT&CK táticas são comuns.
- Os registros antigos são marcados como verdadeiro na coluna descontinuado e falso na coluna ativa.
- Os novos registros mesclados estão disponíveis para uso e são marcados como falso na coluna descontinuado e verdadeiro na coluna ativa.
- Depois de verificar o upgrade e exibir que todas as regras de detecção foram migradas com sucesso, você pode excluir os registros antigos marcados como verdadeiros na coluna Descontinuado.

Procedimento

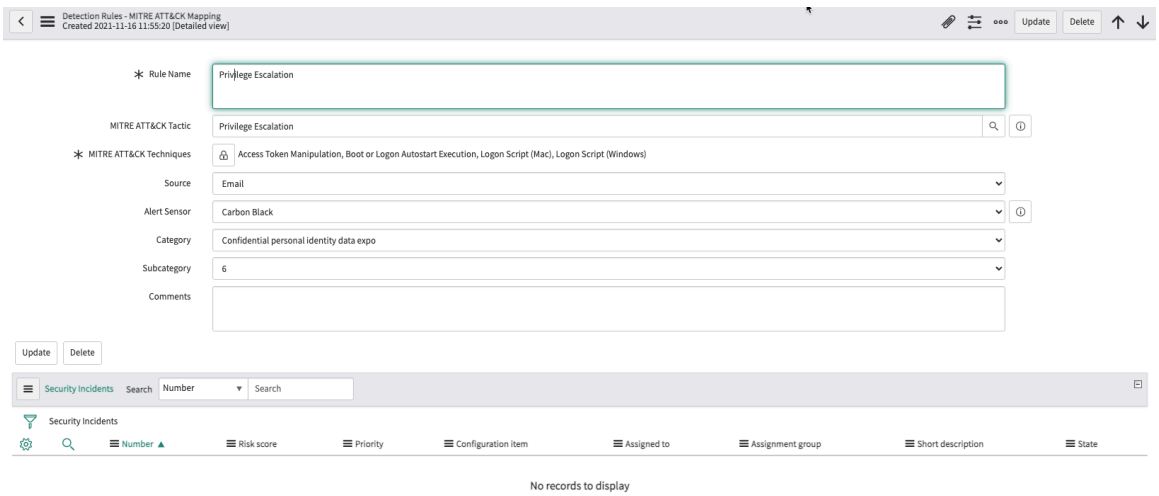
1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regras de detecção — Mapeamentos do MITRE ATT&CK**.
2. Use um dos seguintes métodos para criar sua regra de detecção:
   Método 1: Criar regras de detecção manualmente.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em **Novo** e no formulário, preencha os campos.

Regras de detecção - MITRE-ATT&CK Mapeamento

Campo	Descrição
Nome de Regra	Nome da regra de detecção.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnicas	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Origem	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Subcategoria	Subcategoria que define melhor o problema.
Categoria	Categoria que identifica o tipo de problema de segurança.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Essa contagem aparece quando você habilita o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta a incidentes de segurança.
Preterido	O mapeamento de regra de detecção foi descontinuado.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.



b. Clique em **Enviar**.

Método 2: Importar e criar regras de detecção.

a. Clique com o botão direito do mouse no cabeçalho da coluna Nome da regra.

b. Na lista, clique em **Importação** .

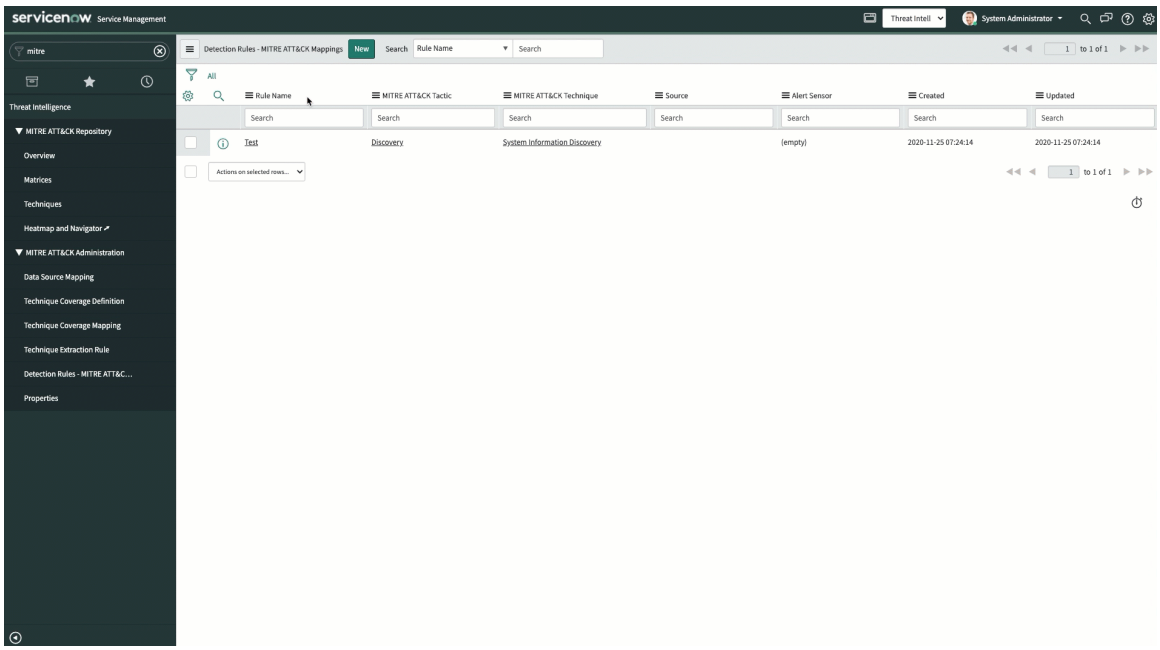
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique em **Criar modelo do Excel** .

d. Clique em **Download** após a conclusão da exportação. Um modelo do excel com o nome de arquivo sn_ti_alert_rules_miter_attack_technique_mapping é baixado para o seu computador.

Na ilustração a seguir, você verá como exportar o modelo do excel, preencher os detalhes na planilha, carregar o arquivo, visualizar os campos e importá-lo de volta para ServiceNow AI Platform.



e. Abra a planilha, selecione a segunda guia da planilha e revise o que você inseriu. No formulário, preencha os campos e salve seu arquivo.

Modelo de importação

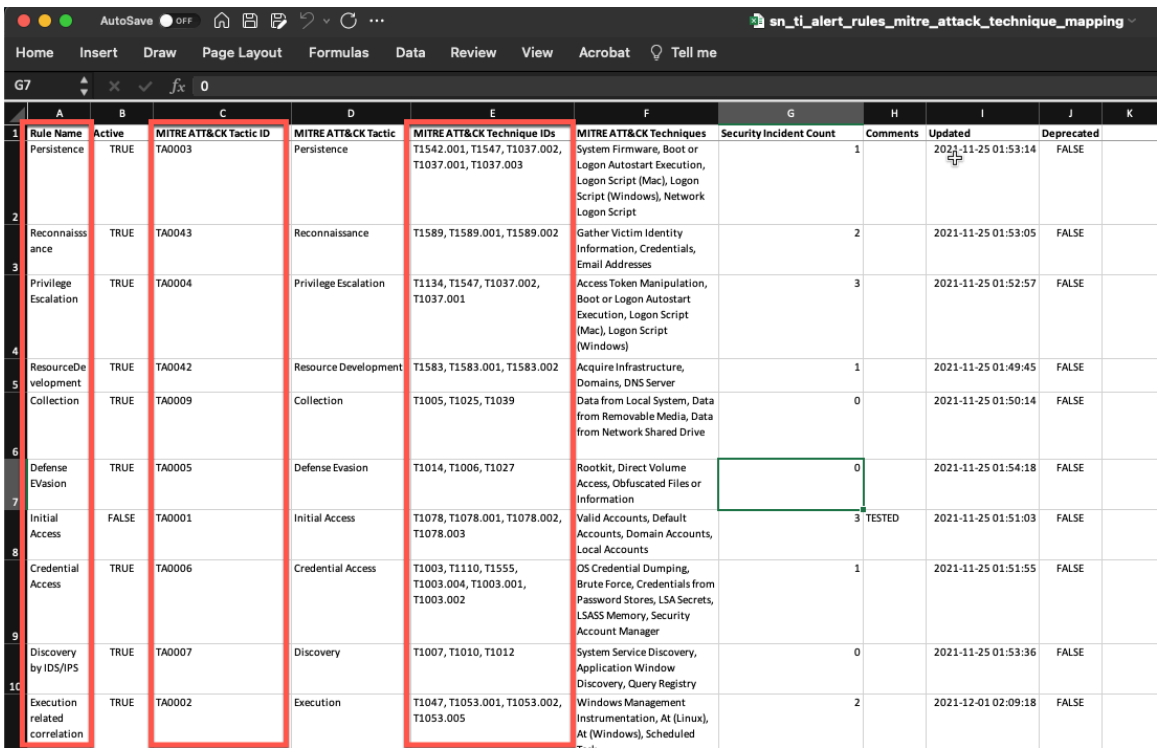
Campo	Descrição
Nome de Regra	Nome da regra de detecção.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Categoria	Categoria que identifica o tipo de problema de segurança.
Comentários	Descrição sobre a regra de detecção.
Preterido	O mapeamento de regra de detecção foi descontinuado.
MITRE-ATT&CK IDs de técnica	MITRE-ATT&CK ID da técnica, como T1546.008, para Recursos de acessibilidade.
MITRE-ATT&CK ID da tática	MITRE-ATT&CK ID da tática, como TA0003, para Persistência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Essa contagem aparece quando você habilita o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta a incidentes de segurança e a regra de detecção está ativa.
Origem	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Subcategoria	Subcategoria que define melhor o problema.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica.

A ilustração a seguir mostra o modelo de planilha. Os campos obrigatórios são realçados em vermelho - Nome da regra, MITRE-ATT&CK ID da tática, e. MITRE-ATT&CK ID da técnica.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

f. Clique em **Escolha o arquivo** e selecione a planilha no seu computador.

g. Clique em **Upload** (Carregar).

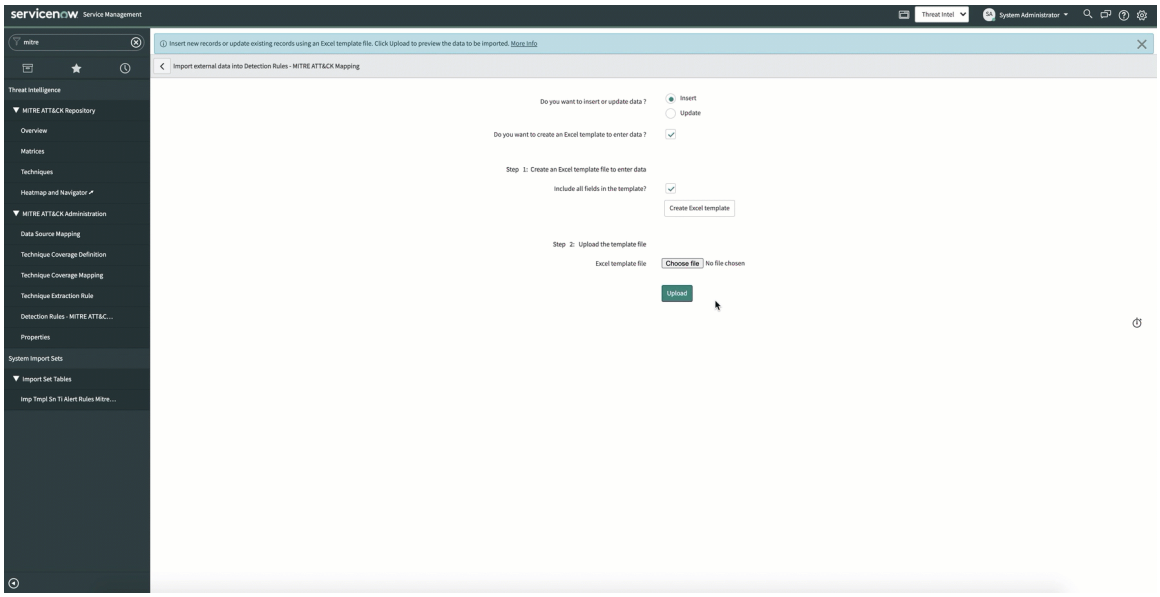
h. Clique em **Visualizar dados importados** .

i. Visualize os mapeamentos e clique em **Importação concluída** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra como carregar a planilha, visualizar os dados, revisar quaisquer erros e concluir o processo de importação de mapeamento de regra de detecção.



Extrair automaticamente regras de técnica para importação MITRE-ATT&CK informações

Use as regras de extração automática do sistema de base para importar o. MITRE-ATT&CK informações de integrações de terceiros existentes.

Use regras de extração automática de pesquisa de ameaças

Use as regras de extração automática de pesquisa de ameaças para importar o. MITRE-ATT&CK informações de qualquer existente Inteligência contra ameaças integrações de terceiros.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Quando houver Inteligência contra ameaças A integração, como Sandbox ou uma TIP, oferece suporte ao MITRE-ATT&CK e se o MITRE-ATT&CK as informações são analisadas em cada nível de integração e, em seguida, as informações são exibidas em cada registro de resultado da pesquisa de ameaças. No entanto, nem todos Inteligência contra ameaças as integrações analisam o. MITRE-ATT&CK informações. A regra de extração automática global de pesquisa de ameaças pode extrair MITRE-ATT&CK informações de todos Inteligência contra ameaças integrações.

Você pode optar por acumular o. MITRE-ATT&CK informações automaticamente dos resultados da pesquisa de ameaças para um incidente de segurança. Para acúmulo automático de resultados de pesquisa de ameaças para incidentes de segurança, habilite a propriedade do sistema . Como alternativa, você pode acumule as informações manualmente para cada pesquisa de ameaça individual.

O sistema de base Inteligência contra ameaças extrai automaticamente o. MITRE-ATT&CK informações da carga bruta de integrações de terceiros para o registro de resultado da

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pesquisa de ameaças, se for Inteligência contra ameaças a integração fornece a você MITRE-ATT&CK informações como a técnica ou tática.

. MITRE-ATT&CK as informações não estão disponíveis no campo de carga bruta do registro de pesquisa de ameaças, então você deve definir sua própria regra para extração automática da integração de terceiros.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de extração de técnica

Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de regra	Tipo de regra de extração automática. Selecione **Pesquisa de ameaças** .
Ignorar extração automática	Definir que, por padrão, é desmarcada. Esta configuração habilita a extração automática de MITRE-ATT&CK técnicas.
Mecanismo de Origem	Mecanismo de origem.
Global	Configuração do mecanismo de origem. Quando você define o mecanismo de origem como **Global** , a extração é executada em todos os resultados de integração da pesquisa de ameaças.
Descrição	Descrição da regra de extração automática.
Método de processo	Regex ou um método de script especificado para vincular as informações da técnica da carga bruta.
Extração de regex	Opção especificada para **Campo de destino** ao usar o método de extração regex. Regex é o padrão.
Extração de script	Processo selecionado ao executar um script. O script revisa o seguinte: ○ ThreatLookupResultSysId:sys_id do registro do resultado da pesquisa de ameaças ○ SourceName: Nome da origem da pesquisa de ameaças.
Extração de tática	Opção especificada para extrair informações relacionadas à tática da carga bruta. Se uma carga contiver informações específicas relacionadas a táticas e técnicas, você poderá extrair e anexar as informações ao incidente de segurança.

4. Clique em **Enviar**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use regras de extração automática DE SIEM

Use as regras de extração automática DO SIEM para importar o. MITRE-ATT&CK informações de qualquer existente Operações de segurança Integrações de terceiros DO SIEM.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

A regra de extração de técnica está disponível para todos os sistemas de base Operações de segurança Integrações DE SIEM, como integrações Splunk, IBM QRadar e ArcSight. . ServiceNow AI Platform Ingere dados de alerta ou evento dessas integrações DE SIEM e eles contêm MITRE-ATT&CK. ServiceNow AI Platform processa a carga bruta e extrai automaticamente o. MITRE-ATT&CK informações.

. ServiceNow AI Platform Contém integrações de SIEM do sistema de base, o que significa que as regras de extração de técnica já foram criadas no MITRE-ATT&CK módulo. Você deve revisar e modificar as regras conforme necessário.

Habilite a regra de extração automática DE SIEM ou a regra de alerta de cada vez.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de extração de técnica

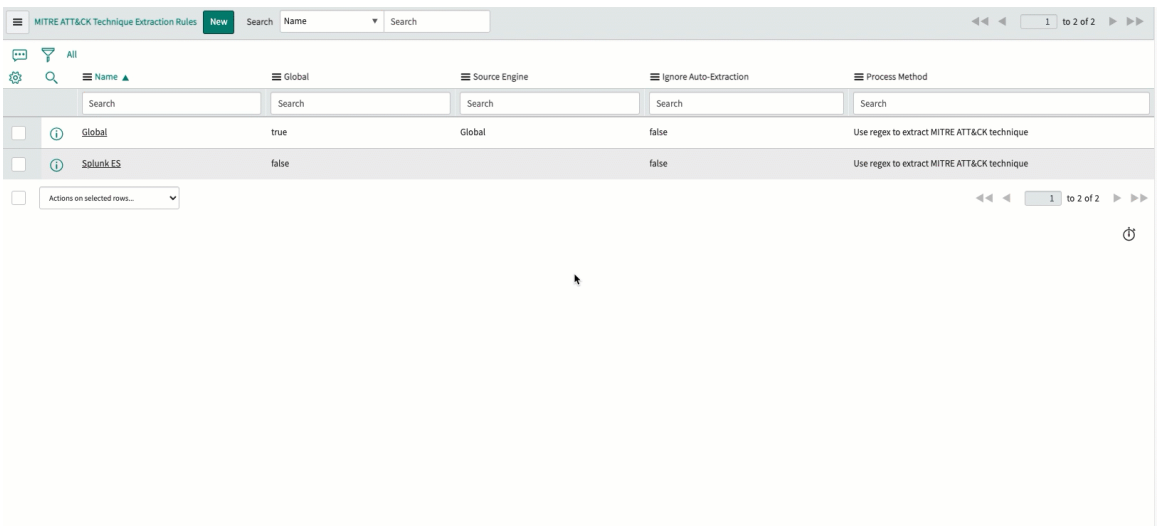
Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de regra	Tipo de regra de extração automática. Selecione **SIEM** .
Ignorar extração automática	A configuração que, por padrão, é desmarcada. Esta configuração habilita a extração automática de MITRE-ATT&CK técnicas.
Importar Tabela	Tabela de importação que é mapeada automaticamente para integrações DE SIEM do sistema de base. Revise este campo para outras integrações DE SIEM para MITRE-ATT&CK e mapa de acordo.
Importar campo	Campo de importação que é mapeado automaticamente para integrações DE SIEM do sistema de base. Revise este campo para outras integrações DE SIEM para MITRE-ATT&CK e mapa de acordo.
Descrição	Regra de extração automática.
Método de processo	Regex ou um método de script especificado para vincular as informações da técnica da carga bruta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Extração de regex	Opção especificada para **Campo de destino** ao usar o método regex. A extração de regex é o método de processo padrão.
Extração de script	Método de processo de script que você usa se quiser personalizar como MITRE-ATT&CK as informações são extraídas.
Extração de tática	Opção especificada para extrair informações relacionadas à tática da carga bruta. Se uma carga contiver informações específicas relacionadas a táticas e técnicas, você poderá extrair e anexar as informações ao incidente de segurança.

Na ilustração a seguir, você vê um exemplo do Splunk Enterprise Regra de extração da técnica SIEM na exibição do formulário. Esta regra é semelhante a todas as outras regras de extração da técnica SIEM.



4. Clique em **Enviar**.

Revise o grupo de ameaças e. MITRE-ATT&CK mapeamento de técnicas

Revise as informações de mapeamento de relacionamento objeto a objeto do grupo de ameaças e técnicas importadas do MITRE TAXII coleções. Este mapeamento permite exibir o grupo de técnicas e o mapeamento de técnica correspondente.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

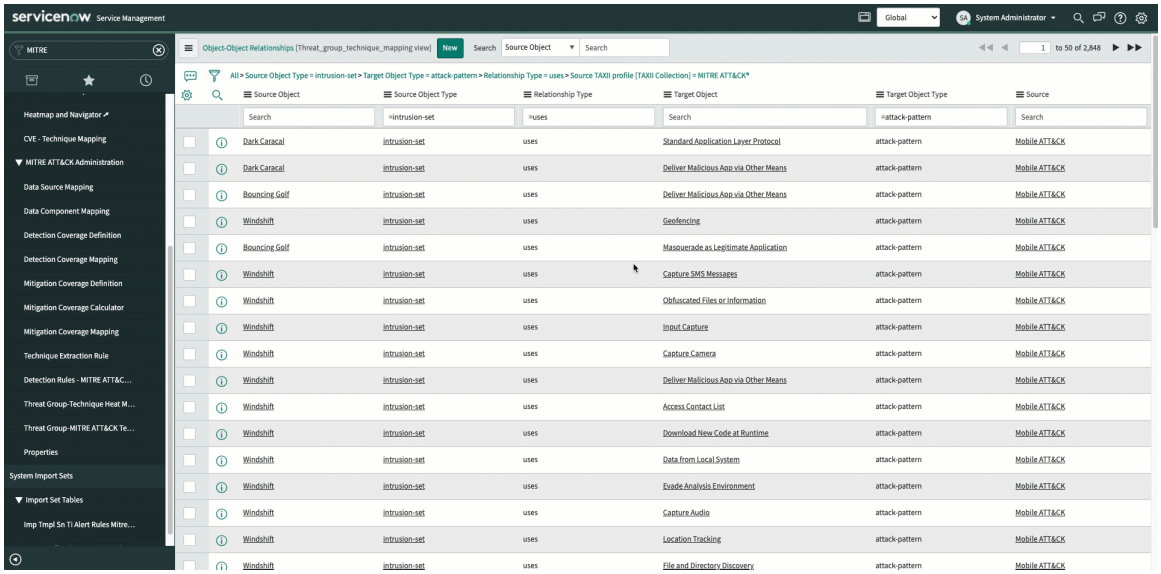
Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Grupo de ameaças - Técnicas MITRE ATT&CK**.
2. Clique com o botão direito do mouse em **Objeto de origem** e selecione **Agrupar por objeto de origem** para exibir todos os padrões de ataque associados a um grupo de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra o administrador do grupo de ameaças em 338 e os vários padrões de ataque adotados por esse grupo de ameaças que fazem parte da origem de ataque empresarial.



Grupo de ameaças para definição do mapa térmico da técnica

Defina o grupo de ameaças para a definição do mapa térmico da técnica para que você possa medir e detectar os padrões de ataque que os grupos de ameaças estão usando para atacar sua organização. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um alto número de invasores.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação
- sn_ti.read: acesso de leitura

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição do mapa térmico da técnica de grupo de ameaças**.
2. Revise o grupo de ameaças para a definição do mapa térmico da técnica e personalize as entradas para o seu ambiente.

Definições do mapa térmico da técnica de grupo de ameaças

Campo	Descrição
Número de grupos de ameaças (intervalo mínimo)	O número mínimo de grupos de ameaças que usam uma técnica específica.
Número de grupos de ameaças (intervalo máximo)	O número máximo de grupos de ameaças que usam uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um alto número de invasores.
Cor do mapa térmico	Cor atribuída à categoria do grupo de ameaças. A cor que você define é usada para realçar a categoria do grupo de ameaças no mapa de calor.

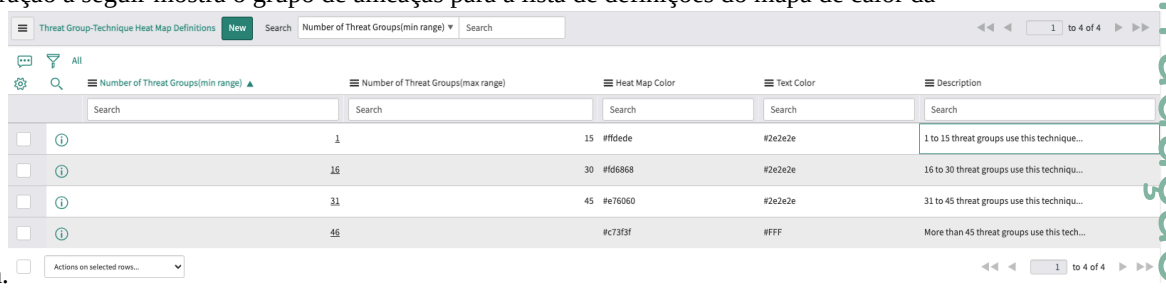
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Você pode personalizar as cores usando códigos HEXADECIMAIS e valores RGB(A).
Cor do texto	Cor atribuída ao texto do grupo de ameaças. A cor que você define é usada para realçar os grupos de ameaças no mapa de calor. Você pode personalizar as cores usando códigos HEXADECIMAIS e valores RGB(A).
Descrição	Descrição sobre o intervalo e a definição do grupo de ameaças.

Nota: Não sobreponha os intervalos de contagem do grupo de ameaças se personalizar o intervalo do grupo de ameaças (mínimo ou máximo).

A ilustração a seguir mostra o grupo de ameaças para a lista de definições do mapa de calor da técnica.



3. Para adicionar uma entrada, clique em **Novo** preencha as entradas e clique em **Enviar** .

Revise MITRE-ATT&CK propriedades do sistema

Revise MITRE-ATT&CK valores de propriedade do sistema.

Antes de Iniciar

Função necessária: sn_ti.admin, sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Propriedades**.
2. No formulário, preencha os campos.

MITRE-ATT&CK Formulário Propriedades

Campo	Descrição
Acumular informações do MITRE ATT&CK automaticamente dos observáveis para o incidente de segurança [sn_ti.rollup_miter_att&ck_technique_observable_si]	Acúmulo de MITRE-ATT&CK informações de observáveis para o incidente de segurança. Para obter mais informações, consulte Associe informações DO MITRE ATT&CK a observáveis . Valor padrão: sim

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Acumular informações do MITRE ATT&CK automaticamente dos resultados da pesquisa de ameaças para o incidente de segurança [sn_ti.rollup_miter_att&ck_technique_threat_lookup_si]	Acúmulo de MITRE-ATT&CK informações dos resultados da pesquisa de ameaças para o incidente de segurança. Para obter mais informações, consulte Extração automática da pesquisa de ameaças . Valor padrão: sim
Acumular informações do MITRE ATT&CK automaticamente das regras de alerta para incidentes de segurança [sn_ti.rollup_miter_att&ck_technique_alert_rule_si]	Acúmulo de MITRE-ATT&CK Informações de TTP automaticamente de regras de alerta a incidentes de segurança. Para obter mais informações, consulte regras de detecção de mapa . Valor padrão: não
Acumular informações do MITRE ATT&CK automaticamente dos incidentes de segurança secundários para o incidente de segurança primário [sn_ti.rollup_miter_att&ck_technique_child_si_value]	Acumular MITRE-ATT&CK informações automaticamente de incidentes de segurança secundários para o incidente de segurança primário. Valor padrão: sim
Habilitar esta propriedade permite o mapeamento de Campos de incidente de segurança, como categoria e subcategoria, com Regras de detecção na tabela "Regras de detecção - Mapeamento MITRE ATT&CK" [sn_ti.enable_category_mapping_with_alert_rule]	Categoria e subcategoria em Regras de detecção - Mapeamento MITRE ATT&CK página. Valor padrão: não
Tempo (em horas) para calcular "CVE — Contagem de VUL" [sn_ti.time_to_calculate_cve_vits_count]	O tempo programado em horas para calcular as informações de CVE e VUL. Valor padrão: 24

3. Clique em **Salvar**.

Usando MITRE-ATT&CK para detectar e analisar ameaças

Use MITRE-ATT&CK em Inteligência contra ameaças e o. SIR módulo para detectar e analisar ameaças à sua organização.

Associar MITRE-ATT&CK™ informações com incidentes de segurança

Associe o. MITRE-ATT&CK táticas e técnicas para o incidente de segurança para melhor análise de incidentes de segurança e ameaças.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Adicione MITRE-ATT&CK informações de táticas e técnicas ao incidente de segurança para que você possa correlacionar suas informações de incidente de segurança e ameaça para uma melhor análise. Por exemplo, sua organização pode estar recebendo informações relacionadas a táticas, técnicas e procedimentos (TTP) de suas fontes de terceiros, como Inteligência contra ameaças relatórios ou outras fontes fora do Resposta a incidentes de segurança. Em seguida, adicione essas informações de volta a SIR para melhor correlação e análise de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode optar por acumular o. MITRE-ATT&CK informações automaticamente dos resultados de extração automática da pesquisa de ameaças, de observáveis ou de um incidente de segurança secundário para um incidente de segurança. Para acúmulo automático de incidentes de segurança, habilite a propriedade do sistema . Como alternativa, você pode acumular as informações manualmente para cada pesquisa de ameaça individual ou observável .

Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja enriquecer com MITRE-ATT&CK informações.
3. Clique em **Associar técnica MITRE ATT&CK** link relacionado.
   O painel Associar técnica MITRE ATT&CK é exibido.

   Esta ilustração mostra como navegar até a lista relacionada e procurar Associar MITRE-ATT&CK Revise o Enterprise ATT&CK de origem, adicione um impacto de tática e adicione uma técnica Desligamento/reinicialização do sistema.

   Associe informações DO MITRE ao incidente de segurança
4. Selecione **Origem** .

   Nota: . coleções e. matrizes que foram ativados aparecem na lista de origens.

   As táticas e técnicas associadas à origem estão disponíveis para seleção. Você também pode associar várias origens.
5. Selecione **Tática** e. **Técnicas** .
6. **Opcional:** Revise as informações com base na relevância com o incidente de segurança e faça o seguinte:
   - Para remover completamente a associação, clique no ícone de lixeira. Clicar neste ícone exclui a origem e suas táticas e técnicas associadas.
   - Para remover uma tática, clique no ícone de menos ao lado da tática.
   - Para remover uma técnica, clique no ícone x ao lado da técnica.
7. Clique em **Salvar**.

Resultado

. MITRE-ATT&CK as informações estão associadas ao incidente de segurança. Agora você pode exibir as informações associadas em **MITRE ATT&CK** .

Associar MITRE-ATT&CK informações com incidentes de segurança encerrados

Agora você pode associar MITRE-ATT&CK táticas e técnicas para os incidentes de segurança encerrados para melhor análise de incidentes de segurança e ameaças.

Associe informações DO MITRE ao incidente de segurança

Usando o. MITRE-ATT&CK Cartão para ver informações relacionadas em um incidente de segurança

Você pode usar MITRE-ATT&CK para ver MITRE-ATT&CK informações relacionadas em um incidente de segurança.

Depois que as informações são acumuladas de uma pesquisa de ameaça, um observável ou uma integração DE SIEM, elas são adicionadas ao incidente de segurança. Em seguida, as informações agregadas são apresentadas em MITRE-ATT&CK Cartão. . **MITRE ATT&CK** fornece duas exibições:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exibição do navegador: Esta exibição, que é semelhante a MITRE-ATT&CK navegador, mostra todas as técnicas que foram adicionadas manualmente ou acumuladas das tabelas observáveis ou de pesquisa de ameaças. **Mostrar origem das técnicas** Exibe a origem da técnica se ela tiver sido acumulada manualmente ou por meio de uma Origem. **Mostrar ID** Exibe o ID da técnica.

  A ilustração a seguir mostra como navegar até **MITRE ATT&CK** exibição do navegador. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no Inteligência contra ameaças módulo.

  MITRE ATT&CK Card: Exibição do navegador e exibição de lista

- Exibição de lista: Esta exibição mostra os dados em um formato de lista ou tabela. Você pode ver todos os dados distribuídos em diferentes tabelas e grupos nesta exibição.

  A ilustração a seguir mostra como navegar até a exibição de lista do MITRE ATT&CK Card. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no Inteligência contra ameaças módulo.

Associar MITRE-ATT&CK informações com observáveis

Associar MITRE-ATT&CK táticas e técnicas para um observável para melhor análise de incidentes de segurança e ameaças em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Alguns SIEMs podem fornecer MITRE-ATT&CK informações com eventos, alertas ou observáveis. Para associar o. MITRE-ATT&CK informações em um nível granular, você pode adicionar as informações com um observável.

Você pode optar por acumular o. MITRE-ATT&CK informações automaticamente dos observáveis para um incidente de segurança. Para acúmulo automático de observáveis para incidentes de segurança, habilite a propriedade do sistema . Como alternativa, você pode acumular as informações manualmente para cada observável.

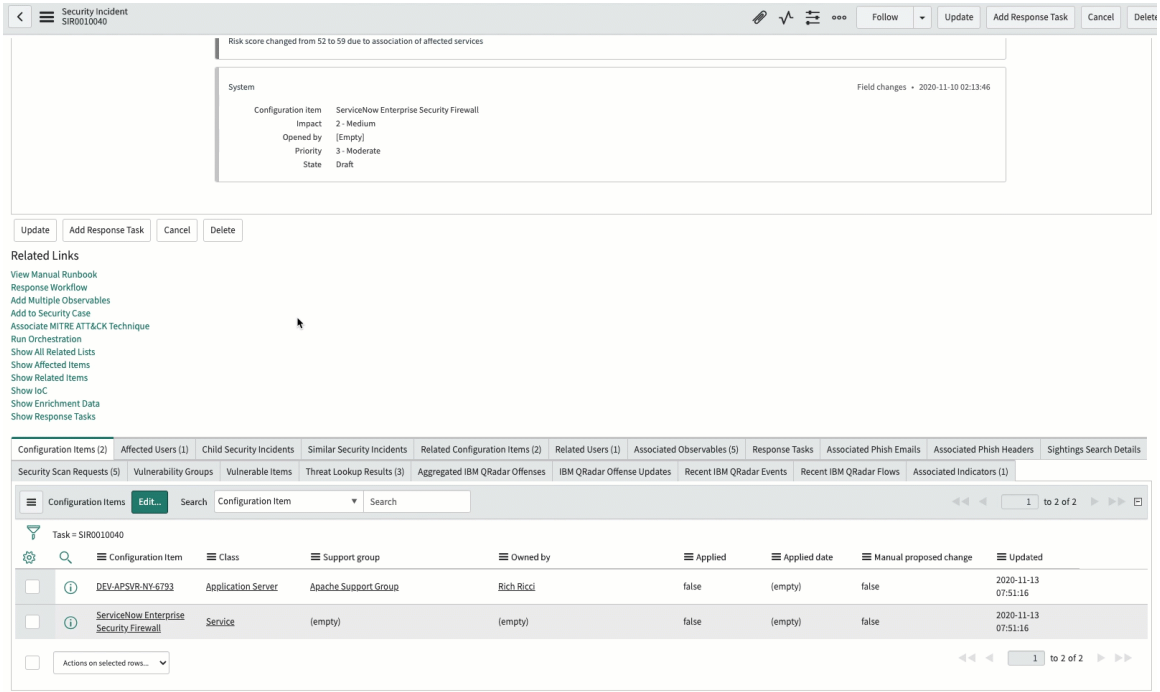
Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja enriquecer com MITRE-ATT&CK informações.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
4. Aponte para o observável que você deseja associar, clique com o botão direito do mouse e selecione **Associar técnica MITRE ATT&CK** .

   Na ilustração a seguir, você pode ver como navegar da lista relacionada para **Associar técnica MITRE ATT&CK** , revise a origem e adicione uma tática e uma técnica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Nas listas de origem, revise **Origem** .

   Nota: . coleções e. matrizes que foram ativados aparecem na lista de origens.

6. Revise **Tática** e. **Técnicas** e adicione ou remova-os com base na relevância com o observável.

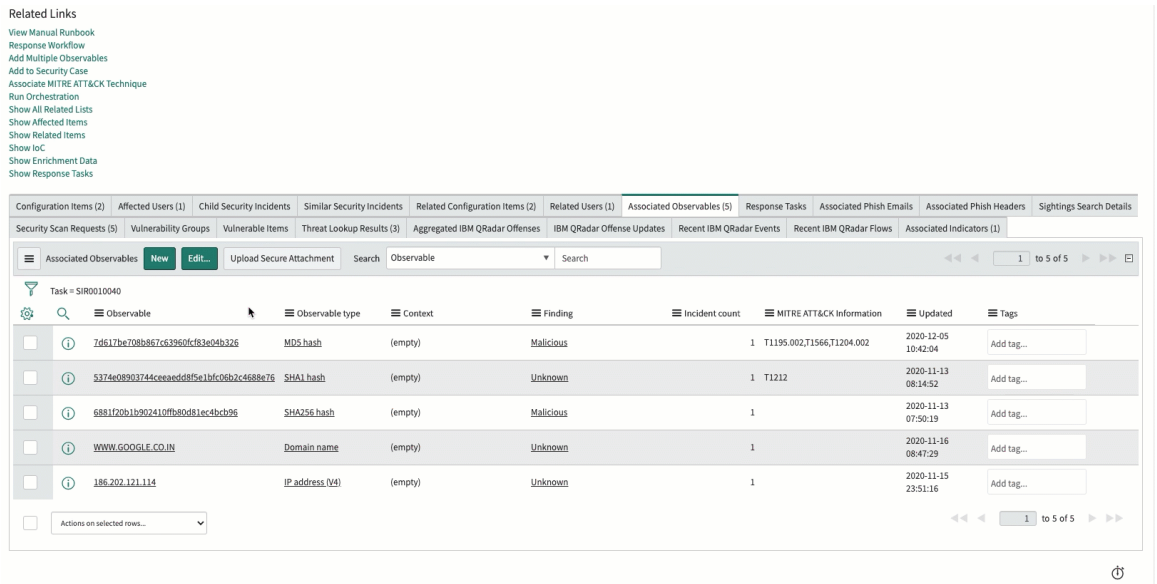
7. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem em MITRE-ATT&CK Coluna de informações na lista relacionada Observáveis.

8. Selecione o observável e, no menu Ações, clique em **Acumular informações DO MITRE ATT&CK para SI** .
   Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações de observáveis a incidentes de segurança, em seguida, as informações são acumuladas automaticamente. Se você não habilitou o rollup automático, será necessário fazer isso manualmente.

   A ilustração a seguir mostra como selecionar um observável e acumular o. MITRE-ATT&CK informações para um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Para ver uma exibição agregada das técnicas associadas aos observáveis, selecione dois ou mais observáveis na lista e, em seguida, em **Ações** na lista linhas selecionadas, clique em **Mostrar informações DO MITRE ATT&CK** .

Resultado
Uma exibição agregada das informações DO MITRE ATT&CK para os observáveis selecionados é exibida.

Associar MITRE-ATT&CK informações com caso de segurança

Associar MITRE-ATT&CK táticas e técnicas para um caso de segurança para melhor gestão de casos de segurança e análise de ameaças em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja enriquecer com as informações DO MITRE-ATT&CK.
3. Na lista relacionada, clique em **Associar técnica MITRE ATT&CK** .

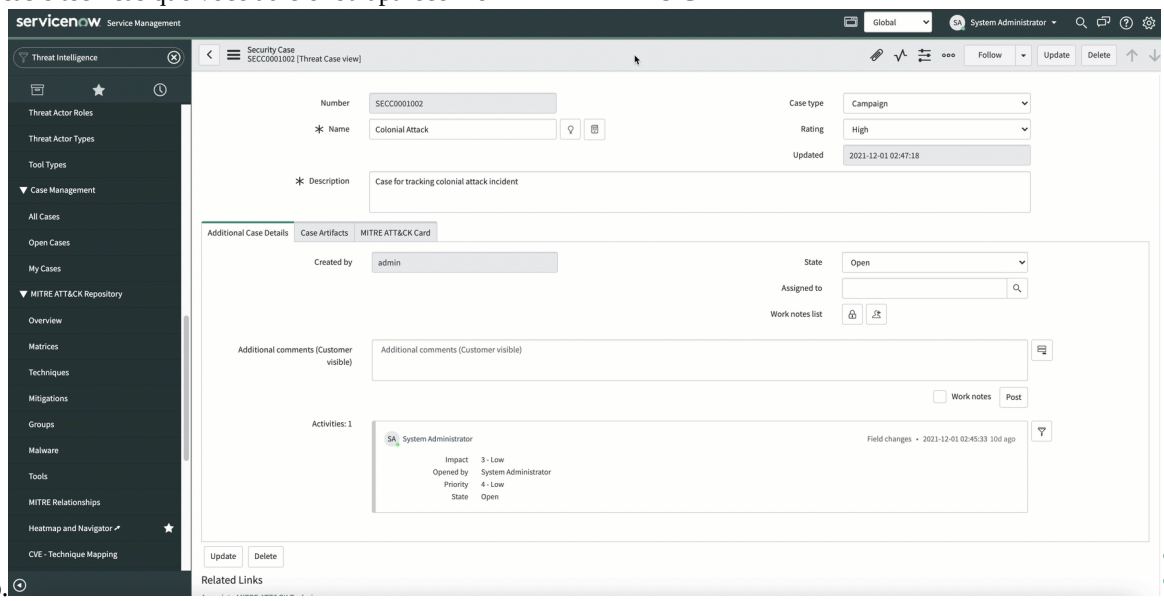
   Na ilustração a seguir, você pode ver como navegar da lista relacionada para **Associar técnica MITRE ATT&CK** , revise a origem e adicione uma tática e uma técnica.

4. Nas listas de origem, revise **Origem** .
5. Revise **Tática** e. **Técnicas** e adicione ou remova-os com base na relevância com o caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem em MITRE-ATT&CK Cartão.



Acúmulo MITRE-ATT&CK Informações que usam resultados da Pesquisa de ameaças

Se você não habilitou o rollup automático de MITRE-ATT&CK, você pode fazer isso manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

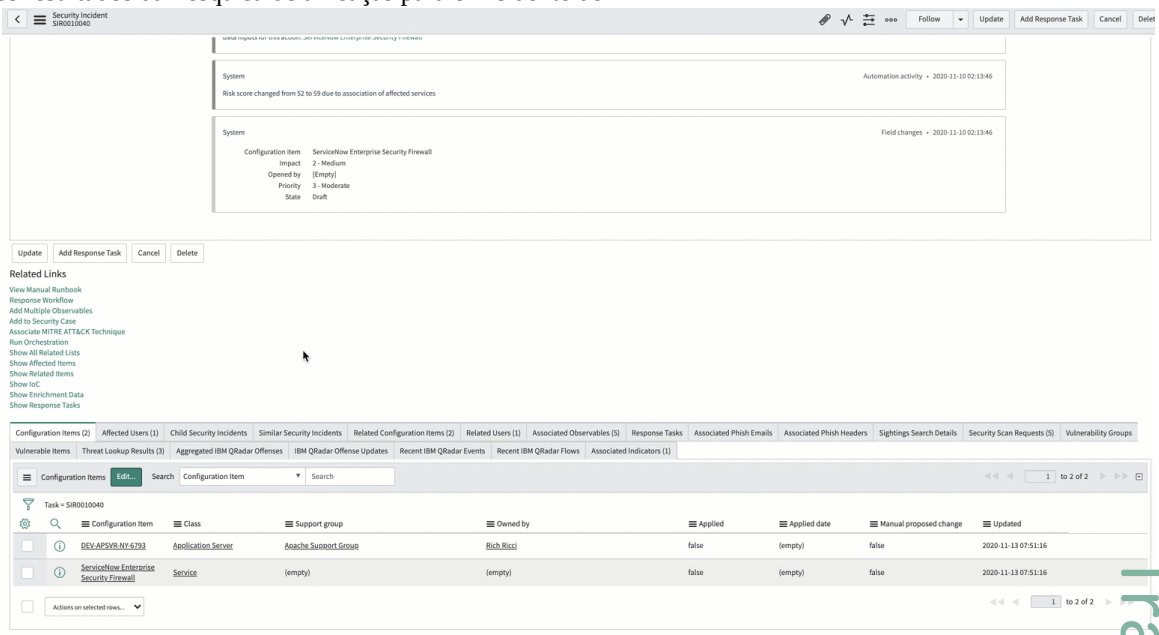
Se você tiver habilitado acúmulo automático de MITRE-ATT&CK Informações dos resultados da Pesquisa de ameaças para incidente de segurança, as informações são acumuladas automaticamente. Se você não habilitou o rollup automático, poderá fazer isso manualmente.

Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja enriquecer com MITRE-ATT&CK informações.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Resultados da pesquisa de ameaças** guia.
4. Selecione o observável e, no menu Ações, clique em **Acumular informações DO MITRE ATT&CK para SI** .
   Você pode selecionar vários observáveis e acumular as informações.
5. Clique em **Recarregar** para confirmar as mudanças.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra como selecionar um observável e acumular os resultados da Pesquisa de ameaças para o incidente de segurança.



Você pode exibir MITRE-ATT&CK Cartão para confirmar que os resultados da Pesquisa de ameaças foram acumulados para o incidente de segurança.

Acúmulo MITRE-ATT&CK informações das regras de detecção

Habilitar rollup de MITRE-ATT&CK informações das regras de detecção aos incidentes de segurança para melhor análise de incidentes de segurança e ameaças.

Antes de Iniciar

Função necessária: nenhuma

Certifique-se de ter realizado o seguinte:

- Habilite o. Acumular informações DO MITRE ATT&ACK automaticamente de regras de alerta para incidentes de segurança propriedade em Propriedades módulo. Por padrão, esta opção está desabilitada. Para obter mais informações, consulte Revise as propriedades do sistema MITRE-ATT&CK .
- Execute o mapeamento de regras de detecção para MITRE-ATT&CK TTPs em Regras de detecção - Mapeamento MITRE ATT&CK TTP módulo. O nome da regra de detecção deve corresponder ao nome da regra de alerta que aciona o incidente de segurança. Para obter mais informações, consulte Crie e mapeie regras de detecção.

Por Que e Quando Desempenhar Esta Tarefa

Se você não pretende usar as regras de extração automática SIEM do sistema de base, habilite o rollup automático de MITRE-ATT&CK TTPs baseados no mapeamento de regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no Regra de alerta campo nome. Você também pode preencher Regra de alerta Nomeie o campo usando integração SIEM, análise de e-mail, criação manual e assim por diante.

Procedimento

1. Navegar até **Administração do MITRE ATT&CK** > **Propriedades**.
2. Habilite a propriedade Rollup MITRE ATT&ACK information from alert rules to security incidents e clique em **Salvar** .
   Por padrão, esta opção está desabilitada.

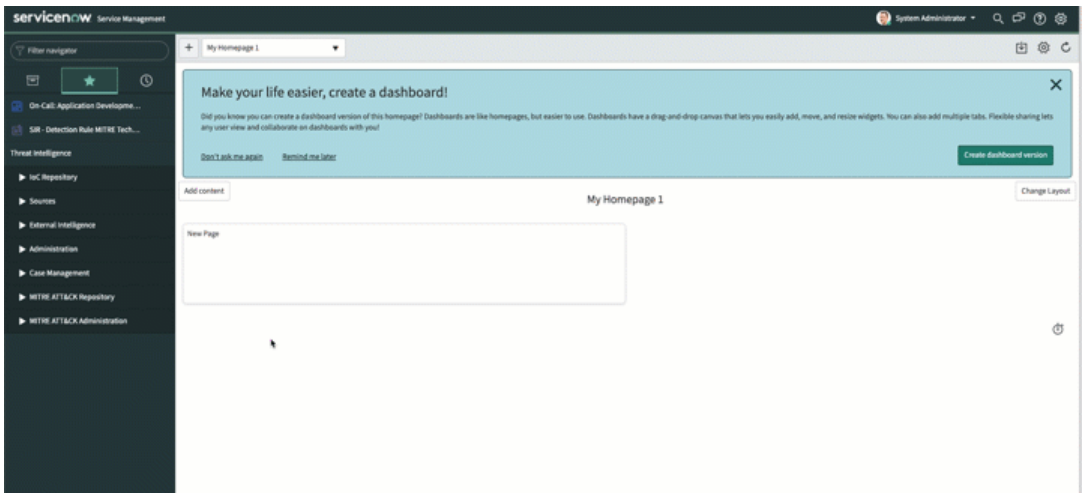
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Você precisa preencher **Regra de alerta** campo nome do incidente de segurança com as regras de alerta necessárias.

   Nota: Adicione o exato Regra de alerta nome. Para adicionar várias regras, você precisa adicionar as regras usando um separador de vírgula.

4. Clique com o botão direito do mouse no formulário e clique em **Salvar** .
   Se o valor do nome da regra de alerta no incidente de segurança corresponder a um registro no módulo Regra de detecção - Mapeamento MITRE ATT&CK TTP, as técnicas e táticas correspondentes associadas à regra de alerta serão vinculadas ao incidente de segurança automaticamente.



5. Abra o incidente de segurança e selecione **MITRE ATT&CK** e valide se as técnicas estão acumuladas.
6. Habilitar **Mostrar origem das técnicas** opção para exibir a origem das técnicas.
   A origem das técnicas deve ser Regra de detecção .

Acúmulo MITRE-ATT&CK informações de incidentes de segurança secundários

Se você não habilitou o rollup automático de MITRE-ATT&CK, você pode fazer isso manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

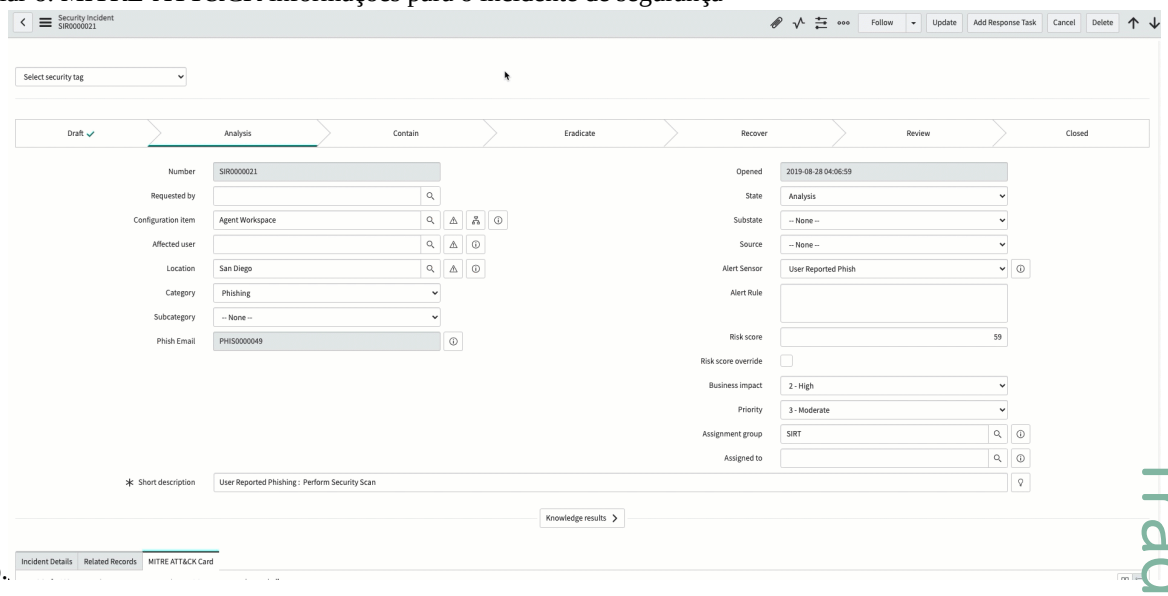
Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações de incidentes de segurança secundários, em seguida, as informações são acumuladas automaticamente. Se você não habilitou o rollup automático, poderá fazer isso manualmente.

Procedimento

1. Navegar até **Tudo** > **incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança primário que você deseja enriquecer com o secundário MITRE-ATT&CK informações.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Incidentes de segurança secundários** guia.
4. Selecione o incidente de segurança secundário e, no menu Ações, clique em **Acumular informações DO MITRE ATT&CK para SI** .
   Você pode clicar em **Mostrar informações DO MITRE ATT&CK** Para exibir as informações DO MITRE do incidente de segurança secundário antes de acumular as informações DO MITRE ATT&CK.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Recarregar** para confirmar as mudanças.
6. Clique em **MITRE ATT&CK** para exibir a origem das técnicas.
   A ilustração a seguir mostra como selecionar o incidente de segurança secundário e acumular o. MITRE-ATT&CK informações para o incidente de segurança primário.



   Você pode exibir o cartão MITRE-ATT&CK para confirmar que o incidente de segurança secundário MITRE-ATT&CK as informações foram acumuladas para o incidente de segurança primário.

Execute a análise de link e a busca de ameaças usando MITRE-ATT&CK filtros específicos

Correlacione e execute a análise de link de observáveis, incidentes de segurança e. MITRE-ATT&CK informações relacionadas para que sua organização possa começar a caçar ameaças.

Antes de Iniciar

Função necessária: sn_ti.miter_analyst, sn_si.read

Por Que e Quando Desempenhar Esta Tarefa

Depois de associar os incidentes de segurança ao MITRE-ATT&CK, você pode usar MITRE-ATT&CK filtros específicos para busca de ameaças. Use MITRE-ATT&CK filtros com o existente Resposta a incidentes de segurança filtros para correlacionar e executar análise de link.

Procedimento

1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Clique em **Atualizar lista personalizada** para adicionar MITRE colunas.
3. Selecione uma condição de filtro para que você possa exibir MITRE associações e informações relacionadas a incidentes de segurança ou observáveis:
   - MITRE-ATT&CK Grupo adversário
   - MITRE-ATT&CK Fonte de dados
   - MITRE-ATT&CK Procedimento (malware)
   - MITRE-ATT&CK Procedimento (Ferramentas)
   - MITRE-ATT&CK Tática
   - MITRE-ATT&CK Técnica

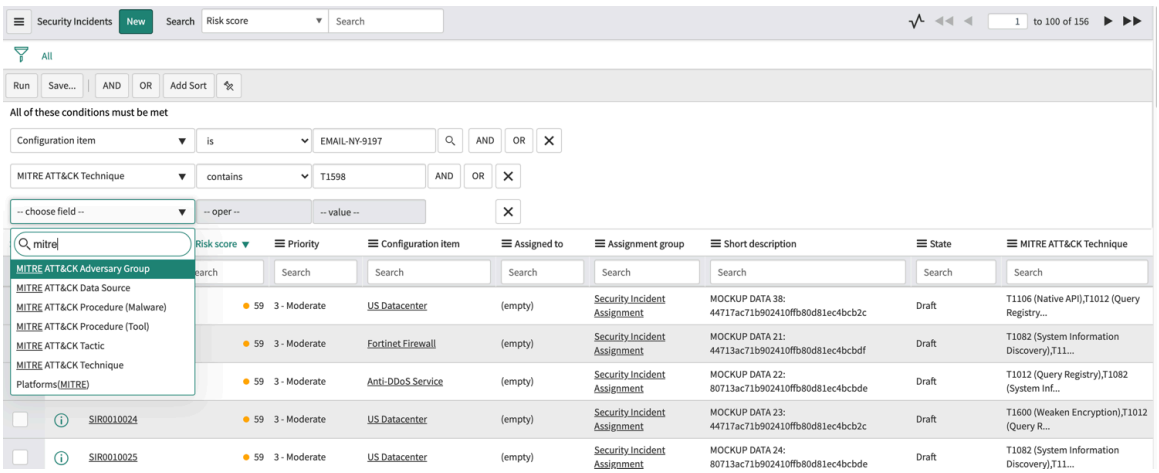
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Crie uma condição de filtro baseada nos critérios acima e clique em **Executar** para executar uma análise de link ou correlação entre incidentes de segurança, observáveis e MITRE-ATT&CK informações relacionadas.

   Nota: . MITRE-ATT&CK os dados são armazenados como uma cadeia de caracteres e você só pode usar **contém** como o operador para condições de filtro.

   Por exemplo, se você quiser revisar se um item de configuração (IC) está comprometido, selecione um IC. Em seguida, você correlaciona o IC com as técnicas que estão presentes adicionando um MITRE-ATT&CK ID da técnica. Você pode continuar a criar seus critérios de filtro para correlacionar as informações e para a busca de ameaças.



MITRE-ATT&CK mapa de calor e navegador

Você pode usar MITRE-ATT&CK mapa de calor e navegador para navegação básica e para visualizar sua cobertura geral de detecção de técnica.

Visão geral do MITRE-ATT&CK mapa de calor e navegador

Você pode usar o navegador com os filtros primários para navegação básica e observação de matrizes ATT&CK. O mapa térmico destaca o espectro da cobertura de detecção, incluindo os pontos cegos em que sua organização não tem cobertura. Isso fica disponível depois que você mapeia o. cobertura de detecção de técnica.

Com o mapa térmico e o navegador, você pode:

- Identifique com rapidez e eficiência os recursos de detecção da sua organização e destaque as lacunas na cobertura de detecção de técnica.
- Busque ameaças e execute correlação de ameaças usando recursos associados.

Acesse MITRE-ATT&CK mapa de calor e navegador

Acesse MITRE-ATT&CK Mapa de calor e navegador para que você possa visualizar a matriz que permite usar o ATT&CK.

Antes de Iniciar

Função necessária: sn_ti.read, sn_ti.miter_analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode revisar o mapa de calor, usar os filtros para correlacionar e executar a análise de link de MITRE-ATT&CK, os observáveis e os incidentes de segurança em sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mapa térmico e Navegador**.
   O mapa de calor e o navegador são abertos em uma nova guia.
2. Selecione a origem para preencher o mapa de calor.

   Nota: . coleções e. matrizes que foram ativados aparecem na lista de origens.

   Na ilustração a seguir, você vê como navegar até o mapa de calor e o navegador e como selecionar a origem, que é Enterprise ATT&CK neste exemplo.

   Navegue até e selecione a origem para preencher o mapa de calor
3. Use a caixa de pesquisa para encontrar rapidamente uma tática ou técnica específica usando seu nome ou ID.

   A ilustração a seguir mostra como pesquisar uma tática, técnica ou qualquer informação contida neles. Use a pesquisa para detalhar rapidamente uma tática ou técnica específica.
4. Clique em **Filtros** e selecione um filtro no Primário ou Avançado filtros.
5. Clique em **Aplicar** e controlam os filtros da seguinte forma:
   - Para salvar seus filtros, crie uma exibição personalizada . Você pode criar e salvar três exibições personalizadas .
   - Para remover os filtros selecionados, clique em **Restaurar filtros padrão** para carregar sua exibição salva padrão.
   - Para limpar todos os filtros e sua exibição existente, clique em **Limpar todos os filtros** .

   Nota: As exibições salvas são específicas para um usuário.
6. Clique em **Ocultar subtécnicas** para remover todas as subtécnicas da exibição de mapa térmico.
   Se uma técnica tiver subtécnicas, você poderá clicar no ícone Expandir para exibir as subtécnicas.

Usando as exibições personalizadas

Exibições personalizadas no MITRE-ATT&CK mapa de calor e navegador ajudam você a salvar e exibir seus filtros favoritos na próxima vez que você aterrar no mapa de calor.

Nota: Você pode criar e salvar três exibições personalizadas para cada MITRE-ATT&CK coleção por usuário.

Crie uma exibição

Depois de selecionar os filtros necessários em Primário ou Avançado clique nas reticências (...) No cabeçalho Filtros e selecione **Crie uma nova exibição** . Insira o nome da exibição personalizada e. **Salvar exibição** .

Exibições padrão

Clique em **Salve como exibição padrão** para carregar diretamente a exibição na próxima vez que você pousar no mapa de calor. Você pode definir uma exibição padrão para cada uma das coleções.

Nota: Se você estiver atualizando o. Inteligência contra ameaças plug-in de uma versão mais antiga, sua exibição padrão existente da versão antiga aparecerá como uma exibição personalizada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração mostra como criar uma exibição personalizada no mapa térmico

Atualizar uma exibição

Você pode fazer atualizações em uma exibição personalizada existente modificando o necessário Primário ou Avançado filtros. Selecione uma exibição personalizada, atualize os filtros conforme necessário e clique nas reticências (...) No cabeçalho Filtros e selecione **Atualizar exibição** para salvar os filtros.

Esta ilustração mostra como atualizar uma exibição personalizada.

Gerenciar exibições personalizadas

Use as caixas de seleção ao lado de cada exibição personalizada para aplicar o filtro de exibição personalizada selecionado.

Clique nas reticências (...) botão ao lado de cada nome de exibição personalizada para controlar as exibições personalizadas da seguinte forma:

- Defina uma exibição padrão.
- Remova uma exibição personalizada como exibição padrão. Isso não exclui a exibição personalizada.
- Renomeie a exibição personalizada.
- Exclua a exibição personalizada.

Esta ilustração mostra como gerenciar exibições personalizadas.

Exporte uma exibição salva

Para exportar as exibições personalizadas salvas para arquivos JSON, clique em reticências (...) No cabeçalho Filtros e selecione **Exportar exibições salvas** . Clique no ícone de download da exibição personalizada que você deseja baixar para o seu computador local.

Esta ilustração mostra como exportar exibições personalizadas.

Importe uma exibição

Você pode importar somente arquivos JSON. Para importar as exibições personalizadas, clique nas reticências (...) No cabeçalho Filtros e selecione **Importar exibição (json)** .

Revise as seguintes condições ao importar exibições:

- Você só pode importar o formato de arquivo JSON.
- Você pode importar apenas uma exibição ou arquivo por vez.
- Você não poderá importar se já tiver três exibições personalizadas em seus filtros. Exclua uma exibição personalizada e importe uma exibição.
- Não é possível importar uma exibição com um nome de exibição personalizado existente. Renomeie uma exibição antes de importar.

Esta ilustração mostra como importar uma exibição.

Navegador com filtros primários

Use os filtros primários para filtrar técnicas no MITRE-ATT&CK navegador. As informações em MITRE-ATT&CK o repositório está disponível para seleção.

Tradução automática

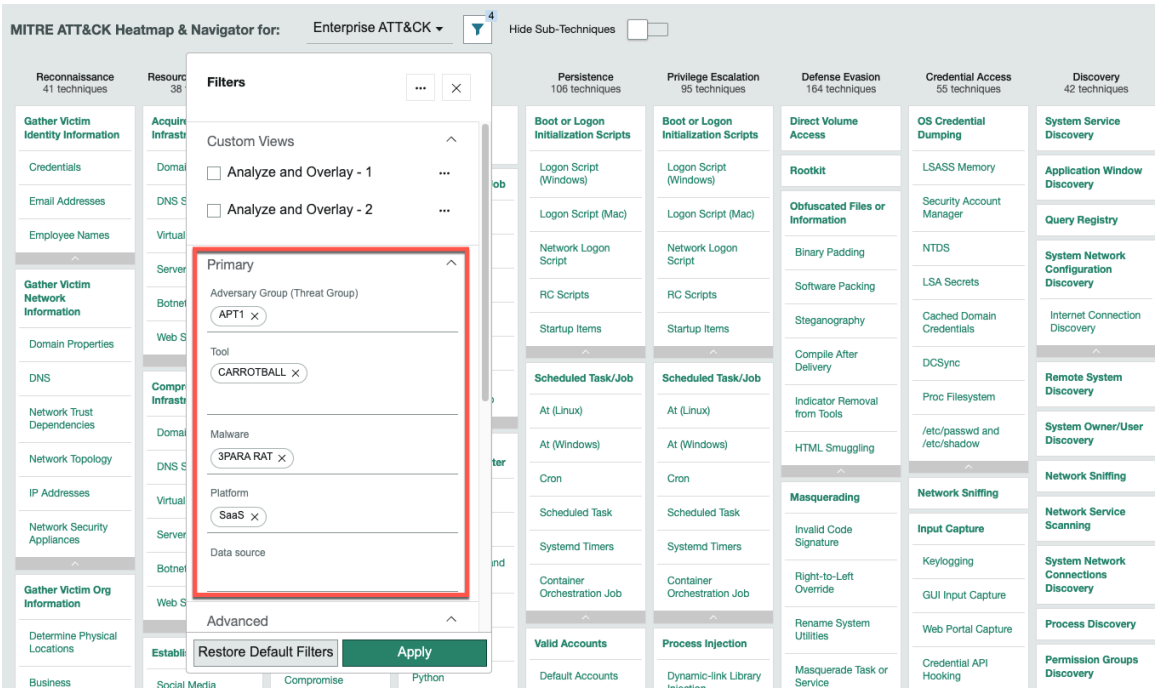
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtrar	Descrição
Grupo adversário (grupo de ameaças)	Conjuntos de atividades de invasão relacionadas que são rastreadas por um nome comum na comunidade de segurança. Grupos podem significar vários grupos de ameaças, grupos de atividades, agentes de ameaça, conjuntos de invasão e campanhas. Você pode adicionar vários grupos ao **Grupo adversário (grupo de ameaças)** filtro. Por exemplo, você adiciona APT1 e AT12, pois ambos são grupos de ameaças atribuídos à China. Ambos os grupos podem ter como alvo fontes diferentes, mas eles podem usar técnicas semelhantes.
Ferramenta	Software legítimo que é usado por agentes de ameaça para executar ataques. Você pode entender como os agentes de ameaça executam campanhas se souber como e quais ferramentas são usadas pelos agentes de ameaça. As ferramentas incluem software que não é encontrado em um sistema empresarial e software que está disponível como parte de um sistema operacional que já está presente em um ambiente como os utilitários do Microsoft Windows. Por exemplo, gsecdump é um dumper de credenciais publicamente disponível que o grupo adversário do APTI1 usa para obter hashes de senha e segredos LSA (autoridade de segurança local) dos sistemas operacionais Microsoft Windows.
Malware	Software comercial, personalizado de código fechado ou de código aberto que se destina a ser usado para fins mal-intencionados por adversários. Os exemplos são PlugX, CHOPSTICK e assim por diante
Plataforma	Táticas e técnicas que representam MITRE-ATT&CK em uma plataforma específica. Por exemplo, MITRE-ATT&CK Oferece suporte a essas plataformas na matriz Enterprise ATT&CK: Microsoft Windows, macOS, Linux, PRE, AWS, Azure, Azure, Azure AD, Office 365, SaaS, rede.
Fonte de dados	Fontes de dados que você está coletando em seu ambiente e usando para detectar MITRE-ATT&CK técnicas. Os exemplos são monitoramento de DLL e extensões do navegador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra todos os filtros primários disponíveis no MITRE-ATT&CK navegador.



Usando um mapa de calor com recursos primários e avançados

Você pode usar um mapa de calor com filtros avançados para executar uma análise correlacionando incidentes de segurança com MITRE-ATT&CK informações.

Exibir IDs de técnica

Você pode exibir MITRE-ATT&CK IDs de técnica com os nomes das técnicas quando você seleciona **IDs de técnica de exibição** filtro.

Exiba IDs de técnica em um mapa térmico

Exibir técnicas relevantes por prioridade

Para filtrar as técnicas com base em sua prioridade relevante no navegador, selecione **Filtrar por prioridade relevante da técnica** filtre e selecione **Prioridade relevante** no menu. Você pode atribuir várias prioridades para filtragem. Você também pode apontar para as técnicas no mapa térmico para saber a prioridade da técnica.

As informações de prioridade relevantes são baseadas na priorização que você definiu em Técnicas campo de prioridade relevante.

Esta ilustração mostra a filtragem por prioridade relevante.

Exibir cobertura de detecção de técnica

Para exibir a cobertura geral de detecção de técnica no mapa de calor, selecione **Exibir cobertura de detecção de técnica** filtro. O mapa de calor destaca o espetro visual da cobertura de detecção, incluindo os pontos cegos onde você não tem cobertura. A definição de pontuação do sistema de base e as cores foram definidas em cobertura de detecção de técnica . As informações foram extraídas automaticamente da cobertura geral de detecção da técnica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, as áreas do mapa térmico marcadas em vermelho indicam falta de detecção. As áreas marcadas em azul indicam a presença de recursos de detecção completos. As áreas marcadas em laranja, amarelo e azul claro refletem as capacidades de detecção parcial.

- A visualização de cores é baseada em definição da técnica e codificação por cores que você define.
- A visualização de cobertura é baseada em mapeamento de cobertura de detecção de técnica que você define.
- Se você modificar a definição de cobertura do sistema de base, os ícones de Tipo de cobertura não serão exibidos com as técnicas no mapa de calor.

Nota: O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que as cores de cobertura e cobertura de detecção de técnica definidas pelo sistema de base.

Nesta ilustração, você vê a cobertura de detecção de técnica para todas as técnicas e subtécnicas e o tipo de cobertura com suas cores e ícones.

Cobertura de detecção da técnica de mapa de calor

Exibir cobertura de mitigação de técnica

Para exibir a cobertura geral de mitigação da técnica no mapa de calor, selecione o filtro Exibir cobertura de mitigação da técnica. O mapa de calor destaca o espectro visual da cobertura de mitigação, incluindo áreas nas quais você não tem cobertura. A cobertura de mitigação, as cores e os intervalos de porcentagem foram definidos em Definição de cobertura de mitigação . As informações são extraídas do Cobertura geral de mitigação de técnica .

Por exemplo, as técnicas realçadas em vermelho indicam que não há cobertura de mitigação, laranja indica cobertura de mitigação ruim e azul indica cobertura de mitigação excelente.

- A visualização de cores é baseada em definição de mitigação de técnica e codificação por cores que você define.
- A visualização de cobertura é baseada em mapeamento de cobertura de mitigação de técnica que você define.
- Se você modificar a definição de cobertura de mitigação do sistema de base, os ícones de Tipo de cobertura de mitigação não serão exibidos com as técnicas no mapa de calor.

Nota: O mapa de calor funciona conforme o esperado quando você modifica os mesmos campos da cobertura de mitigação da técnica definida pelo sistema de base e as cores de cobertura.

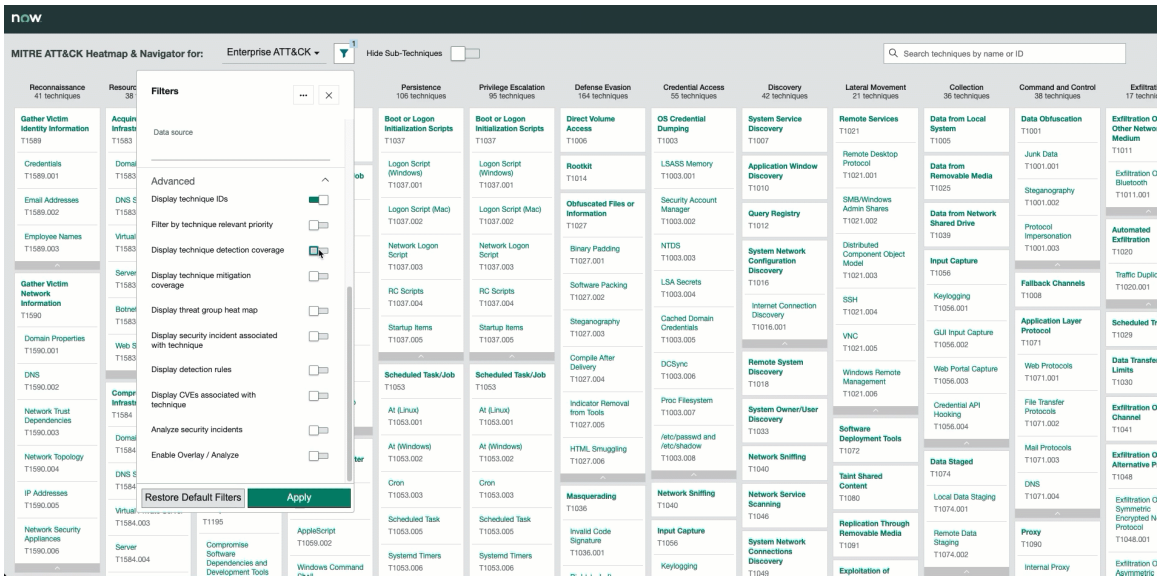
Esta ilustração mostra o mapa térmico da cobertura de mitigação da técnica

Exiba a cobertura de detecção e mitigação

Você pode usar os filtros de detecção de técnica e cobertura de mitigação de técnica juntos para obter uma visão sobre a relevância da detecção de técnica e mitigar a cobertura para sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Esta ilustração mostra como usar o filtro de detecção e mitigação juntos.

Exibir grupo de ameaças

Para exibir as informações do grupo de ameaças para a técnica no mapa de calor, selecione **Exibir mapa térmico do grupo de ameaças** . Você pode medir o número de grupos de ameaças que estão usando uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um alto número de invasores. Os intervalos do grupo de ameaças e as cores do mapa de calor foram definidos em Definição do mapa térmico da técnica de grupo de ameaças .

- A visualização de cores do mapa térmico e do texto é baseada em grupo de ameaças para definição do mapa térmico da técnica .
- A visualização do intervalo do grupo de ameaças é baseada em mapeamento de grupo de ameaças para técnica .
- Não é possível usar **Exibir mapa térmico do grupo de ameaças** filtre quando a cobertura de detecção de técnica ou a cobertura de mitigação de técnica estiverem habilitadas. Esta ilustração mostra as informações do grupo de ameaças no mapa de calor.

Exibir incidentes de segurança associados à técnica

Para exibir as técnicas que são frequentemente exploradas em sua organização e que resultaram em incidentes de segurança, clique em **Exiba o incidente de segurança associado à técnica** . Você pode exibir mais informações sobre cada um dos incidentes de segurança associados ao clicar no link que abre em uma nova janela para análise. Incidentes de segurança associados a uma técnica.

- Prioridade: Selecione **Prioridade do incidente de segurança** para filtrar pela prioridade do incidente de segurança.
- Intervalo de datas: Selecione **Intervalo de datas do incidente de segurança** para filtrar problemas de segurança por intervalo de datas.
- Falsos positivos: Selecione **Filtrar incidente de segurança falso-positivos** para remover problemas falso-positivos. Selecionar este filtro reduz o número de incidentes de segurança que você vê no mapa de calor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você usa este filtro com **Exibir cobertura de detecção de técnica** ele fornece informações sobre a relevância da cobertura de detecção de técnica para sua organização até a data selecionada.

Por exemplo, ao ativar ambos os filtros, você pode ver que, na tática de evasão de defesa, a técnica de mascaramento não tem cobertura. Se você procurar mais, a técnica de mascaramento está relacionada à Tarefa ou Serviço de mascaramento, que também tem um incidente de segurança associado a ela. Isso mostra que há uma lacuna na cobertura de detecção de técnica para a técnica de mascaramento e você pode querer revisar a cobertura geral de detecção de técnica.

Exibir regras de detecção

Para exibir se você tem as regras de detecção definidas para uma técnica específica, clique em **Regras de detecção de exibição** . Você também pode ver cada regra de detecção associada com sua definição.

Essas informações são baseadas em mapeamento de regras de detecção que você definiu. Exibir regras de detecção associadas.

Exibir CVEs associados à técnica

Para exibir as informações CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) associadas a cada uma das técnicas, clique em **Exibir CVEs associados à técnica** . As informações da técnica CVE TO são baseadas nas informações disponíveis em CVE - Módulo de mapeamento de técnica . Isso fornece informações sobre vulnerabilidades conhecidas e permite que você saiba se os adversários podem explorar sua organização.

Importante: O mapa de calor foi aprimorado para exibir somente os CVEs relevantes associados aos Vits

Para exibir Vits associados a CVEs e técnicas, selecione **Exiba Vits associados a CVE e técnicas** . Para filtrar ainda mais técnicas sem Vits, selecione **Ocultar técnicas sem Vits** . As informações de CVE e VIT exibidas são obtidas do Resposta a vulnerabilidades produto em seu ambiente. Você pode exibir a lista filtrada de CVEs e Vits no mapa de calor e navegar até cada CVE ou VIT para cada técnica do mapa de calor.

Nota:

- . **Exibir CVEs associados à técnica** está disponível somente quando Resposta a vulnerabilidades o produto está instalado em seu ambiente.
- As informações de VIT e CVE são calculadas com base no trabalho agendado definido no MITRE-ATT&CK propriedades. O trabalho de programação do sistema de base está definido para 24 horas.

Quando você usa este filtro com **Exiba o incidente de segurança associado à técnica** , você pode saber se as vulnerabilidades conhecidas causaram incidentes de segurança em sua organização.

Você pode exibir mais informações sobre cada CVE para analisar se o CVE é relevante para sua organização. Para fazer isso, exiba os itens de vulnerabilidade. Se itens de vulnerabilidade forem criados, você poderá exibir mais informações sobre quaisquer informações de IC associadas em Resposta a vulnerabilidades módulo. Você também pode revisar a gravidade e a prioridade para tomar decisões informadas. Revise os CVEs para tomar decisões informadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Analisar incidentes de segurança

Para analisar incidentes de segurança e revisar as técnicas usadas por um adversário para um ataque, clique em **Analisar incidentes de segurança** . Você pode adicionar vários incidentes de segurança para análise usando cadeias de caracteres separadas por vírgulas.

Este filtro ajuda você a analisar um incidente de segurança. Você pode saber por que o incidente ocorreu, quais técnicas foram exploradas, se algum agente de ameaça conhecido estava envolvido, se os agentes de ameaça usaram uma sequência específica para um ataque e assim por diante. Como você pode analisar vários incidentes de segurança ao mesmo tempo, você pode correlacionar as informações para ver se eles estão relacionados ou se são um incidente isolado. Se os incidentes de segurança estiverem relacionados e você observar um padrão, poderá revisar o andamento deles na cadeia de destruição para interromper o ataque ou formar uma estratégia de defesa para sua organização.

Quando você usa o. **Analisar incidentes de segurança** filtro com filtros primários, como um **Grupo adversário** , você pode correlacionar se adversários conhecidos estiverem envolvidos. Por exemplo, quando vários incidentes de segurança estão sendo analisados, as técnicas associadas aos incidentes de segurança estão presentes na forma de uma cadeia de destruição. Ao sobrepor as informações com o adversário, você notará uma sobreposição entre as técnicas associadas ao incidente de segurança e as técnicas associadas ao adversário. Somente as informações de técnica sobrepostas serão mostradas se ambos os filtros estiverem habilitados.

Analisar incidentes de segurança

Uso de sobreposição para analisar incidentes de segurança e grupos adversários

Use **Habilitar Sobreposição/Análise** filtre para exibir o comportamento do adversário e analisar um ou mais incidentes de segurança e correlacionar as informações para ver se um ataque é um incidente isolado ou um ataque coordenado por um adversário conhecido.

Por exemplo, agora você pode exibir os incidentes de segurança e o comportamento da cadeia de destruição do adversário da ameaça na mesma exibição. Esta exibição fornece informações de sobreposição que informam sobre o ataque e o comportamento do adversário conhecido. Isso permite que você analise se este é um ataque isolado ou coordenado por um adversário conhecido.

Habilitar o filtro de análise de sobreposição ignora todos os filtros primários, exceto **Grupo adversário** e ignora o filtro avançado **Filtrar por prioridade relevante da técnica** ao gerar uma exibição.

Depois de habilitar o filtro de análise de sobreposição, use a paleta de cores para atribuir cores para o seguinte:

- Analisar incidente de segurança
- Grupo adversário
- Sobreposição

A ilustração a seguir mostra que o grupo adversário APT18 está espalhado por várias técnicas e táticas na cadeia de destruição. A análise também mostra que há três técnicas que sobrepõem o grupo adversário e os incidentes de segurança que você está rastreando.
Esta ilustração mostra as informações de sobreposição de incidente de segurança e adversário.

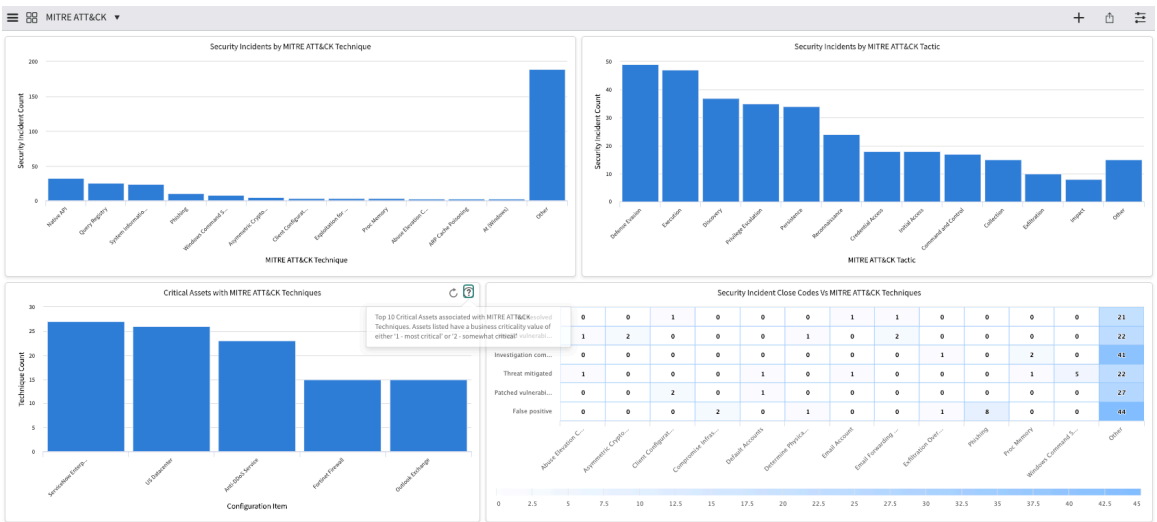
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o. MITRE-ATT&CK painel

. MITRE-ATT&CK o painel fornece uma exibição executiva da cobertura, das táticas e das técnicas da fonte de dados que são usadas em sua organização.

. MITRE-ATT&CK O módulo Visão geral é exibido MITRE-ATT&CK informações sobre incidentes de segurança, incluindo tendências e relatórios. Você pode clicar em qualquer parte de um widget (barra, ponto de dados, tabela e assim por diante) para exibir dados específicos dessa parte.



Use MITRE-ATT&CK painel para ver seus dados relacionados à segurança

Use MITRE-ATT&CK para obter uma visão geral da cobertura, táticas e técnicas da fonte de dados que são usadas em sua organização.

Antes de Iniciar

Função necessária: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Visão geral**.
2. Clique em qualquer um dos widgets a seguir para ver detalhes adicionais:
   - Incidentes de segurança por MITRE-ATT&CK Técnica
   - Incidentes de segurança por MITRE-ATT&CK Tática
   - Ativos críticos com MITRE-ATT&CK Técnicas
   - Códigos de fechamento de incidente de segurança versus MITRE-ATT&CK Técnicas
   - Técnicas MITRE-ATT&CK por cobertura de detecção
   - Técnicas MITRE-ATT&CK por cobertura de mitigação
   - Grupos de ameaças por técnica MITRE-ATT&CK
   - CVEs por técnica MITRE-ATT&CK

Widgets do MITRE-ATT&CK

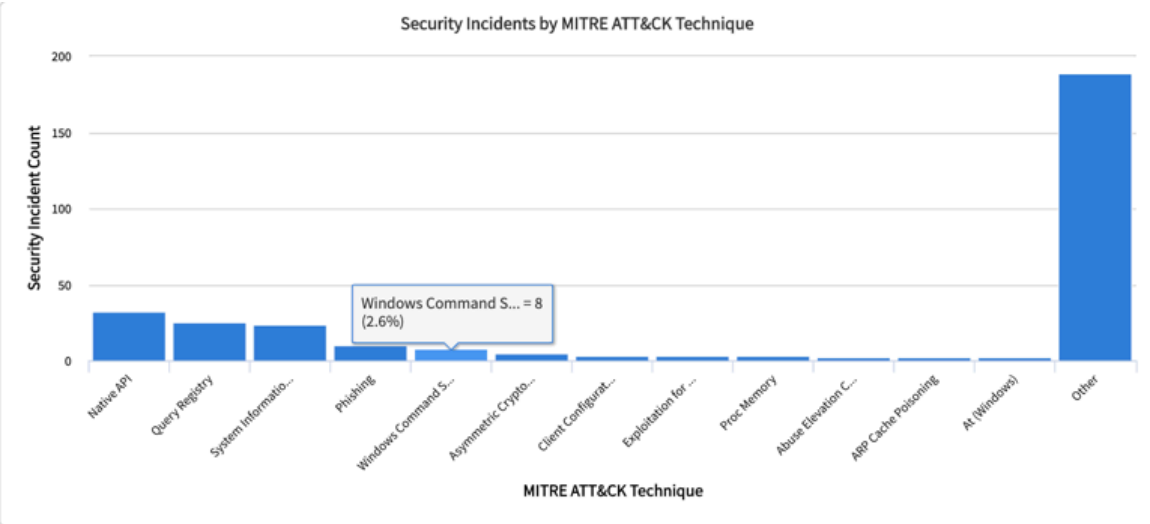
. MITRE-ATT&CK O módulo Visão geral consiste em widgets que permitem correlacionar o. MITRE-ATT&CK informações com as informações do incidente de segurança em seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

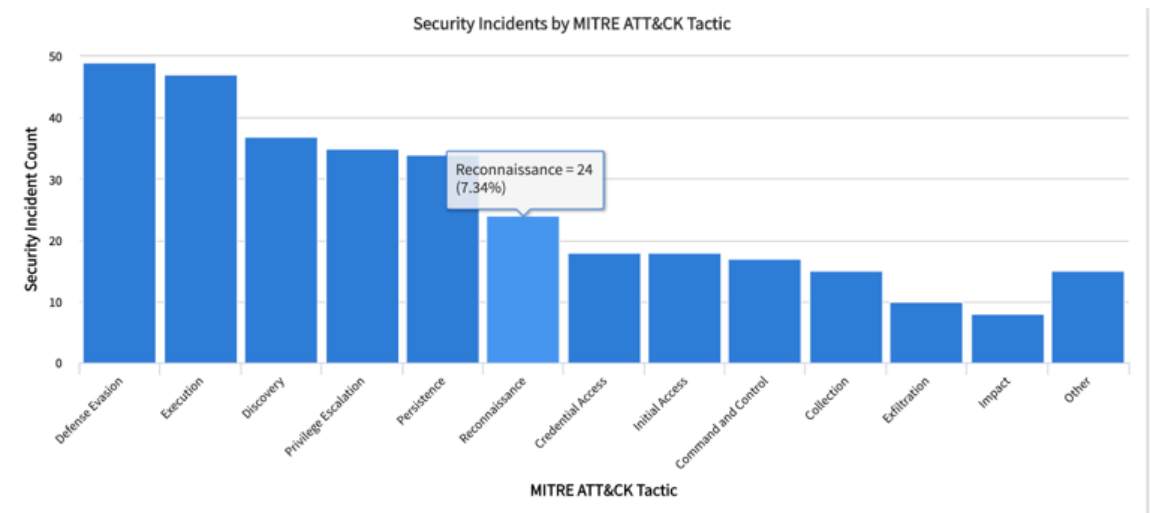
Exemplo de incidentes de segurança por MITRE-ATT&CK Técnica

Neste exemplo, **Incidentes de segurança pela técnica MITRE ATT&CK** o widget exibe as técnicas por incidente de segurança no ambiente de uma organização nos últimos 90 dias.



Exemplo de incidentes de segurança por MITRE-ATT&CK Tática

Neste exemplo, **Incidentes de segurança pela tática MITRE ATT&CK** o widget exibe as principais táticas por incidente de segurança no ambiente de uma organização nos últimos 90 dias.



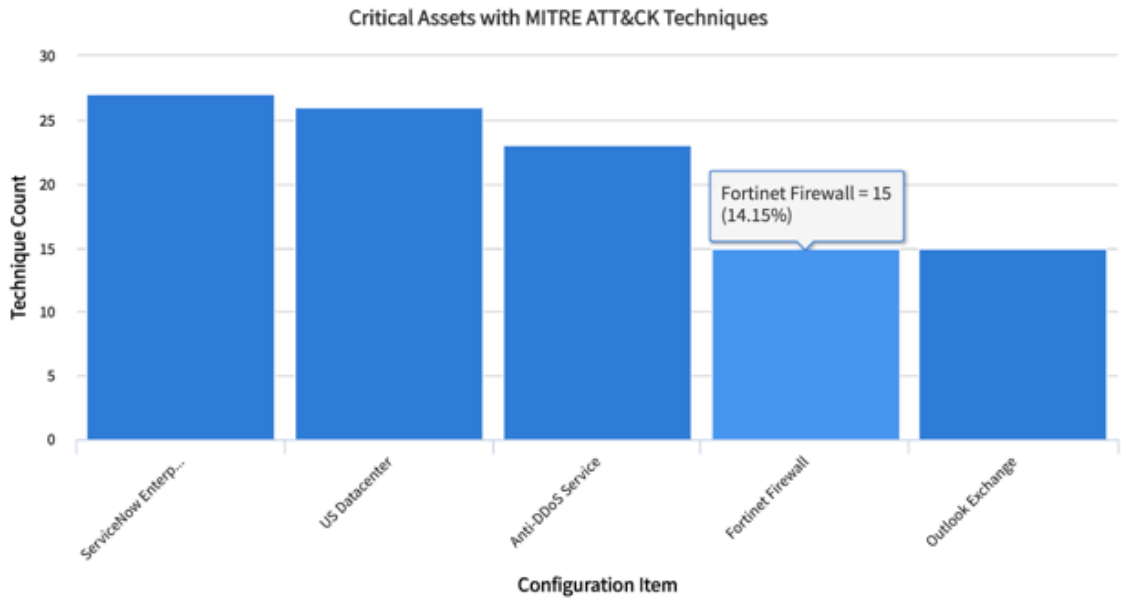
Exemplo de ativos críticos com MITRE-ATT&CK Técnicas

Neste exemplo, **Ativos críticos com técnicas MITRE ATT&CK** o widget exibe os 10 principais ativos críticos associados ao MITRE-ATT&CK técnicas. Os ativos têm uma criticidade comercial de 1 (mais crítica) ou 2 (um pouco crítica).

Este relatório permite que uma organização veja os tipos e o número de técnicas usadas na realização de ataques contra os ativos críticos.

Tradução automática

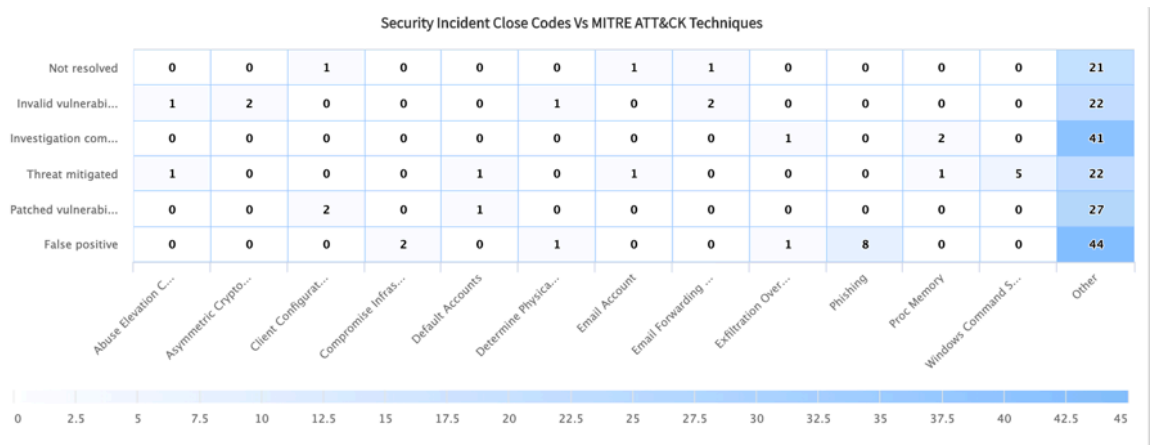
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de códigos de fechamento de incidentes de segurança versus MITRE-ATT&CK Técnicas

Neste exemplo, **Códigos de fechamento de incidente de segurança versus** *MITRE-ATT&CK* **Técnicas** o widget exibe os códigos de fechamento de incidentes de segurança que foram mapeados em relação às principais técnicas identificadas no ambiente de uma organização.

O eixo x exibe as principais técnicas que foram usadas para realizar ataques contra a empresa, e o eixo y exibe os códigos encerrados.



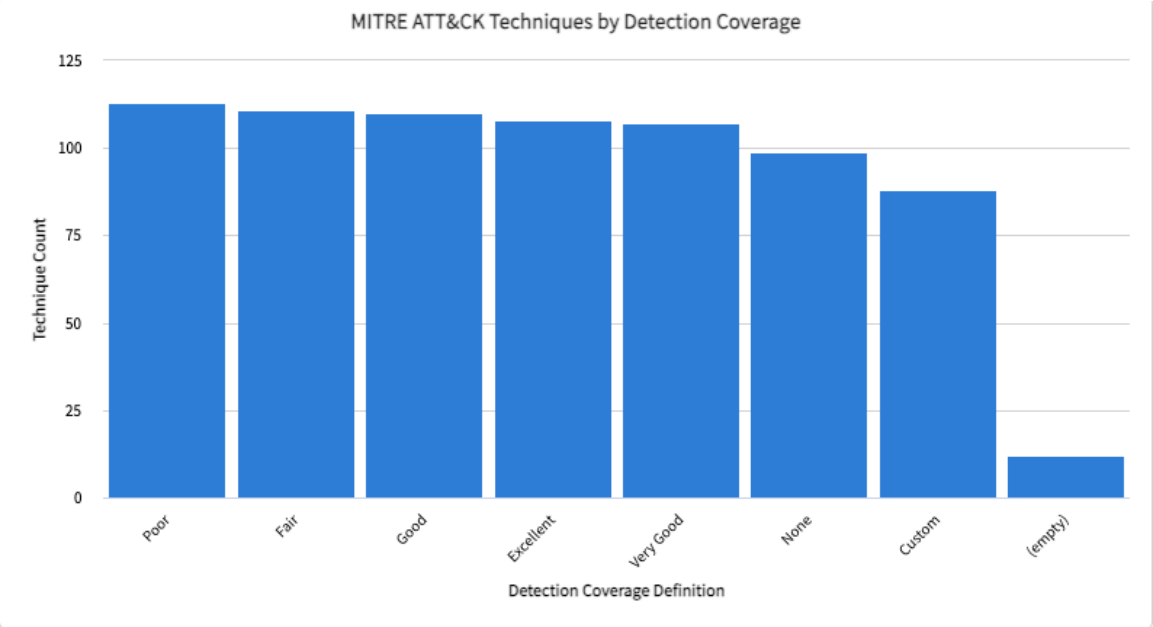
Exemplo de cobertura de detecção por MITRE-ATT&CK técnicas

Neste exemplo, **Técnicas MITRE-ATT&CK por cobertura de detecção** o widget exibe a contagem de técnicas pela cobertura de detecção em seu ambiente.

O eixo x exibe a contagem da técnica e o eixo y exibe os tipos de cobertura de detecção.

Tradução automática

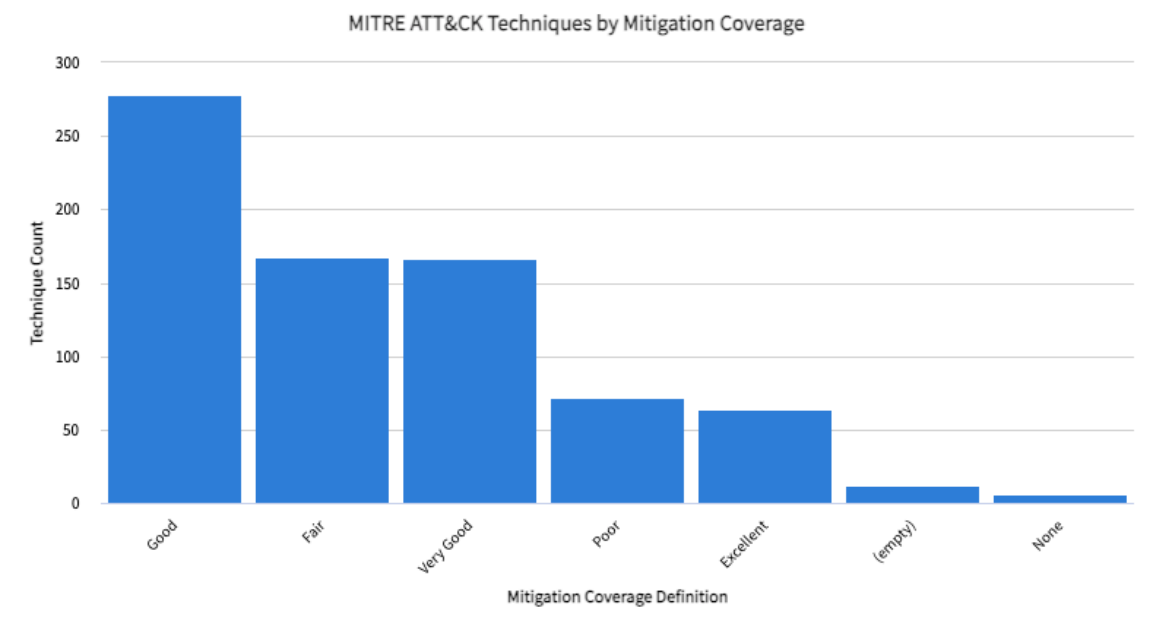
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de cobertura de mitigação por MITRE-ATT&CK técnicas

Neste exemplo, **Técnicas MITRE-ATT&CK por cobertura de mitigação** o widget exibe a contagem de técnicas pela cobertura de mitigação em seu ambiente.

O eixo x exibe a contagem de técnicas e o eixo y exibe os tipos de cobertura de mitigação.



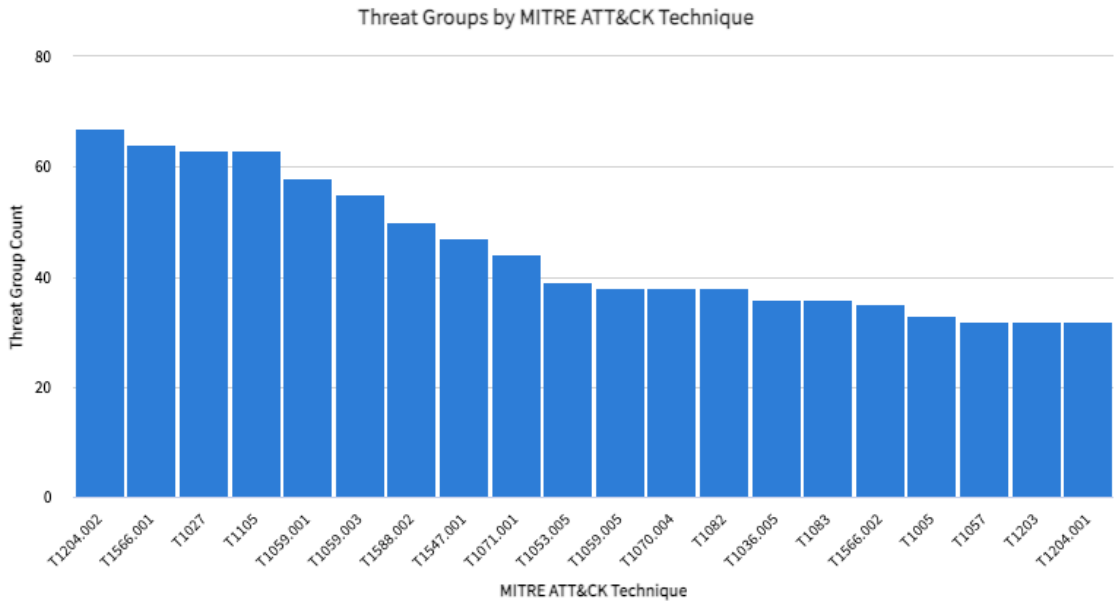
Exemplo de grupos de ameaças por MITRE-ATT&CK técnicas

Neste exemplo, **Grupos de ameaças por técnica MITRE-ATT&CK** o widget exibe as técnicas pela contagem do grupo de ameaças. Este widget exibe 20 técnicas com a maior contagem de grupos de ameaças.

O eixo x exibe a contagem do grupo de ameaças e o eixo y exibe MITRE-ATT&CK técnicas.

Tradução automática

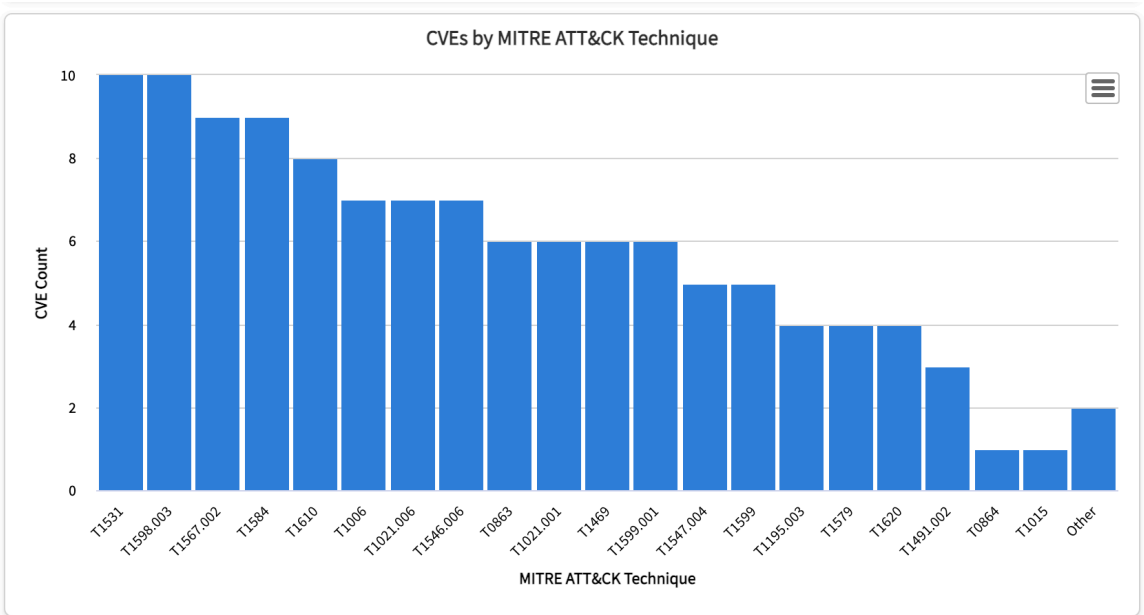
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de CVEs por MITRE-ATT&CK técnicas

Neste exemplo, **CVEs por técnica MITRE-ATT&CK** O widget exibe as técnicas com a contagem de CVE relevante em seu ambiente.

O eixo x exibe a contagem de CVE relevante e o eixo y exibe MITRE-ATT&CK técnicas.



Administração do Inteligência contra ameaças

. Inteligência contra ameaças o sistema de base está pronto para uso na ativação. Você pode adicionar registros a determinados módulos no menu da aplicação Administração, mas a maioria já está preenchida com informações padrão do setor.

As aplicações a seguir estão disponíveis em **Administração** módulo do Inteligência contra ameaças barra de navegação:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de administração do Inteligência contra ameaças

Aplicação	Descrição
Propriedades	Inteligência contra ameaças propriedades Permite que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.
Mecanismos de Ataque	Este módulo organiza padrões de ataque hierarquicamente, com base em mecanismos que são frequentemente empregados ao explorar uma vulnerabilidade.
Motivações de ataque	Este módulo lista as possíveis motivações de ataque que moldam a intensidade de um ataque por um agente de ameaça ou conjunto de invasão.
Métodos de Descoberta	Este módulo descreve como os incidentes de segurança são descobertos.
Feeds	Este recurso foi descontinuado.
Tipos de Indicador	Este módulo é usado para caracterizar indicadores de ameaça cibernética compostos por padrões que identificam determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões e como e quando eles são agidos.
Tipos de infraestrutura	Este módulo lista as possíveis classificações de infraestrutura.
Efeitos Pretendidos	Esta aplicação é usada para expressar o efeito pretendido de um agente de ameaça.
Capacidades do malware	Este módulo lista os possíveis recursos de malware.
Tipos de malware	Este módulo lista as possíveis classificações de malware.
Notificações	Este módulo é usado para criar notificações por e-mail . Especificar quando eles são enviados, quem os recebe e o que eles contêm.
Tipos de observável	Este módulo lista as possíveis classificações de um observável, como um endereço IP ou hash de arquivo.
Tipos de relatório	Este módulo lista as possíveis classificações de relatórios de ameaças.
Funções de agente da ameaça	Este módulo lista as funções que os agentes de ameaça desempenham.
Tipos de Agente da Ameaça	Este módulo caracteriza agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo intenção presumida e comportamento observado historicamente.
Calculadoras descobertas de pesquisa de ameaças	Este módulo calcula as descobertas com base nas respostas recebidas. Para integrações de terceiros que fornecem os resultados calculados, a calculadora de descoberta da pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças.
Tipos de Ferramentas	Este módulo lista a possível classificação de ferramentas.

Calculadoras descobertas de pesquisa de ameaças

A Calculadora de descoberta da pesquisa de ameaças ajuda a calcular as descobertas observáveis com base nas respostas recebidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar uma Calculadora de descoberta de pesquisa de ameaças para sua integração e usar um script para determinar como você deseja identificar as várias descobertas observáveis. A Calculadora de descoberta de pesquisa de ameaças inclui um script de amostra que vem com o sistema de base, que você pode usar para identificar as descobertas observáveis ou modificar esse script de acordo com seus requisitos.

Para integrações de terceiros que fornecem os resultados calculados, a Calculadora de descoberta da pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema de base.

Resultados da pesquisa de ameaças de acúmulo

Quando você tem vários resultados de pesquisa de ameaças para um observável de vários fornecedores de integração, os resultados recentes da pesquisa de ameaças de todos os fornecedores são considerados e as descobertas gerais do observável são marcadas da seguinte forma:

Acúmulos de descobertas da Pesquisa de ameaças

Descoberta observável mais recente	Descoberta observável geral
Mal-intencionado	Se um dos fornecedores de integração relatar o observável como mal-intencionado, a descoberta geral do observável será marcada como mal-intencionada.
Suspeito	Se nenhum dos fornecedores de integração relatar o observável como mal-intencionado, um deles o relatará como suspeito e a descoberta geral do observável será marcada como suspeita.
Limpar	Se todos os fornecedores de integração relatarem o observável como limpo, a descoberta geral do observável será marcada como limpa.
Desconhecido	Se nenhum dos fornecedores de integração relatar o observável como mal-intencionado ou suspeito e um deles relatar como Desconhecido, a descoberta geral do observável será marcada como Desconhecido.

Usando Calculadoras de descoberta da Pesquisa de ameaças

Use a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis para sua integração.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Administração** > **Calculadoras descobertas de pesquisa de ameaças**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Campo	Descrição
Fornecedor da Pesquisa de ameaças	Nome do fornecedor de pesquisa de ameaças.
Tipo de Observável	Especifique a classificação do tipo de observável ao qual o script se aplica. Por exemplo, endereço IP ou hash de arquivo e assim por diante. O script se apli-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ca a todos os observáveis se você não selecionar nenhum tipo de observável.
Localizando script	Editor de script para determinar como você deseja identificar as várias descobertas observáveis. A Calculadora de descoberta da pesquisa de ameaças contém um script de amostra com o sistema de base. Você pode usar este script para determinar as descobertas observáveis ou modificar este script de acordo com seus requisitos.

4. Clique em **Atualizar**.

Integrações do Inteligência contra ameaças

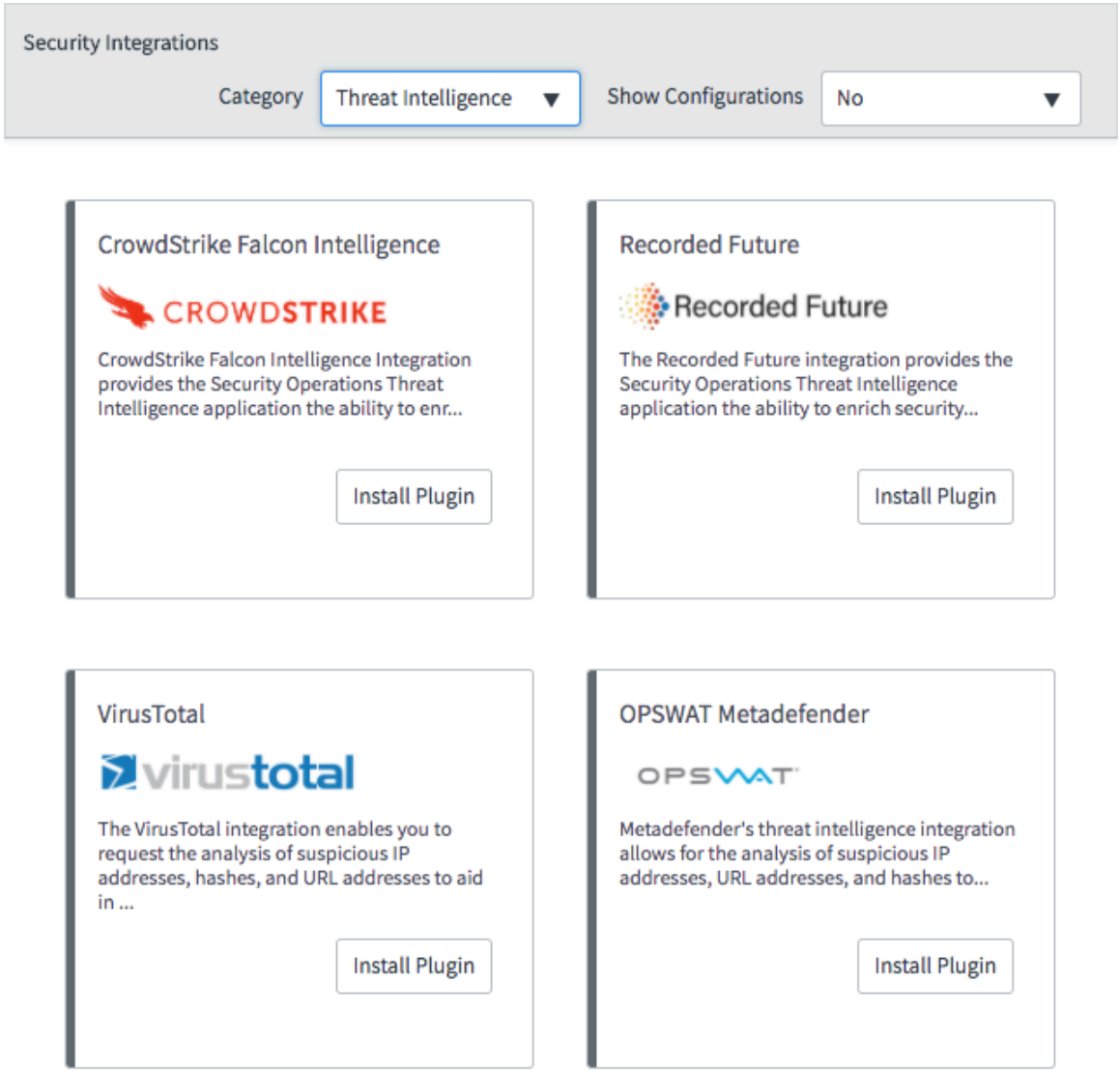
. Inteligência contra ameaças o sistema de base inclui integrações com pacotes de software de detecção de malware de terceiros. Esta seção fornece instruções para ativar os plug-ins e configurar ambos ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema de base inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências em Operações de segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode filtrar as integrações visíveis usando **Categoria** menu suspenso. . **Mostrar Configurações** o menu suspenso permite que você veja várias instâncias de implementações que permitem sua criação.

Botões nos cartões de integração

Os cartões de integração exibem botões diferentes dependendo do estado atual da integração e da origem do cartão.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar** .
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos do site da integração de terceiros.
Novo(a)	Determinadas integrações, como Carbon Black e IBM QRadar, permitem definir várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in é ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Botão	Descrição
Abrir página	No sistema de base, sua instância executa uma consulta à ServiceNow Store para todas as aplicações que têm dependências em Operações de segurança plug-ins. Quando essas aplicações são encontradas e os plug-ins de aplicações associados são ativados, os cartões de integração para elas são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o **Abrir página** o botão muda para **Configurar** .

Integração do CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence enriquece Inteligência contra ameaças com dados para incidentes de segurança e observáveis associados.

Explorar

- CrowdStrike Falcon Intelligence visão geral da integração
- Integrações do Resposta a incidentes de segurança

Configurar

Ativar e configurar o. CrowdStrike Falcon Intelligence integração

---

Usar

- Realizar pesquisas em observáveis
- Pesquisa de ameaças - CrowdStrike Falcon Intelligence fluxos

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

CrowdStrike Falcon Intelligence visão geral da integração

CrowdStrike Falcon Intelligence fornece inteligência de segurança cibernética que se integra facilmente ao Operações de segurança.

Nota: . Inteligência contra ameaças o plug-in é necessário para implementar o. CrowdStrike Falcon Intelligence integração.

Tradução automática

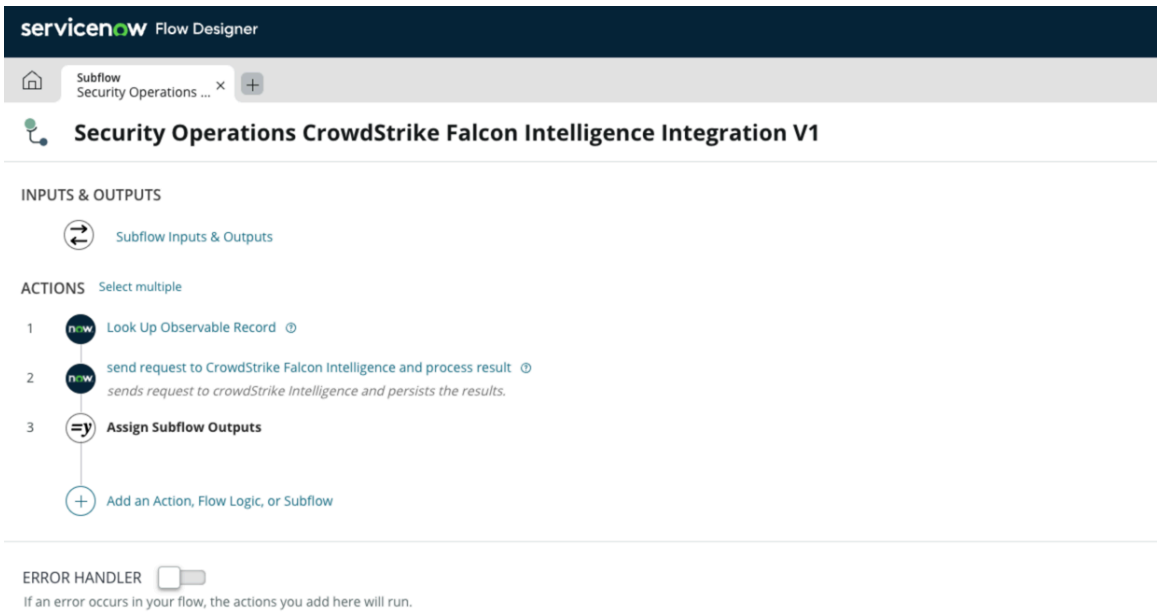
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - CrowdStrike Falcon Intelligence fluxos

A Pesquisa de ameaças - CrowdStrike Falcon Intelligence o flow designer executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por CrowdStrike Falcon Intelligence, os observáveis são verificados em busca de malware e os resultados são retornados.

Este fluxo é acionado pelo Integração de operações de segurança - Recurso de pesquisa de ameaças Quando você publica um ou mais observáveis em uma lista de observação e a implementação do CrowdStrike Falcon Intelligence é selecionada. Depois que são publicadas, as listas de observação podem ser exibidas no software CrowdStrike Falcon Host.

Função necessária: administrador



Para obter informações sobre as atividades usadas por este Flow Designer, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Ativar e configurar o. CrowdStrike Falcon Intelligence integração

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo CrowdStrike Falcon Intelligence integração. Antes de poder usar CrowdStrike Falcon Intelligence, você deve baixá-lo do ServiceNow Store E adicione a chave e o ID de API apropriados.

Antes de Iniciar

Função necessária: administrador

- . Inteligência contra ameaças o plug-in deve ser instalado e ativado antes que você possa usar CrowdStrike Falcon Intelligence integração.
- Obtenha o ID do cliente da API e o segredo do cliente da API em seu CrowdStrike Falcon Intelligence perfil.
- Se você estiver atualizando CrowdStrike Falcon Intelligence integração de uma versão anterior, em seguida, você deve excluir a configuração existente e definir uma nova configuração. A integração oferece suporte à autenticação OAUTH2. Esta atualização

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

requer que você insira **ID do cliente da API** e o. **Segredo do cliente da API** para autenticar e concluir a configuração.

- Em CrowdStrike Falcon Intelligence portal **Escopos de API** habilite o. **Leitura** configuração para **Indicadores (Falcon X)** ou **IOCs (indicadores de comprometimento)** .

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. Em CrowdStrike Falcon Intelligence cartão, clique em **Configurar** .
4. No formulário, preencha os campos para concluir a configuração:

CrowdStrike Falcon Intelligence Configuração

Campo	Descrição
Nome	Nome da integração, por exemplo, `demonstração-1` .
ID do cliente da API	O ID do cliente que você obtém na seção de configurações do seu perfil de conta em CrowdStrike Falcon Intelligence portal.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do seu perfil de conta em CrowdStrike Falcon Intelligence portal.

5. Clique em **Enviar**.

Resultado

Depois de configurado, CrowdStrike Falcon Intelligence pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Have I been pwned? integração

. Operações de segurança Have I been pwned? a integração permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar

Integrações do Resposta a incidentes de segurança

Configurar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Have I been pwned? configuração de integração
- Ativar

Usar	Desenvolver
Realizar pesquisas em observáveis Pesquisa de ameaças - Have I been pwned? fluxo	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Have I been pwned? configuração de integração

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido à conta on-line ter sido comprometida ou "pungida" em uma violação de dados. Ele se integra facilmente ao Operações de segurança.

Antes de poder usar Have I been pwned? integração, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

. Resposta a incidentes de segurança, Inteligência contra ameaças e Operações de segurança Have I been pwned? plug-ins são necessários para implementar o. Operações de segurança Have I been pwned? integração.

Pesquisa de ameaças - Have I been pwned? fluxo

A Pesquisa de ameaças - Have I been pwned? o fluxo executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, os observáveis são verificados em busca de malware e os resultados são retornados.

Função necessária: sn_si_admin

Este fluxo é acionado pelo Integração de operações de segurança - Recurso de pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis, e o. Have I been pwned? a implementação está selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Eu tenho sido pwwned fluxo



Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Ativar

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Operações de segurança Have I been pwned? integração. Antes de poder usar Have I been pwned?, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser instalado e ativado antes que você possa usar Operações de segurança Have I been pwned? Integração.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.
Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereços do navegador.
   Por exemplo: `https://<3rdparty>/` .

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e clique em **Segurança** guia.

   d. Clique em **Exibir certificado** e clique em **Detalhe** guia.

   e. Clique em **Exportação** Para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Deve começar com `------ INICIAR CERTIFICADO------` e termine com `------ CERTIFICADO FINAL-------` .

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e. crie um novo registro para a integração.
4. Em **Certificado PEM** cole o certificado baixado e copiado para a área de transferência anteriormente.
5. Adicione o certificado ao registro do Provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até **Certificados X.509** lista relacionada e clique em **Editar** .
   d. Mova o certificado recém-criado para **Selecionado** coluna.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

> **Nota:** Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituição de um certificado SAML prestes a expirar .

MISP integration for Security Operations

Com MISP integration for Security Operations, você pode investigar incidentes de segurança com pesquisas de detecções, aprimoramento de observáveis e criar ou atualizar eventos em MISP. Usando MISP, você pode investigar ataques direcionados mais rapidamente, melhorar a taxa de detecção e reduzir o número de falsos positivos em seu ambiente.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

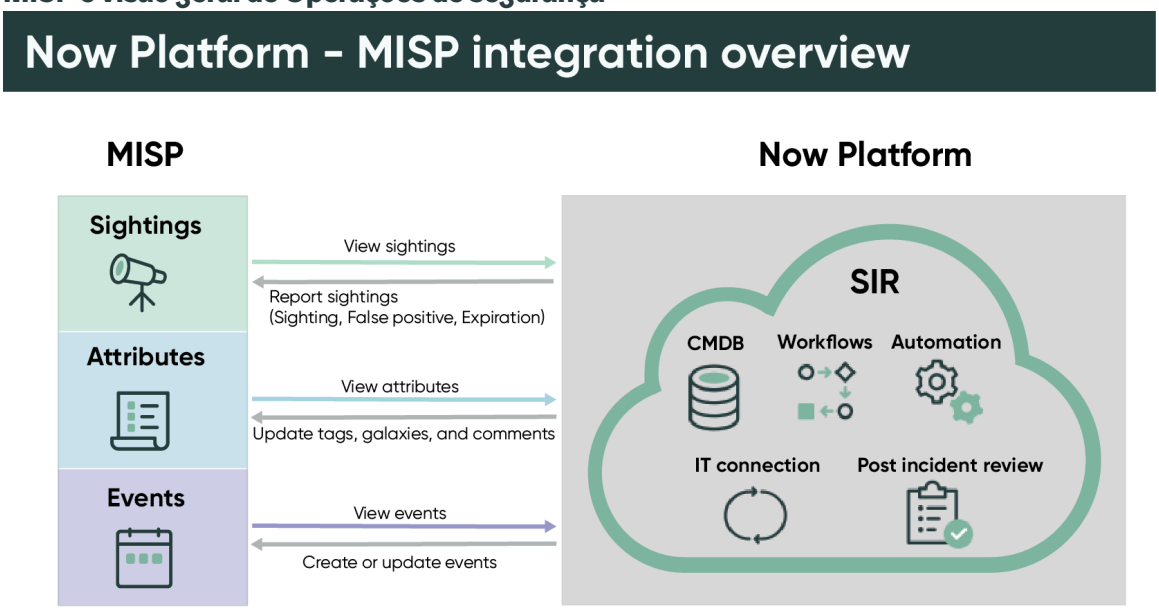
MISP Visão geral

MISP, que significa Malware Information Sharing Platform, Permite trocar e compartilhar inteligência contra ameaças e indicadores de comprometimento (IOCs) sobre o malware direcionado e ataques em sua comunidade de membros confiáveis. Você também pode compartilhar MISP informações com comunidades privadas ou abertas. Trocando MISP, você pode investigar ataques direcionados mais rapidamente, melhorar a taxa de detecção e reduzir o número de falsos positivos em seu ambiente.

MISP E Operações de segurança

Consulte o exemplo a seguir para saber como MISP As informações fluem com aplicações de operações de segurança.

MISP e visão geral de Operações de segurança



Principais recursos

Esta integração inclui o que você pode fazer com o. MISP principais recursos:

- Conecte-se a privado e público MISP instâncias.
- Suporte à pesquisa de detectores manual e automática .
- Execute a pesquisa de vistas na Gestão de casos .
- Relate ou atualize vistas para um atributo :
  - Relatar um observável como uma vista (global)
  - Relatar um observável como falso positivo (global)
  - Relate um observável como expirado
- Suporte ao aprimoramento de observável manual e automático . Os resultados incluem MISP informações de atributo e evento associadas aos observáveis.
- Aprimoramento de atributo em MISP que inclui adicionar ou atualizar marcadores , galáxias ou comentários .
- Criação de evento em MISP de SIRCompatível com a criação manual e automática de eventos no MISP de SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atualize um MISP evento de SIR que inclui adicionar ou atualizar marcadores , galáxias ou atributos .
- Adicione observáveis associados a incidentes de segurança como atributos a um MISP evento.
- Extração automática MITRE-ATT&CK™ informações de MISP atributos e associam as informações a. SIR incidentes de segurança.
- Adicionar automaticamente SIR MITRE-ATT&CK™ informações como galáxias para a. MISP evento.

Conceitos-chave

Esta integração inclui os seguintes conceitos-chave que você deve conhecer:

- MISP É uma plataforma de inteligência contra ameaças (TIP). Você usa dicas para coletar, correlacionar, categorizar, compartilhar e integrar dados de ameaças à segurança em tempo real para dar suporte à priorização de ações e ajudar na prevenção, detecção e resposta a ataques.
- MISP É uma Gestão de inteligência contra ameaças (TIM). Você usa TIMs para transformar dados de ameaças em inteligência contra ameaças por meio de contexto e priorizar automaticamente as ameaças por pontuação e relevância definidas pelo usuário.
- MISP Camada de dados
  - Eventos são encapsulamentos para informações vinculadas contextualmente.
  - Atributos são pontos de dados individuais, que podem ser indicadores ou dados de suporte.
  - Os objetos são composições de atributo de modelo personalizado.
  - Referências de objeto são os relacionamentos entre os outros blocos de construção.
  - As vistas são ocorrências específicas do tempo de um ponto de dados detectado.
- MISP Camada de contexto
  - Marcadores são rótulos anexados a eventos ou atributos e podem vir de taxonomias.
  - Galaxy-clusters são itens de base de conhecimento que você pode usar para rotular eventos ou atributos que vêm de galáxias.
  - Os relacionamentos de cluster denotam relacionamentos predefinidos entre clusters.
- Os indicadores contêm um padrão que você pode usar para detectar atividades cibernéticas suspeitas ou mal-intencionadas.
- Atributos em MISP Indicadores de rede (endereço IP), indicadores do sistema (uma cadeia de caracteres na memória) ou até mesmo detalhes da conta bancária. Os atributos em MISP São conhecidos como observáveis em outros SIEMs ou formatos como STIX.
  - Um tipo descreve o atributo. Por exemplo, MD5 ou um URL.
  - A categoria de atributo descreve um atributo. Por exemplo, uma entrega de carga.
  - Um marcador IDS determina se um atributo pode ser usado automaticamente para detecção.

Nota: Para obter mais informações sobre MISP conceitos, consulte Site de documentação do MISP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como sua organização pode se beneficiar MISP integration for Security Operations

Os analistas de segurança devem obter e manter a conscientização situacional do cenário de ameaças, o que significa que eles devem consolidar e integrar manualmente uma quantidade enorme de dados de ameaças. Coletar, consolidar e integrar esses dados leva um tempo valioso, o que retarda a detecção e a análise de ameaças. MISP integration for Security Operations permite que os analistas detectem mais ameaças e respondam mais rapidamente, integrando o. MISP inteligência de segurança em um existente ServiceNow AI Platform instância.

Usando o. MISP integration for Security Operations sua organização pode executar as seguintes ações:

- Permita que seus analistas de segurança respondam rapidamente e com o contexto certo.
- Melhore a eficiência da sua equipe de segurança automatizando os fluxos de incidentes para detectar e conter ameaças.
- Reduza o tempo de pesquisa manual e permita que os analistas de segurança operacionalizem e selecionem indicadores de dentro do ServiceNow AI Platform.

Conheça esta integração

Identificador do documento	Título do documento
MISP site de documentação	Site de documentação do MISP
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Administração do MISP

Você pode configurar MISP integração no ServiceNow AI Platform para executar uma pesquisa de detecções, aprimoramento de observáveis e criar e atualizar eventos em MISP.

Comece com MISP integration for Security Operations

Revise as informações a seguir antes de configurar seu MISP integration for Security Operations.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform, Inteligência contra ameaças e Resposta a incidentes de segurança funções.	As funções a seguir são usadas em MISP recursos no ServiceNow AI Platform: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_si.admin e sn_ti.admin podem configurar a integração e configurar o automático MISP perfis de criação de evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• sn_sec_misp.write - o. MISP a função de analista tem permissões de leitura e gravação para MISP dados que incluem o evento e os dados do atributo. Para obter mais informações, consulte Configurar Inteligência contra ameaças .
Atribua o necessário MISP funções do usuário.	Revise MISP funções do usuário e as permissões necessárias para usar o. MISP integration for Security Operations. **Nota:** Para obter mais informações sobre as funções do usuário em MISP, Consulte a seção Funções em Site de documentação do MISP .
Verifique se você está usando MISP versão 2.4.137 ou posterior.	. MISP integration for Security Operationsé testado com um mínimo MISP versão 2.4.137 .
Verifique se o ServiceNow aplicações principais que são necessárias para oferecer suporte ao MISP estão instalados e ativados.	Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação tranquila. • Resposta a incidentes de segurança • Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) • Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest) Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um produto de Operações de segurança ou aplicação e. Ativar uma aplicação da ServiceNow Store .
Domain Separation	Verifique seção domain separation se você pretende separar dados, processos e tarefas administrativas.

MISP funções e permissões do usuário

Revise as funções de usuário necessárias no MISP integration for Security Operations integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprimoramento de observável e permissões de pesquisa de vistas

Nota:

- *Todos* **ServiceNow** *Os recursos de integração do MISP precisam das permissões básicas para* **Gerenciar eventos da organização** *e.* **Acesso à chave de autenticação** *. Certifique-se de ter essas permissões básicas antes de prosseguir.*
- *Para adicionar galáxias locais, o usuário que configura a integração deve pertencer à organização host do servidor MISP correspondente.*

Capacidade MISP	Marcador	Editor de marcadores
Aprimoramento de observável (somente leitura)	#	#
Pesquisa de vistas (somente leitura)	#	#

Permissões de avistamento do relatório

Capacidade MISP	Criador de avistamentos
Relatar vista	#

Atributos e permissões de evento

Capacidade MISP	Marcador	Editor de marcadores
Editar marcadores de evento/ atributo	#	#
Editar galáxias de evento/atributo	#	#
Editar comentários do atributo	#	#
Adicionar novo atributo ao evento	#	#
Criar evento no MISP	#	#

Tradução automática

Instale e configure o. MISP integration for Security Operations

Instale e configure o. MISP integration for Security Operations em ServiceNow Store em seu ServiceNow AI Platform para que você possa começar a investigar incidentes de segurança usando MISP dados.

Antes de Iniciar

Certifique-se de ter instalado os certificados SSL válidos no servidor MISP.

Função necessária: sn_si.admin

Procedimento

1. Baixe o. MISP integration for Security Operations em ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE MISP Bloco Integração SIR/TI e clique **Configurar** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

MISP - Formulário de configuração de integração SIR/TI

Campo	Descrição
Nome	Nome do MISP configuração da instância.
MISP URL do servidor	URL do MISP Servidor que serve como endpoint REST para MISP servidor.
Chave de API	Chave de API configurada para sua conta de usuário no MISP servidor. A chave de API corresponde ao **Authkey** em MISP servidor.
Implantação no Local	Opção que você pode selecionar se for sua MISP o servidor está implantado em uma instância no local. Ao selecionar **Implantação no local** , você deve usar MID Server para se conectar ao MISP servidor.
Aplicação de MID	Campo de cadeia de caracteres que identifica o nome da aplicação MID que é usado para se comunicar com MISP. Este campo é obrigatório quando você seleciona **Implantação no local** opção. Para obter informações sobre como configurar o MID Server para sua aplicação, consulte Configure um MID Server para cada aplicação

5. Clique em **Enviar**.

Resultado

Depois de validar e enviar a configuração com êxito, o MISP- A integração SIR/TI é salva na página Integrações de segurança como um bloco.

Revise MISP configurações de integração

Revise MISP integration for Security Operations e modifique as propriedades do sistema padrão para se adequar ao seu ambiente.

Antes de Iniciar

Função necessária: sn_si.admin, sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Integração MISP** > **Configurações de integração**.
2. Modifique as configurações a seguir conforme necessário.

Configurações de integração do MISP

Nome da propriedade		Descrição
Aprimoramento de Observável	Tempo (em horas) antes de buscar novos dados	Tempo em horas antes que você possa buscar novos dados. Tipo: inteiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
		Valor padrão: 24
Pesquisa de Vistas	Executar pesquisa de detecções automaticamente quando novos observáveis forem associados ao incidente de segurança	Pesquisa de vistas que é executada sempre que um novo observável é associado a um incidente de segurança. Valor padrão: sim
	Intervalo de pesquisa (em dias) para pesquisa de vistas no MISP	Número de dias em que os dados de pesquisa de vistas são pesquisados MISP. Use esta opção somente para o recurso de pesquisa de detecção automática. Valor padrão: 90
Sincronização de dados	Período de intervalo (em minutos) para que marcadores sejam obtidos e sincronizados com o MISP	MISP marcadores obtidos no momento da configuração da integração. Depois que os dados estão em ServiceNow AI Platform, esta propriedade define a frequência com que os dados com MISP o servidor está sincronizado. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para atualizar galáxias MISP de fontes configuradas	MISP galáxias que são obtidas no momento da configuração de integração. Depois que os dados estão em ServiceNow AI Platform, esta propriedade define a frequência com que os dados com MISP o servidor está sincronizado. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para as organizações serem buscadas e sincronizadas com o MISP	MISP organizações que são obtidas no momento da configuração de integração. Depois que os dados estão em ServiceNow AI Platform, esta propriedade define a frequência com que os dados com MISP o servidor está sincronizado. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
MITRE™ Extração de técnica	Acúmulo MITRE-ATT&CK Técnicas automaticamente de resultados de aprimoramento observável do MISP (marcadores) para incidente de segurança	Acúmulo de MITRE-ATT&CK informações de MISP resultados de aprimoramento observável (marcadores) para o incidente de segurança. Valor padrão: sim
	Acúmulo MITRE-ATT&CK Técnicas automaticamente de resultados de aprimoramento observável do MISP (galáxias) para incidente de segurança	Acúmulo de MITRE-ATT&CK informações do MISP resultados de aprimoramento observável (galáxias) para o incidente de segurança. Valor padrão: sim

Nota:

- Para usar o. MITRE™ recursos de extração de técnica em MISP, você deve habilite o. MITRE-ATT&CK recurso no Inteligência contra ameaças módulo.
- . MISP integration for Security Operations apresenta dois sistemas de base MITRE-ATT&CK regras de extração de técnica para MISP- MISP galáxias e. MISP marcadores. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte Extrair automaticamente regras de técnica para importar informações DO MITRE-ATT&CK .

3. Clique em **Salvar**.

Resultado
Suas configurações de integração modificadas são salvas e aplicadas.

Configurar MISP pesquisas de vistas

Configure o. ServiceNow AI Platform para fazer pesquisas de detectores no MISP instância. Com essas informações, você pode determinar com que frequência as ameaças ocorrem.

Antes de Iniciar

- Revise MISP função e permissões do usuário necessários para usar o. MISP recursos bidirecionais.
- Função necessária: sn_si.admin, sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

. Integração de operações de segurança - Fluxo de trabalho de pesquisa de vistas executa as pesquisas de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vistas e executa as pesquisas baseadas no fluxo de trabalho configurado.

. MISP integration for Security Operations fornece um perfil de pesquisa de detecções do sistema de base que permite configurar pesquisas de detecções automáticas. Com este perfil, você pode acessar as informações de avistamento observável relacionadas de uma organização e também ver as vistas externas de outras organizações.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração MISP** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome do perfil de capacidade.
Pesquisa salva	Configuração de pesquisa que é salva quando você seleciona esta opção. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações de pesquisa salvas adicionais conforme necessário.
Origem da pesquisa de detecções	Origem da pesquisa de vistas. Selecione MISP armazenamento de log como a origem.
Ativo	Opção que habilita a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de vistas.
Tipo de observável	Tipo de observável, como endereço IP, valor de hash, URL e nome de domínio.
Observável máximo por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.
Pesquisar	Cadeia de caracteres de pesquisa padrão que é `(observável)` . No entanto, você define sua própria consulta de pesquisa especificando MISP parâmetros compatíveis de armazenamento de log.

4. Clique em **Enviar**.

Resultado
Você criou um MISP perfil de configuração de pesquisa de vistas.

Configure como um evento automático é criado

Configure o. ServiceNow AI Platform para criar eventos automaticamente em MISP.

Antes de Iniciar

- Revise MISP função e permissões do usuário necessários para usar o. MISP recursos bidirecionais.
- Função necessária: sn_si.admin, sn_ti.admin

Procedimento

1. Navegar até **Tudo** > **Integração MISP** > **Perfis automáticos de criação de evento**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Nome

Campo	Descrição
Nome	Nome do perfil de criação de evento automático.
Descrição	Breve descrição sobre o perfil. Uma descrição mais detalhada é compartilhada por meio dos atributos na próxima fase da criação do evento.
Ordem	Ordem do perfil quando as condições de acionamento são atendidas. O padrão é 100. Deixe esta configuração como padrão. Se você criar vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O perfil com o número mais baixo tem a prioridade mais alta.
Origem	MISP origem da criação do evento.
Ativo	Opção que indica se o perfil está ativo ou inativo. Por padrão, a opção é desmarcada para indicar que o perfil está desativado. Este perfil não estará ativo até que você conclua todas as etapas de configuração do perfil e clique em **Concluir** .

4. Clique em **"Continuar"**.

Configurar condições do gatilho de evento

Configure as condições do gatilho de evento no ServiceNow AI Platform para que você possa acionar automaticamente um evento em MISP quando as condições são atendidas.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário Condições do gatilho, preencha os detalhes que podem acionar um evento.
   Você pode criar uma lógica composta fornecendo as condições do gatilho baseadas em campos de incidente de segurança ou campos observáveis. Você também pode criar eventos em MISP se os observáveis não tiverem um evento correspondente em MISP. Você pode optar por criar uma lógica composta usando uma combinação das três condições do gatilho - Acionar com base em campos de incidente de segurança, Acionar com base em campos observáveis e Criar evento MISP, se um observável não tiver eventos correspondentes no MISP. Se você selecionar vários gatilhos, poderá ingressar neles usando a condição E. Considere criar um perfil com novas condições se você precisar usar a condição OU.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Condições do gatilho de evento

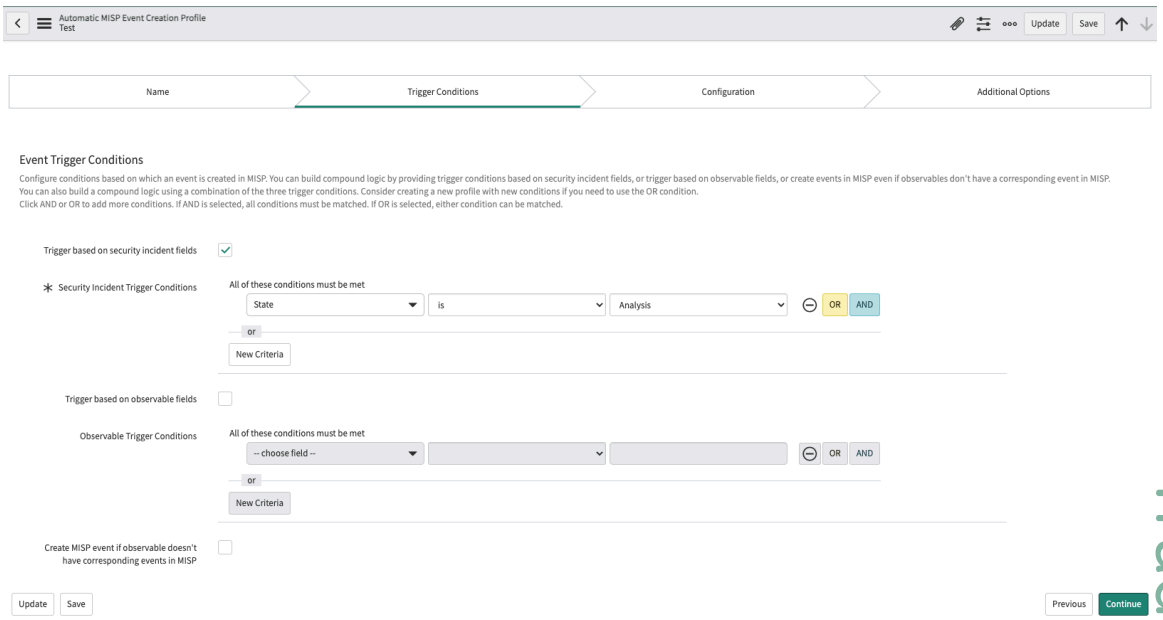
Campo	Descrição
Acionar com base nos campos de incidente de segurança	MISP evento que você pode criar se todas as condições do gatilho de incidente de segurança forem atendidas.
Condições do gatilho de incidente de segurança	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em E ou OU. Se E for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer condição poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** .
Acionar com base em campos observáveis	MISP evento que você pode criar se todas as condições do gatilho do observável forem atendidas.
Condições do gatilho observáveis	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em E ou OU. Se E for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer condição poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** .
Criar evento MISP se o observável não tiver eventos correspondentes no MISP	MISP evento que você pode criar se um observável não tiver eventos correspondentes em MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições do gatilho de evento

O exemplo a seguir mostra as condições do gatilho de evento conforme você configura o. MISP perfil de criação de evento.



2. Clique em **"Continuar"**.

Mapeie o. MISP campos de evento

Mapeie o. MISP campos de evento no ServiceNow AI Platform para que as informações do incidente de segurança estejam disponíveis quando MISP eventos são criados.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário, preencha os campos.

Formulário de mapeamento de campo de evento MISP padrão

Campo	Descrição
Informações do evento	Informações do evento que são criadas automaticamente a partir do ServiceNow AI Platform Resposta a incidentes de segurança. . **Informações do evento** O campo oferece suporte a variáveis de substituição usando Durante a criação de um evento, essas variáveis são substituídas pelos valores de campo de incidente de segurança real. A variável de substituição "URL" é substituída pela URL do incidente de segurança.
Distribuição	Opção que controla quem pode exibir este evento após a publicação do evento. Esta opção também

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ○ Somente sua organização: Permite que somente membros da sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, em que somente sua organização pode ter acesso para exibi-lo. Os eventos com esta configuração não são sincronizados. ○ Somente esta comunidade: Habilita usuários que fazem parte do seu MISP para exibir o evento, incluindo sua própria organização, organizações neste MISP e organizações que executam MISP servidores que sincronizam com este servidor. Todas as outras organizações que se conectam aos seus servidores vinculados estão impedidas de exibir o evento. ○ Comunidades conectadas: Habilita os usuários que fazem parte do seu MISP para exibir o evento, incluindo todas as organizações neste MISP servidor, todas as organizações no MISP servidores que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que esteja a dois saltos de distância. Todas as outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância estão impedidas de exibir o evento. ○ Todas as comunidades: Compartilha o evento com todos MISP comunidades.
Nível de ameaça	Campo que indica o nível de risco do evento. Você pode categorizar incidentes em três categorias de ameaça diferentes (baixa, média, alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções: ○ Baixo: Malware geral em massa ○ Médio: Ameaças persistentes avançadas (APT) ○ Alto: APTs sofisticados e ataques de 0 dias
Status da análise	Fase atual da análise do evento, com as seguintes opções possíveis:

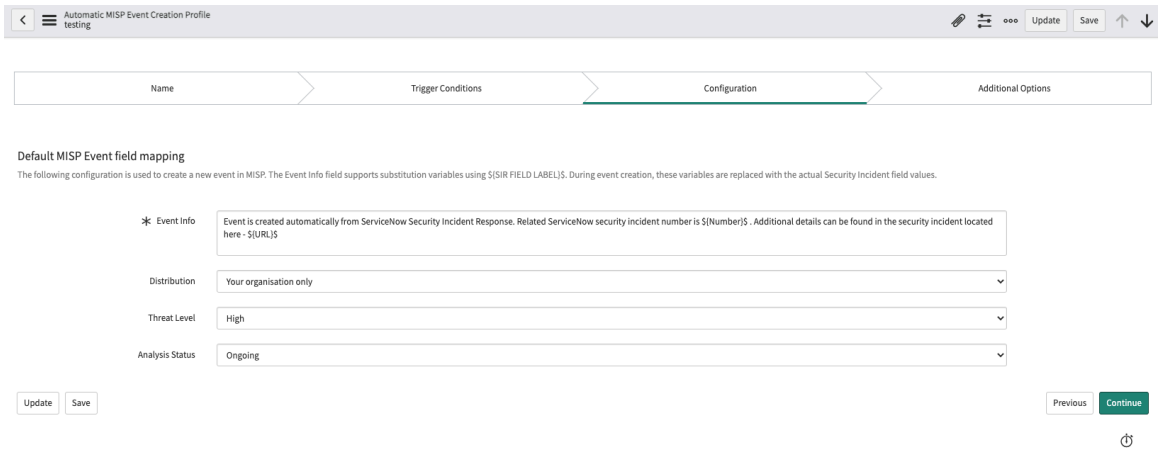
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Inicial: A análise está apenas começando ○ Em andamento: A análise está em andamento ○ Concluído: A análise está concluída

O exemplo a seguir mostra o formulário que você pode usar para criar um evento no MISP.

Mapeamento de campo de evento MISP padrão



2. Clique em **"Continuar"**.

Mapear ou associar SIR observáveis como atributos para MISP eventos

Mapeie o. Resposta a incidentes de segurança tipos de observáveis para MISP tipos de atributo porque MISP tipos de atributo e SIR observáveis podem ser diferentes.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Por Que e Quando Desempenhar Esta Tarefa

. MISP integration for Security Operations fornece um mapeamento do sistema de base que você usa ao adicionar SIR observáveis como atributos para um MISP evento.

Você pode optar por modificar o mapeamento do sistema de base para se adequar ao seu ambiente. Por exemplo, você pode mapear vários SIR observáveis para apenas um MISP tipo de atributo. Se algum tipo de observável não estiver mapeado, o **outro** MISP o tipo de atributo é selecionado por padrão.

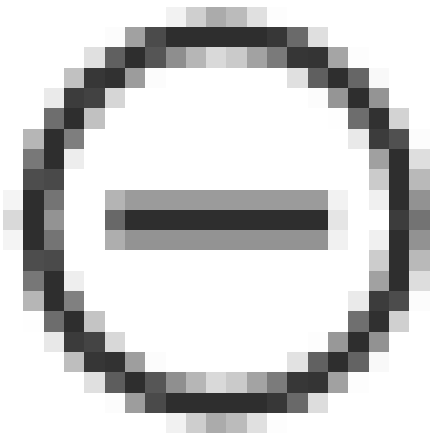
Procedimento

1. No formulário Opções adicionais, mapeie o. SIR observável e. MISP tipos de atributo.
2. Mapeie o. Resposta a incidentes de segurança tipos de observáveis para MISP tipos de atributo conforme descrito na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento do observável de SIR e tipo de atributo do MISP

Campo	Descrição
Adicionar todos os observáveis associados como atributos	Opção que você habilita para adicionar observáveis disponíveis em um incidente de segurança a um MISP evento como atributos. Esta opção habilita o mapeamento na seção Tipo de observável para Mapeamento de tipo de atributo.
Mapeamento de tipo de observável para tipo de atributo	Opção para mapear SIR tipos de observáveis para MISP tipos de atributo. Por exemplo, você pode mapear o número CVE em SIR para o atributo de vulnerabilidade em MISP. Você pode adicionar um SIR tipo de observável para apenas um MISP tipo de atributo. O sistema de base fornece um mapeamento do SIR tipos de observáveis para MISP tipos de atributo. Se houver SIR os tipos de observáveis não são mapeados para um MISP e, em seguida, o observável é mapeado para **outro** tipo de atributo em MISP. Para adicionar um novo mapeamento, clique em **Adicionar tipo de observável** , pesquise SIR tipo de observável e, em seguida, mapeie para o correspondente MISP tipo de atributo. Clique no ícone Remover mapeamento  para remover o. SIR e. MISP associação de mapeamento de atributos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para obter mais informações sobre MISP tipos de atributo, consulte Documentação do MISP .
Filtrar observáveis com base em marcadores de segurança	Opção para filtrar os observáveis com base nos marcadores de segurança selecionados. **Marcadores de segurança** : Adicione marcadores para filtrar os observáveis. Por exemplo, se você estiver adicionando um marcador chamado "Bloquear compartilhamento" ou "TLP: Branco", se um dos observáveis tiver algum desses marcadores associados, esses observáveis não serão adicionados como um atributo ao evento MISP durante a criação do evento MISP.
Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Opção que permite que você saiba se um observável está marcado como mal-intencionado em SIR, em seguida, o atributo correspondente em MISP Tem o sinalizador IDS habilitado. Se o sinalizador IDS não estiver definido, o atributo será considerado como informações contextuais e não será usado para detecção automática de invasão.

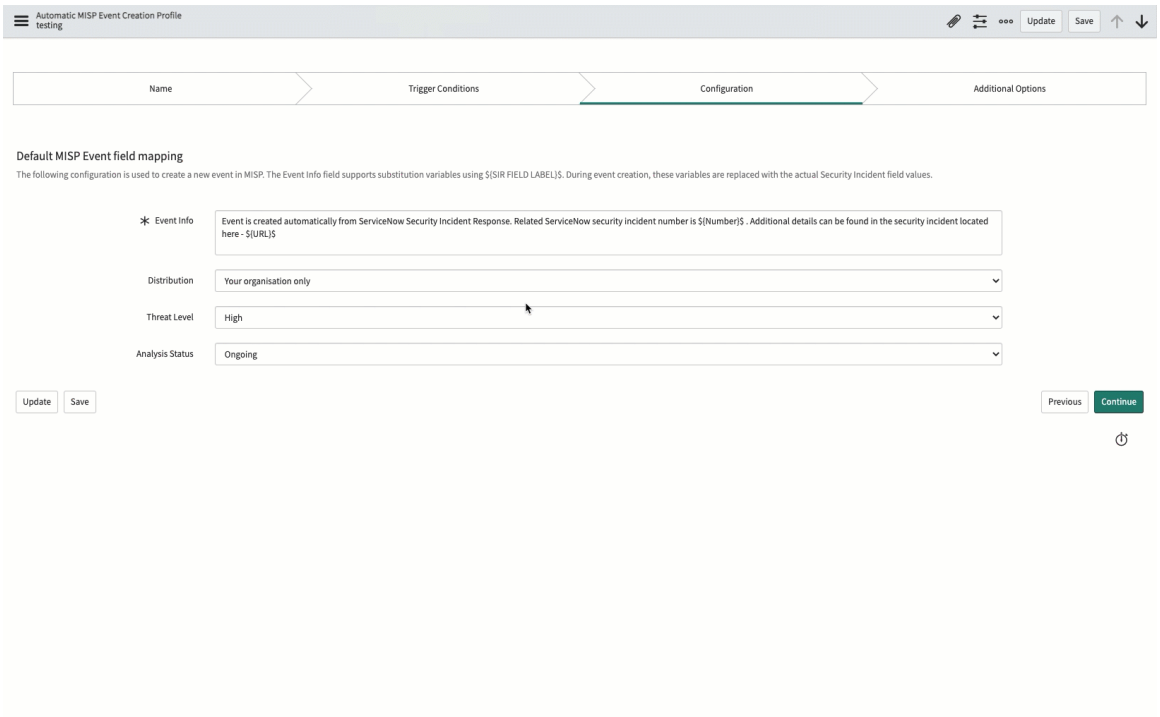
O exemplo a seguir mostra como navegar até a página de opções adicionais. Nesta página, você pode habilitar o mapeamento de observáveis SIR e tipos de atributo MISP,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adicionar novo SIR Tipos observáveis, como a rede IPV6 e a rede IPV4, e mapeiam para MISP Endereço IP do domínio do tipo de atributo.

Mapeamento SIR observáveis e. MISP tipos de atributo



Sincronizar MITRE-ATT&CK informações para MISP eventos

Sincronize o. MITRE-ATT&CK informações com MISP atributos para melhor análise de incidentes de segurança e ameaças.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

No formulário Opções adicionais, revise as opções para sincronizar o. MITRE-ATT&CK informações com MISP atributos.

Formulário Opções avançadas

Campo	Descrição
Incidente de segurança de sincronização MITRE-ATT&CK™ galáxias locais até MISP evento	Opção para sincronizar o. ServiceNow AI Platform SIR incidente de segurança MITRE-ATT&CK™ galáxias locais no MISP evento. **Nota:** Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do correspondente MISP servidor.
Incidente de segurança de sincronização MITRE-ATT&CK™ galáxias globais até MISP evento	Opção para sincronizar o. ServiceNow AI Platform SIR incidente de segurança MITRE-ATT&CK™ galáxias globais em MISP evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado
Você criou um perfil que permite criar eventos automaticamente em MISP em ServiceNow AI Platform. Agora você pode exibir os eventos na lista relacionada Eventos MISP associados.

Adicione marcadores MISP aos eventos

Adicione marcadores MISP aos eventos MISP criados.

Antes de Iniciar
Função necessária: sn_sec_misp.write

Procedimento

1. No formulário Opções adicionais, navegue até **Selecione marcadores MISP para adicionar ao evento** exibição do formulário.
2. Revise as opções para adicionar marcadores aos eventos criados.

Formulário Opções avançadas

Campo	Descrição
Adicionar marcadores ao evento MISP criado	Opção que permite adicionar automaticamente marcadores MISP aos eventos criados a partir da ServiceNow.
Marcadores (local)	Os marcadores selecionados serão adicionados como marcadores locais ao evento MISP.
Marcadores (global)	Os marcadores selecionados serão adicionados como marcadores globais ao evento MISP.

3. Clique em **Salvar**.

Resultado
Adicionar marcadores MISP ajuda na classificação do evento.

MISP dados do evento

Você pode revisar MISP dados do evento para que você possa ver informações detalhadas sobre MISP eventos.

MISP dados do evento na exibição de lista

Acesse a exibição de lista de **MISP** > **Dados do evento de MISP**.

Use a exibição de lista para obter uma visão geral rápida do MISP dados do evento.

Exibição da lista Eventos do MISP

Campo	Descrição
ID do evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para MISP servidor.
Informação	Descrição resumida do evento.
Análise	Fase atual da análise do evento com as seguintes opções possíveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição da lista Eventos do MISP

Campo	Descrição
	• Inicial: A análise está apenas começando • Em andamento: A análise está em andamento • Concluído: A análise está concluída
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média, alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: Malware geral em massa • Médio: Ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de 0 dias
Marcadores MISP	Marcadores associados ao MISP evento.
Galáxias MISP	Galáxias associadas a MISP evento.
Organização do proprietário	Organização responsável pelo evento no MISP instância. Este campo está visível somente para administradores.
Organização do criador	Organização que criou o evento no MISP instância.
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Hiperlink de evento MISP	Link para MISP evento armazenado no MISP servidor.
Origem do MISP	MISP origem em que o evento é criado.

MISP dados do evento na exibição do formulário

Use a exibição de formulário para obter informações detalhadas sobre MISP eventos.

Exibição do formulário de evento do MISP

Campo	Descrição
ID do evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para MISP servidor.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento no MISP instância.
Organização do proprietário	Organização responsável pelo evento no MISP instância. Este campo está visível somente para administradores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição do formulário de evento do MISP

Campo	Descrição
Usuário do criador	Usuário que criou o evento em MISP.
Última Mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez em MISP servidor.
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média, alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: Malware geral em massa • Médio: Ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de 0 dias
Análise	Fase atual da análise do evento com as seguintes opções possíveis: • Inicial: A análise está apenas começando • Em andamento: A análise está em andamento • Concluído: A análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifica os usuários que se inscreveram nos alertas de evento.
Hiperlink de evento MISP	Link para MISP evento armazenado no MISP servidor.
Informação	Descrição resumida do evento.
Marcadores (local)	Marcadores que estão disponíveis na organização host MISP instância para habilitar marcação para sincronização e filtragem de exportação. MISP os eventos não são modificados quando você usa marcadores locais. Marcadores locais são sempre removidos antes de serem sincronizados com outros MISP e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outros MISP e comunidades de compartilhamento. Quando você adiciona marcadores globais a. MISP, você pode modificar eventos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição do formulário de evento do MISP

Campo	Descrição
Galáxias (local)	Galáxias que estão disponíveis na organização host MISP instância para filtragem de sincronização e exportação. MISP os eventos não são modificados quando você usa galáxias locais. Estas galáxias locais são sempre despojadas antes de serem sincronizadas com outras MISP e comunidades de compartilhamento.
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP e comunidades de compartilhamento. Quando você adiciona galáxias globais, MISP você pode modificar eventos.

Associado MISP eventos

Você pode usar o associado MISP exibição da lista de eventos para exibir os eventos que foram criados manual ou automaticamente no contexto de um incidente de segurança.

Eventos de MISP associados

Campo	Descrição
Incidente de segurança	SIR incidente de segurança. Clique no incidente de segurança para exibir o incidente de segurança.
Evento MISP	MISP ID do evento. Clique em MISP evento para exibir MISP evento no ServiceNow AI Platform.
Origem do MISP	MISP origem em que o evento é criado. Clique em MISP origem para exibir a origem.
Modo de criação de evento	Se o evento foi criado manual ou automaticamente com o perfil de criação de evento. Clique em MISP evento para exibir o associado MISP evento.
Perfil de criação automática de evento	Perfil de criação de evento que é usado para criar o evento automático. Clique no perfil para exibir o Perfil de criação automática de eventos MISP.

MISP informações do usuário

Você pode usar MISP página de informações do usuário para exibir todos os usuários associados ao ServiceNow AI Platform MISP integration for Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informação do usuário de MISP

Campo	Descrição
Origem	Contas de usuário MISP origem.
ID do usuário	ID de usuário atribuído pelo MISP quando uma conta de usuário é criada.
E-mail do Usuário	Endereço de e-mail de um usuário. Somente os administradores da organização podem ver os endereços de e-mail dos usuários da própria organização.
Organização	Organização à qual um usuário pertence.
Nome da função	Nome da função que define os privilégios do usuário atribuídos a um usuário. Para obter mais informações sobre funções em MISP, consulte Documentação do MISP .
ID de Função	ID da função do usuário em MISP. Por exemplo, Administrador de Perm, Auditoria de Perm ou Marcador de Perm e assim por diante.
Permissão	Permissões que um usuário tem. As permissões disponíveis no MISP são as seguintes: • Somente leitura • Gerenciar eventos próprios • Gerenciar eventos da organização • Publicar eventos da organização
Permissão de vista	Permissão que permite que um usuário execute pesquisas de vistas.
Permissão do tagger	Permissão que permite que um usuário faça marcação.

Separação de domínios e MISP

Separação de domínios é compatível com MISP. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com MISP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com funções necessárias em seu domínio.
- Execute MISP integration for Security Operations procedimentos em seu domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas de integração do MISP

Esta seção aborda dicas importantes de solução de problemas que podem ajudá-lo a resolver problemas comuns que você pode encontrar ao configurar ou executar a integração do MISP.

Problemas de SSL

Ao se conectar por meio da integração MISP, certifique-se de ter instalado um certificado de CA válido no servidor MISP, que não expirou. Você pode importar RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Para obter mais informações, consulte Instale e configure o. MISP integration for Security Operations e MISP funções e permissões do usuário.

Usando MISP para investigar e analisar ameaças

Você pode usar MISP dados em ServiceNow AI Platform Inteligência contra ameaças e ServiceNow AI Platform SIR módulo para investigar e analisar ameaças à sua organização.

Pesquisas de vistas em MISP

Você pode executar pesquisas de vistas em observáveis no MISP Instância para determinar com que frequência determinados tipos de ataques, como ataques de phishing ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada um avistamento.

Vistas em MISP

As vistas indicam que um indicador, objeto ou atributo foi visto e sua validade foi confirmada. Vistas em MISPé um sistema que permite responder a atributos em um evento. Ele foi projetado para fornecer um método fácil para que seus usuários confirmem que viram um determinado atributo, dando mais credibilidade. Você pode ver um atributo várias vezes.

Nota: Observáveis são conhecidos como atributos no MISP.

Alguns atributos são considerados falsos positivos, o que significa que não são avistamentos válidos. Outros atributos são válidos por apenas uma determinada duração, como uma campanha de phishing executada por apenas uma semana. Você pode atribuir uma data de expiração aos atributos que são válidos por uma determinada duração, mas cada organização pode atribuir apenas uma data de expiração válida a um atributo.

Vistas criadas em MISP Por usuários de organizações marcadas como locais no servidor MISP correspondente são conhecidas como vistas internas. Vistas criadas em MISP por usuários de organizações marcadas como remotas no correspondente MISP os servidores são conhecidos como vistas externas.

Pesquisas de vistas em SIR

. Integração de operações de segurança - Fluxo de trabalho de pesquisa de vistas executa a pesquisa de vistas. Isso o flow aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vistas e executa as pesquisas baseadas no configurado fluxo.

As pesquisas de detecções ajudam os analistas a determinar a prevalência de uma ameaça ao longo do tempo. Você pode selecionar observáveis individuais ou vários observáveis e o intervalo de datas para sua pesquisa a partir de um incidente de segurança. Os resultados são incluídos no Incidente de segurança Vistas , Resultados da pesquisa de vistas e Detalhes da pesquisa de vistas listas relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao começar a analisar um incidente, você pode configurar seu ServiceNow AI Platform. executar automaticamente uma pesquisa de vistas ou execute manualmente uma pesquisa de vistas observáveis identificar outros usuários em sua organização que são afetados pelo mesmo ataque de phishing.

Habilite pesquisas automáticas de vistas em MISP

Habilite a pesquisa de vistas em MISP Para ser executado automaticamente para que o fluxo de trabalho Integração de operações de segurança - Pesquisa de vistas seja acionado sempre que novos observáveis forem associados a um incidente de segurança.

Antes de Iniciar

Verifique se o Perfil de configuração de pesquisa de vistas para MISP ativo.

Função necessária: sn_si.analyst

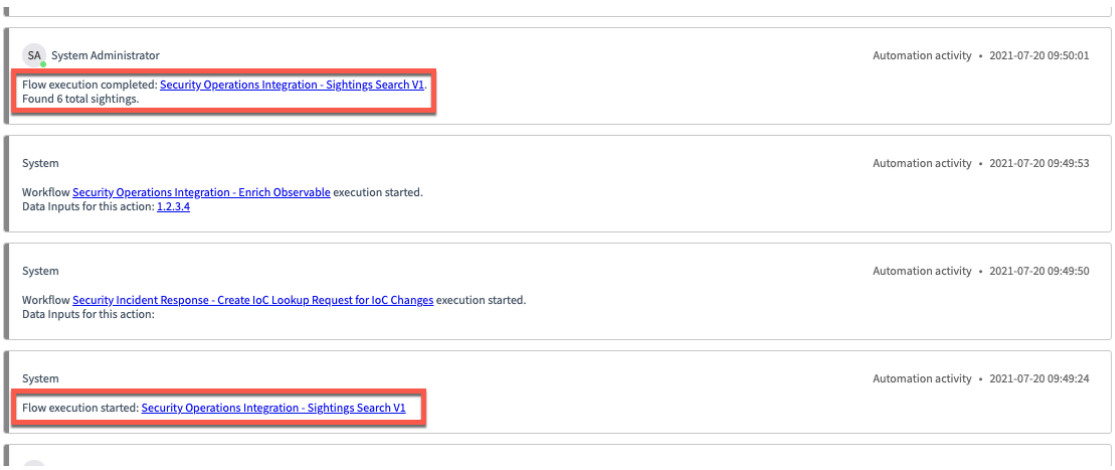
Por Que e Quando Desempenhar Esta Tarefa

Se você habilitar o recurso de pesquisa de vistas a ser executado automaticamente no MISP configuração de integração, a pesquisa de vistas em MISP acionado quando novos observáveis são associados a um incidente de segurança. Por padrão, o **Execute a Pesquisa de vistas automaticamente quando novos observáveis forem associados ao incidente de segurança** a opção está habilitada.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis que você deseja exibir no MISP dados de pesquisa de vistas.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança. Uma anotação de trabalho é publicada quando Integração de operações de segurança - Fluxo de trabalho de pesquisa de vistas acionado.

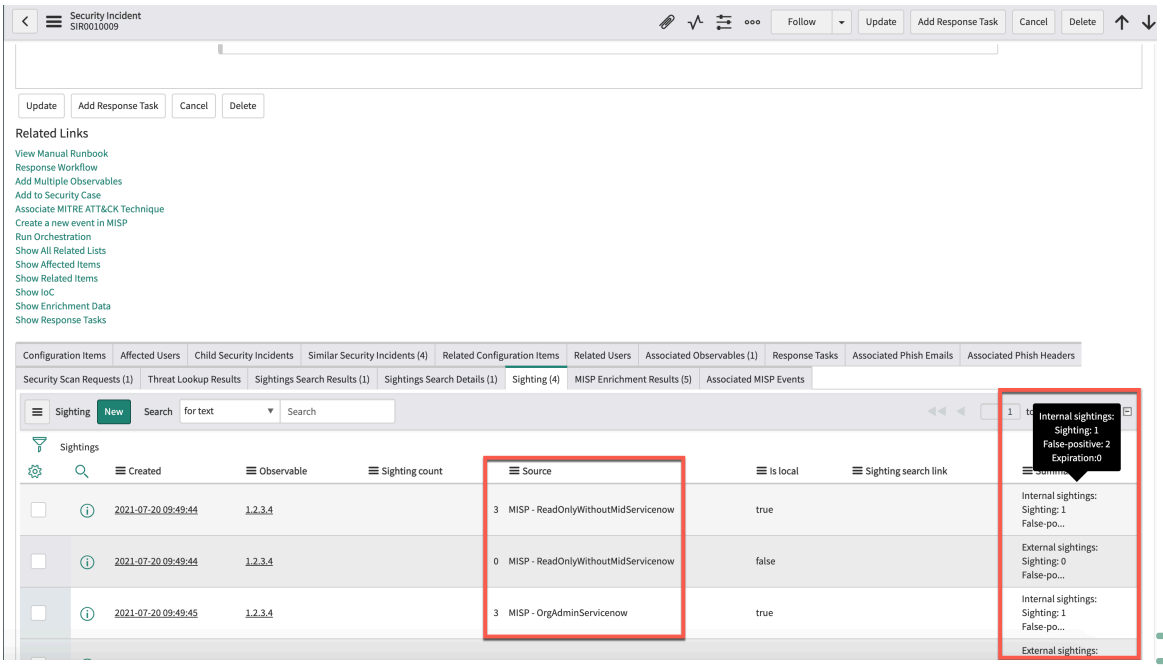
   O exemplo a seguir mostra a seção Anotações de trabalho.



4. Exiba as informações agregadas de observáveis que são vistos em todos os eventos (globais) e categorizados por suas vistas internas ou externas após a conclusão da execução do fluxo de trabalho.
   Exiba as informações no Vistas , Resultados da pesquisa de vistas e. Detalhes da pesquisa de vistas Listas relacionadas.O exemplo a seguir mostra o registro de pesquisa de vistas que foi criado na lista relacionada Vistas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Registro de pesquisa de vistas

Campo	Descrição
Criação em	Data e hora em que o registro de pesquisa de vistas foi criado.
Observável	Observável pesquisado pela consulta.
Contagem de detecções	Contagem de avistamentos internos e externos.
Origem	Origem do observável. Se o observável for de um MISP organização, o registro é precedido pelas palavras MISP .
É local	Status que indica se a detecção foi relatada por um usuário interno.
Link de pesquisa de detecção	Link de pesquisa de vistas em MISP instância.
Resumo	Tipos de vistas associadas ao registro. Os três tipos de avistamentos são avistamento, falso-positivo e expiração. A coluna Resumo aparece somente quando MISP integration for Security Operations instalado. Se houver origens diferentes de MISP For exibida, a entrada da coluna Resumo está vazia para esse registro.

Execute uma pesquisa de detecção manual em MISP

Selecione observáveis individuais ou múltiplos e execute uma pesquisa de vista manual no ServiceNow AI Platform MISP integration for Security Operations aplicação para determinar a prevalência de uma ameaça ao longo do tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis que você deseja executar MISP pesquisa de vistas.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
4. Selecione o observável e, no menu Ações, clique em **Executar Pesquisa de vistas** .
   Você pode selecionar vários observáveis para uma pesquisa de detecções.
   A caixa de diálogo Executar pesquisa de vistas é aberta.
5. Especifique o intervalo de datas para pesquisar os dados de pesquisa de vistas.

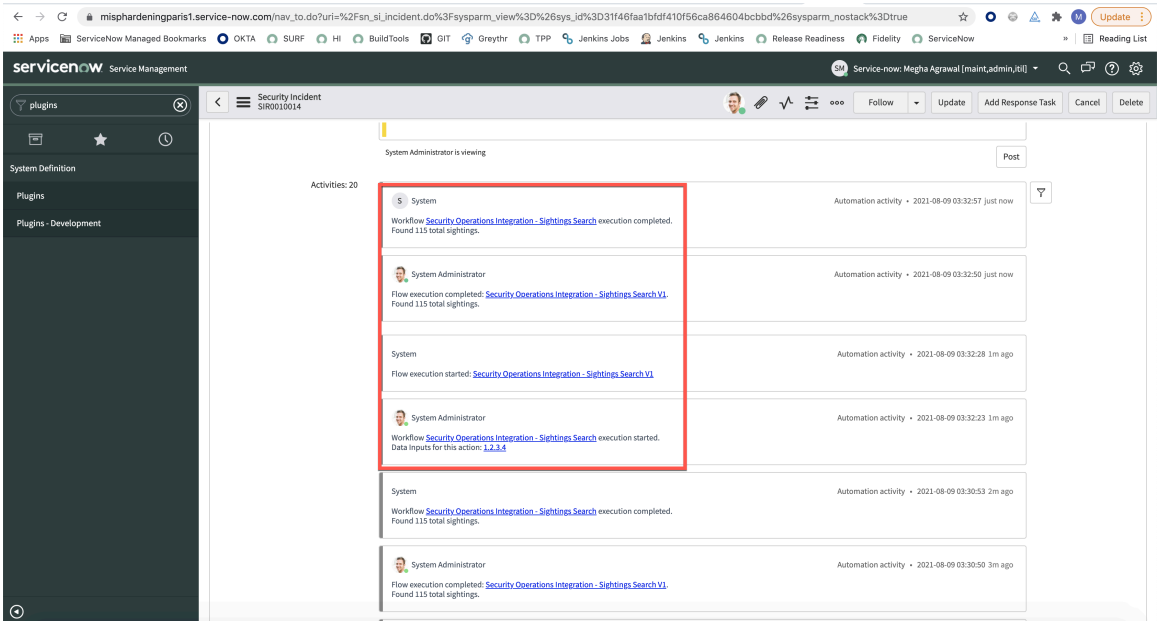
Caixa de diálogo Executar pesquisa de vistas

Campo	Descrição
Último	Número de horas ou dias antes da criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas para pesquisar. As datas padrão são as seguintes: ○ A data e a hora em que o incidente foi criado. ○ A data e a hora que são sete dias antes da abertura do incidente.

6. Clique em **Pesquisar**.
   O exemplo a seguir mostra os resultados da pesquisa de vistas manuais nas anotações de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Resultado

Um registro de Pesquisa de vistas é criado. Após a conclusão da execução do fluxo de trabalho, você pode exibir as informações agregadas de observáveis que são vistos em todos os eventos (globais) e categorizados por suas vistas internas ou externas. Os dados agregados e de vistas associados são exibidos no incidente de segurança em Vistas , Resultados da pesquisa de vistas e Detalhes da pesquisa de vistas listas relacionadas.

Relatar avistamentos para MISP

Relate detecções de dados de ameaças para que você possa reagir a falsos positivos em seus dados e aumentar sua conscientização quando ocorrer uma ameaça positiva verdadeira. Você também pode adicionar uma data de expiração para um observável ou atributo específico.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

. MISP integration for Security Operations permite relatar avistamentos para MISP globalmente em todos os eventos. Para relatar uma vista para um evento específico, você deve usar MISP e relate a vista localmente.

Para relatar uma observação MISP, o observável ou o atributo deve estar disponível em MISP instância.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja relatar as vistas MISP para.
3. Clique em **Mostrar todas as listas relacionadas** E a lista relacionada Observações.
4. Selecione o observável e, no menu Ações, selecione uma das seguintes opções.

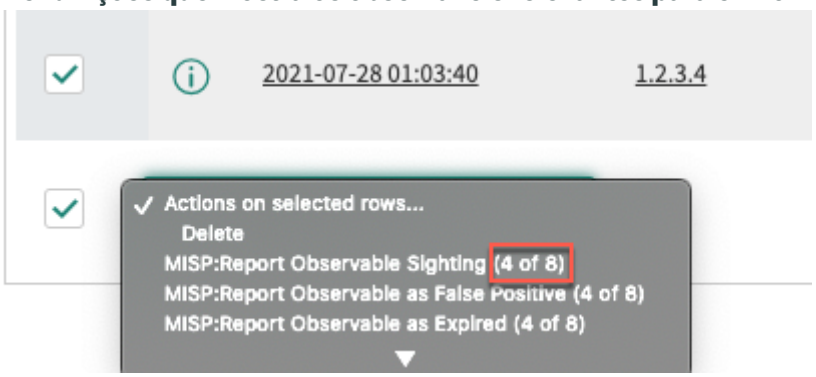
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
MISP: Relatar avistamento observável	Relate o observável como avistado para MISP. Se o observável estiver associado a vários eventos, ele será atualizado em todos os eventos.
MISP: Relatar observável como falso positivo	Relate o observável como falso positivo para MISP.
MISP: Relatar observável como expirado	Relate o observável como expirado para MISP.

Se você selecionar observáveis que não são específicos de um MISP Origem, o menu Ações mostra a contagem de relevantes MISP origens. O exemplo a seguir mostra quatro de oito observáveis como relevantes para MISP.O exemplo a seguir mostra o menu Ações e os observáveis relevantes para envio.

Menu Ações que mostra os observáveis relevantes para envio



5. **Opcional:** Se você selecionou **MISP: Relatar avistamento observável** , você deve preencher os campos da caixa de diálogo Relatar vista observável para MISP.

Relatar avistamento observável para MISP caixa de diálogo

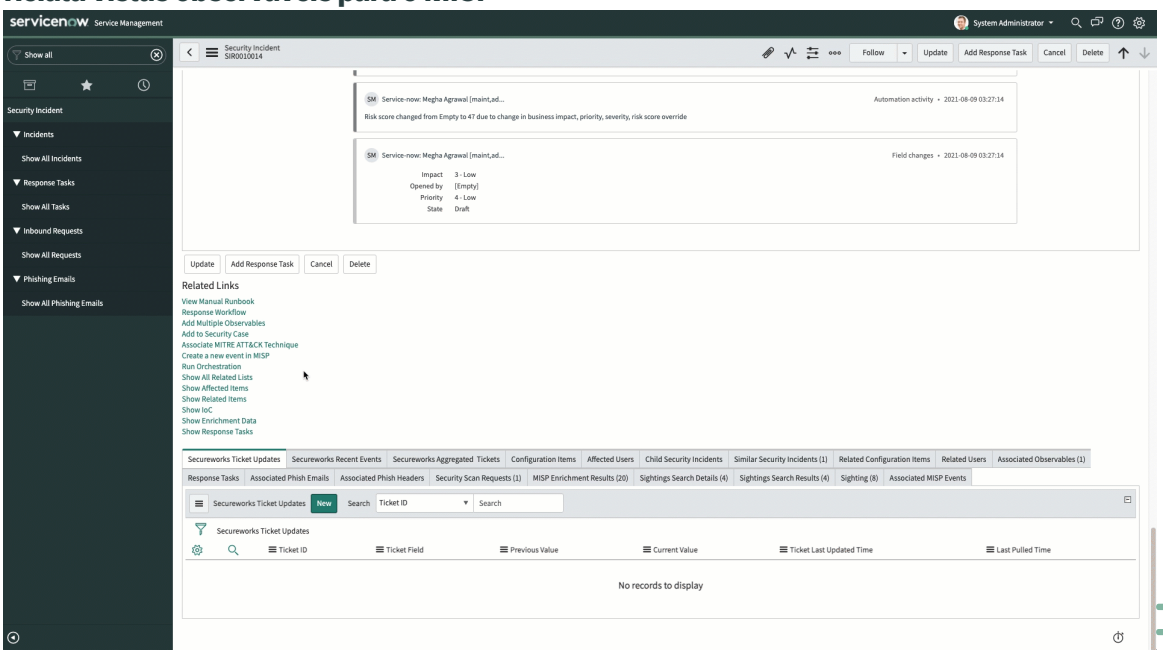
Campo	Descrição
Origem	Campo de origem que corresponde a. MISP origem do avistamento.
Data	Campo de data que corresponde à data em que o observável foi avistado. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

O exemplo a seguir mostra como navegar até a lista relacionada Observações no incidente de segurança. Nessa lista, você pode selecionar um observável e relatar a vista do observável para MISP. A mensagem de sucesso mostra que a detecção foi enviada com sucesso para MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relata vistas observáveis para o MISP



a. Clique em **Relatar detecções** .

6. **Opcional:** Se você selecionou **MISP: Relatar observável como falso positivo** , você deve preencher os campos do Relatório observável como falso positivo para MISP caixa de diálogo.

Relatar observável como falso positivo para MISP caixa de diálogo

Campo	Descrição
Origem (opcional)	Campo de origem que corresponde a. MISP origem. Use este campo para declarar o observável como falso positivo.
Data	Campo de data que corresponde à data em que o observável foi considerado um falso positivo. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

a. Clique em **Relatar falso-positivo** .

7. **Opcional:** Se você selecionou **MISP: Relatar observável como expirado** , você deve preencher os campos do Relatório de expiração do observável para MISP caixa de diálogo.

Caixa de diálogo Relatar expiração do observável para MISP

Campo	Descrição
Origem	Campo de origem que corresponde a. MISP origem. Use este campo para definir um observável como expirado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Data	Campo de data que corresponde à data em que o observável expirou. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

a. Clique em **Expiração do relatório** .

Resultado
As vistas são atualizadas com sucesso para MISP servidor.

Aprimoramento de observável em MISP

Enriquecendo observáveis com informações adicionais de vários MISP durante as investigações de resposta a incidentes, você pode conter ameaças identificadas.

Habilitar aprimoramento automático de observável em MISP

Habilitar aprimoramento automático de observável no ServiceNow AI Platform MISP quando novos observáveis são associados ao incidente de segurança.

Antes de Iniciar

- Habilite o. Resposta a incidentes de segurança propriedade do sistema para **Habilita ou desabilita o trabalho agendado, Pesquisar observáveis de incidentes de segurança** opção para acionar a capacidade de aprimoramento de observável em SIR.
- Função necessária: sn_si.analyst

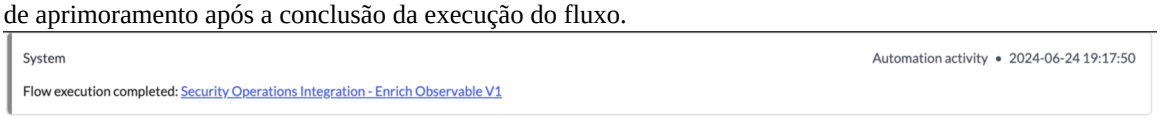
Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis nos quais você deseja enriquecer os dados observáveis MISP para.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança.

   O exemplo a seguir mostra que uma anotação de trabalho é publicada quando Integração de operações de segurança - Enrich o fluxo observável gatilhos.



4. Em MISP Lista relacionada aos resultados de aprimoramento do incidente de segurança, exiba os resultados de aprimoramento após a conclusão da execução do fluxo.

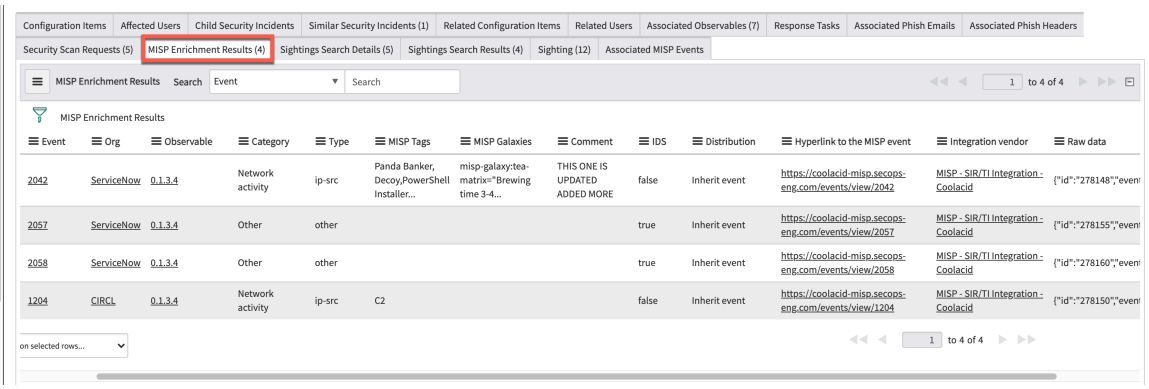


Nota: Você deve configurar esse MISP A lista relacionada Resultados de aprimoramento aparece nas listas relacionadas a incidentes de segurança. Para obter mais informações, consulte configuração da lista relacionada .

O exemplo a seguir mostra os resultados de aprimoramento no MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tabela a seguir mostra os resultados de aprimoramento do MISP.

Resultados de enriquecimento de MISP

Campo	Descrição
Evento	ID do evento. Clique em Abrir para exibir o registro no ServiceNow AI Platform instância.
Organização	Organização que criou originalmente o evento.
Observável	Observável associado ao evento.
Categoria	Categoria do atributo. Exiba a lista de categorias no Documentação do MISP .
Tipo	Tipo do atributo. Exiba a lista de tipos no Documentação do MISP .
Marcadores MISP	Lista de marcadores associados ao MISP atributo.
Galáxias MISP	Lista de galáxias associadas ao MISP atributo.
Comentário	Comentário contextual para descrever melhor o atributo. Esses comentários não são usados para correlação e são puramente informativos.
IDS	Indicador de compromisso, que permite que seja incluído em todas as exportações elegíveis.
Distribuição	Distribuição do atributo depois que ele é publicado. Um atributo pode ter um nível de distribuição diferente do evento. Em ambos os casos, o nível de distribuição mais baixo é usado.
Hiperlink para o evento MISP	Link para MISP, que é armazenado no MISP servidor.
Fornecedor de integração	Fornecedor de integração que fornece os dados para aprimoramento.
Dados brutos	Dados brutos associados ao MISP atributo.

Execute um aprimoramento de observável manual em MISP

Selecione observáveis individuais ou múltiplos e execute um aprimoramento de observável manual para que você possa enriquecer observáveis com informações adicionais de vários MISP origens.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

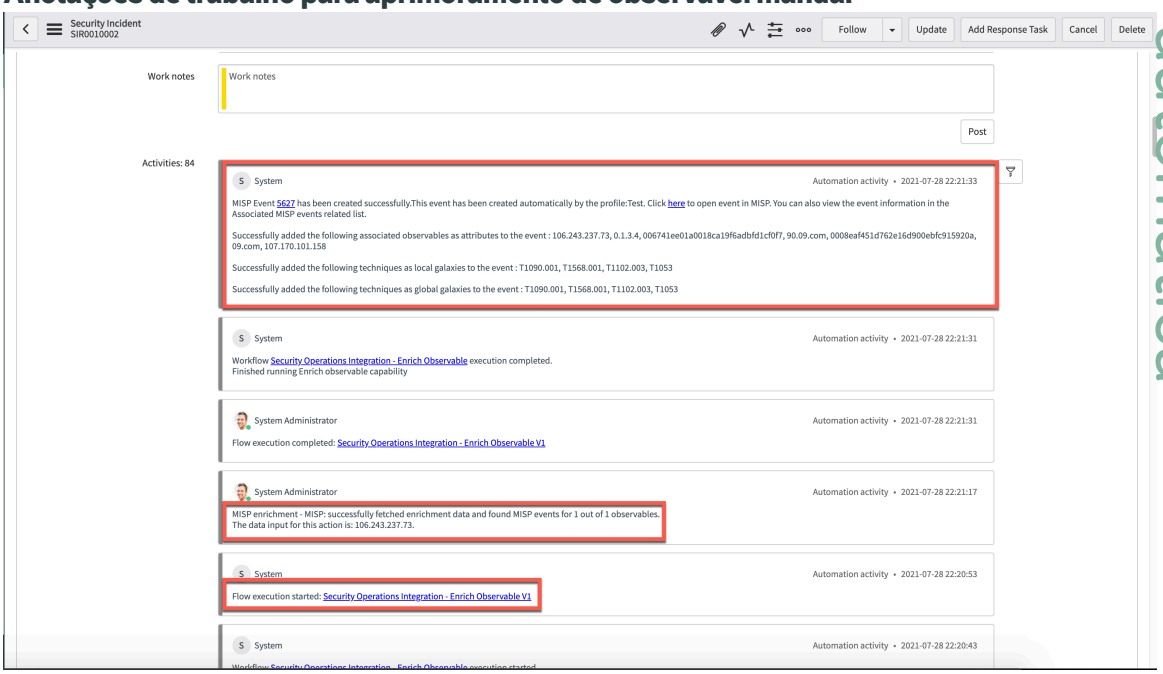
- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja executar o aprimoramento.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Observáveis associados** guia.
4. Selecione o observável e, no menu Ações, clique em **Executar aprimoramento de observável** .
   Você pode selecionar vários observáveis para uma pesquisa de detecções.
   A caixa de diálogo Executar aprimoramento do observável é exibida.
5. Selecione um MISP Origem e, na coluna Selecionado, selecione uma implementação para enriquecer os observáveis selecionados.
6. Clique em **Enviar**.
   Uma anotação de trabalho mostra que Integração de operações de segurança - Enrich o fluxo de trabalho do observável acionado. Os fluxos de trabalho de implementação associados são executados para executar o aprimoramento. Você pode exibir as anotações de trabalho no incidente de segurança para exibir o status.

   O exemplo a seguir mostra como exibir as anotações de trabalho para um aprimoramento de observável manual.

Anotações de trabalho para aprimoramento de observável manual



A mensagem de aprimoramento lista o evento criado. Você pode exibir o evento em ServiceNow AI Platform ou em MISP E exiba os detalhes do registro na guia Resultados de aprimoramento do MISP.

Adicionar ou remover marcadores a MISP atributos

Adicione ou remova marcadores em MISP para classificar eventos ou atributos. Você pode usar a marcação globalmente para habilitar sua classificação ou usar marcadores localmente quando não quiser MISP eventos a serem modificados durante sua classificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Verifique se o atributo que você está editando pertence à mesma organização que MISP usuário.
- Observe que os marcadores e galáxias que estão disponíveis para você são baseados em MISP origem e suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis, atributos ou eventos para os quais você deseja adicionar os marcadores.
3. Clique em **Mostrar todas as listas relacionadas** E a lista relacionada Resultados de aprimoramento do MISP.
4. Clique no ícone de visualização ⓘ ao lado de um registro e clique em **Registro em aberto** .
   O exemplo a seguir mostra como revisar o. **Resultados de aprimoramento do MISP** e como abrir um MISP registro de aprimoramento.

   Registro do resultado de aprimoramento do MISP
   Abrindo o registro de resultado de aprimoramento do MISP

5. Revise o registro de resultado de aprimoramento do MISP.

Resultado do aprimoramento de MISP

Campo	Descrição
Observável	
Evento	ID do evento atribuído pelo MISP servidor quando o evento foi criado ou importado pela primeira vez MISP. Visualize o evento ou clique no registro para exibir os dados do evento no MISP Página Dados do evento.
Organização	Organização que criou o. MISP atributo.
Categoria	Categoria do atributo que você adiciona ao evento específico em MISP. Você pode selecionar uma opção como uma referência interna, atividade de rede, fraude financeira e assim por diante.
Tipo	Tipo de MISP atributo.
Fornecedor de integração	Fornecedor de integração que fornece os dados para o aprimoramento do observável.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
IDS	Se um observável está marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Distribuição	Controles de opção de distribuição, como quem pode exibir este evento depois que ele é publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ○ Somente sua organização: Permite que somente membros da sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, em que somente sua organização tem acesso para exibi-lo. Os eventos com esta configuração não são sincronizados. ○ Somente esta comunidade: Habilita usuários que fazem parte do seu MISP para exibir o evento, incluindo sua própria organização, organizações neste MISP e organizações que executam MISP servidores que sincronizam com este servidor. Todas as outras organizações conectadas a esses servidores vinculados estão impedidas de exibir o evento. ○ Comunidades conectadas: Habilita os usuários que fazem parte do seu MISP para exibir o evento, incluindo todas as organizações neste MISP servidor, todas as organizações em MISP servidores que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que esteja a dois saltos de distância). Todas as outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância estão impedidas de exibir o evento. ○ Todas as comunidades: Compartilha o evento com todos MISP, o que permite que o evento esteja disponível gratuitamente.
Hiperlink para o evento MISP	Link para MISP evento armazenado no MISP servidor.
Dados brutos	Detalhes brutos do registro de dados de aprimoramento do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Comentário	Comentários que você adiciona aos atributos. Esses comentários são apenas para fins informativos e não são usados para correlação.
Marcadores (local)	Marcadores que estão disponíveis na organização host MISP instância para habilitar marcação para sincronização e filtragem de exportação. MISP os eventos não são modificados quando você usa marcadores locais. Esses marcadores são sempre removidos antes de serem sincronizados com outros MISP e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outros MISP e comunidades de compartilhamento. Quando você adiciona marcadores globais a. MISP, você modifica eventos.
Galáxias (local)	Galáxias que estão disponíveis na organização host MISP instância para filtragem de sincronização e exportação. MISP os eventos não são modificados quando você usa galáxias locais. Estas galáxias são sempre despojadas antes de serem sincronizadas com outras MISP e comunidades de compartilhamento.
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP e comunidades de compartilhamento. Quando você adiciona galáxias globais, MISP os eventos são modificados.

6. Para editar um marcador local ou global, clique no ícone de edição em uma das seguintes opções:

   - **Marcadores (local)**
   - **Marcadores (global)**

7. Na caixa de diálogo Marcadores de atributo MISP, insira o nome do marcador a ser pesquisado e adicionado.
8. Clique em **Atualizar marcadores para atributo MISP** .

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores foram atualizados em MISP.

   Adição de marcadores locais no atributo MISP.
   Os marcadores são atualizados com sucesso no MISP servidor.

9. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Adicione ou remova galáxias a um MISP evento ou atributo

Adicione ou remova galáxias em MISP para que você possa classificar esses objetos como um cluster em MISP e anexe-os a. MISP eventos ou atributos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do correspondente MISP servidor.
- Observe que os marcadores e galáxias que estão disponíveis para você são baseados em MISP origem e suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Clique no ícone de edição em uma das seguintes opções.

- **Galáxias (local)**
- **Galáxias (global)**

2. Na caixa de diálogo Galaxies de evento MISP, preencha os detalhes.

Caixa de diálogo Galáias de evento MISP

Campo	Descrição
ID do evento	ID do evento atribuído pelo MISP servidor quando o evento foi criado ou importado pela primeira vez MISP.
Namespace	Namespace onde a galáxia está armazenada. Você pode usar namespaces para agrupar galáxias semelhantes.
Galáxias	Galaxy onde você armazena as informações do cluster.
Clusters	Informação sobre os enxames na galáxia.

3. Clique em **Atualize galáxias para atributo MISP** .
O exemplo a seguir mostra que, ao clicar no ícone de edição das galáxias locais, você pode selecionar o namespace descontinuado, selecionar a galáxia Ataque empresarial - padrão de ataque e adicionar as informações do cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

Adição de informações da galáxia no MISP por meio de ServiceNow AI Platform

4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultado
As informações da galáxia foram atualizadas com sucesso no MISP servidor.

Adicionar comentários a. MISP atributo

Adicione comentários para MISP atributos. Os comentários adicionados são apenas para fins informativos e não são usados para correlação de MISP dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Verifique se o atributo que você está editando pertence à mesma organização que MISP usuário.
- Função necessária: sn_sec_misp.write

Procedimento

1. Clique no ícone de edição No campo Comentário.
2. Insira seu comentário no campo Comentário do atributo.
3. Clique em **Atualizar comentário para atributo MISP** .
   O exemplo a seguir mostra que, ao clicar no ícone de edição ao lado do campo de comentário, você pode adicionar um comentário e atualizar o. MISP atributo. Depois que o comentário for atualizado, você poderá exibir a mensagem de sucesso.

   Adição de informações da galáxia no MISP por meio de ServiceNow AI Platform.
4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultado
O comentário foi atualizado com sucesso em MISP servidor.

Gerenciar eventos no MISP

Você pode criar eventos em MISP automática ou manualmente a partir do ServiceNow AI Platform. Você também pode editar os dados do evento em MISP em ServiceNow AI Platform.

Verificando eventos criados automaticamente em MISP

Você pode verificar os eventos criados automaticamente depois de configurar o perfil de criação de evento em seu ServiceNow AI Platform instância.

Perfil de criação automática de eventos

Configurar o perfil de criação automática de eventos é feito pelas funções de usuário sn_si.admin ou sn_ti.admin no **Integração MISP** > **Perfis automáticos de criação de evento** módulo.

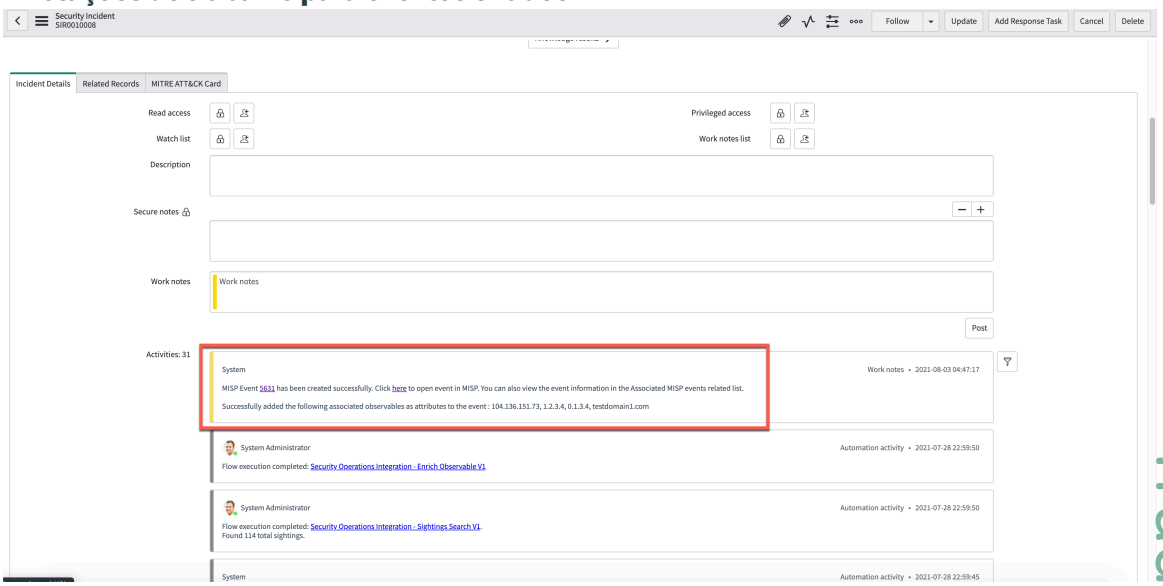
Exibindo o. MISP dados do evento

Você pode exibir os eventos criados das seguintes maneiras:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

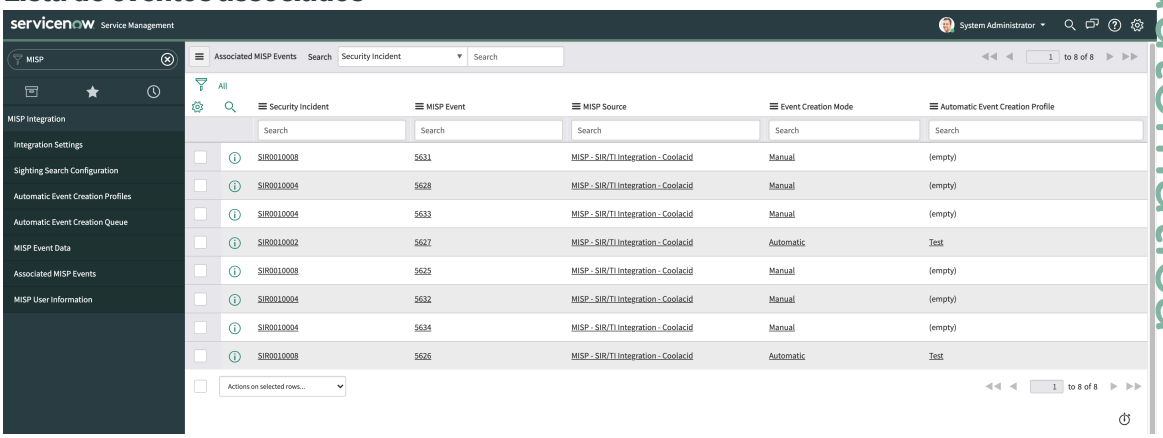
- Exiba as anotações de trabalho dos eventos criados. Você pode exibir os detalhes do evento em ServiceNow AI Platform e também como aparece em MISP servidor conforme mostrado no exemplo a seguir.

Anotações de trabalho para eventos criados



- Clique em Eventos MISP associados lista relacionada. Aqui, você pode exibir o evento em relação ao incidente de segurança e ao MISP recursos conforme mostrado no exemplo a seguir.

Lista de eventos associados

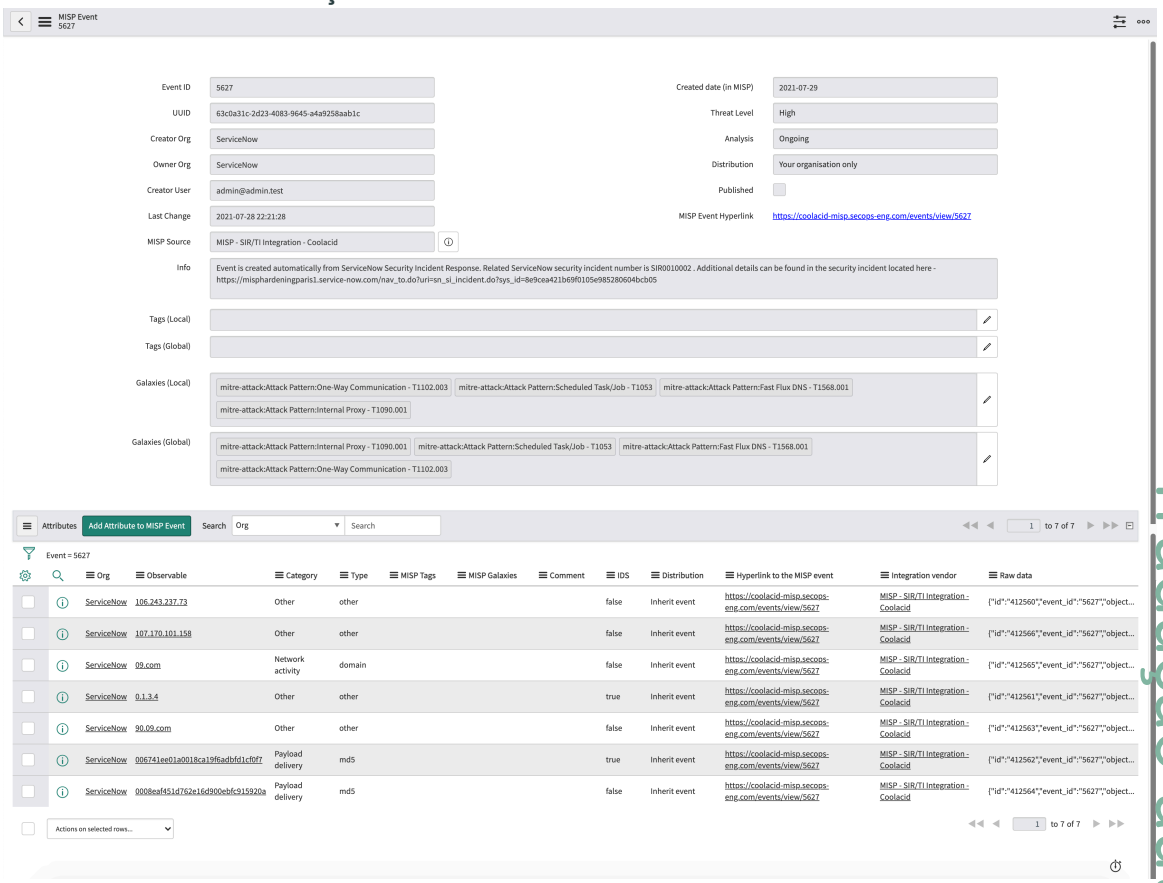


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exiba MISP dados do evento na exibição de formulário para revisar as informações detalhadas sobre MISP eventos conforme mostrado no exemplo a seguir.

Dados do evento na exibição do formulário



Criar manualmente um evento no MISP

Criar eventos manualmente em MISP em ServiceNow AI Platform capturar informações contextualmente relacionadas representadas como atributos e objetos.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar um evento.
3. Clique em **Crie um novo evento no MISP** .
4. Na caixa de diálogo Criar um novo evento no MISP, preencha os detalhes.

Criar um evento na caixa de diálogo MISP

Campo	Descrição
Data	Data de criação do evento em MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informações do evento	Informações do evento que são criadas automaticamente a partir do ServiceNow AI Platform Resposta a incidentes de segurança.
Nível de ameaça	Nível de risco do evento. Você pode categorizar os incidentes em três categorias de ameaça diferentes (baixa, média, alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções: ◦ Baixo: Malware geral em massa ◦ Médio: Ameaças persistentes avançadas (APT) ◦ Alto: APTs sofisticados e ataques de 0 dias
Origem	MISP origem da criação do evento.
Distribuição	Opção que controla quem pode exibir este evento após a publicação do evento. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos. A configuração mais restritiva vence. As opções de distribuição são as seguintes: ◦ Somente sua organização: Permite que somente os membros de sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, em que somente sua organização tem acesso para exibi-lo. Os eventos com esta configuração não são sincronizados. ◦ Somente esta comunidade: Habilita usuários que fazem parte do seu MISP para exibir o evento, incluindo sua própria organização,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
		organizações neste MISP e organizações que executam MISP servidores que sincronizam com este servidor. Todas as outras organizações conectadas a servidores vinculados estão impedidas de exibir o evento. ○ Comunidades conectadas: Habilita os usuários que fazem parte do seu MISP para exibir o evento, incluindo todas as organizações neste MISP servidor, todas as organizações em MISP servidores que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que esteja a dois saltos de distância. Todas as outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância deste servidor estão impedidas de exibir o evento. ○ Todas as comunidades: Compartilha o evento com todos MISP comunidades.
Análise		Fase atual da análise do evento com as seguintes opções possíveis: ○ Inicial: A análise está apenas começando ○ Em andamento: A análise está em andamento ○ Concluído: A análise está concluída
Opções avançadas	Adicionar observáveis associados do SIR como atributos ao evento MISP	Opção para adicionar observáveis disponíveis em um incidente de segurança a um MISP evento como atributos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
		Esta opção habilita **Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada** opção.
	Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Observável marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
	Filtrar observáveis com base em marcadores de segurança	Opção para filtrar os observáveis com base nos marcadores de segurança selecionados. Esta opção fornece a capacidade de distinguir e gerenciar os eventos MISP na inteligência contra ameaças. **Marcadores de segurança** : Adicione marcadores para filtrar os observáveis. Por exemplo, se você estiver adicionando um marcador chamado "Bloquear compartilhamento" ou "TLP: Branco", se um dos observáveis tiver algum desses marcadores associados, esses observáveis não serão adicionados como um atributo ao evento MISP durante a criação do evento MISP.
	Sincronizar técnicas MITRE ATT&CK de incidentes de segurança como galáxias locais com evento MISP	Opção para sincronizar o. ServiceNow AI Platform SIR incidente de segurança MITRE-ATT&CK™ galáxias locais no MISP evento.
	Sincronizar técnicas de incidente de segurança MITRE ATT e CK como galáxias globais para evento MISP	Opção para sincronizar o. ServiceNow AI Platform SIR incidente de segurança MITRE-ATT&CK™ galáxias globais em MISP evento.
	Adicionar marcadores ao evento MISP	Opção que permite adicionar marcadores MISP aos eventos criados a partir da ServiceNow. Esta opção exibe as seguintes opções:

Tradução automática

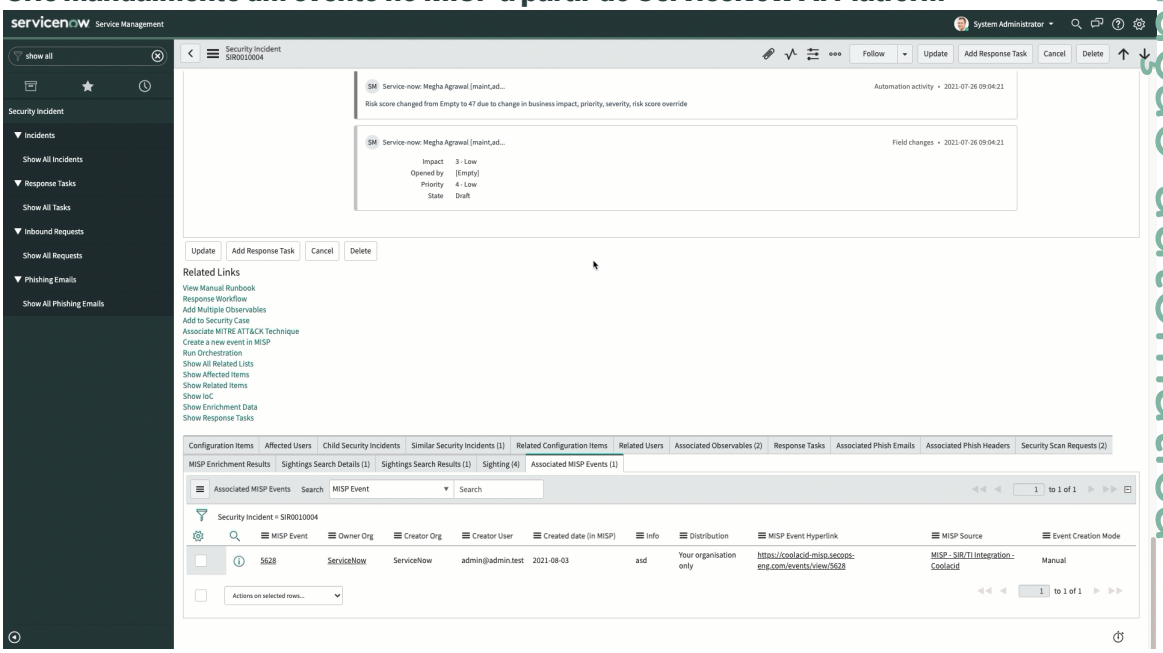
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
		○ **Local (marcadores):** Os marcadores selecionados serão adicionados como marcadores locais ao evento MISP. ○ **Global (marcadores):** Os marcadores selecionados serão adicionados como marcadores globais ao evento MISP.

5. Clique em **Novo evento MISP** .

O exemplo a seguir mostra isso criando um evento em MISP, você pode exibir os resultados no incidente de segurança. Você também pode exibir as anotações de trabalho, o evento em ServiceNow AI Platform e o evento em MISP servidor conforme mostrado no exemplo a seguir.

Crie manualmente um evento no MISP a partir do ServiceNow AI Platform



Você pode exibir os resultados das seguintes maneiras:

- Uma mensagem de sucesso aparece na parte superior da página do incidente de segurança. Você pode exibir os detalhes do evento em ServiceNow AI Platform e também como aparece em MISP servidor.
- Nas anotações de trabalho, você pode exibir a mensagem de sucesso com mais detalhes. Você também pode exibir os detalhes do evento em ServiceNow AI Platform e também como aparece em MISP servidor.
- Em Eventos MISP associados lista relacionada, você pode exibir o evento em relação ao incidente de segurança e ao MISP recursos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione atributos a um MISP evento

Adicione atributos a um evento, como o tipo, a categoria e outras informações contextuais sobre o evento.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Verifique se o evento que você está adicionando ou atualizando o atributo pertence à mesma organização que MISP usuário.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Tudo** > **MISP** > **Eventos de MISP associados**.
   Você também pode navegar até a lista relacionada ao evento MISP associado em qualquer incidente de segurança.
2. Clique no evento MISP ao qual você deseja adicionar um atributo.
3. Clique em **Adicionar atributo ao evento MISP** .
4. Na caixa de diálogo Adicionar atributo ao evento, preencha os detalhes.

Caixa de diálogo Adicionar atributo à caixa de diálogo do evento

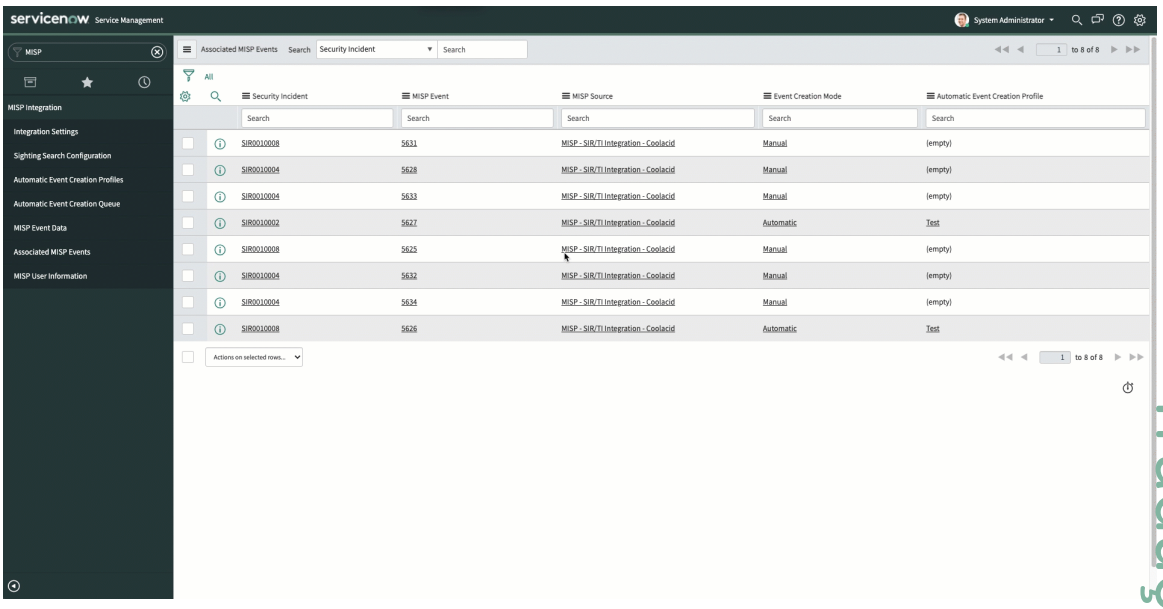
Campo	Descrição
Valor	Valor real do atributo. Insira dados sobre o valor baseado no que é válido para o tipo de atributo escolhido. Por exemplo, para um atributo do tipo ip-src (endereço IP de origem), 11.11.11.11 é um valor válido. **Nota:** Você só pode selecionar atributos ou observáveis que compartilham contexto com o evento. Os observáveis ainda não podem ter um atributo em MISP.
Categoria	Categoria do atributo. A categoria descreve o aspecto do malware para este atributo. Um exemplo seriam os mecanismos de persistência do malware ou da atividade de rede.
Tipo	Tipo que explica a categoria. Por exemplo, se um invasor usar um endereço IP para um ataque, um endereço de e-mail de origem ou um arquivo enviado por meio de um anexo poderão descrever a entrega de carga de um malware. Esses tipos de atributos têm a categoria de entrega de carga.
Distribuição	Usuários que podem exibir este atributo. A distribuição é herdada por atributos. A configuração mais restritiva vence.
Usar atributo como uma assinatura de IDS	Observável marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Comentários	Comentários que você adiciona aos atributos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo a seguir mostra que, navegando na lista Eventos MISP associados, você pode exibir o registro de evento 5627 e adicionar atributos ao evento. Os atributos incluem o valor (testdomain.com), categoria como análise externa, tipo como domínio. Você também pode habilitar o IDS. A mensagem de sucesso no registro do evento mostra que o atributo foi adicionado ao evento conforme mostrado no exemplo a seguir.

Adicione atributo a um evento MISP



5. Clique em **Adicionar atributo ao evento MISP** .

Resultado

Você pode exibir o atributo adicionado na seção Atributos.

Adicione marcadores a um MISP evento

Adicionar marcadores em ServiceNow AI Platform MISP para classificar eventos ou atributos. Você pode usar a marcação globalmente para habilitar sua classificação ou usar marcadores localmente quando não quiser MISP eventos a serem modificados durante sua classificação.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar o. MISP recursos bidirecionais.
- Verifique se o evento que você está editando pertence à mesma organização que MISP usuário.
- Observe que os marcadores e galáxias que estão disponíveis para você são baseados em MISP origem e suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém o evento ao qual você deseja adicionar marcadores.
3. Clique em **Mostrar todas as listas relacionadas** E a lista relacionada Resultados de aprimoramento do MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no ID do evento na lista de resultados de aprimoramento.
   Você também pode navegar do **MISP** > **Eventos de MISP associados** módulo.
5. Revise o registro de evento MISP.

Exibição do formulário de evento do MISP

Campo	Descrição
ID do evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para MISP servidor.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento no MISP instância.
Organização do proprietário	Organização responsável pelo evento no MISP instância. Este campo está visível somente para administradores.
Usuário do criador	Usuário que criou o evento em MISP.
Última Mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez em MISP servidor.
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média, alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: ○ Baixo: Malware geral em massa ○ Médio: Ameaças persistentes avançadas (APT) ○ Alto: APTs sofisticados e ataques de 0 dias
Análise	Fase atual da análise do evento com as seguintes opções possíveis: ○ Inicial: A análise está apenas começando ○ Em andamento: A análise está em andamento ○ Concluído: A análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifica os usuários que se inscreveram nos alertas de evento.
Hiperlink de evento MISP	Link para MISP evento armazenado no MISP servidor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informação	Descrição resumida do evento.
Marcadores (local)	Marcadores que estão disponíveis na organização host MISP instância para habilitar marcação para sincronização e filtragem de exportação. MISP os eventos não são modificados quando você usa marcadores locais. Marcadores locais são sempre removidos antes de serem sincronizados com outros MISP e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outros MISP e comunidades de compartilhamento. Quando você adiciona marcadores globais a. MISP, você pode modificar eventos.
Galáxias (local)	Galáxias que estão disponíveis na organização host MISP instância para filtragem de sincronização e exportação. MISP os eventos não são modificados quando você usa galáxias locais. Estas galáxias locais são sempre despojadas antes de serem sincronizadas com outras MISP e comunidades de compartilhamento.
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP e comunidades de compartilhamento. Quando você adiciona galáxias globais, MISP você pode modificar eventos.

6. Para editar um marcador local ou global, clique no ícone de edição em uma das seguintes opções:

   - **Marcadores (local)**
   - **Marcadores (global)**

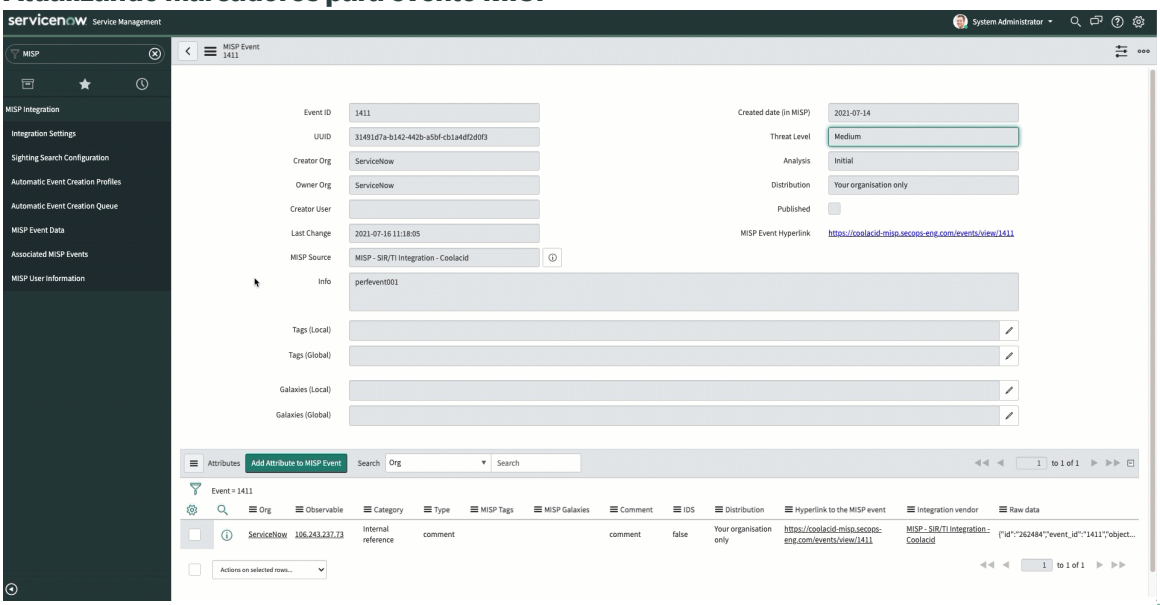
7. Na caixa de diálogo Marcadores de evento MISP, insira o nome do marcador para pesquisar e adicionar os marcadores.
8. Clique em **Atualizar marcadores para evento MISP** .

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores estão atualizados no MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizando marcadores para evento MISP



9. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Resultado

Os marcadores foram atualizados com sucesso no MISP servidor.

Atualize galáxias para A. MISP evento ou atributo

Adicione ou remova galáxias em ServiceNow AI Platform MISP para que você possa classificar esses objetos como um cluster no MISP e anexe-as a. MISP eventos ou atributos.

Antes de Iniciar

- Revise MISP função e permissões do usuário necessário para usar o. MISP recursos bidirecionais.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do correspondente MISP servidor.
- Os marcadores e galáxias disponíveis para você são baseados em MISP origem e suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Clique no ícone de edição em uma das seguintes opções.

- **Galáxias (local)**
- **Galáxias (global)**

2. Na caixa de diálogo Galaxies de evento MISP, digite e pesquise para adicionar os marcadores.

3. Clique em **Atualizar galáxias para evento MISP** .

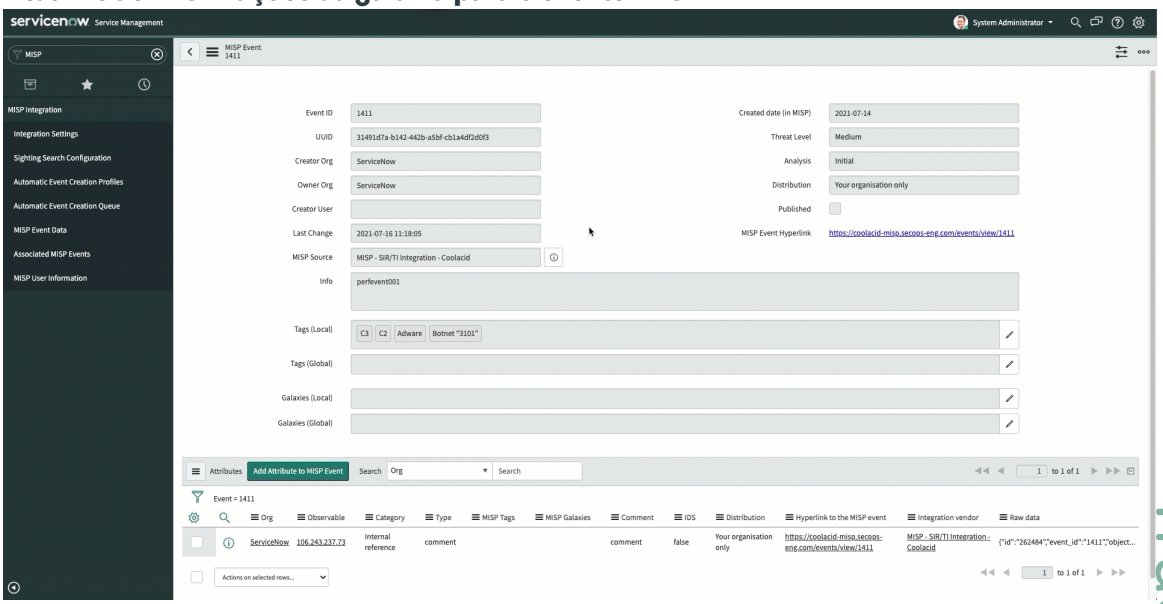
O exemplo a seguir mostra como clicar no ícone de edição das galáxias locais, selecionar o namespace descontinuado, selecionar a galáxia Ataque empresarial - padrão de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ataque e adicionar informações de cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

Atualize as informações da galáxia para o evento MISP



As galáxias foram atualizadas com sucesso em MISP servidor.

4. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Acumular MITRE-ATT&CK informações usando MISP resultados de aprimoramento

Acumule os resultados de aprimoramento do MISP manualmente se você não tiver habilitado o rollup automático de MISP informações.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Use as regras de extração automática do sistema de base para importar o. MITRE-ATT&CK informações do MISP integração. . MISP integration for Security Operations apresenta dois sistemas de base MITRE-ATT&CK regras de extração de técnica para MISP- MISP galáxias e. MISP marcadores. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte Extrair automaticamente regras de técnica para importar informações DO MITRE-ATT&CK .

Se você tiver habilitado rollup automático de MITRE-ATT&CK informações usando MISP resultados de aprimoramento para um incidente de segurança, as informações são acumuladas automaticamente. Se você não habilitou o rollup automático, poderá executar esta tarefa manualmente.

Procedimento

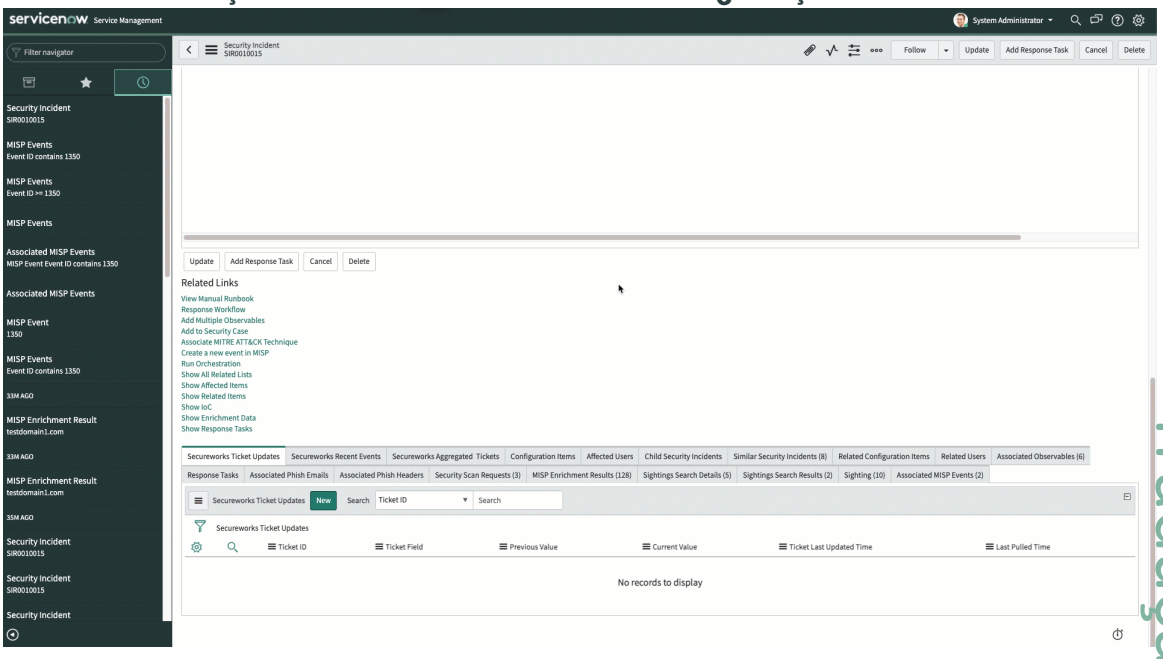
1. Navegar até **Tudo** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja enriquecer com MITRE-ATT&CK informações.
3. Clique em **Mostrar todas as listas relacionadas** e o. **Resultados de aprimoramento do MISP** guia.
4. Selecione o observável e, no menu Ações, clique em **Acumular informações DO MITRE ATT&CK para SI** .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode selecionar vários observáveis e, em seguida, acumular as informações.

5. Para confirmar as mudanças, clique em **Recarregar** .
   O exemplo a seguir mostra como selecionar um observável e acumular o. MISP resultados de aprimoramento para o incidente de segurança.

Acumule informações DO MITRE em um incidente de segurança



Resultado

Você pode exibir MITRE-ATT&CK Cartão para confirmar que os resultados de aprimoramento do MISP foram acumulados para o incidente de segurança.

Integração do OPSWAT Metadaga

OPSWAT Metadefender Permite que os dados de ameaças, detectados pelo scanner Metadender de terceiros, sejam baixados para o. Inteligência contra ameaças aplicação para acompanhamento, priorização e resolução.

Explorar	Configuração
• OPSWAT Metadefender visão geral da integração • Integrações do Inteligência contra ameaças	Ativar e configurar o. OPSWAT Metadefender integração
Usar	**Desenvolver**
Realizar pesquisas em observáveis	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

OPSWAT Metadefender visão geral da integração

OPSWAT Metadefenderé uma solução de segurança que fornece acesso a várias máquinas antimalware e se integra facilmente ao Operações de segurança.

Antes de poder usar OPSWAT Metadefender integração, você deve ativar o plug-in e configurar a integração. Se necessário, você também pode atualizar sua certificação SSL X509.

Pesquisa de ameaças - Fluxo do OPSWAT Metdefender

O fluxo Pesquisa de ameaças - OPSWAT Metdefender executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo OPSWAT Metadender, os observáveis serão verificados em busca de malware e os resultados serão retornados.

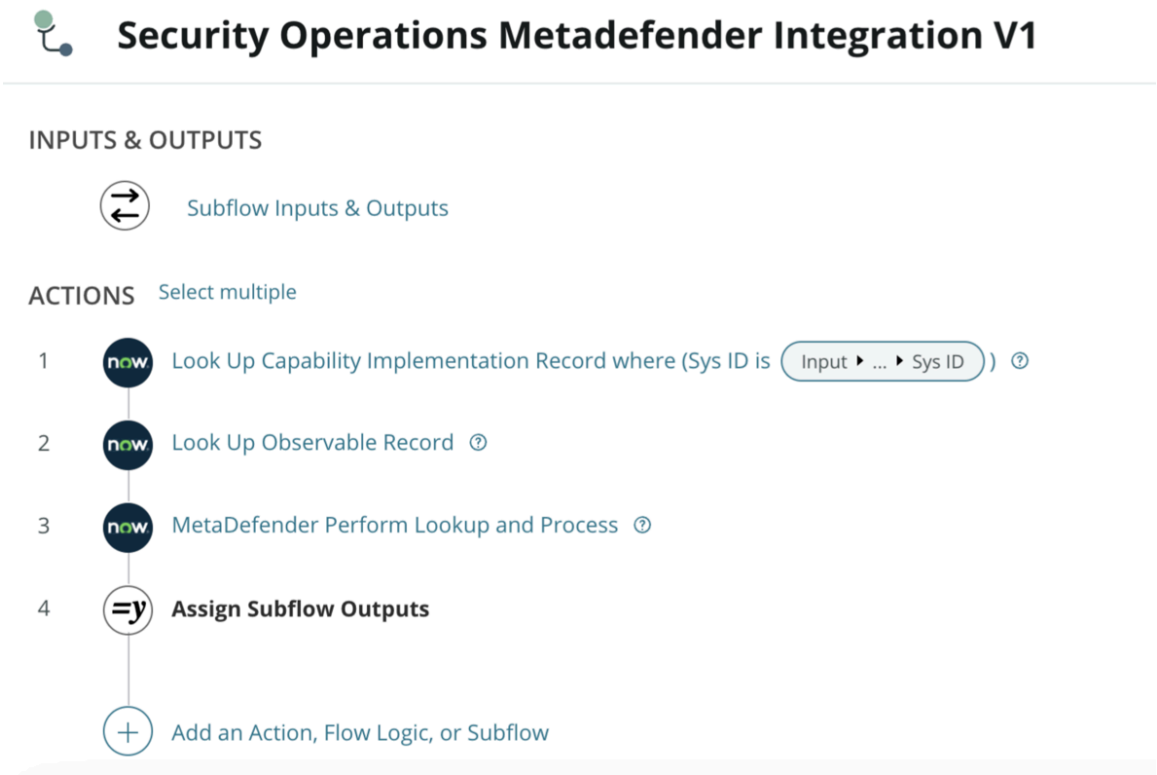
Este fluxo é acionado pelo Integração de operações de segurança - Recurso de pesquisa de ameaças Quando você executa uma pesquisa de ameaça em um ou mais observáveis e a implementação OPSWAT Metadaga é selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo do OPSWAT Metdefender



Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Ativar e configurar o. OPSWAT Metadefender integração

Antes de poder usar OPSWAT Metadefender, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a integração estiver concluída, acesse o portal OPSWAT e obtenha a chave de API do Metaddefender Cloud
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão OPSWAT Metafender, clique em **Configurar** .
5. Insira (ou cole) o. **Chave de API** Adquirido do portal OPSWAT.
6. Clique em **Enviar**.

Resultado

Depois de configurado, o OPSWAT Metafider pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereços do navegador.
   Por exemplo: `https://<3rdparty>/` .

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e clique em **Segurança** guia.

   d. Clique em **Exibir certificado** e clique em **Detalhe** guia.

   e. Clique em **Exportação** Para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Deve começar com `------ INICIAR CERTIFICADO------` e termine com `------ CERTIFICADO FINAL-------` .

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e. crie um novo registro para a integração.
4. Em **Certificado PEM** cole o certificado baixado e copiado para a área de transferência anteriormente.
5. Adicione o certificado ao registro do Provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até **Certificados X.509** lista relacionada e clique em **Editar** .
   d. Mova o certificado recém-criado para **Selecionado** coluna.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

   Nota: Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituição de um certificado SAML prestes a expirar .

Integração do VirusTotal

. VirusTotal A integração permite que você solicite a análise de endereços IP suspeitos, arquivos, hashes de arquivo e endereços de URL para ajudar na investigação e determinar se eles são mal-intencionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar	Configurar
Integrações do Inteligência contra ameaças	• VirusTotal configuração de integração • Ativar e configurar a integração do VirusTotal

Usar	Desenvolver
• Realizar pesquisas em observáveis • Pesquisa de ameaças - Fluxo de trabalho do VirusTotal	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

VirusTotal configuração de integração

VirusTotal É um serviço gratuito que analisa arquivos e URLs suspeitos e facilita a deteção rápida de vírus, worms, cavalos de troia e todos os tipos de malware. Ele se integra facilmente ao Operações de segurança.

Antes de poder usar VirusTotal, você deve ativar o plug-in e adicionar a chave de API apropriada. Se necessário, você também pode atualizar sua certificação SSL X509.

. VirusTotal a origem da pesquisa é usada e o malware é encontrado, um observável é criado. Para pesquisas de IP, uma lista adicional de URLs que compartilham o endereço IP é criada e observáveis são criados para cada um dos URLs.

Nota:

- . Inteligência contra ameaças o plug-in é necessário para implementar VirusTotal integração.
- . VirusTotal A integração foi atualizada para as APIs da versão 3.

Ativar e configurar a integração do VirusTotal

Antes de usar a integração do VirusTotal, você deve baixá-lo do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

Inteligência contra ameaças Deve ser instalado e ativado antes que você possa usar o VirusTotal. . VirusTotal A integração foi atualizada para as APIs da versão 3.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse o VirusTotal e obtenha a chave de API no seu perfil VirusTotal.
3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão VirusTotal, clique em **Configurar** .

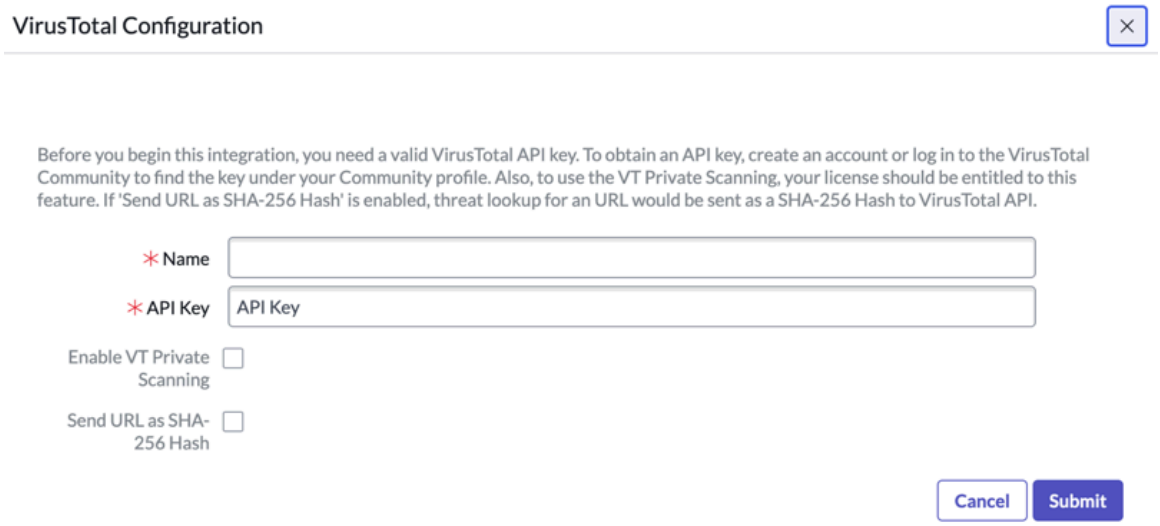
Configuração virtual

Campo	Descrição
Nome	Nome da integração. Por exemplo, VirusTotal.
Chave de API	Insira (ou cole) o. **Chave de API** Adquirido do site VirusTotal.
Habilitar verificação privada de VT	Marque esta caixa de seleção para analisar arquivos com o VirusTotal de forma a preservar a privacidade. Os arquivos carregados por meio desta oferta não serão compartilhados com ninguém além da sua organização e permanecerão no VirusTotal somente por um breve período de tempo. As análises resultantes também serão efêmeras e visíveis somente para o seu grupo VirusTotal. **Importante:** Para usar a Varredura privada de VT, sua licença do VirusTotal deve ter direito a esse recurso.
Enviar URL como hash SHA-256	Marque esta caixa de seleção para enviar os URLs como hashes para pesquisa de ameaças e proteger a privacidade dos usuários na integração. **Nota:** Se desabilitado, o URL será enviado como codificação Base64 para a API VirusTotal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.



Resultado

Depois de configurado, o VirusTotal pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Pesquisa de ameaças - Fluxo de trabalho do VirusTotal

A Pesquisa de ameaças - VirusTotal o fluxo de trabalho executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por VirusTotal, os observáveis são verificados em busca de malware e os resultados são retornados.

Antes de Iniciar

Função necessária: administrador

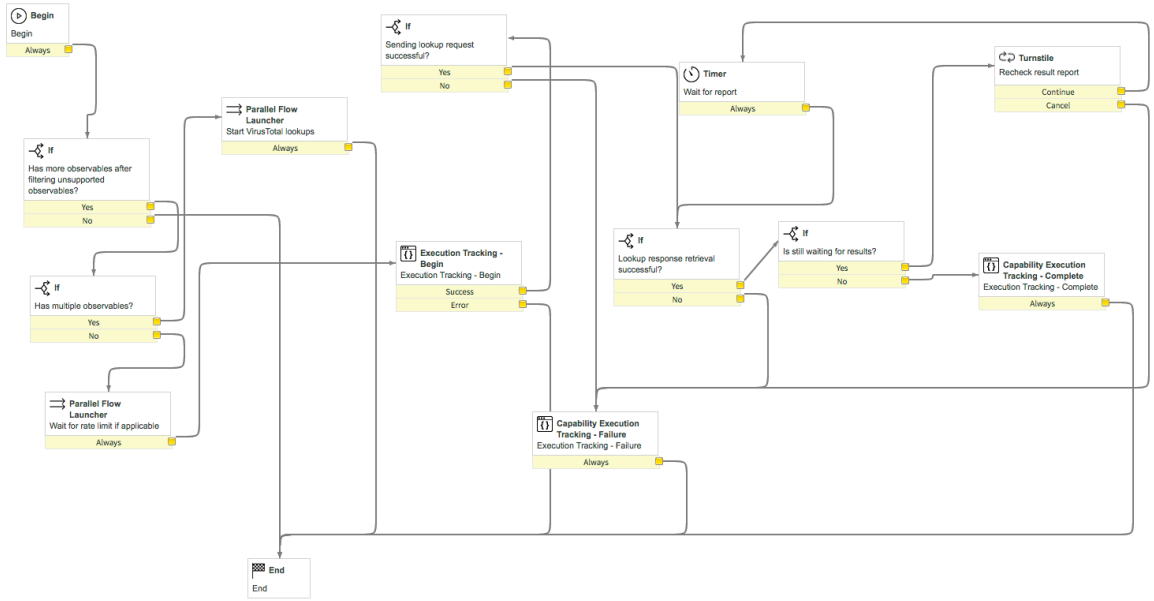
Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pelo Integração de operações de segurança - Recurso de pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis, e o. VirusTotal a implementação está selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo de trabalho do VirusTotal



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração da API WhoisXML

A integração da API WhoisXML permite que você envie pesquisas Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

Explorar

Integrações do Inteligência contra ameaças

Configurar

- Configuração de integração da API WhoisXML
- Ativar e configurar a integração do Whois de operações de segurança

---

Usar

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IOC

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Encontre componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Ou responda perguntas na comunidade de Operações de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configuração de integração da API WhoisXML

Antes de usar a integração do Whois, você deve ativar o plug-in e adicionar as credenciais. Se necessário, você também pode atualizar sua certificação SSL X509.

. Inteligência contra ameaças E os plug-ins de integração da API WhoisXML são necessários para implementar a integração da API WhoisXML.

Ativar e configurar a integração do Whois de operações de segurança

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração Whois de operações de segurança. Antes de usar a integração do Whois de operações de segurança, você deve baixá-lo do ServiceNow Store E você deve ter uma conta válida da API WhoisXML.

Antes de Iniciar

Inteligência contra ameaças Deve ser instalado e ativado antes que você possa usar a integração do Whois de operações de segurança.

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão API Whois, clique em **Configurar** .
4. Insira o nome de usuário e a senha da sua conta da API WhoisXML.
5. Clique em **Enviar**.

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereços do navegador.
   Por exemplo: `https://<3rdparty>/` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Clique no ícone de cadeado na linha de endereço.

c. Clique em **Mais informações** e clique em **Segurança** guia.

d. Clique em **Exibir certificado** e clique em **Detalhe** guia.

e. Clique em **Exportação** Para salvar o PEM em seu sistema de arquivos local.

f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
Deve começar com `------ INICIAR CERTIFICADO------` e termine com `------ CERTIFICADO FINAL-------` .

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e. crie um novo registro para a integração.
4. Em **Certificado PEM** cole o certificado baixado e copiado para a área de transferência anteriormente.
5. Adicione o certificado ao registro do Provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até **Certificados X.509** lista relacionada e clique em **Editar** .
   d. Mova o certificado recém-criado para **Selecionado** coluna.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

> **Nota:** Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituição de um certificado SAML prestes a expirar .

Enriquecer o fluxo de trabalho do WHOIS observável

. **Enriquecer o WHOIS observável** o fluxo de trabalho executa o aprimoramento nos observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo Integração com WhoisXML API, os observáveis são enriquecidos.

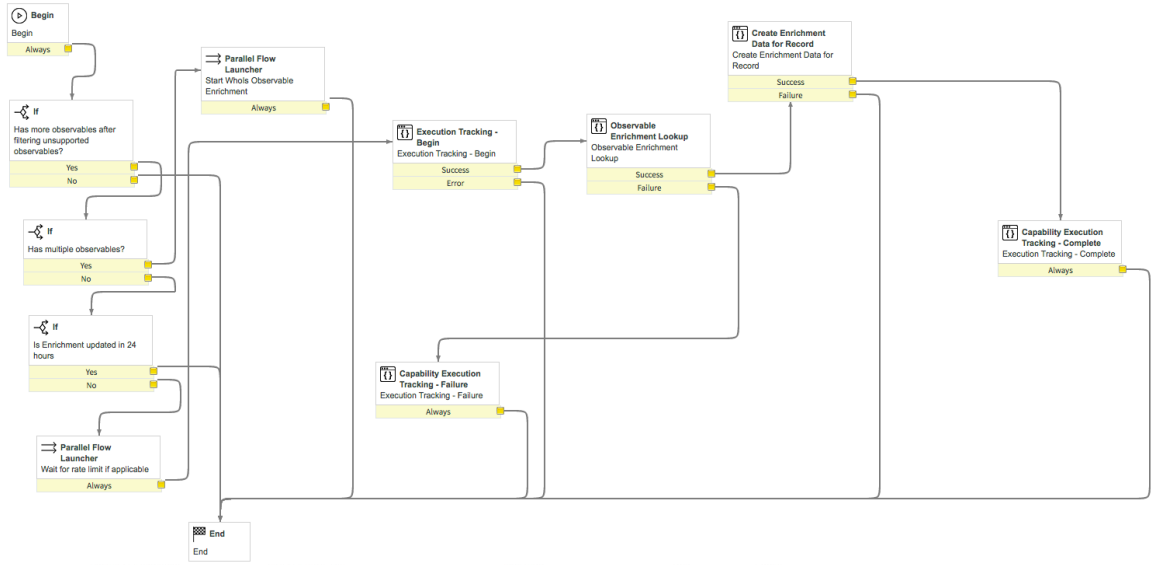
Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração de operações de segurança- Enrich a capacidade observável Quando você executa o aprimoramento em um ou mais observáveis e a implementação do WHOIS é selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enriquecer o fluxo de trabalho do WHOIS observável



As atividades específicas desta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Atividade Pesquisa de aprimoramento de observável

. **Pesquisa de aprimoramento de observável** a atividade de fluxo de trabalho inicia o processo de aprimoramento do observável.

. **Pesquisa de aprimoramento de observável** a atividade pode ser usada com qualquer fluxo de trabalho de observáveis para iniciar o aprimoramento.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	A pesquisa foi bem-sucedida.
Falha	Ocorreu um erro ao tentar executar a pesquisa. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
implementation_id	Identificador do sistema da implementação usada para executar a pesquisa.
domain_id	O identificador de domínio do domínio no qual a pesquisa está sendo realizada.
observable_ids	Um ou mais observáveis para executar a ação desejada. Os IDs são usados como uma entrada de fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
CapacidadeID de ExcutionCapabilitionExcutionId	Identificador do sistema da capacidade que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação de capacidade de integração, como Splunk, Elasticsearch.
task_sys_id	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
response_data	Dados brutos retornados pelo endpoint da API da implementação para o domínio fornecido.
mapping_id	O identificador do mapeamento de aprimoramento. Por exemplo, a integração WHOIS retorna dados em dois formatos diferentes, IP e URL, com um ID de mapeamento para cada um.

Orquestração de inteligência contra ameaças

Orquestração de inteligência contra ameaças as atividades permitem que os usuários determinem se uma ameaça foi vista antes em outros incidentes de segurança ou em outros sistemas usando a orquestração de fluxo de trabalho.

Para obter mais informações sobre edição Orquestração de Resposta a incidentes de segurança fluxos de trabalho ou criação de fluxos de trabalho personalizados, consulte Introdução aos fluxos de trabalho e. Editor de fluxo de trabalho Editor de fluxo de trabalho .

Configurar Orquestração de inteligência contra ameaças

Antes de usar Orquestração de inteligência contra ameaças Execute as etapas para configurar várias partes do sistema, incluindo preencher o CMDB, configurar o MID Server e configurar credenciais.

Antes de Iniciar

Função necessária: administrador

Para usar Orquestração de inteligência contra ameaças Você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ativar o plug-in Inteligência contra ameaças.
2. Configure o MID Server
3. Configure credenciais de serviço DO MID Server
   Agora você está pronto para usar Orquestração de inteligência contra ameaças atividades em um fluxo de trabalho.

Fluxos de trabalho e atividades da Orquestração de inteligência contra ameaças

O sistema de base inclui fluxos de trabalho e atividades de fluxo de trabalho que você pode usar para automatizar ações em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IOC

. **Inteligência contra ameaças - Executar pesquisa de IOC** o fluxo de trabalho verifica se há um observável não expirado e, em caso afirmativo, a pesquisa será definida como **Concluído** e atualizados com os dados do observável.

Antes de Iniciar

Função necessária: sn_si.basic

Nota: Este fluxo de trabalho substitui Orquestração de inteligência contra ameaças regras de negócio (**Preencha com tabelas IOC existentes** , **Enfileirar a pesquisa** e **Atualizar observável**) com atividades.

Se uma pesquisa for inserida ou atualizada e atender às condições, a regra de negócios Pesquisar acionará este fluxo de trabalho.

Por Que e Quando Desempenhar Esta Tarefa

. **Inteligência contra ameaças - Executar pesquisa de IOC** o fluxo de trabalho verifica se há um observável não expirado e, em caso afirmativo, a pesquisa será definida como **Concluído** e atualizados com os dados do observável. Todos os indicadores associados ao observável são reativados.

Se o observável expirar, o fluxo de trabalho executará as pesquisas e incrementará o. **Contagem de vistas** no observável existente expirado.

Se não existir nenhum observável correlacionado, um novo observável com indicador será criado.

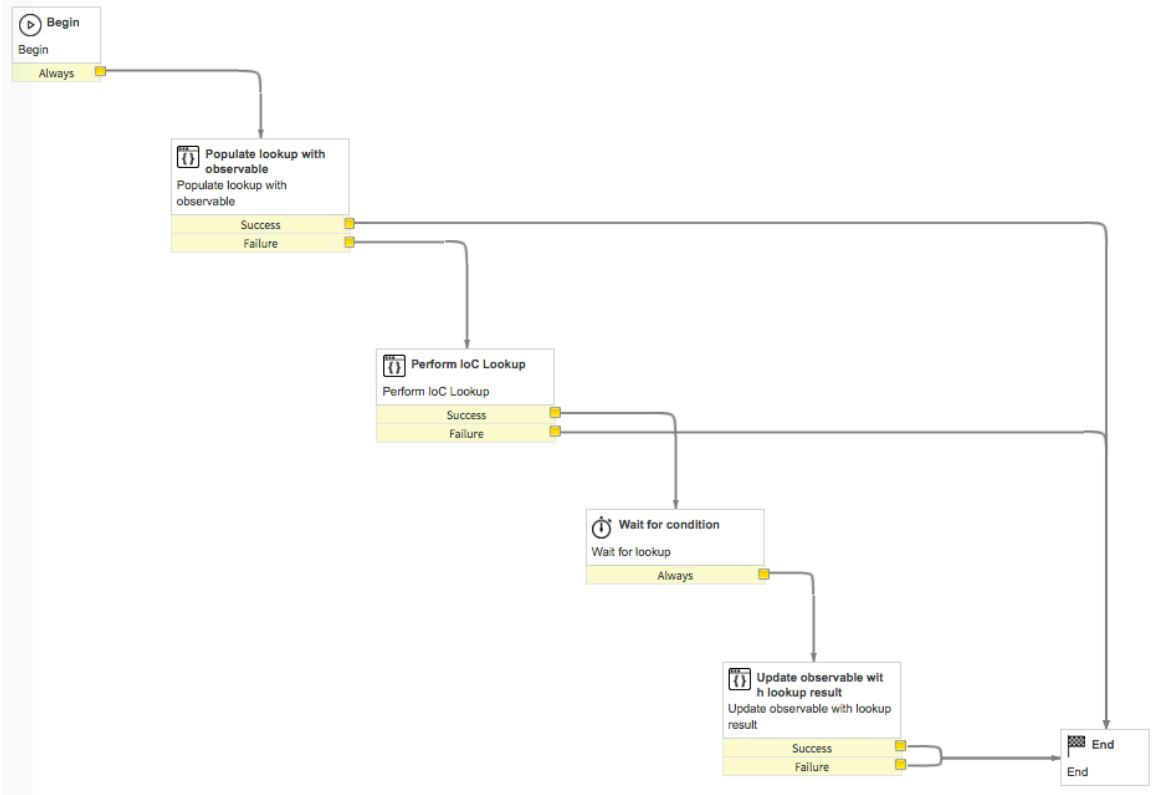
As atividades do processo de fluxo de trabalho incluem:

- Preencher pesquisa com atividade observável
- Executar atividade de pesquisa de IOC
- Aguardar pesquisa (atividade principal)
- Atualizar observável com atividade de resultado de pesquisa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IOC



Preencher pesquisa com atividade observável

Se um observável não expirado for encontrado, o. **Orquestração de inteligência contra ameaças - Preencher pesquisa com observável** a atividade de fluxo de trabalho fornece dados de um observável existente para uma pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por um fluxo de trabalho **Preencher pesquisa com observável** tenta encontrar um observável existente para uma pesquisa que corresponda a. **valor** e. **tipo** da pesquisa fornecida à atividade como entrada.

Se o observável existir e não tiver expirado, esta atividade:

- Atualiza a pesquisa com as informações encontradas no observável
- Reativa um indicador se ele estiver inativo, incrementa o. **Contagem encontrada** e atualiza o. **Visto pela última vez** data
- Conjuntos **Estado** Para concluir.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável de entrada	Descrição
ScanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída	Descrição
Verdadeiro(a)	Observável válido encontrado e pesquisa atualizada.
Falso(a)	Observável válido não encontrado. O observável está ausente ou expirou.

Executar atividade de pesquisa de IOC

. **Orquestração de inteligência contra ameaças - Executar pesquisa de IOC** a atividade de fluxo de trabalho executa uma determinada pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por um fluxo de trabalho, **Executar pesquisa de IOC** Usa um ScanID, pesquisa o registro de pesquisa e adiciona a pesquisa à fila criando uma entrada de fila de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
ScanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro(a)	Acionou a pesquisa.
Falso(a)	Não acionou a pesquisa.

Atualizar observável com atividade de resultado de pesquisa

. **Orquestração de inteligência contra ameaças - Atualize o observável com o resultado da pesquisa** a atividade de fluxo de trabalho atualiza o registro do observável. Se um não existir, ele criará um novo observável. Esta atividade é útil para registrar informações em log.

Quando acionado por um fluxo de trabalho **Atualizar observável com resultado da pesquisa** atualiza um observável existente para incluir o novo **Contagem de vistas** adiciona uma anotação e, se inativo, reativa todos os indicadores. . **Contagem encontrada** e. **Visto pela última vez** as datas no indicador também são atualizadas.

Se não houver observável correlacionado, o fluxo de trabalho criará um novo observável com o indicador da seguinte forma:

- Executa as pesquisas de IOC
- Cria um novo observável
- Cria um indicador para o observável

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adiciona um **Contagem de vistas** para o observável
- Adiciona um **Contagem encontrada** e. **Visto pela última vez** data do indicador
- Adiciona uma mensagem indicando a partir de qual pesquisa foi criada

.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
ScanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro(a)	A atualização ou criação do observável foi bem-sucedida.
Falso(a)	Falha na atualização ou criação do observável.

Atividade Executar origens de pesquisa de IOC padrão

Quando acionado por um fluxo de trabalho, Inteligência contra ameaças- **Executar origens de pesquisa de IOC padrão** Obtém um ID de solicitação de pesquisa e cria várias pesquisas dependendo dos valores de dados inseridos.

Para cada tipo de dados, o **varredura include_in_bulk** a coluna da tabela de tipo de pesquisa compatível de cada origem de pesquisa é avaliada. Se verdadeiro, uma pesquisa será adicionada à solicitação de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scan_request_id	Identificador do sistema de solicitação de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
Número de verificações criadas	Inteiro

Security Case Management

Gestão de casos de segurança fornece um meio para que os analistas de segurança envolvidos na busca de ameaças coletem informações sobre atividades suspeitas em seu ambiente. Registros relacionados a casos, como incidentes de segurança, observáveis, ICs e usuários afetados, podem ser adicionados a casos para acomodar análises amplas e específicas.

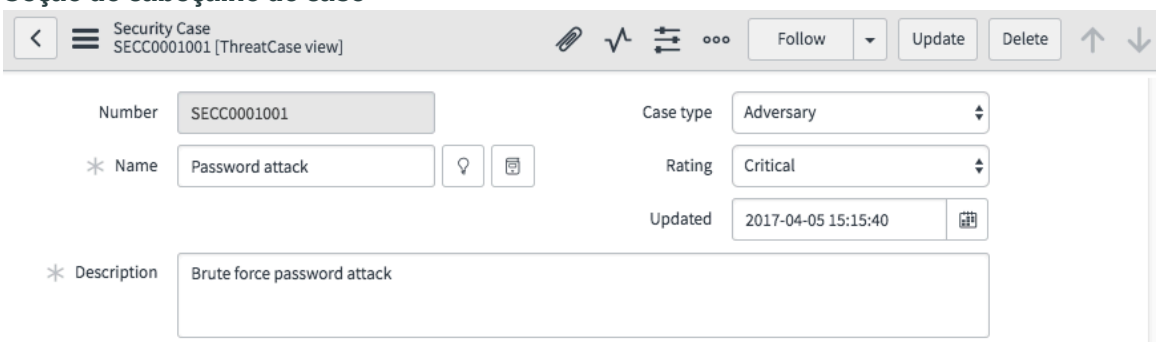
Com a capacidade de alternar facilmente os registros e as informações relacionadas, os analistas podem avaliar se estão enfrentando uma campanha direcionada, ameaça persistente avançada e assim por diante.

Casos de segurança podem ser criados a partir de várias origens em sua instância, incluindo Gestão de casos de segurança, Resposta a incidentes de segurança e Inteligência contra ameaças. Você também pode criar casos a partir de itens de configuração e usuários afetados nas tabelas Itens de configuração [cmdb.ci] e Usuários [sys.user], respectivamente. Após a criação dos casos, cada uma dessas origens também pode ser usada para adicionar recursos de análise valiosos aos casos existentes.

Cada caso de segurança consiste em três seções principais, uma seção de cabeçalho, uma seção com detalhes adicionais do caso e uma seção de artefatos de caso que contém uma coleção de registros que ajudam a criar um argumento para identificar e lidar com ameaças específicas.

Cabeçalho do caso

Seção do cabeçalho do caso



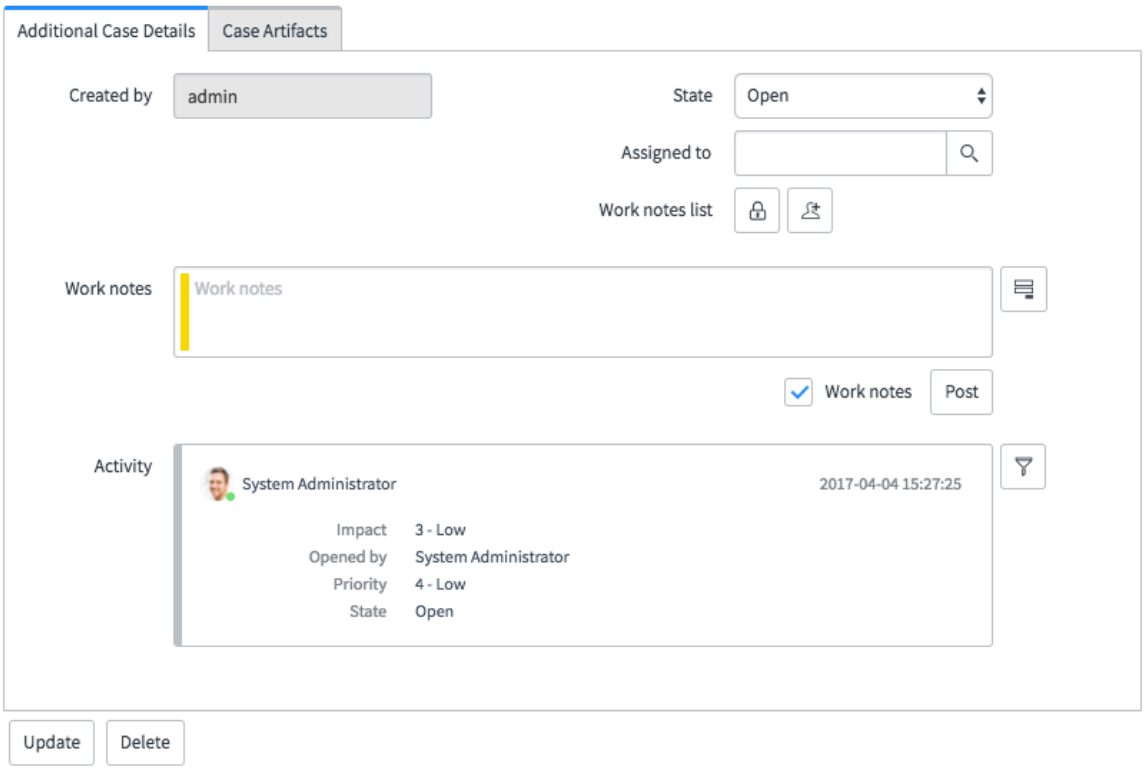
O cabeçalho do caso fornece informações básicas usadas para identificar e classificar o caso de segurança. O número do caso usa o prefixo SECC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes adicionais do caso

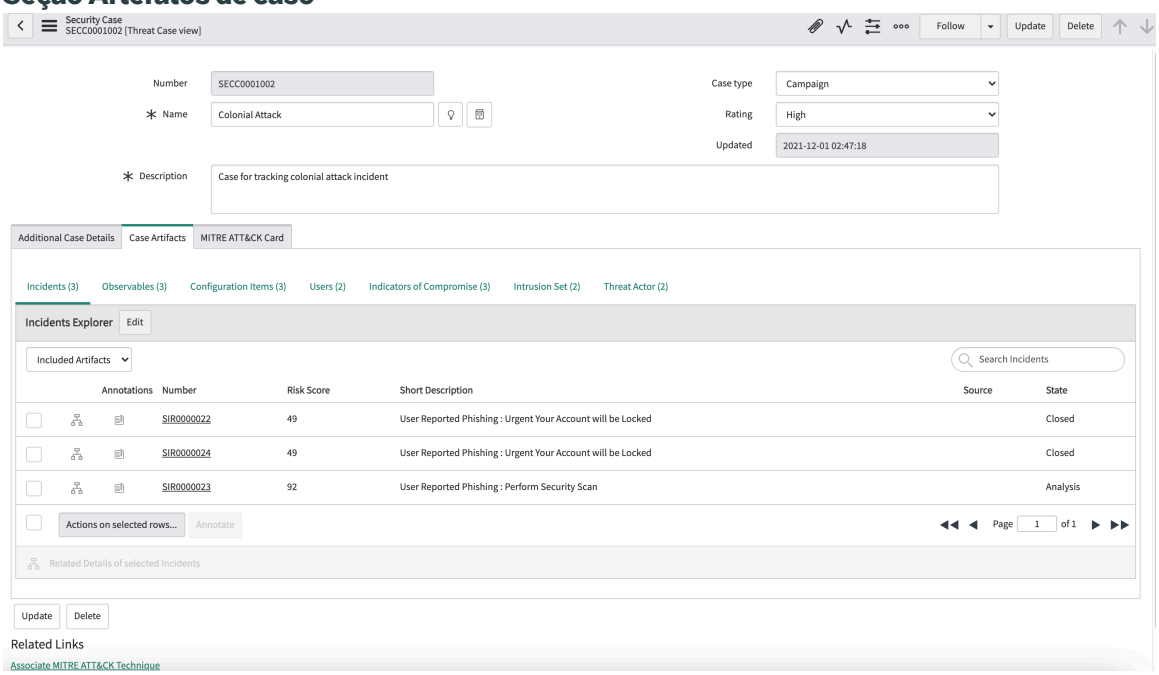
Seção Detalhes adicionais do caso



. **Detalhes adicionais do caso** a seção fornece informações específicas da análise que já foi realizada no caso, incluindo seu estado atual e anotações de trabalho e atividades registradas para o caso.

Artefatos de caso

Seção Artefatos de caso



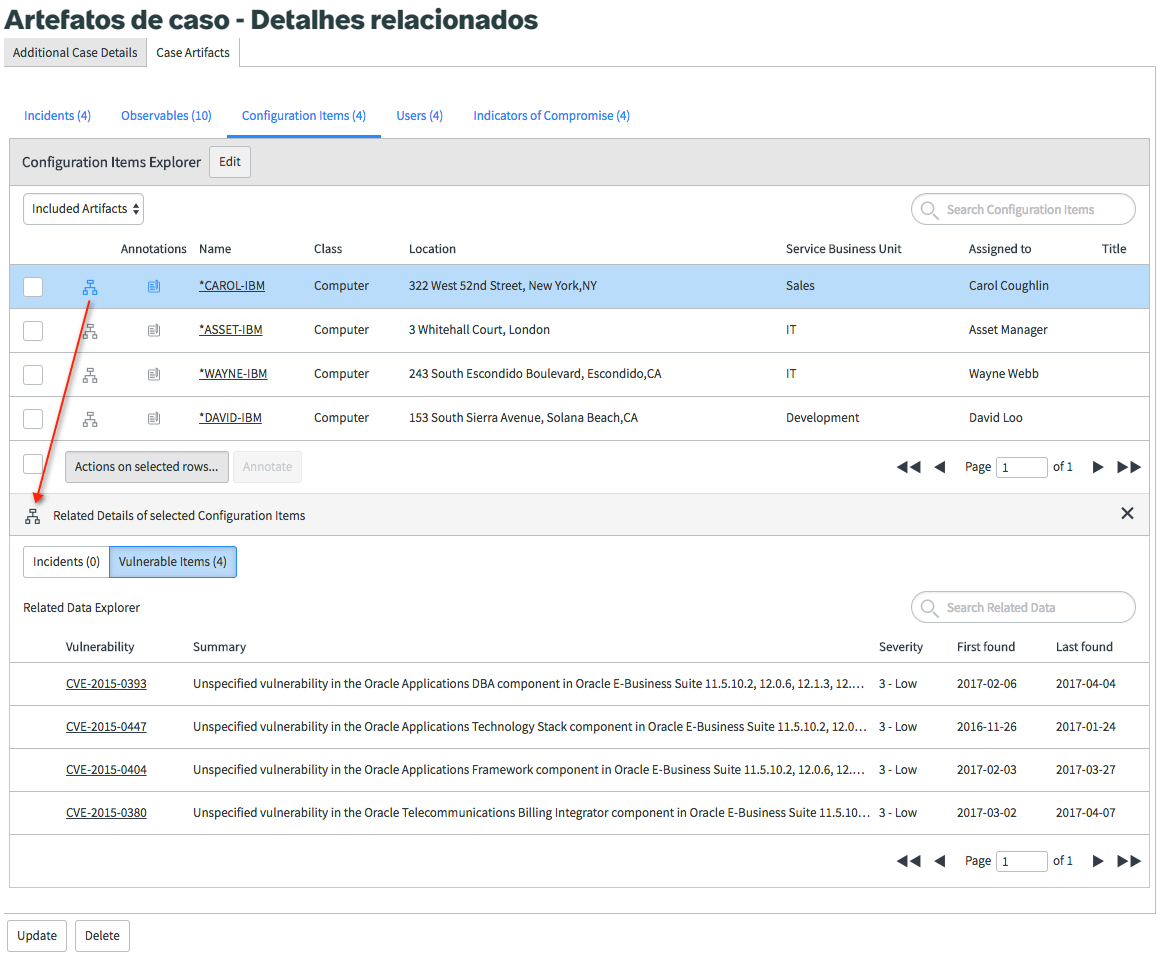
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. **Artefatos de caso** a seção fornece uma série de guias de informações contidas no caso de segurança.

Você pode executar pesquisas no conteúdo de cada guia. Você também pode excluir registros específicos que você já avaliou como seguros ou que não têm valor em sua investigação. Os registros excluídos não são excluídos, mas ficam ocultos da exibição. Se necessário, você pode exibir registros excluídos e adicioná-los novamente.

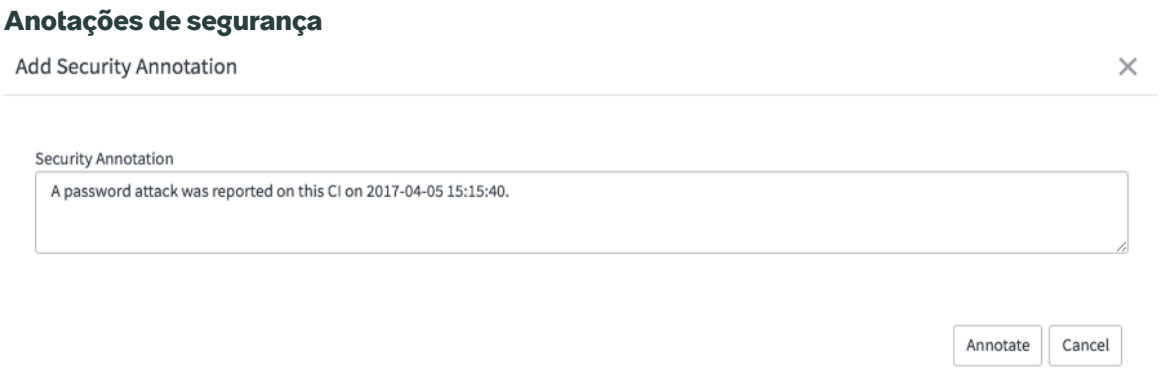
Em cada guia, você pode clicar no ícone Detalhes adicionais para mostrar informações relacionadas ao registro selecionado. Por exemplo, se você clicar em **Itens de configuração** Para exibir o Gerenciador de itens de configuração e clicar em Detalhes adicionais para um IC específico, você pode exibir incidentes, itens vulneráveis e anotações associadas a esse IC.



Você também pode selecionar um registro e clicar em **Anote** botão para um artefato relacionado ao caso para adicionar anotações ao registro. Anotações são simplesmente anotações que cada analista pode fazer em um artefato específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Outras ferramentas que o analista pode usar para examinar casos incluem:

- Execute uma pesquisa de vistas em observáveis em um caso
- PESQUISE artefatos de segurança

Criar casos no Gestão de casos de segurança

Os casos são usados para rastrear informações sobre um agente de campanha ou estado que ameaça sua organização. Depois que um caso é criado, você pode adicionar artefatos que permitem revisar e analisar todas as informações relacionadas em um único registro de caso.

Antes de Iniciar

Função necessária: sn_ti.case_use

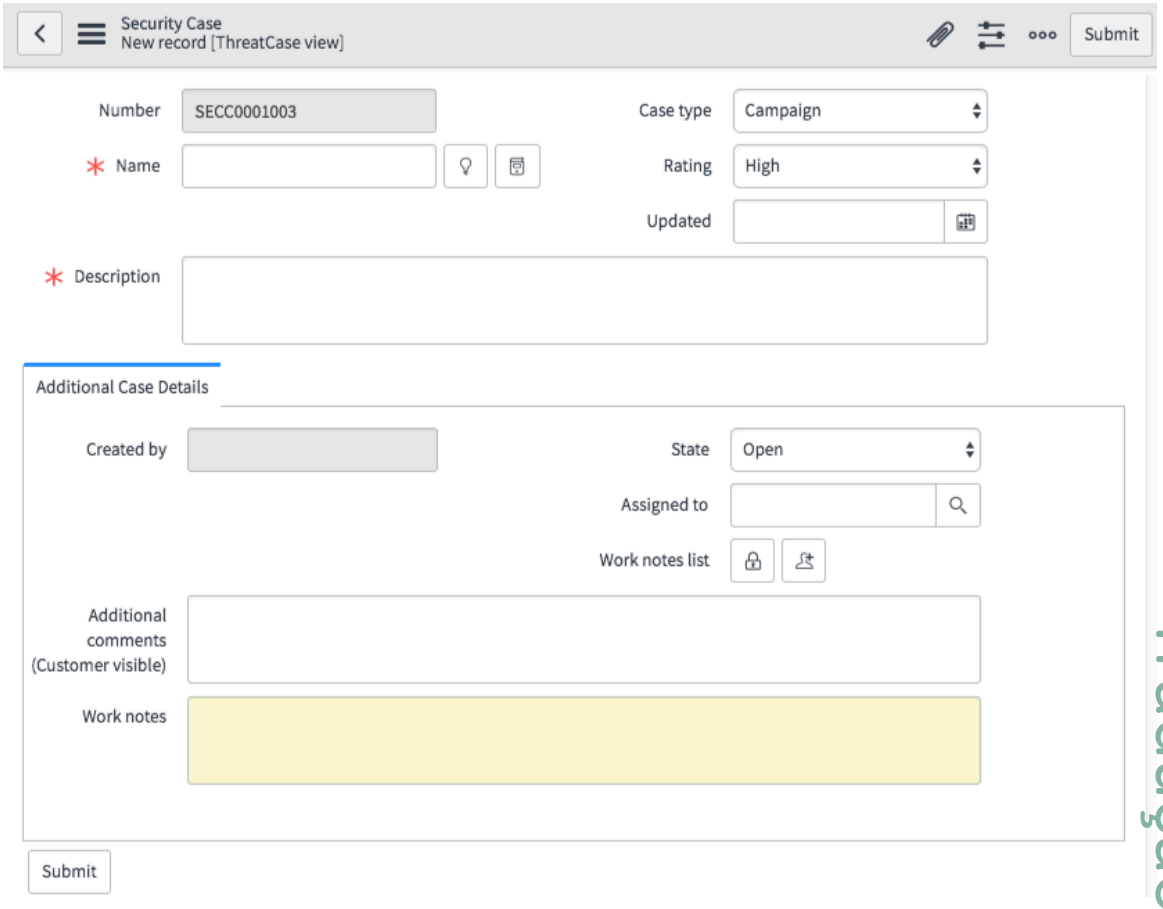
r

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Clique em **Nova**.
   A tela Casos de segurança é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



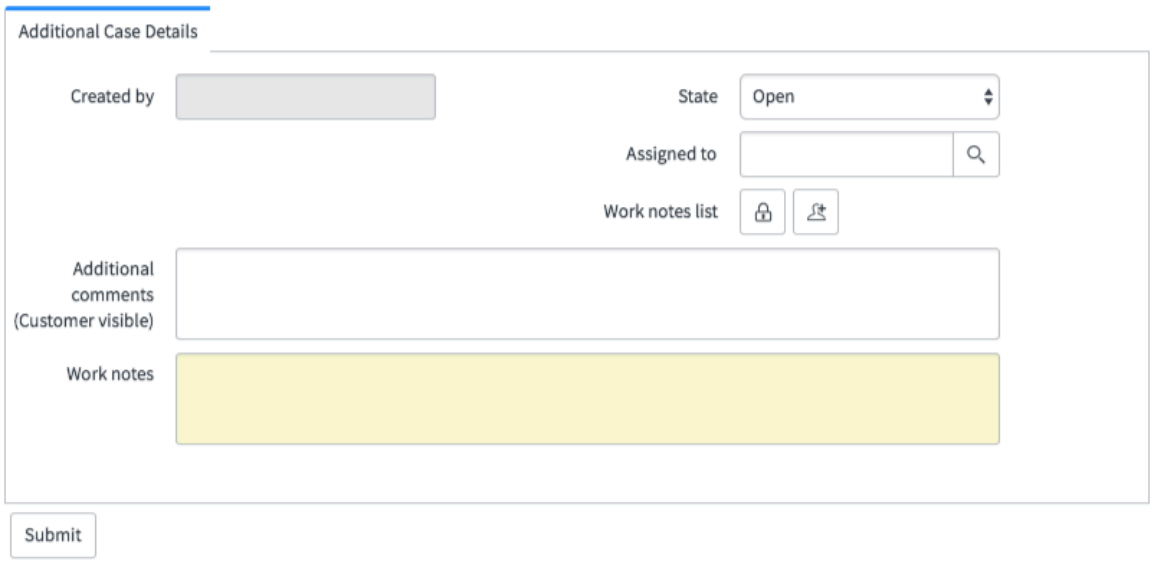
3. Preencha os campos, se for o caso.

Campo	Descrição
Número do caso	[Somente leitura] O número do caso.
Nome de Caso	Insira um nome descritivo para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Classificação	Selecione a importância deste caso (de Crítico a Baixo).
Última atualização	[Somente leitura] A data e hora em que o caso foi atualizado pela última vez.
Descrição Resumida	Uma breve descrição do caso.

4. Clique em **Detalhes adicionais do caso** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, se for o caso.

Campo	Descrição
Criada por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o estado é padronizado como Rascunho.
Atribuição a	Clique no ícone de pesquisa e atribua o caso a um analista.
Lista de anotações de trabalho	Clique no ícone de cadeado e adicione usuários internos que podem exibir anotações de trabalho.
Comentários adicionais	Conforme necessário, insira anotações sobre o caso que ficarão visíveis para o cliente.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso.

6. Clique em **Enviar**.
Depois que o registro for salvo, você pode clicar em **Artefatos de caso** guia e. adicione artefatos ao caso .

Adicionar artefatos a um caso

Depois de criar um caso, você pode adicionar artefatos, como incidentes de segurança, ICs e indicadores de comprometimento, ao caso. Esses artefatos atuam como pistas na resolução do caso.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

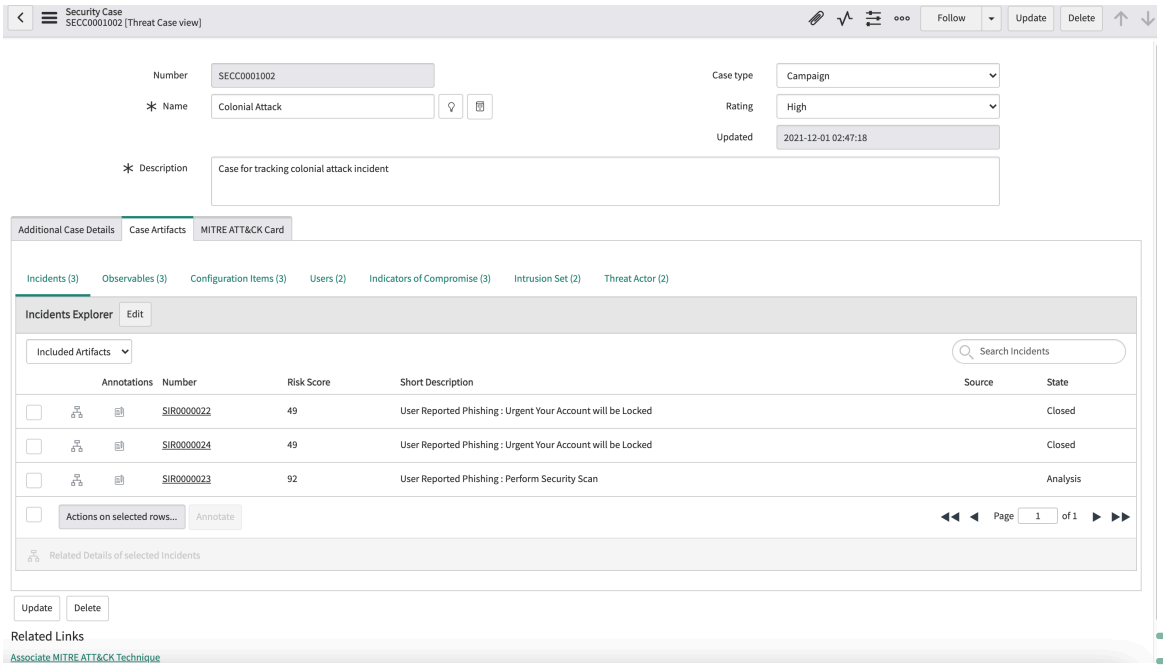
Procedimento

1. Abra um caso ao qual você deseja adicionar artefatos.

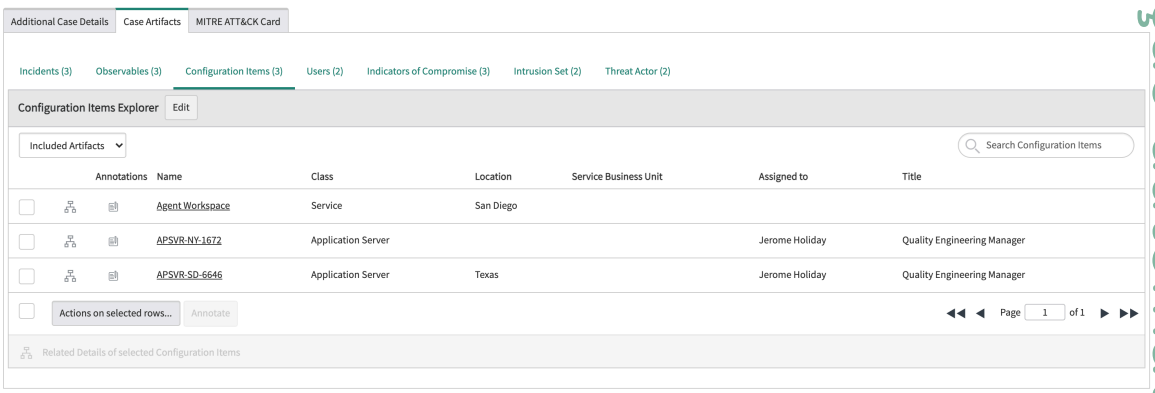
2. Clique em **Artefatos de caso** lista relacionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



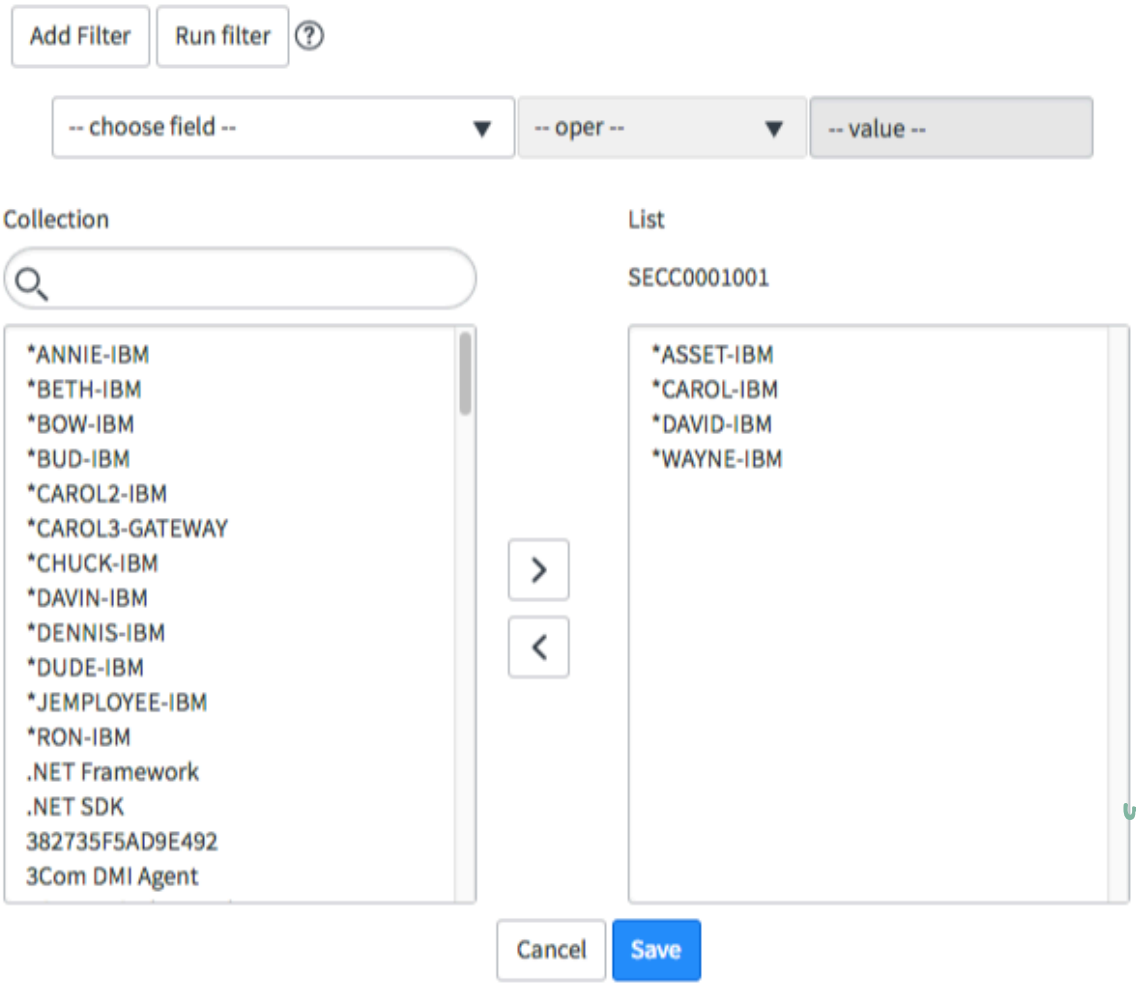
3. Clique na guia associada ao tipo de artefato que você deseja adicionar ao caso.
Por exemplo, clique em **Itens de configuração** Para adicionar um ou mais ICs ao caso.



4. Clique em **Editar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Usando a caixa de listagem e os filtros, localize os registros de artefato que você deseja adicionar ao caso, mova-os do bucket de coleção para o bucket de lista e clique em **Salvar** .
   A lista aparece na guia Selecionado e os artefatos selecionados são adicionados à lista.

Tópicos relacionados

- Adicione IOCs e observáveis a um caso existente
- Adicionar incidentes de segurança a um caso existente
- Adicionar ICs a casos existentes
- Adicione usuários afetados a casos existentes

Associar MITRE-ATT&CK informações com caso de segurança

Associar MITRE-ATT&CK táticas e técnicas para um caso de segurança para melhor gestão de casos de segurança e análise de ameaças em um nível granular.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja enriquecer com as informações DO MITRE-ATT&CK.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

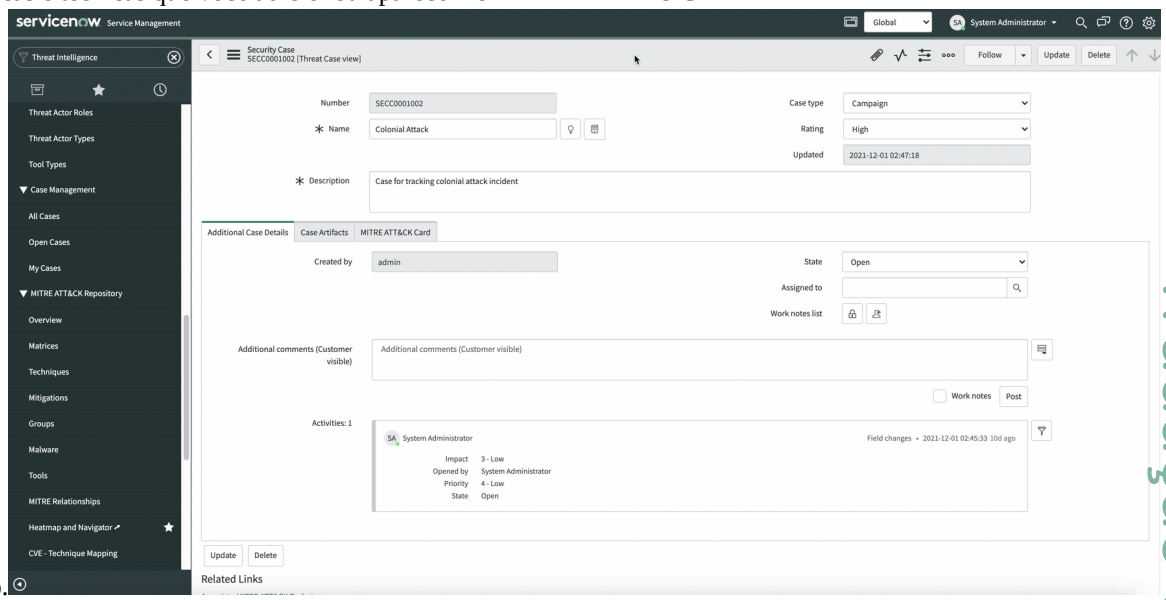
3. Na lista relacionada, clique em **Associar técnica MITRE ATT&CK** .

   Na ilustração a seguir, você pode ver como navegar da lista relacionada para **Associar técnica MITRE ATT&CK** , revise a origem e adicione uma tática e uma técnica.

4. Nas listas de origem, revise **Origem** .

5. Revise **Tática** e. **Técnicas** e adicione ou remova-os com base na relevância com o caso.

6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem em MITRE-ATT&CK Cartão.



Tradução automática

Criação de caso a partir de artefatos de segurança

Além de criar casos manualmente a partir de Gestão de casos de segurança você também pode criar casos a partir de artefatos de segurança, como incidentes de segurança, indicadores de comprometimento, usuários afetados e itens de configuração.

IOCs e observáveis em casos

Em Inteligência contra ameaças, Você pode criar casos de IOCs e observáveis, bem como adicionar IOCs e observáveis a casos existentes. Você também pode criar observáveis diretamente de um caso.

Crie um caso a partir de IOCs ou observáveis

Em Inteligência contra ameaças, Você pode criar um caso a partir de artefatos (IOCs ou observáveis). Depois que os IOCs ou observáveis tiverem sido usados para criar um caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

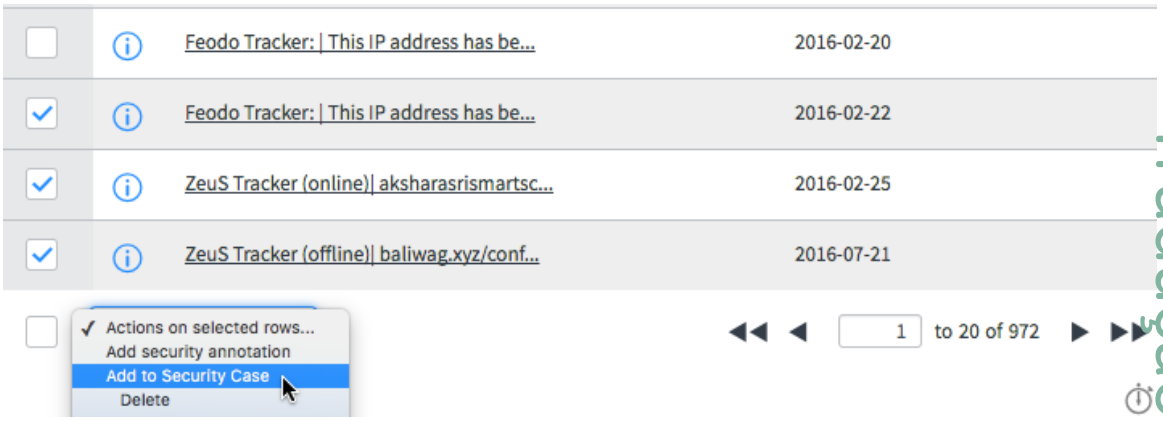
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

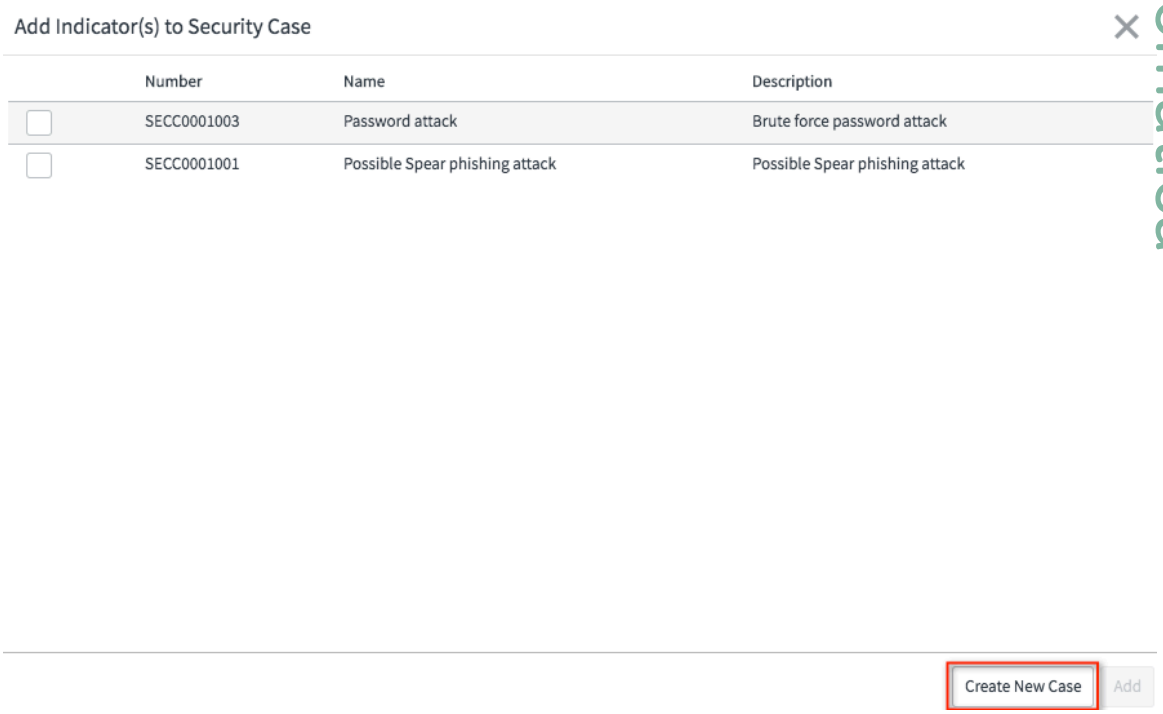
1. Navegue até os artefatos (IOCs ou observáveis) que você deseja usar para criar um caso.
   - Para criar um caso do IOCs, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para criar um caso a partir de observáveis, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os artefatos que você deseja adicionar a um novo caso.

   Nota: Se você selecionar vários IOCs ou observáveis, todos eles serão adicionados ao caso.

3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .



. **Adicionar ao Caso de segurança** a caixa de diálogo é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique em **Criar Novo Caso** .
5. Preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicione IOCs e observáveis a um caso existente

Você pode adicionar IOCs e observáveis a casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

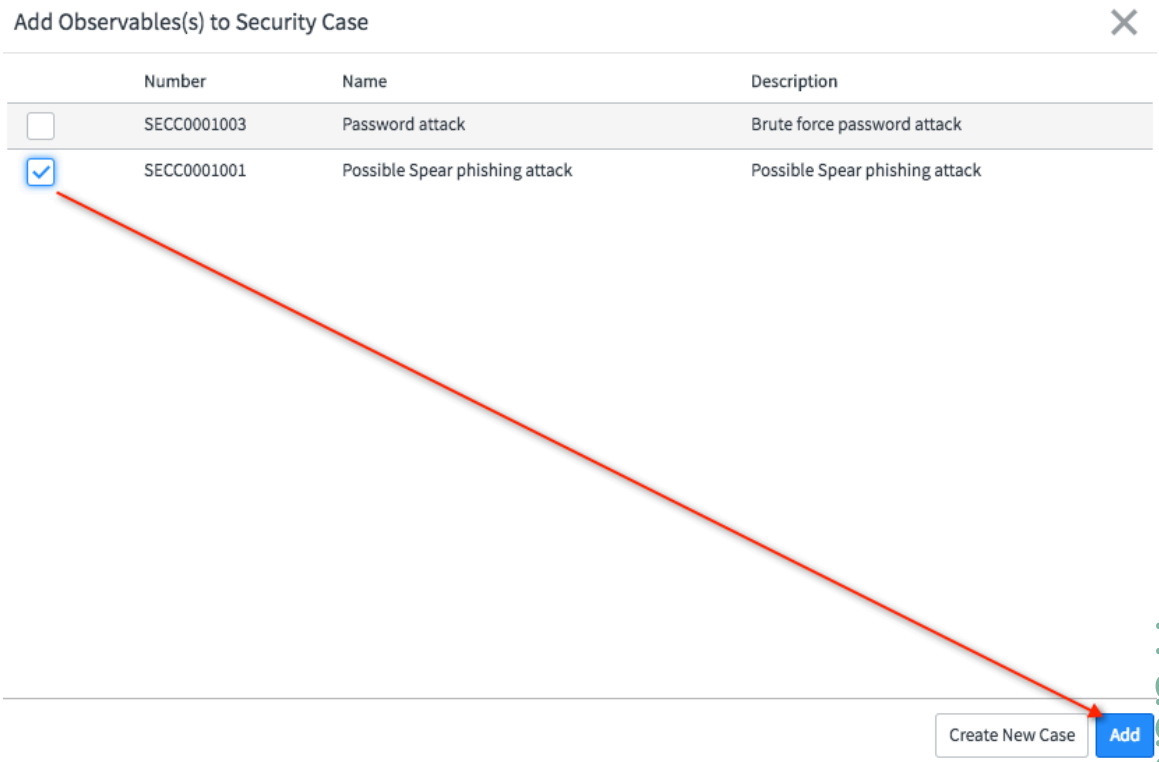
1. Navegue até os artefatos (IOCs ou observáveis) que você deseja adicionar aos casos existentes.
   - Para adicionar IOCs a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para adicionar observáveis a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os registros de artefato que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários casos, os IOCs ou observáveis selecionados serão adicionados a cada um dos casos selecionados.

3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .
   . **Adicionar ao Caso de segurança** a caixa de diálogo é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.
4. Selecione os casos aos quais você deseja adicionar os IOCs ou observáveis selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Crie um observável a partir de um caso

Novos observáveis podem ser criados a partir de casos em Gestão de casos de segurança.

Antes de Iniciar

Função necessária: sn_ti.case_user

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Abra um caso existente ou clique em **Novo** . crie um novo caso .
3. Clique em **Artefatos de caso** link relacionado e clique em **Observáveis** guia.
4. Clique em **Novo** e insira as informações solicitadas.

Campo	Descrição
Valor	[Somente leitura] O número do caso.
Tipo de observável	Insira um nome descritivo para o caso.
Categoria de tipo de observável	Selecione o tipo de caso que está sendo investigado.
Contagem de incidentes	Selecione a importância deste caso (de Crítico a Baixo).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descoberta	[Somente leitura] A data e hora em que o caso foi atualizado pela última vez.
Anotações	Uma breve descrição do caso.

5. Clique em **Detalhes adicionais do caso** guia.
6. Preencha os campos, se for o caso.

Campo	Descrição
Criada por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o estado é padronizado como Rascunho.
Lista de anotações de trabalho	Clique na caixa de seleção para exibir as anotações de trabalho na seção Detalhes adicionais do caso do registro do caso.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso. . **Lista de anotações de trabalho** Estiver selecionado, a anotação de trabalho aparecerá na seção Detalhes adicionais do caso do registro do caso.

7. Clique em **Enviar**.
   Conforme necessário, você pode clicar em **Artefatos de caso** guia e. adicione artefatos ao caso .

Execute uma pesquisa de vistas em observáveis em um caso

Você pode pesquisar observáveis usando o recurso Pesquisa de vistas para determinar com que frequência eles ocorrem. Cada ocorrência é considerada uma *vista* . Você pode limitar a pesquisa ao número de vistas em um número selecionado de dias ou em um intervalo de datas.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

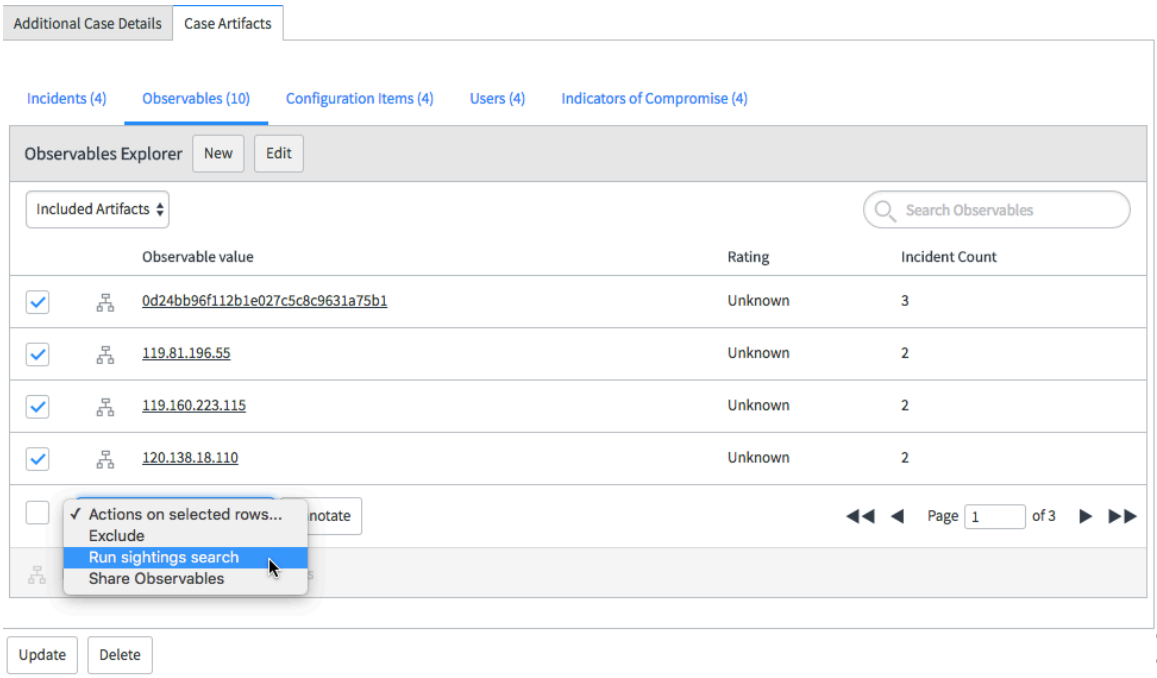
Função necessária: sn_ti.case_user_write

Procedimento

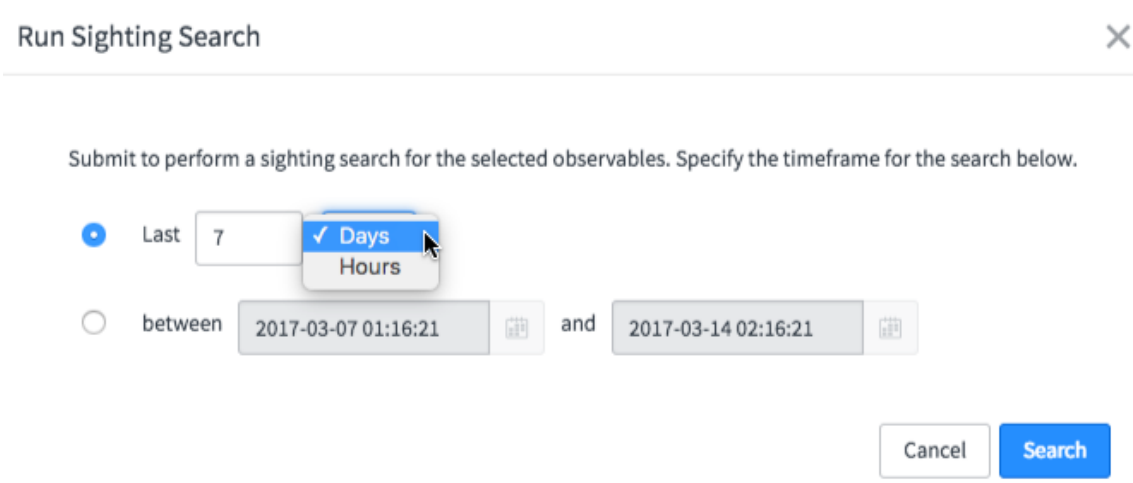
1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Abra o caso que contém observáveis para os quais você deseja executar uma pesquisa de vistas.
3. Clique em **Artefatos de caso** link relacionado.
4. Clique em **Observáveis** guia.
5. Selecione um ou mais observáveis cujos avistamentos você deseja pesquisar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Em **Ações nos itens selecionados** lista suspensa, selecione **Executar pesquisa de vistas** .
. **Executar Pesquisa de vistas** a caixa de diálogo é exibida.



7. Insira o número de dias ou horas em que você deseja pesquisar as vistas dos observáveis selecionados ou selecione um intervalo de datas.
8. Clique em **Pesquisar**.

Incidentes de segurança em casos

Em Resposta a incidentes de segurança, Você pode criar casos a partir de incidentes de segurança, ICs e usuários afetados, bem como adicionar esses artefatos a casos existentes.

Crie um caso a partir de incidentes de segurança

Em Resposta a incidentes de segurança, você pode criar casos a partir de incidentes de segurança. Depois que os incidentes de segurança tiverem sido usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

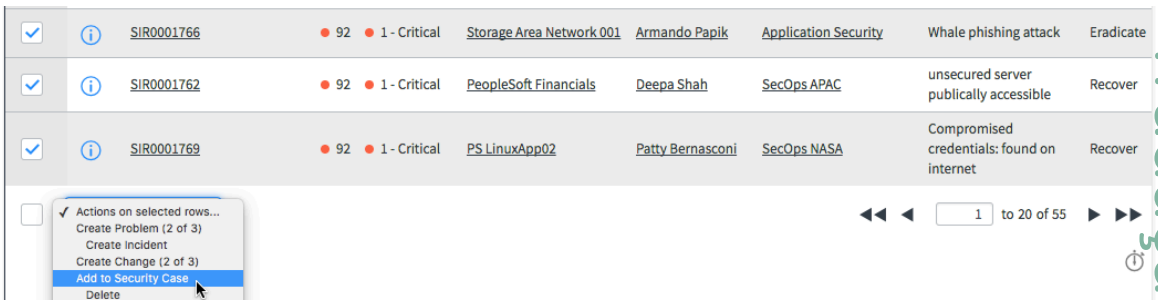
Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

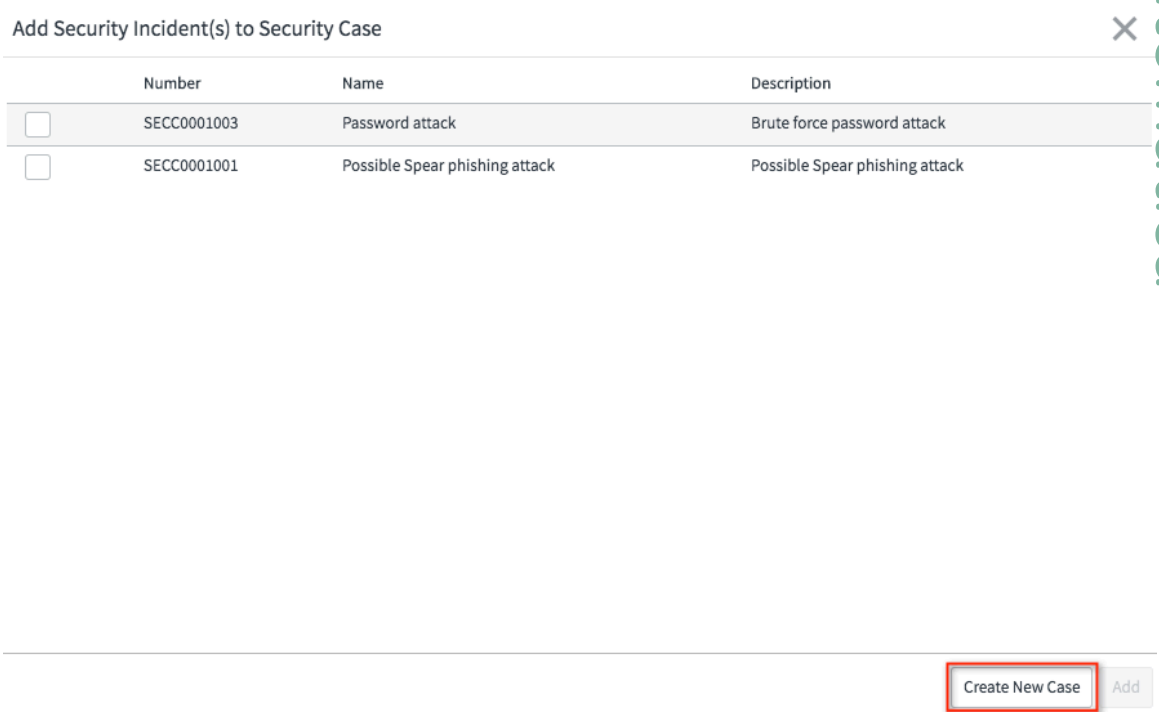
Você precisa navegar até os incidentes de segurança que deseja usar para criar casos.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar incidentes em aberto**.
   A lista Incidentes de segurança é aberta. Na lista, você pode criar um novo caso a partir de um ou mais incidentes de segurança ou selecionar um incidente de segurança específico e criar um novo caso no formulário.
2. Para criar um caso na lista, selecione os artefatos que você deseja adicionar a um novo caso.
3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .



. **Adicionar ao Caso de segurança** a caixa de diálogo é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique em **Criar Novo Caso** .
5. Preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicionar incidentes de segurança a um caso existente

Você pode adicionar incidentes de segurança a um ou mais casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os incidentes de segurança que deseja adicionar aos casos existentes.

Procedimento

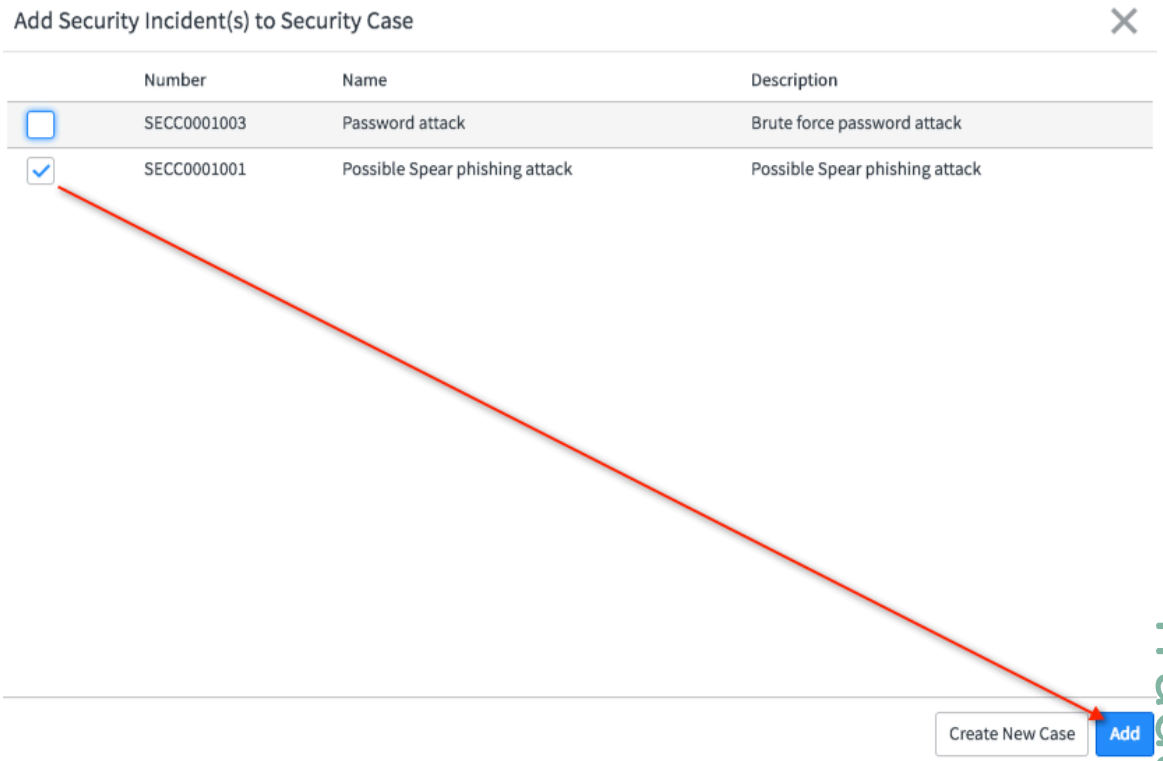
1. Navegar até **Tudo** > **Incidente de segurança** > **incidentes** > **Mostrar incidentes em aberto**.
   A lista Incidentes de segurança é aberta.
2. Na lista, selecione um ou mais incidentes de segurança que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários incidentes de segurança, os incidentes de segurança selecionados serão adicionados a cada um dos casos selecionados.

3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .
   . **Adicionar ao Caso de segurança** a caixa de diálogo é aberta e exibe os casos atribuídos a você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione os casos aos quais você deseja adicionar os incidentes de segurança selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Itens de configuração em casos

Você pode criar um novo caso a partir de um ou mais itens de configuração (IC) na tabela Item de configuração [cmdb_ci]. Você também pode adicionar ICs a casos existentes.

Crie um caso a partir de ICs

Você pode criar um caso de segurança a partir de itens de configuração na tabela Item de configuração [cmdb_ci]. Depois que os ICs forem usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os itens de configuração que deseja usar para criar um caso.

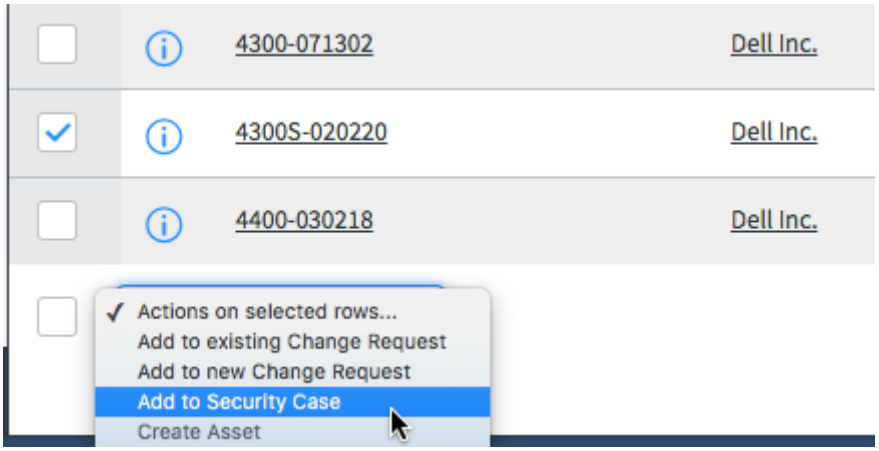
Procedimento

1. Navegar até **Tudo** > **Configuração** > **Itens de Base** > **Computadores** Para exibir ICs para computadores.
   A lista do tipo de IC selecionado é aberta. Na lista, você pode criar um novo caso a partir de um ou mais ICs ou selecionar um IC específico e criar um novo caso no formulário.
2. Na lista, selecione os ICs que você deseja adicionar a um novo caso.

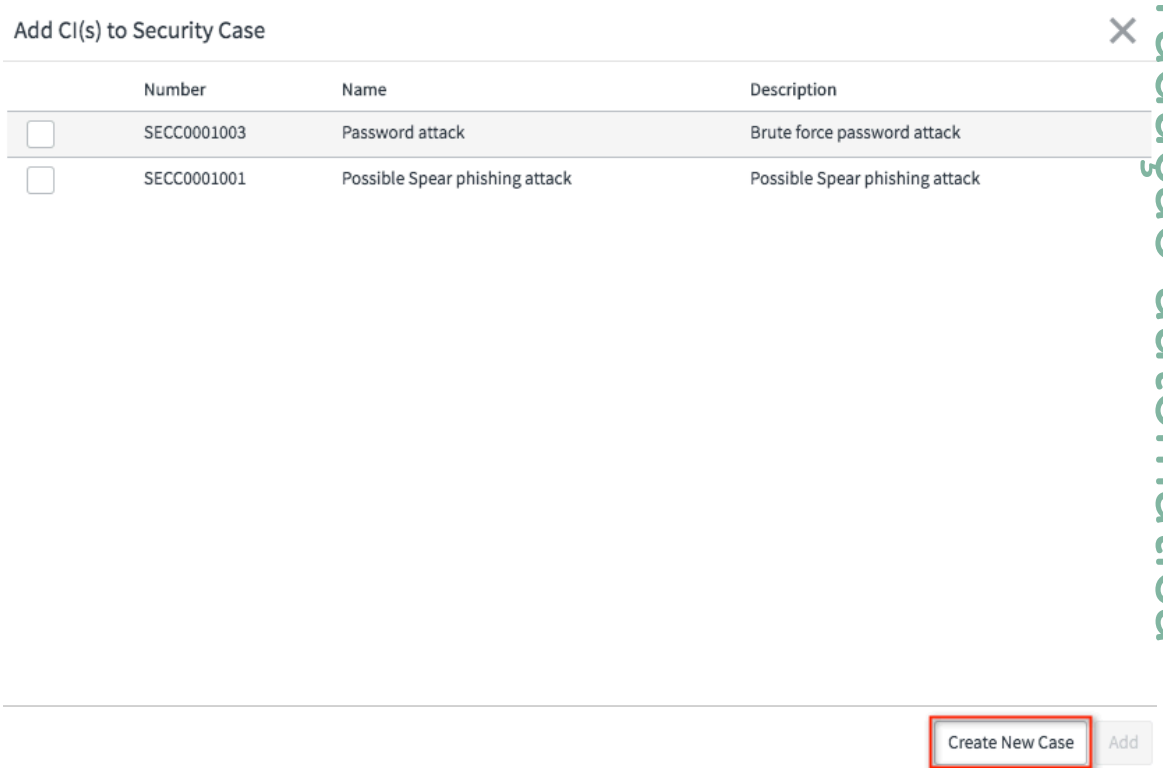
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .



. **Adicionar ao Caso de segurança** a caixa de diálogo é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique em **Criar Novo Caso** .

5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.

7. Clique no link para exibir o novo caso.

Adicionar ICs a casos existentes

Você pode adicionar itens de configuração a um ou mais casos existentes. Depois que os ICs forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

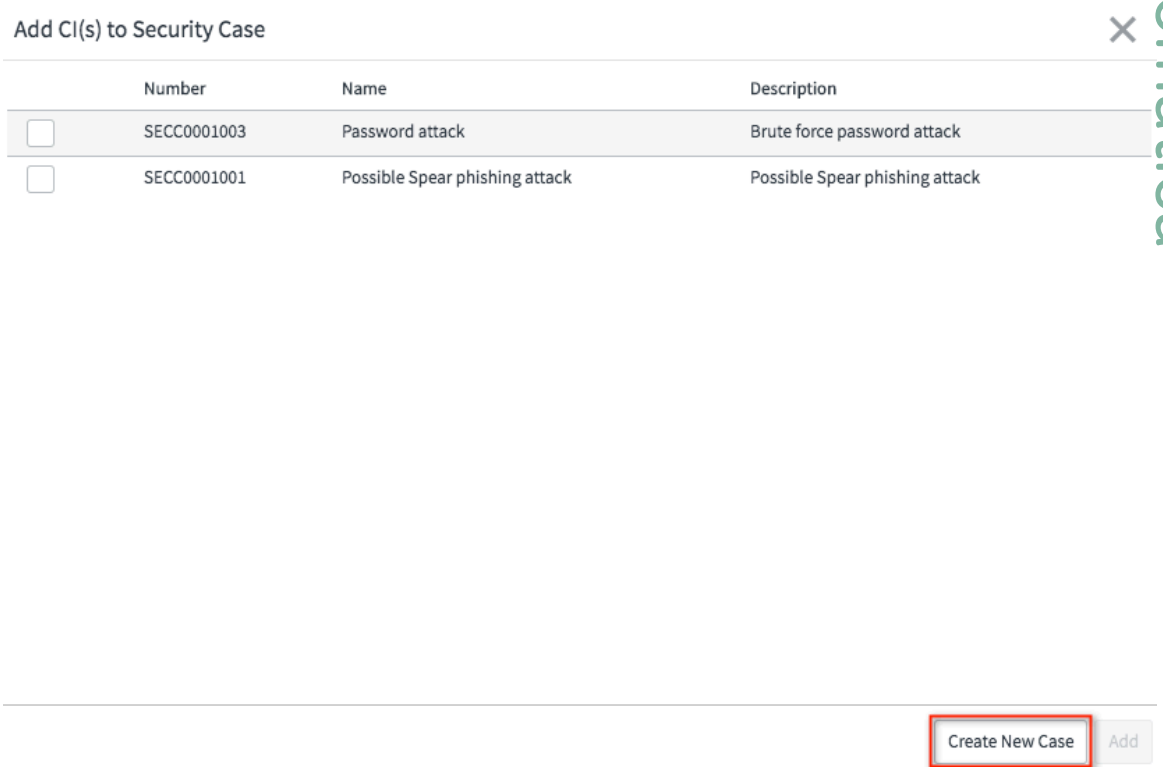
Você precisa navegar até os ICs que deseja adicionar aos casos existentes.

Procedimento

1. Navegar até **Tudo** > **Configuração** > **Itens de Base** > **Computadores** Para exibir ICs para computadores.
   A lista de ICs selecionados é aberta.
2. Na lista, selecione um ou mais ICs que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários ICs, os ICs selecionados serão adicionados a cada um dos casos selecionados.

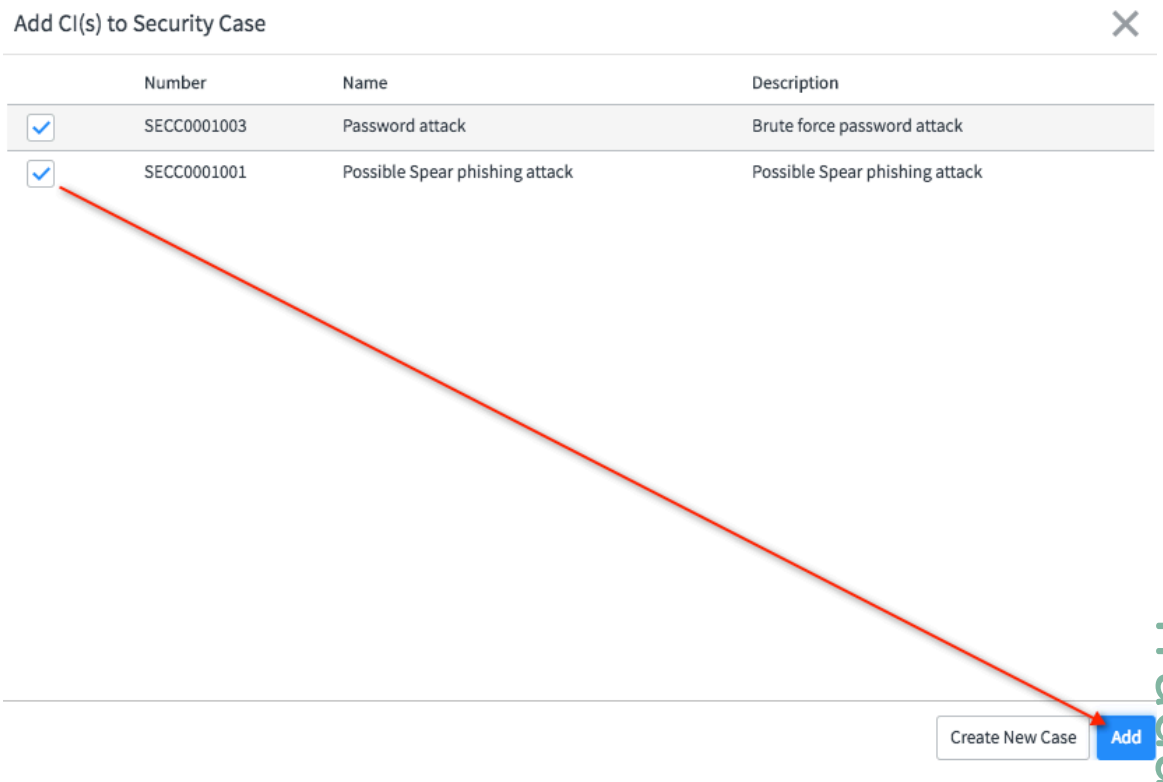
3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .
   . **Adicionar ao Caso de segurança** a caixa de diálogo é aberta e exibe os casos atribuídos a você.



4. Selecione os casos aos quais você deseja adicionar os ICs selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Usuários afetados em casos

Você pode criar um novo caso a partir de um ou mais usuários afetados na tabela Usuário [sys_user]. Você também pode adicionar usuários a casos existentes.

Crie um caso a partir de usuários afetados

Você pode criar um caso de segurança a partir de usuários afetados na tabela Usuário [sys_user]. Depois que os usuários afetados tiverem sido usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

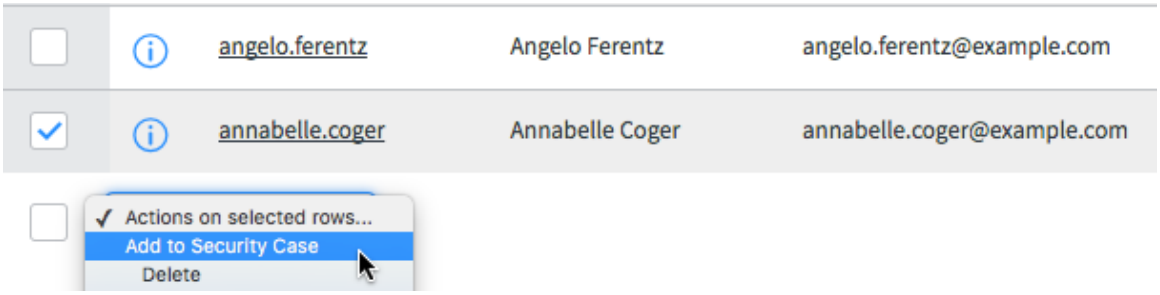
Você precisa navegar até os usuários que deseja usar para criar um caso.

Procedimento

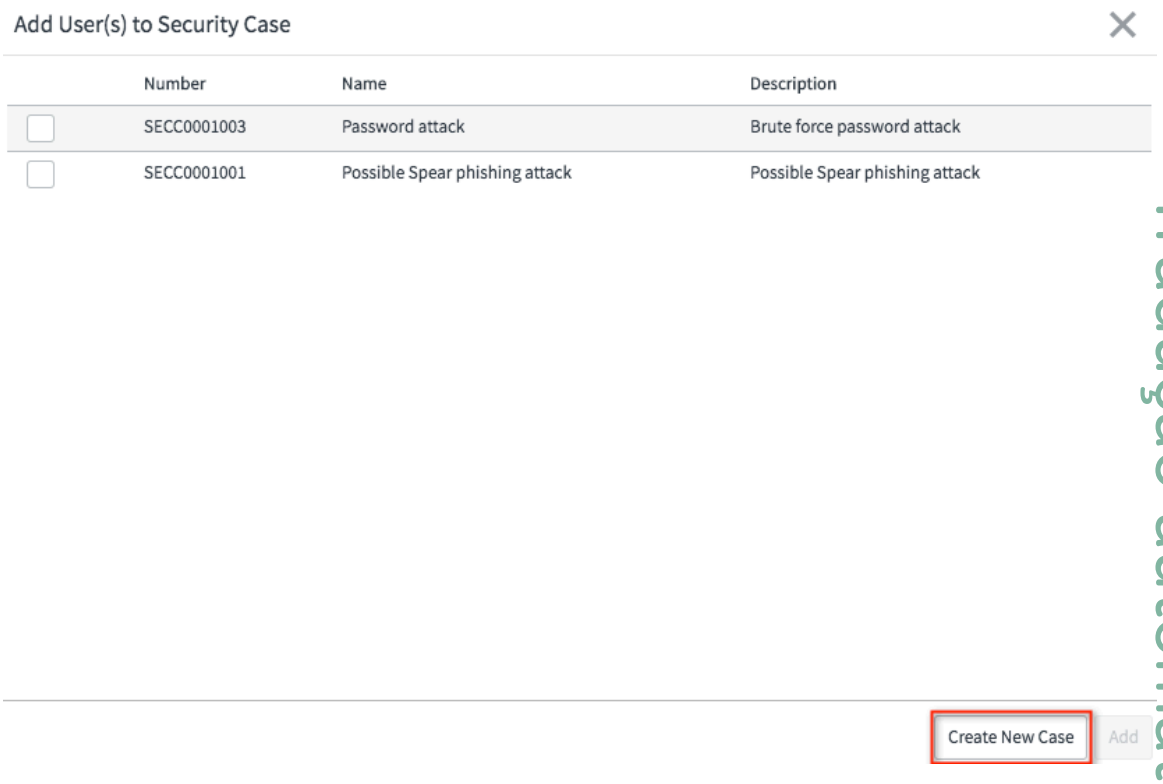
1. Navegar até **Tudo** > **Administração de Usuários** > **Usuários**.
   A lista dos usuários selecionados é aberta. Na lista, você pode criar um novo caso a partir de um ou mais registros de usuário ou selecionar um registro de usuário específico e criar um novo caso a partir do formulário.
2. Na lista, selecione os usuários que você deseja adicionar a um novo caso.
3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



. **Adicionar ao Caso de segurança** a caixa de diálogo é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique em **Criar Novo Caso** .
5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione usuários afetados a casos existentes

Você pode adicionar usuários afetados a um ou mais casos existentes. Depois que os registros do usuário forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

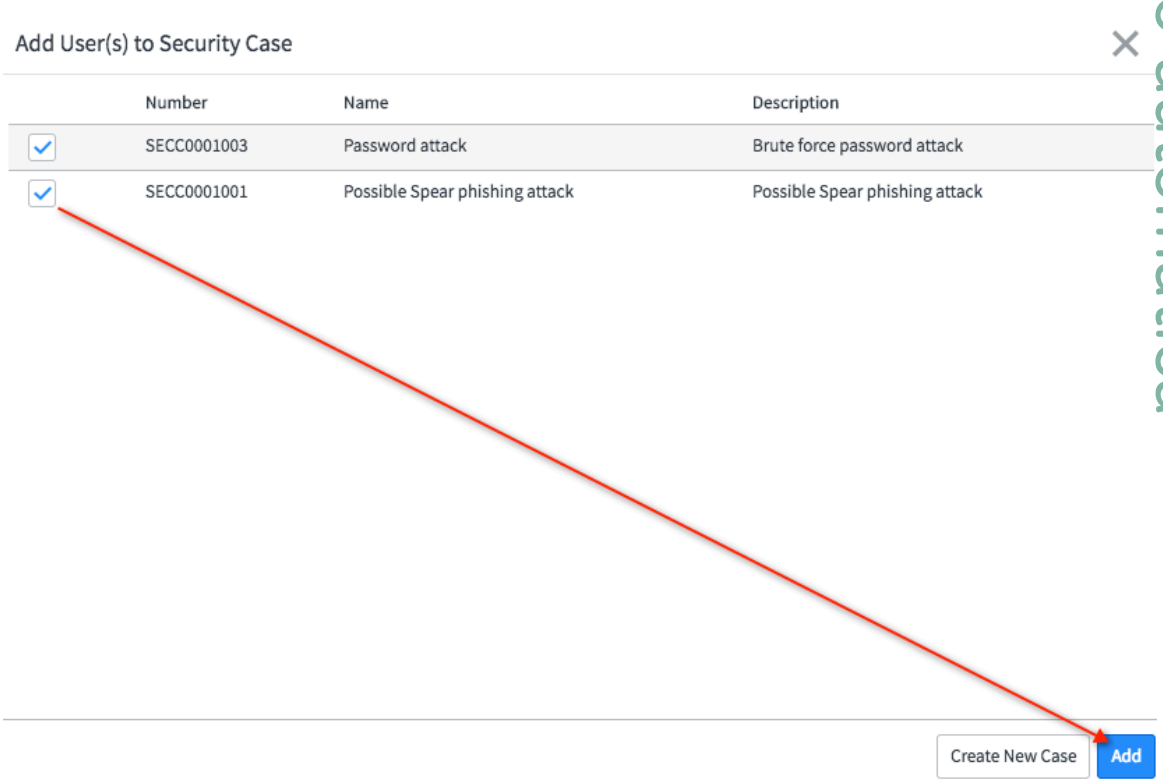
Você precisa navegar até os registros de usuário que deseja adicionar aos casos existentes.

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Usuários**.
   A lista de registros do usuário é aberta.
2. Na lista, selecione um ou mais usuários que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários usuários, os registros de usuário selecionados serão adicionados a cada um dos casos selecionados.

3. Em **Ações nos itens selecionados** lista suspensa, selecione **Adicionar ao Caso de segurança** .
   . **Adicionar ao Caso de segurança** a caixa de diálogo é aberta e exibe os casos atribuídos a você.



4. Selecione os casos aos quais você deseja adicionar os usuários selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Análise de artefatos de segurança

Depois de criar casos, usando Gestão de casos de segurança Ou a partir de artefatos como IOCs, observáveis, incidentes de segurança e assim por diante, você pode continuar adicionando artefatos para ajudar na análise das ameaças identificadas.

Detalhes relacionados a artefatos de caso

À medida que você adiciona artefatos a um caso, detalhes relacionados adicionais para cada artefato também podem ser adicionados automaticamente. Por exemplo, se você adicionar um incidente de segurança, ele poderá conter ICs afetados e registros de usuário. Você pode exibir rapidamente os detalhes relacionados de um artefato selecionado sem sair da lista de artefatos.

Exibir detalhes relacionados de um artefato de incidente de segurança

Se o seu caso incluir artefatos de incidente de segurança, você poderá exibir todos os detalhes relacionados contidos em cada incidente de segurança referenciado pelo caso.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

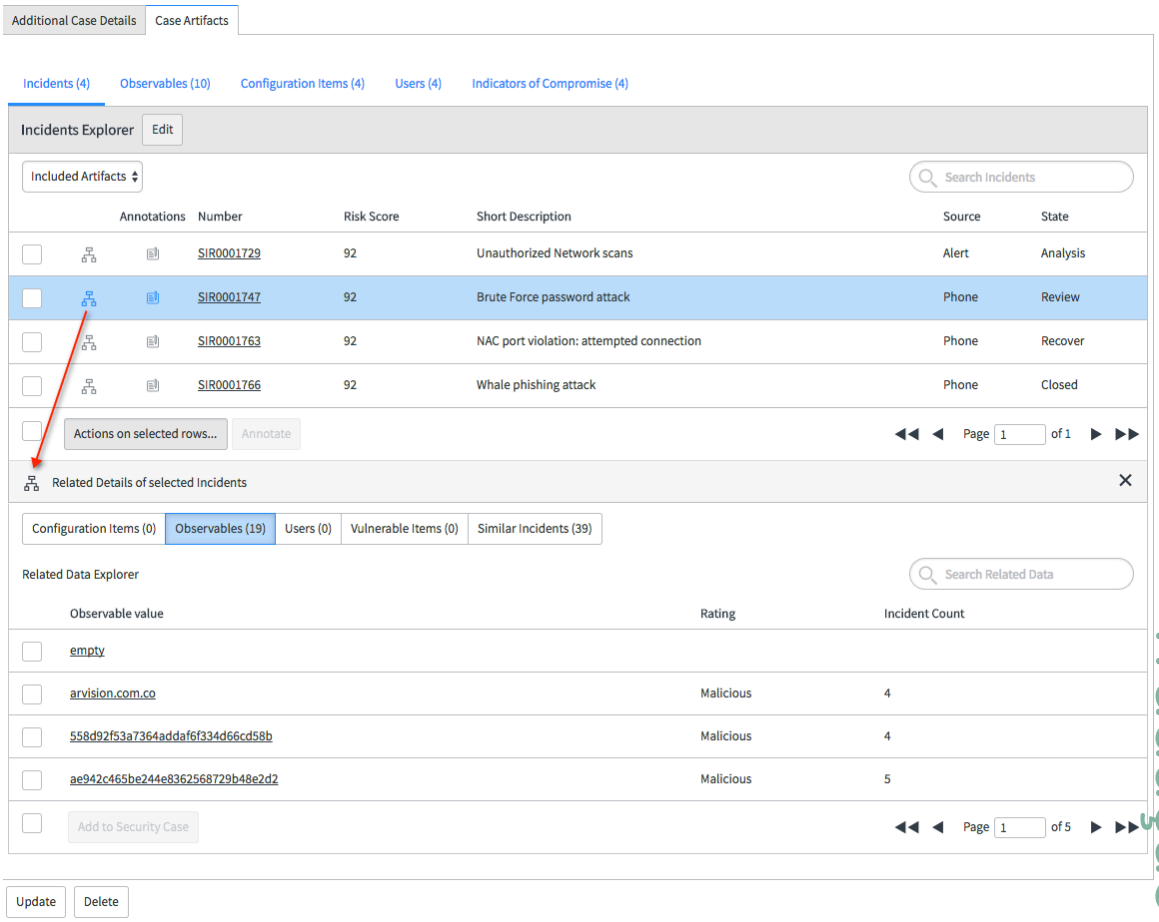
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos de incidente de segurança.
2. Clique em **Incidentes** guia.
3. Clique no ícone Detalhes adicionais do incidente de segurança para o qual você deseja exibir os detalhes relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar em **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados de um artefato de item de configuração

Se o seu caso incluir artefatos de item de configuração, você poderá exibir todos os detalhes relacionados contidos em cada IC referenciado pelo caso.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

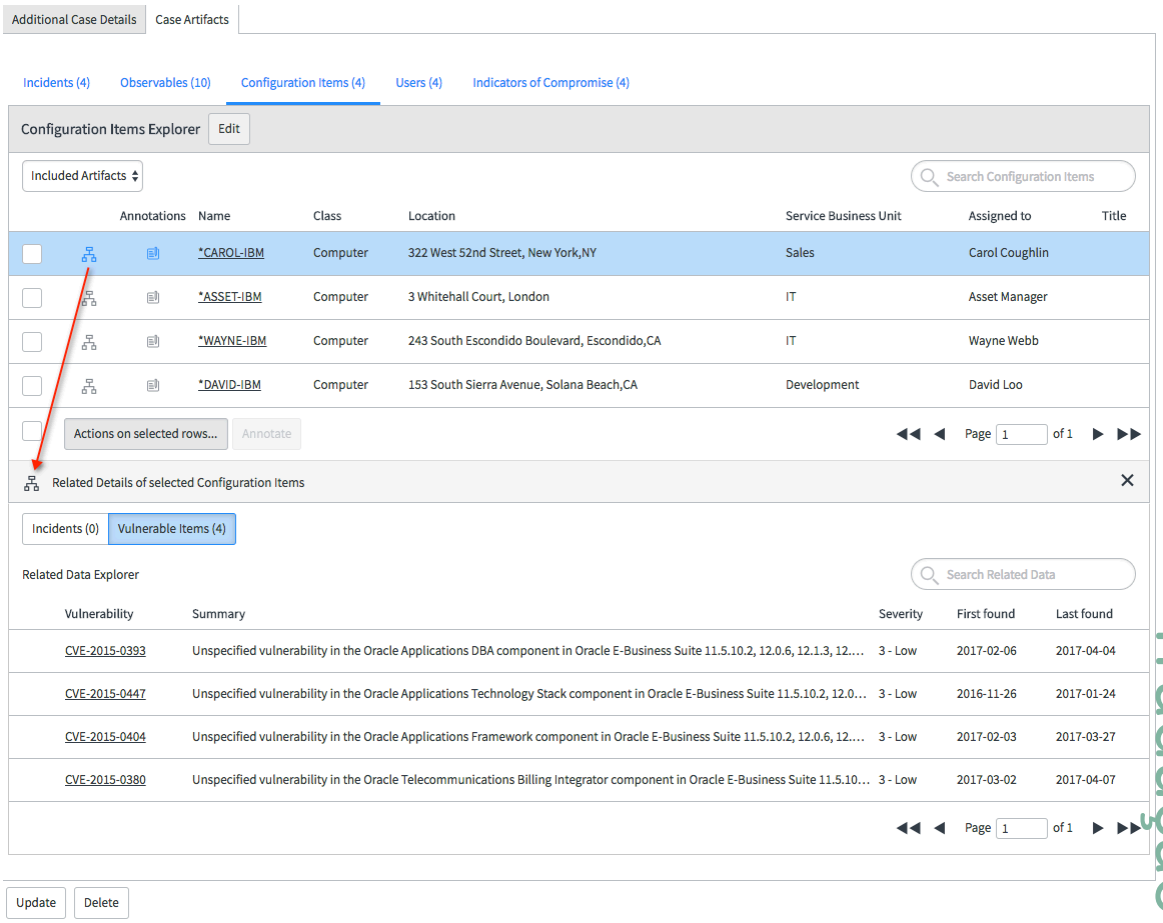
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos de IC.
2. Clique em **Itens de configuração** guia.
3. Clique em Detalhes adicionais para o artefato de IC cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar em **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados de um artefato IOC

Se o seu caso incluir artefatos de indicadores de comprometimento (IOC), você poderá exibir todos os detalhes relacionados contidos em cada IOC referenciado pelo caso.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

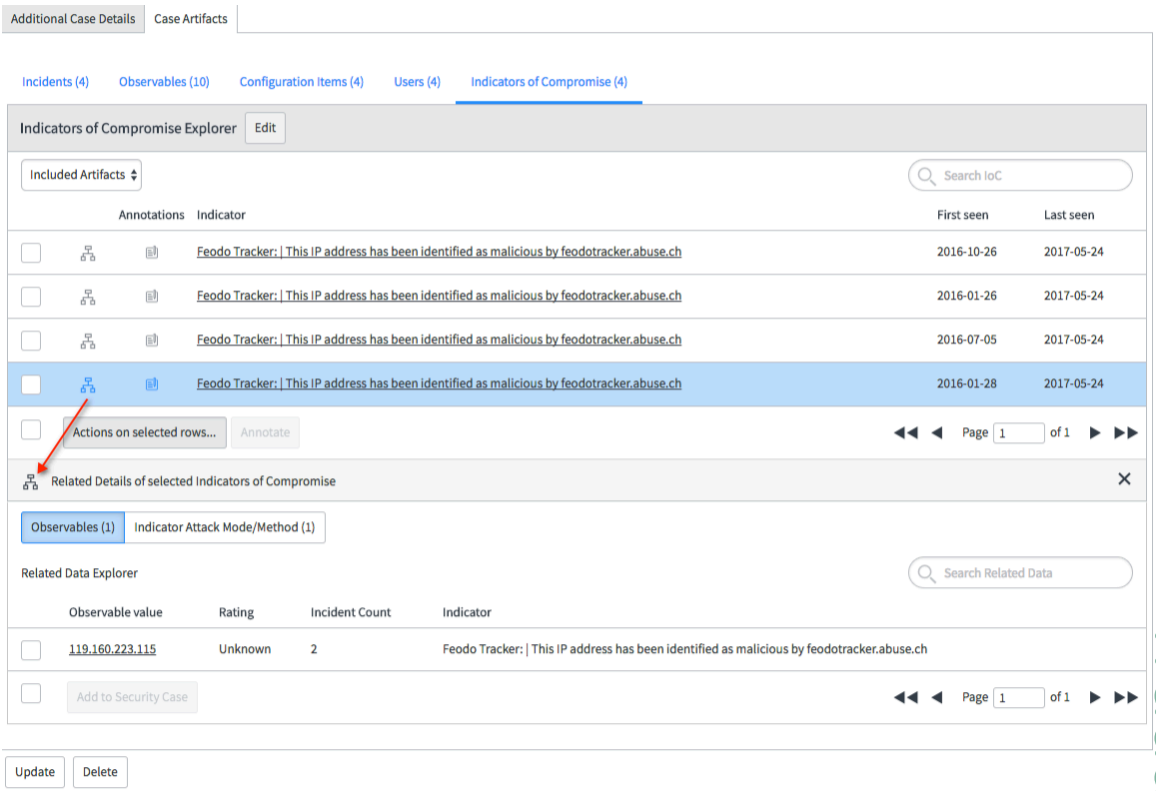
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos de IOC.
2. Clique em **Indicadores de compromisso** guia.
3. Clique no ícone Detalhes adicionais do artefato IOC cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar em **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados de um artefato de usuário afetado

Se o seu caso incluir artefatos do usuário afetado, você poderá exibir todos os detalhes relacionados contidos em cada usuário afetado referenciado pelo caso.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

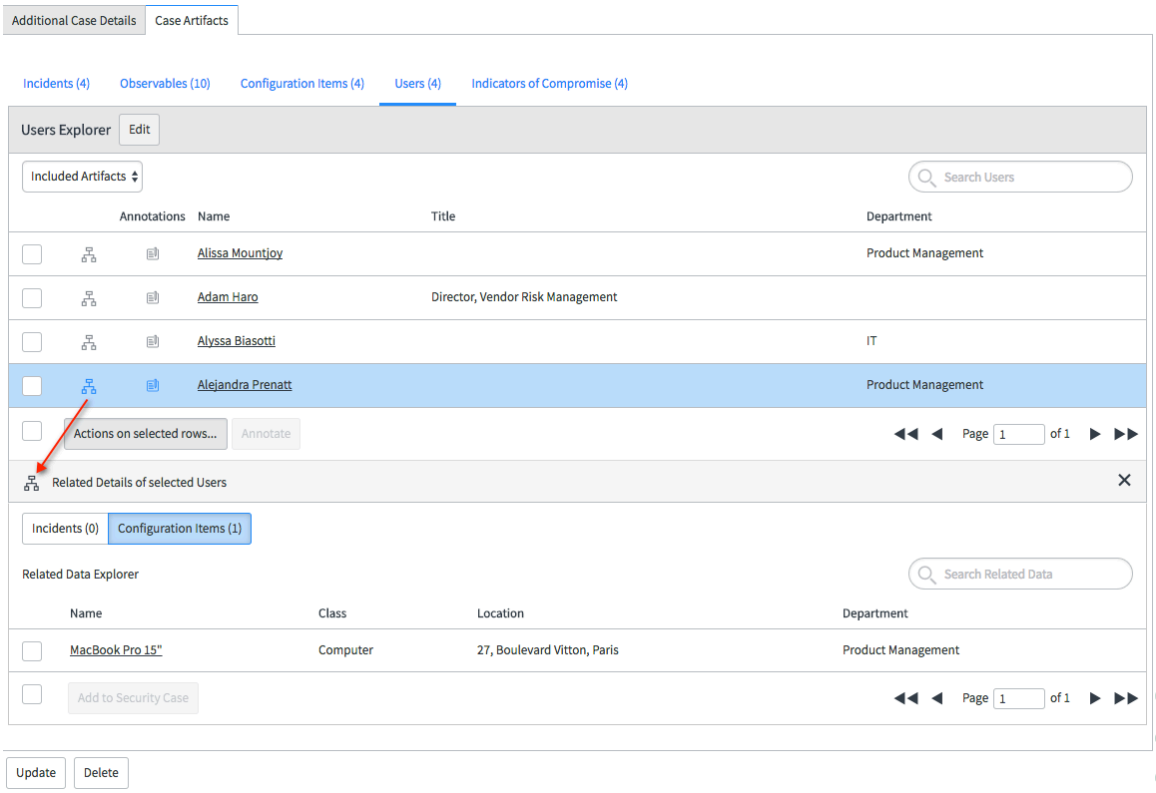
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos do usuário afetado.
2. Clique em **Usuários** guia.
3. Clique em Detalhes relacionados para o artefato do usuário afetado cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar em **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados de um artefato observável

Se o seu caso incluir artefatos observáveis, você poderá exibir todos os detalhes relacionados contidos em cada observável referenciado pelo caso.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

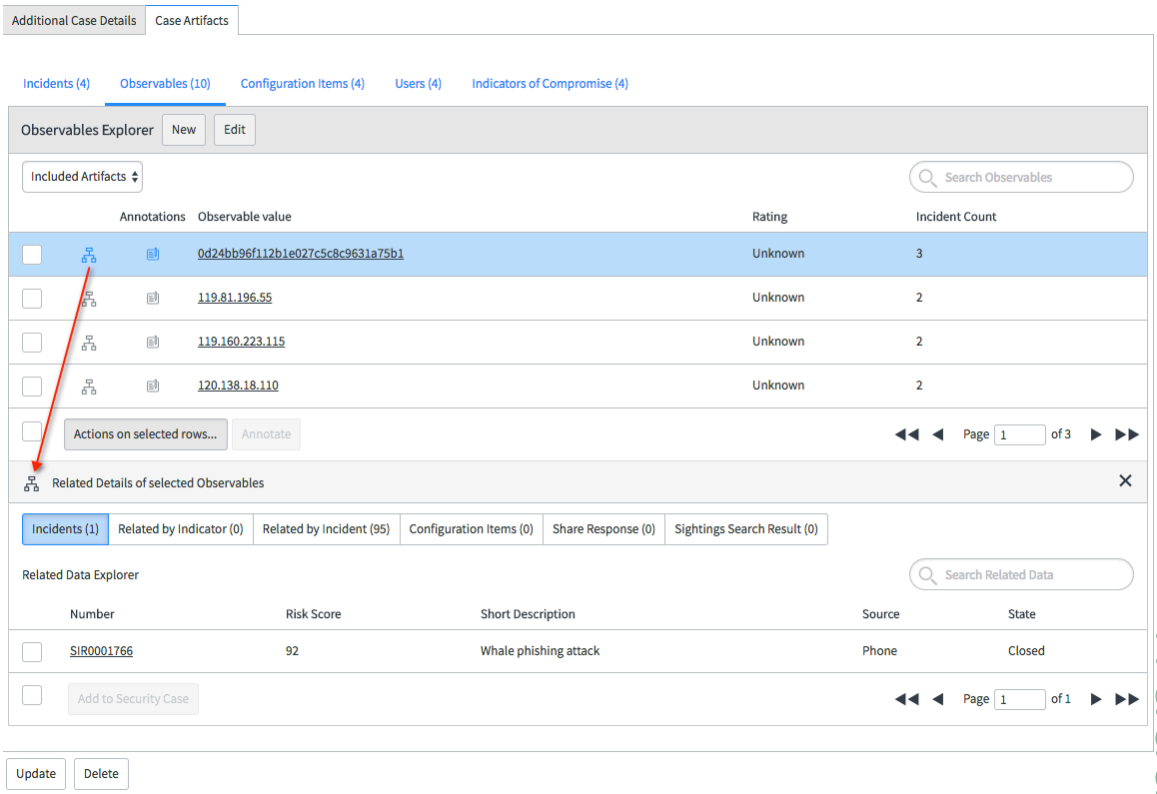
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos observáveis.
2. Clique em **Observáveis** guia.
3. Clique no ícone Detalhes adicionais do artefato observável cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar em **Anotação de segurança** para exibir anotações do artefato selecionado.

Exclusão e inclusão de artefato de segurança

Às vezes, as listas de artefatos de suporte atribuídos a um caso podem ser longas e pode haver instâncias em que você deseja remover artefatos específicos de uma lista. Em vez de remover permanentemente os artefatos, você pode excluí-los da lista e, conforme necessário, devolvê-los à lista posteriormente.

Exclua artefatos de segurança de um caso

Você pode remover artefatos das listas de artefatos de suporte. Eles não são removidos permanentemente e podem ser retornados ao caso conforme necessário.

Antes de Iniciar

- . Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

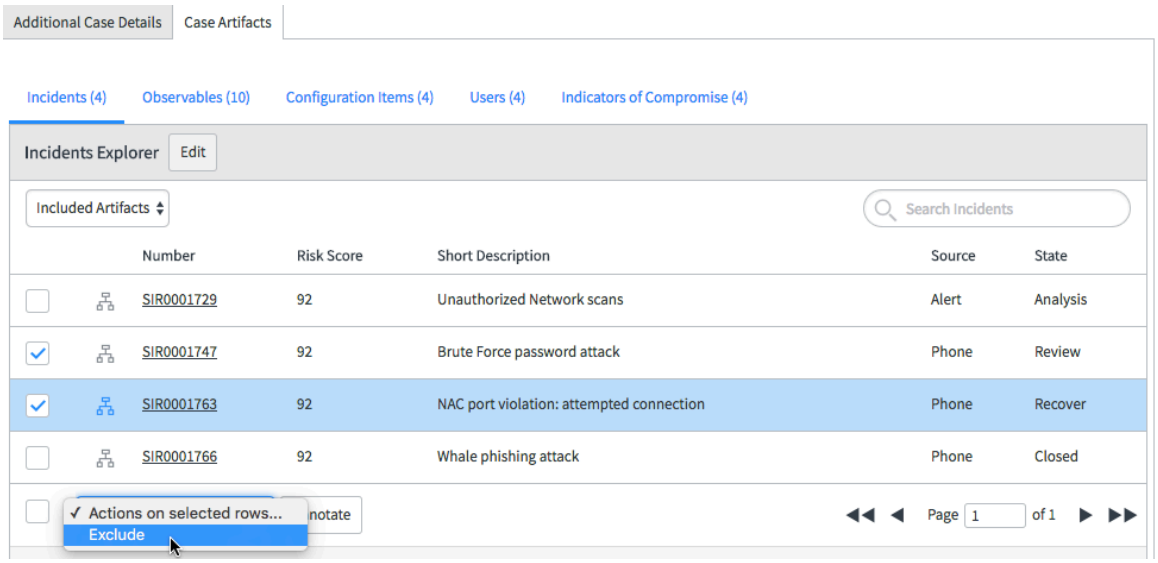
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos que você deseja excluir de uma lista.
2. Clique em **Artefatos de caso** lista relacionada.
3. Clique na guia associada aos artefatos que você deseja excluir.
   Por exemplo, clique em **Incidentes** para excluir incidentes de segurança da lista.
4. Selecione um ou mais registros de artefato que você deseja excluir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Em **Ações nos itens selecionados** lista suspensa, selecione **Excluir** .
6. Clique em **Excluir** na caixa de confirmação.
   Os artefatos selecionados são removidos da lista.

Retorna artefatos de segurança excluídos para um caso

Depois de excluir artefatos de uma lista em um caso, você pode devolvê-los ao caso e continuar trabalhando neles.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

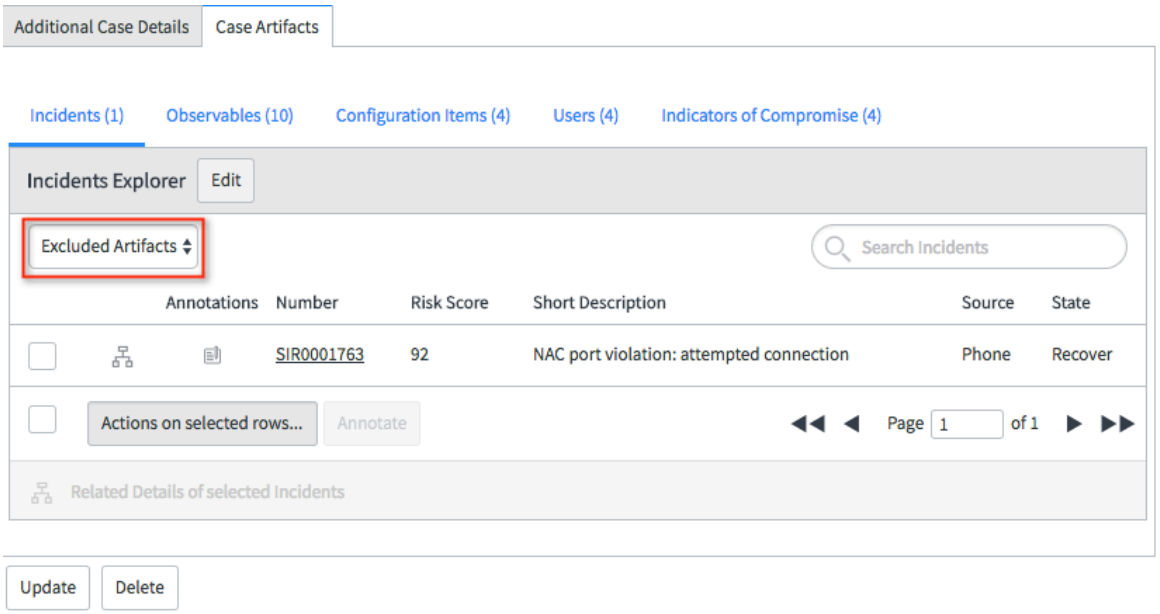
Função necessária: sn_ti.case_user_write

Procedimento

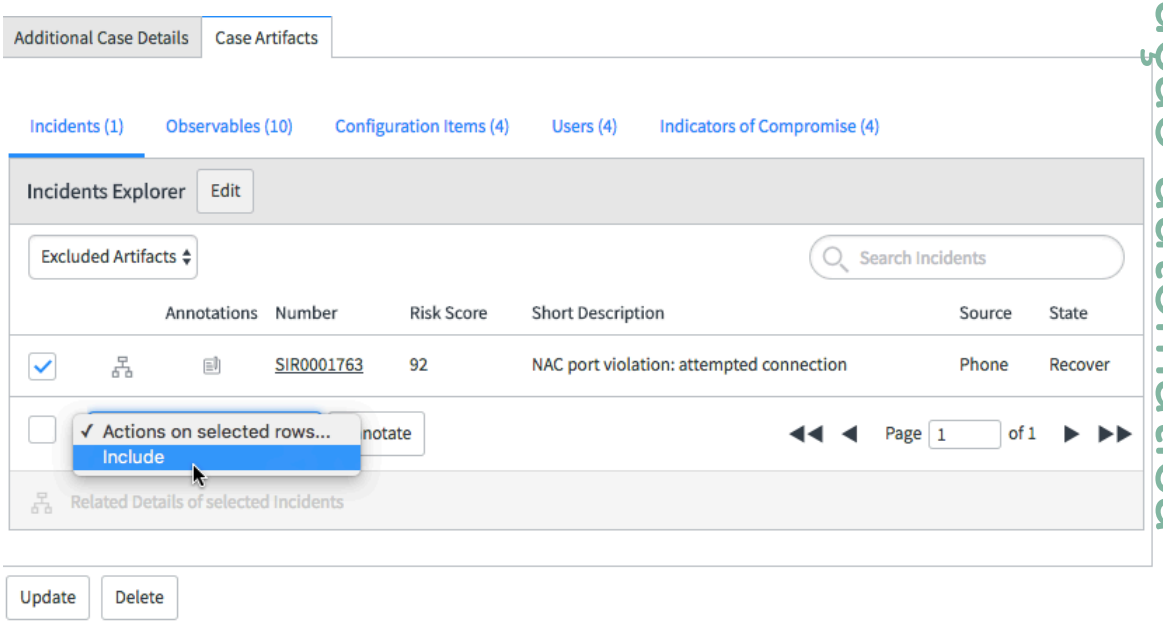
1. Abra um caso que contém artefatos que você excluiu anteriormente de uma lista que você deseja retornar à lista.
2. Clique em **Artefatos de caso** lista relacionada.
3. Clique na guia associada aos artefatos que você deseja retornar à lista.
4. Clique na lista suspensa Filtro de artefato e selecione **Artefatos excluídos** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Selecione um ou mais registros de artefato que você deseja retornar para a lista Incluir.
6. Em **Ações nos itens selecionados** lista suspensa, selecione **Incluir** .



7. Clique em **Incluir** na caixa de confirmação.
   Os artefatos selecionados são removidos da lista de artefatos excluídos e retornados à lista de artefatos incluídos no caso.

Anote artefatos de segurança

Ao analisar um caso, você pode adicionar anotações a qualquer artefato.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

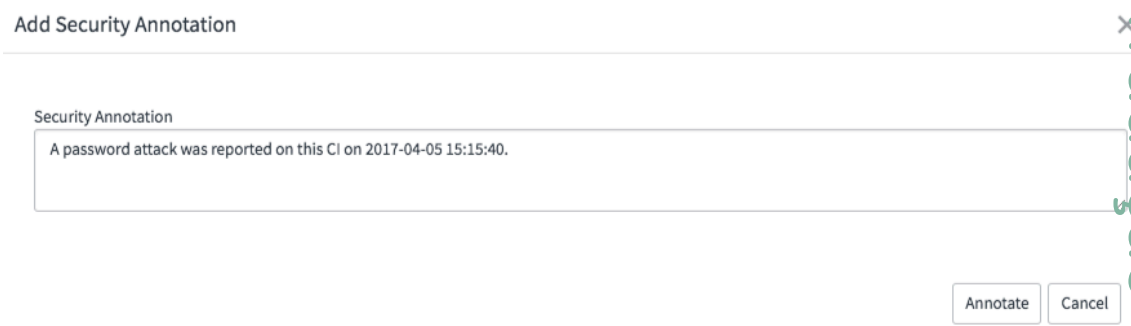
- sn_ti.case_user_write para adicionar anotações
- sn_ti.case_user_read para exibir anotações

Procedimento

1. Abra um caso que contém artefatos que você deseja anotar.
2. Clique em **Artefatos de caso** lista relacionada.
3. Clique na guia associada aos artefatos que você deseja anotar.
   Por exemplo, clique em **Indicadores de compromisso** Para adicionar anotações aos IOCs.
4. Para adicionar uma anotação a um ou mais artefatos, execute as seguintes etapas:

   a. Selecione os artefatos aos quais você deseja adicionar uma anotação.

   b. Clique em **Anote** .

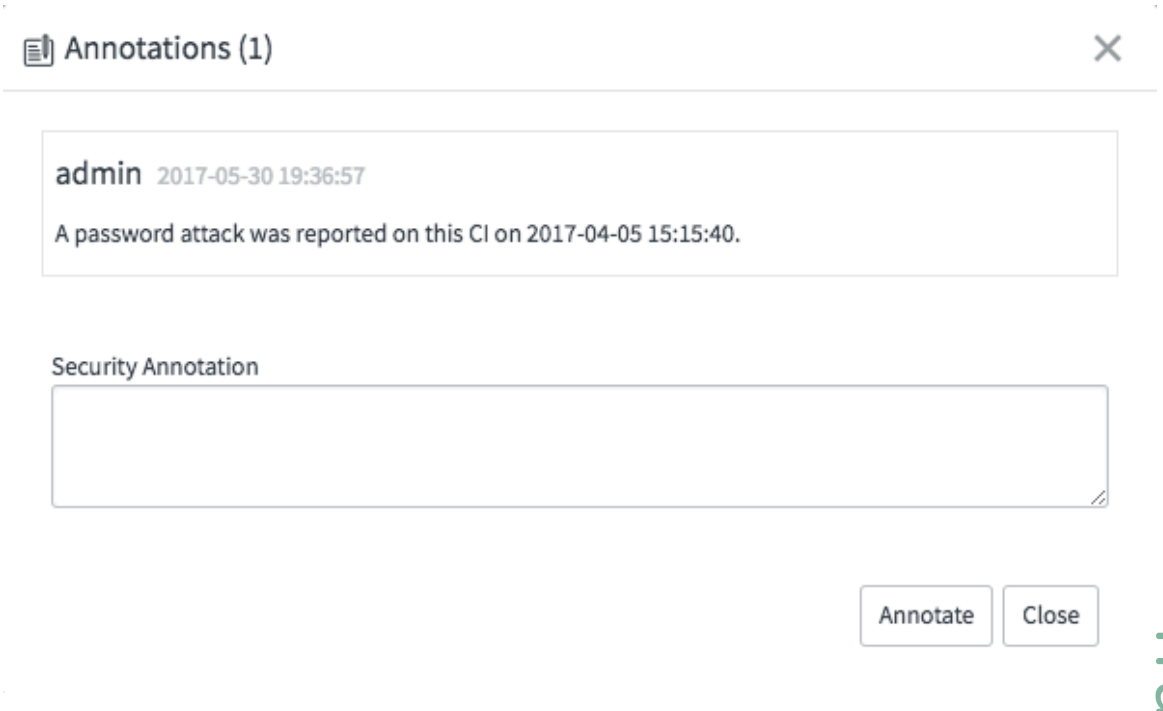


   c. Digite a anotação e clique em **Anote** .
   A anotação é adicionada aos artefatos selecionados.

5. Para exibir anotações de um artefato, clique no botão Exibir anotações (ícone).
   As anotações existentes aparecem na caixa de diálogo Anotações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Você também pode inserir uma nova anotação para o artefato em **Anotação de segurança** e clique em **Anote** .

PESQUISE artefatos de segurança

Você pode executar uma pesquisa de palavra-chave em qualquer lista de artefatos de segurança.

Antes de Iniciar

. Inteligência contra ameaças o plug-in deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contém artefatos de segurança.
2. Clique na guia dos artefatos de segurança nos quais você deseja executar uma pesquisa de palavra-chave.
3. Em **Pesquisa por palavra-chave** , comece a digitar o nome do artefato que você deseja localizar. Quando artefatos que correspondem à sua entrada são encontrados, eles são exibidos.

Controle de posturas de segurança

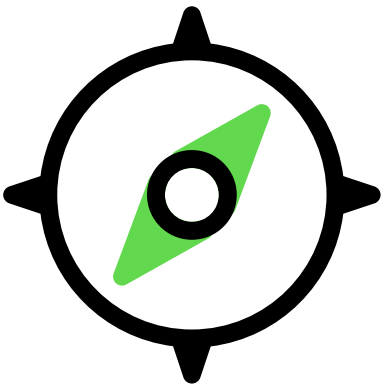
Obtenha visibilidade do inventário de ativos empresariais e da cobertura da ferramenta de segurança. Use as políticas fornecidas com o produto ou crie as suas próprias para identificar ativos que não têm ferramentas de segurança importantes, como proteção de endpoint, gestão de configuração e verificação de vulnerabilidades. Monitore ativos para configurações de ferramentas de segurança específicas para seu ambiente e automatize o fluxo de trabalho de correção de falhas de segurança no Conformidade de configurações aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

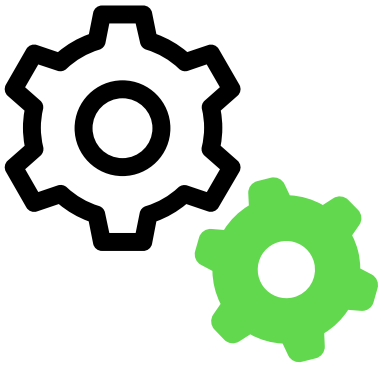
Iniciar

Explorar



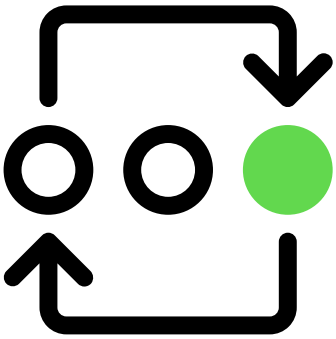
Saiba mais sobre os conceitos e recursos do Controle de postura de segurança

Instalar



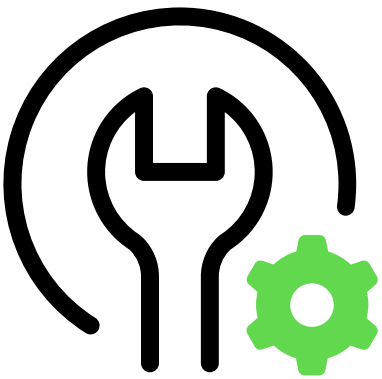
Instale aplicações de Controle de postura de segurança

Integrar



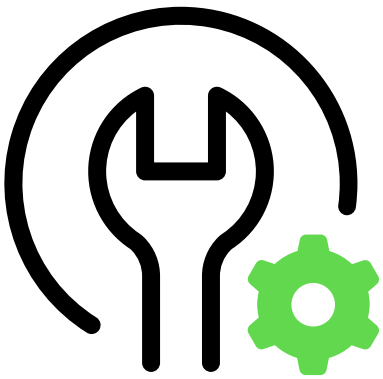
Integrar Conectores do Service Graph ao Controle de postura de segurança

Uso



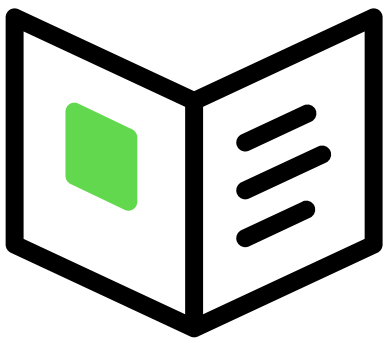
Saiba como usar o espaço para pesquisar seus ativos e identificar lacunas de segurança

Monitoramento de controles de mitigação



Obtenha informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis

Referência



Obtenha detalhes sobre cenários que ajudam a identificar tipos específicos de lacunas de cobertura da ferramenta. Consulte exemplos de políticas básicas, secundárias e clonadas e veja uma lista de conectores de gráfico de serviço de hardware e software compatíveis.

Solucionar problemas e obter ajuda

- Biblioteca de recursos de operações de segurança
- Comunidade de Operações de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorando Controle de posturas de segurança

Controle de posturas de segurança permite que as equipes de segurança cibernética tenham visibilidade de todo o inventário de ativos empresariais e determinem sua postura geral de segurança.

Os analistas de segurança obtêm informações sobre como as ferramentas de segurança são implantadas e cobrem seus ativos com base no inventário de ativos e nos dados importados de conectores do Service Graph e produtos da ServiceNow, como Gestão de ativos de hardware - HAM(HAM) e. ITOM Descoberta.

Os analistas de segurança também podem criar políticas personalizadas e configurar informações para monitorar a conformidade de ativos com padrões de segurança internos. Os gerentes de vulnerabilidades podem usar informações do Controle de posturas de segurança(SPC para priorizar a correção de vulnerabilidades em ativos de alto risco.

O produto SPC é baseado no Cloud Security Posture Management (CSPM) e no Cyber Asset Hygiene Management (CAHM). Controle de posturas de segurança consiste em duas aplicações que estão disponíveis por assinatura separada do ServiceNow® Store.

Versão de lançamento	Notas de versão
Núcleo de controle de postura de segurança: v6.2, v6.1, v6.0.	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão Controle de posturas de segurança notas da versão
Gestão de posturas de segurança para ativos v5.3, v5.1, v5.0	
Monitoramento de controles de mitigação v4.0, v3.0, v2.0	

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Com SPC Produto, as equipes do Info-Sec podem executar as seguintes tarefas:

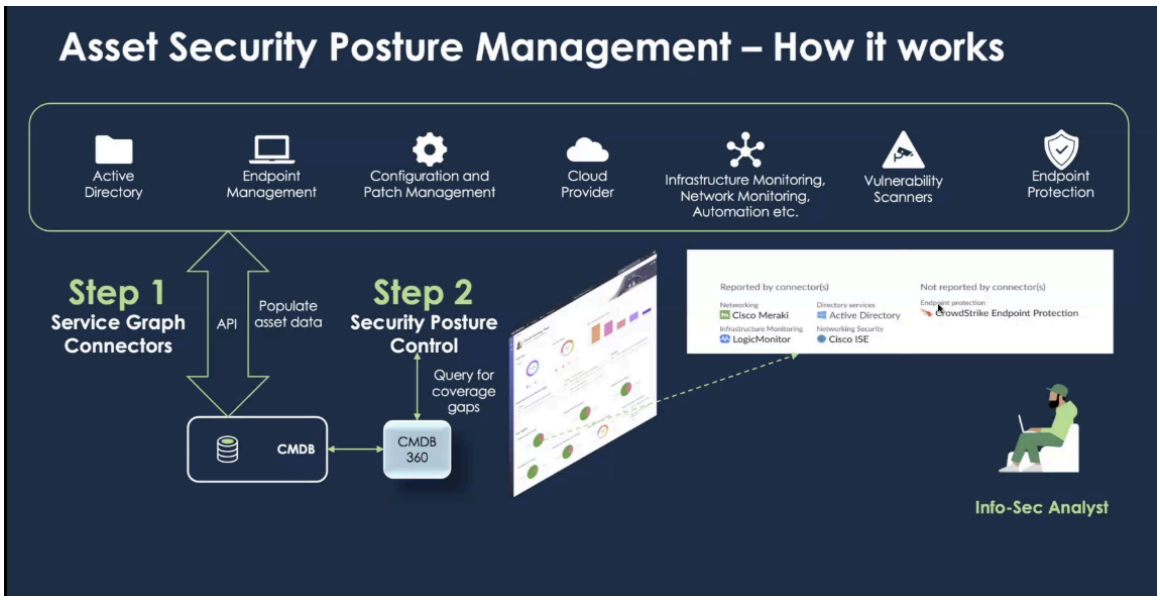
- Exiba informações de postura de segurança para seus ativos no local e na nuvem. SPC Ajuda suas equipes do Info-Sec a identificar ativos que não têm proteção de endpoint, ativos não gerenciados, ativos expostos à Internet e quaisquer combinações de alto risco que envolvam vulnerabilidades.
- Monitore seus ativos quanto à conformidade com os padrões de configuração da ferramenta de segurança interna. Por exemplo, certifique-se de que a versão mais recente de um produto de proteção de endpoint esteja sendo usada.
- Automatize seu fluxo de trabalho de correção para as lacunas de postura de segurança encontradas com o. ServiceNow Aplicação de conformidade de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie políticas e informações personalizadas com base em metadados de ativos, dados de cobertura da ferramenta de segurança e dados de vulnerabilidade.
- Obtenha informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis com base em como várias ferramentas de segurança são configuradas com o. Monitoramento de controles de mitigação .

Como o Gestão de posturas de segurança para ativos funciona



A Gestão de postura de segurança de ativos (ASPM) identifica lacunas de cobertura da ferramenta de segurança em ativos usando integrações de API com várias ferramentas de terceiros (Conectores do Service Graph) junto com os produtos da ServiceNow.

O ASPM depende dos dados preenchidos no CMDB sobre seus ativos. Os dados do ativo são importados por várias categorias de ferramentas de monitoramento e comparados para identificar possíveis falhas de segurança.

Por exemplo, digamos que haja dados de ativos preenchidos no CMDB que são relatados por ferramentas que cobrem monitoramento de infraestrutura e ferramentas de rede. No entanto, esses dados desses mesmos ativos não são preenchidos ou relatados por ferramentas de proteção de endpoint. Se você comparar os dados de ativos relatados por essas diferentes ferramentas, poderá ver que há ativos sem um agente de proteção de endpoint.

Gestão de posturas de segurança para ativos Identifica lacunas de cobertura da ferramenta de segurança em ativos usando integrações de API com várias ferramentas (Conectores do Service Graph) e produtos da ServiceNow. As categorias incluem, mas não estão limitadas ao seguinte:

- Experiência do Funcionário Digital
- Descoberta
- Gestão de endpoint
- IT Asset Management
- Monitoramento de infraestrutura
- Rede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Segurança de rede
- Monitoramento de desempenho de rede
- Gestão de configuração e patches
- Proteção de endpoint
- Provedor de nuvem
- Monitoramento de desempenho da aplicação
- Serviços de diretório
- Avaliação de vulnerabilidade

. Controle de posturas de segurança fluxo de trabalho

Identificar lacunas da ferramenta de segurança envolve as seguintes etapas:

1. Configure e ative conexões de API com qualquer uma das ferramentas que você está usando em várias categorias. Você pode usar Conectores do Service Graph para produtos que estão disponíveis na ServiceNow Store para as conexões de API necessárias. Para obter mais informações sobre os conectores do Service Graph compatíveis, consulte Conectores do Service Graph . Os conectores do Service Graph compatíveis estão disponíveis no ServiceNow® Store com assinaturas separadas.
2. Ative as políticas enviadas com o. Controle de posturas de segurança aplicação. . Controle de posturas de segurança o produto encontra lacunas na ferramenta de segurança executando as seguintes tarefas:
   a. Identifica a lista de todos os ativos exclusivos preenchidos por vários conectores do Service Graph no CMDB.
   b. Identifica ativos que não são relatados por categorias específicas deste grupo de ativos, por exemplo, Proteção de endpoint. Os ativos são identificados com base na política ativa que está sendo avaliada.
   c. Os ativos identificados como não relatados por categorias específicas são relatados como "Descobertas" ou "Resultados de teste" em Conformidade de configurações aplicação.
3. Atribua automaticamente "descobertas" a diferentes equipes para correção com a aplicação Conformidade de configuração.

Combinações de alto risco

Com Gestão de posturas de segurança para ativos você também pode identificar ativos que têm combinações de alto risco. Um exemplo de uma combinação de alto risco pode mostrar ativos que não têm ferramentas de segurança, têm vulnerabilidades críticas e estão expostos à Internet.

Algumas das políticas enviadas com o. Controle de posturas de segurança procure essas combinações de alto risco de vulnerabilidades críticas e lacunas de cobertura da ferramenta de segurança. No entanto, para que essas políticas de combinação funcionem, você deve ter Resposta a vulnerabilidades e pelo menos um produto de integração de scanner de vulnerabilidades, como Qualys, Rapid7 ou Integrações de vulnerabilidade da Tenable aplicação instalada. Esses aplicativos estão disponíveis com assinaturas separadas da ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Monitoramento de controles de mitigação

Em Controle de posturas de segurança(SPC) Espaço, obtenha informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis com base em como as várias ferramentas de segurança são configuradas. Consulte Monitoramento de controles de mitigação para obter mais informações.

Instale as aplicações compatíveis com o Controle de postura de segurança

As aplicações necessárias para esta integração estão disponíveis no ServiceNow Store. Alguns aplicativos têm dependências que você deve baixar e instalar separadamente.

Antes de Iniciar

Função necessária: administrador para download, instalação e ativação de todos os aplicativos.

Procedimento

1. Baixe as aplicações necessárias do ServiceNow Store em seu ServiceNow instância.

   . Controle de posturas de segurança(SPC Core) fornece a estrutura principal e é necessária para Gestão de posturas de segurança para ativos(ASPM). . Conformidade de configurações a aplicação e suas dependências permitem criar tarefas de correção para as lacunas de controle de segurança encontradas usando Gestão de posturas de segurança para ativos.

Aplicações de Gestão de postura de segurança de ativos

Aplicação	ID de app
Gestão de posturas de segurança para ativos	(ID do plug-in: sn_sec_caasm)
Licença de Descoberta do ITOM	(ID do plug-in: com.snc.itom.discovery.license)
Base para controle de posturas de segurança	(ID do plug-in: sn_sec_spc_core)
Monitoramento de controles de mitigação	(ID do plug-in: sn_sec_mit_ctr)
Conformidade de configuração (inclui app secundário secops_shared_components)	(ID do plug-in: sn_vulc)
Licenciamento e uso do Vulnerability Response	(ID do plug-in: sn_vul_licensing)

Aplicações de Gestão de postura de segurança na nuvem

Aplicação	ID de app
Plug-in Descoberta	(ID do plug-in: com.snc.discovery)
Governança de configuração de nuvem	(ID do plug-in: sn_itom_ccg)
Pacote de conteúdo do CCG	(ID do plug-in: sn_itom_ccg_cp)
CMDB CI Class Models	(ID do plug-in: sn_cmdb_ci_class)
Biblioteca de ações na nuvem	(ID do plug-in: com.sn.itom.cal)

Para obter mais informações sobre como baixar e ativar aplicações, consulte os seguintes tópicos:

- Baixar uma aplicação do ServiceNow Store pela primeira vez.
- Ativar um ServiceNow Store aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Depois de baixar os aplicativos, navegue até **Tudo** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
3. Localize os aplicativos que você baixou e selecione **Instalar** para ativá-los junto com suas dependências. Todas as aplicações de dependência que também são instaladas automaticamente junto com uma aplicação são exibidas na caixa de diálogo de instalação da aplicação. No entanto, se você for solicitado a instalar plug-ins de dependência durante a instalação, siga os prompts fornecidos. Verifique se todas as aplicações e dependências listadas na tabela anterior estão instaladas e ativadas.

   Uma caixa de diálogo é exibida depois que uma aplicação é ativada com sucesso.

   Para obter mais informações sobre como baixar e instalar aplicações do ServiceNow Store:

   - Para aceitar ServiceNow produtos, siga as etapas em Aceite . ServiceNow Store produtos .
   - Para instalar uma aplicação que você comprou do ServiceNow Store, siga as etapas em Instale um ServiceNow Store aplicação .
   - Se você quiser gerenciar seu direito para as aplicações em outro ServiceNow AI Platform, siga as etapas em Gerencie direitos do seu ServiceNow instância .
4. Depois de instalar e ativar as aplicações, atribua usuários aos seguintes grupos de controle de postura de segurança:

   Esses grupos herdam todas as funções necessárias para ler e editar registros do SPC.

   Grupo de administradores do SPC

   Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, incluindo informações de licenciamento. As funções granulares deste grupo incluem: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin e sn_sec_spc_core.configure].

   Grupo de analistas do SPC

   Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, mas não podem exibir as informações de licenciamento. As funções granulares deste grupo incluem [pa_power_user e sn_sec_spc_core.analyst].

   Analista do SPC somente leitura

   Os usuários neste grupo têm acesso total de leitura a todos os registros do produto, mas não podem exibir informações de licenciamento. As funções granulares deste grupo incluem [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read e cmdb_ms_user].

   Funções da aplicação de suporte

   As funções a seguir são exigidas pelas aplicações listadas na tabela anterior compatíveis com SPC e. Gestão de posturas de segurança para ativos.

   - Conformidade de configurações Administrador [sn_vulc.admin] - Configura o. Conformidade de configurações a aplicação tem visibilidade de todos os registros e pode modificar propriedades. Atribui funções no Conformidade de configurações aplicação.
   - Resposta a vulnerabilidades Administrador [sn_vulc.admin] - Configura a aplicação Resposta a vulnerabilidades e as calculadoras de risco de vulnerabilidade.
   - MID Server [mid_server] - Configura um MID Server.
5. **Opcional:** Defina **IgnoreCIClass** Propriedade do sistema [sn_sec_cmn.ignoreCIClass] para ignorar algumas classes de item de configuração (IC) ao executar regras de pesquisa de IC.

   (Optional) Como administrador de SPC e analista de SPC, pode ser necessário ignorar determinados hardwares ou classes virtuais para não ingerir informações sobre ativos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que não deseja controlar. Para obter mais informações, consulte Crie uma regra de pesquisa de IC de resposta a vulnerabilidades e Ignorar classes de IC.

6. Modifique a reconciliação e recalcule as fontes de dados do CMDB para definir a origem da verdade dos valores de atributo.

   O painel do CMDB 360 fornece agregações e análises de dados do CMDB 360. O CMDB 360 coleta dados sobre todas as origens de descoberta que relatam valores de atributo para ICs. Use a exibição do CMDB 360 no Espaço do Configuration Management Database (CMDB) para rastrear atividades e identificar possíveis problemas de origens de descoberta. Para obter mais informações, consulte Exibição do CMDB 360 no Espaço do CMDB .

Conectores do Service Graph para Controle de posturas de segurança

Controle de posturas de segurança Depende de integrações de API ou conectores do Service Graph como uma fonte-chave para os dados de ativos usados para identificar lacunas de segurança.

Controle de posturas de segurança Atualmente oferece suporte a conectores de Service Graph (SGC) que podem fornecer uma ampla variedade de dados sobre seus ativos. Esses aplicativos de integração estão disponíveis no ServiceNow Store.

Escolha os conectores que você deseja usar e baixe os aplicativos e ative-os. A lista de conectores compatíveis na Store crescerá conforme Controle de posturas de segurança oferece suporte a mais conectores.

Para aproveitar ao máximo Controle de posturas de segurança, talvez você queira baixar e ativar os seguintes produtos do Conector do Service Graph para oferecer suporte às categorias listadas abaixo.

Conectores do Service Graph compatíveis com Controle de posturas de segurança atualmente incluem as seguintes categorias:

- Experiência do Funcionário Digital
- Descoberta
- Endpoint Management: Microsoft Intune Ou Jamf Device and Endpoint Management.
- IT Asset Management
- Monitoramento de infraestrutura
- Rede
- Segurança de rede
- Monitoramento de desempenho de rede
- Configuração e gestão de patches: Microsoft SCCM ou IBM Bigfix.
- Proteção de endpoint: CrowdStrike Ou SentinelOne.
- Provedor de nuvem: Nuvem da Amazon AWS, Microsoft Azure, GCP.

  Nota: Se a Descoberta em nuvem estiver ativada, esses produtos do conector do Service Graph não serão necessários.

- Monitoramento de desempenho da aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Serviços de diretório (Active Directory) Microsoft Active Directory
- Avaliação de vulnerabilidades: Qualys, Rapid7 Ou Tenable.

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela Conector [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os Tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Consulte Conectores do Service Graph de hardware compatíveis com Controle de posturas de segurança e. Conectores do Service Graph de software compatíveis para Controle de posturas de segurança para obter mais informações e exemplos dessas tabelas. Embora não sejam listas extensas, você pode ver como os conectores compatíveis fornecem uma ampla variedade de dados.

Controle de posturas de segurança Oferece suporte a produtos da ServiceNow, como SAM (Software Asset Management, gestão de ativos de software) e. Gestão de ativos de hardware - HAM(HAM) que você pode usar junto com os conectores do Service Graph para ajudá-lo a procurar discrepâncias existentes entre o software instalado relatado por seus produtos de verificação de vulnerabilidades e o software relatado por scanners que já está contabilizado no SAM e em outros produtos da ServiceNow.

Para obter mais informações sobre como baixar, configurar e ativar aplicações compatíveis com conectores do Service Graph, consulte os seguintes tópicos:

- Conectores do Service Graph .
- Baixar uma aplicação do ServiceNow Store pela primeira vez.
- Ativar um ServiceNow Store aplicação.

Políticas para Controle de posturas de segurança

As políticas auditam seus ativos com base nos dados importados dos conectores do Service Graph para ajudar você a encontrar possíveis violações.

Políticas

Controle de posturas de segurança as políticas são criadas em um modelo de dados asset-relationships-properties. Há políticas incluídas com a aplicação e você pode criar suas próprias políticas para procurar critérios específicos.

Os critérios para políticas podem ser especificados na forma de condições nas propriedades desse ativo ou nas propriedades de uma entidade relacionada. No construtor de políticas no módulo Políticas e descobertas no espaço, você pode definir políticas para procurar um tipo de ativo (hardware, software) e uma conexão (relatado por, não relatado por) ou uma entidade (origem do ativo, produto do conector do Service Graph ou metadados do CMDB) ou você pode corresponder a outros tipos de critérios específicos.

Para ajudá-lo a modificar ou criar políticas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Defina suas condições no módulo Pesquisa de ativos e pesquise ativos por produtos do conector do Service Graph específicos ou ativos que tenham dados específicos relatados por um conector. Você pode salvar suas pesquisas como políticas.
- Clone as políticas incluídas com a aplicação para criar políticas mais expansivas. Você copia e, em seguida, refina as condições de uma apólice existente sem precisar inseri-las novamente.
- Crie novas políticas (políticas secundárias) usando as políticas de base selecionadas como ponto de partida para novas políticas.

Tipos de ativos e políticas

Você usa esses tipos de ativos primários ou de nível superior como ponto de partida para definir políticas.

Ativo de hardware

Ativo de hardware é uma abstração que representa qualquer dispositivo que inclui dispositivos de computação pessoal, servidores, dispositivos de rede, máquinas virtuais em nuvem e outros hardwares. As políticas auditam seus ativos em busca de possíveis violações com base nos dados importados dos produtos do conector do Service Graph e. ServiceNow® Produtos como SAM (Software Asset Management) e Descoberta do ITOM.

Ativo de Software

O Ativo de software permite que você procure discrepâncias existentes entre o software instalado relatado por dados importados dos conectores do Service Graph, seus produtos de verificação de vulnerabilidades e o software relatado por scanners que já está contabilizado na Gestão de ativos de software (SAM) e outros produtos da ServiceNow.

Entidades e seus relacionamentos com entidades secundárias

Entidade	Relacionamento	Entidade de destino	Descrição
Ativo de hardware	Relatado por	Origem do ativo	Representa uma origem que relatou este ativo no CMDB.
Ativo de hardware	Relatado somente por	Origem do ativo	Representa a única origem que relata este ativo no CMDB.
Ativo de hardware	Não relatado por	Origem do ativo	Representa uma origem que não relatou este ativo no CMDB.
Ativo de hardware	Com exceção de IRM	Exceção de IRM	Representa um registro de exceção na Gestão integrada de riscos.
Ativo de hardware	Com vulnerabilidade	Vulnerabilidade	Representa uma vulnerabilidade encontrada neste ativo.
Ativo de hardware	Tem descoberta de configuração	Configuração	Representa uma configuração e um problema de conformidade encontrados neste ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entidades e seus relacionamentos com entidades secundárias

Entidade	Relacionamento	Entidade de destino	Descrição
Ativo de hardware	Com metadados do CMDB	Metadados do CMDB	Representa a coleção de propriedades de IC do CMDB neste ativo.
Ativo de hardware	Com dados do conector	Conector do Service Graph	Representa uma coleção de propriedades relatadas pelo conector do Service Graph selecionado para este ativo.
Ativo de hardware	Com dados agregados	Dados agregados	Coleção de propriedades com valores agregados relatados por diferentes origens para um determinado ativo. Um exemplo é o SO.
Ativo de hardware	Da classe de IC	Classe de IC do CMDB	Usado para definir condições em propriedades de classe de IC específicas.
Ativo de hardware	Tem metadados de nuvem	Metadados da nuvem	Representa metadados em nuvem (aplicáveis a VMs em nuvem).
Ativo de hardware	Porta exposta à internet	OpenPort	Representa uma porta aberta para a Internet (aplicável a VMs em nuvem).
Software	Relatado por	Origem do ativo	Representa uma origem que relatou este software.
Software	Relatado somente por	Origem do ativo	Representa a única origem que relata este software.
Software	Não relatado por	Origem do ativo	Representa uma origem que não relatou este software.
Software	Com detalhes do software	Software	Representa a coleção de propriedades de software, como fornecedor e versão, por exemplo.

Auditoria de política de exemplo e preenchimento de dados: Classes de IC no CMDB

Se uma política tentar recuperar uma classe de ativo relatada ou não relatada por um conector do Service Graph específico, o Controle de postura de segurança mapeará todas as classes de item de configuração (IC) relevantes relacionadas a essa classe de ativo no CMDB que são preenchidas ou não preenchidas por esse Conector do Service Graph ou Categoria de conector.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, digamos que uma política procure todos os ativos de hardware relatados pelo Jamf Pro do Conector do Service Graph. A lógica a seguir se aplica.

1. O Controle de postura de segurança identifica quais classes de IC no CMDB são mapeadas para a classe "Ativo de hardware" do Jamf Pro.

   Nota: Diferentes Conectores do Service Graph preenchem diferentes classes de IC no CMDB, e o mapeamento para classes de IC de "Ativo de hardware" varia de um Conector do Service Graph para outro.

2. Controle de posturas de segurança Determina que as Classes de IC, Computador, Servidor e Impressora no CMDB são mapeados para a classe de ativo "Ativo de hardware" para o Jamf Pro do Conector do Service Graph.
3. Controle de posturas de segurança Em seguida, consulta todos os registros de ativos preenchidos em qualquer uma dessas três classes de IC: Servidor, Computador e Impressora pelo Conector Jamf Pro Service Graph no CMDB e retorna esses ativos.

   A coluna "Classes de IC compatíveis com SPC" na tabela a seguir indica quais classes de registros de IC são consideradas durante uma consulta pelo produto Controle de postura de segurança como parte de uma avaliação de política. Esta tabela não é uma lista abrangente, mas você pode usá-la para ver como os dados ingeridos de várias categorias e origens geralmente são mapeados e consultados.

Políticas incluídas com a aplicação

Ative os perfis de ativo e as políticas no Controle de posturas de segurança espaço que são Incluído com a aplicação para que você possa identificar lacunas na configuração ou na cobertura das ferramentas de segurança.

Criar suas próprias políticas

Consulte Criando suas próprias políticas no Controle de posturas de segurança aplicação para obter mais informações sobre como criar suas próprias políticas.

Por exemplo, políticas, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança.

Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

SGCs compatíveis

Para obter uma lista de alguns dos conectores do Service Graph compatíveis, consulte Conectores do Service Graph de hardware compatíveis com Controle de posturas de segurança e. Conectores do Service Graph de software compatíveis para Controle de posturas de segurança.

Políticas de controles de mitigação

Em Controle de posturas de segurança(SPC) Espaço, obtenha informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis com base em como as várias ferramentas de segurança são configuradas. Para obter mais informações, consulte Políticas de controles de mitigação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Políticas incluídas com Controle de posturas de segurança aplicação

Algumas políticas estão incluídas com Controle de posturas de segurança Aplicações vinculadas a casos de uso importantes e que são mostradas como informações importantes no painel na página principal (módulo inicial) no SPC Espaço.

Exibindo políticas

Para exibir essas políticas, navegue até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Tudo**.

Essas políticas são desativadas por padrão. Você deve ativá-los antes de exibir os resultados retornados (descobertas). Você não pode editar essas políticas, mas pode usá-las para ajudar a criar outras políticas clonando suas condições como ponto de partida. Para obter mais informações, consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.

Você pode clonar essas políticas para criar suas próprias políticas personalizadas, mas observe que todas as políticas clonadas não são refletidas como informações importantes no painel na página principal da Página inicial com as principais informações incluídas na aplicação. No entanto, você pode configurar descobertas para essas políticas clonadas e ver os resultados retornados dessas políticas.

Você pode configurar informações ou relatórios personalizados para as políticas clonadas ou, como alternativa, configurar descobertas para essas políticas clonadas para gerenciar a correção. Você também pode criar suas próprias políticas personalizadas do zero para monitorar a cobertura dos controles de segurança de acordo com seus requisitos internos.

As políticas enviadas com a aplicação incluem as seguintes categorias:

- Políticas que monitoram a cobertura dos controles de segurança (proteção de endpoint e verificador de vulnerabilidades).
- Políticas que identificam dispositivos não gerenciados.
- Políticas que monitoram combinações tóxicas que envolvem combinações críticas, como ausência de controles de segurança, exposição à internet e assim por diante.
- Políticas para SPC Integrações de API para monitoramento de controles de mitigação.

Depois de clonar e ativar todas as políticas criadas, você deve criar seu próprio registro de informações personalizadas no módulo Construtor de informações personalizadas no espaço (o último módulo no painel do navegador). Só então você poderá exibir os dados de suas políticas no painel Informações personalizadas (o segundo ícone de cima no espaço).

Políticas e perfis de ativos incluídos com a aplicação

Obtenha informações sobre sua postura geral de segurança e lacunas de configuração em suas ferramentas de segurança usando as políticas e os perfis de ativos incluídos com a aplicação. Ative esses perfis de ativo e políticas no Controle de posturas de segurança espaço para que você possa identificar lacunas na configuração ou cobertura das seguintes ferramentas:

- CrowdStrike
- Microsoft Intune, Defender e SCCM
- HCL Big Fix

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Qualys
- Rapid7

Criar suas próprias políticas

Consulte Criando suas próprias políticas no Controle de posturas de segurança aplicação para obter mais informações sobre como criar suas próprias políticas.

Por exemplo, políticas, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança.

Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Consulte Políticas de controles de mitigação para obter mais informações para obter mais informações sobre políticas usadas para monitoramento de controles de mitigação.

Criando suas próprias políticas no Controle de posturas de segurança aplicação

Você pode criar suas próprias políticas personalizadas para monitorar dados específicos dos ativos em seu ambiente. Você baseia essas políticas nos dados que importará dos vários conectores do Service Graph instalados e ativados.

Como começar

Você pode clonar políticas existentes e adicionar mais condições a elas ou criar uma política do zero. Para suas políticas personalizadas, você pode incluir critérios para propriedades comuns do CMDB preenchidas por vários conectores do Service Graph.

Como alternativa, você pode usar uma política de base como ponto de partida e incluir condições para exceções aprovadas com políticas para a aplicação Governance, Risk, and Compliance (GRC), por exemplo. Essas exceções são para ativos que você não deseja monitorar e incluir em suas contagens de ativos.

Para suas políticas personalizadas, você pode incluir condições para metadados como SO, versão do SO e FQDN, por exemplo, para ajudar a monitorar ativos com software mais antigo. Observe que essas propriedades são propriedades comuns do CMDB preenchidas por vários conectores do Service Graph para qualquer ativo específico.

Consulte Políticas incluídas com Controle de posturas de segurança aplicação Para obter mais informações sobre Tipos de ativos de nível superior e seus relacionamentos nas políticas do construtor de condições de política para você.

Por exemplo, políticas, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança.

Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Usando os decoradores E OU no construtor de condições

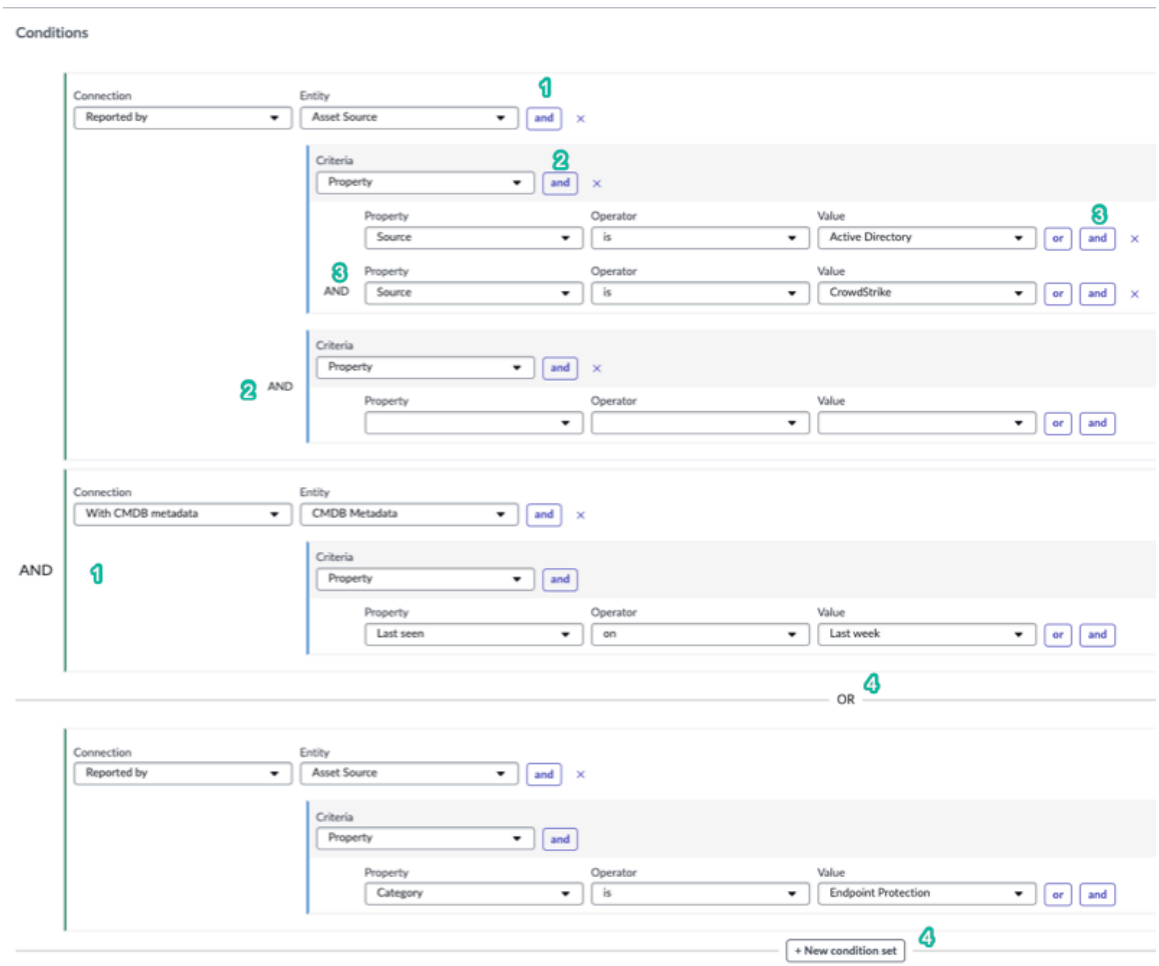
Você navega dos tipos de ativos de nível superior para hardware e software para suas entidades secundárias usando o construtor de condições no módulo Políticas e descobertas no espaço. Dependendo das suas escolhas, os campos serão exibidos para você e você modificará ou adicionará critérios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os decoradores E, OU no construtor de condições permitem que você configure a lógica dos dados retornados que você deseja retornar para a política.

Decorador	Descrição	Número referenciado na imagem
Selecione **E.** Ao lado dos campos Conexão e Entidade superiores para o novo conjunto de condições.	Adiciona um E lógico entre os critérios de entidade de conexão atuais e novos critérios de outra entidade de conexão.	1
Selecione **E.** À direita de um campo Critérios ou Propriedade para o novo conjunto de critérios e condições de propriedade.	Adiciona um E lógico entre os critérios de entidade de conexão atuais e um novo critério na mesma entidade de conexão.	2
Selecione **E/E** À direita de um campo de propriedade para o novo conjunto de condições de propriedade.	Adiciona um OR/AND lógico entre a propriedade atual e uma nova propriedade do mesmo Connection-entity-criteria.	3
Selecione **Novo conjunto de condições** para um novo conjunto de condições.	Adiciona um OR lógico entre o conjunto de condições de todos os critérios atuais e um novo conjunto de condições.	4



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando políticas base, clonagem e políticas secundárias

Você pode usar várias políticas para avaliar seus ativos e criar suas próprias informações personalizadas. Você tem as seguintes opções para ajudá-lo a criar políticas personalizadas ou editar políticas existentes rapidamente:

- Clonar política - Crie uma cópia de uma política. O nome da política e suas condições são exibidos com uma "cópia" no título. As condições são exibidas e você pode editá-las. Consulte Edite uma política ativada em Controle de posturas de segurança.
- Criar política secundária - O nome da política a partir da qual você iniciou é exibido como a "Política de base" no novo registro. As condições da sua política de base são herdadas na nova política e um novo conjunto de condições vazio é exibido. Consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.
- Políticas de exclusão - Adicione políticas às políticas personalizadas para que as descobertas de ativos das políticas selecionadas sejam excluídas dos resultados. Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança.

Metadados e filtragem do CMDB

Pode ser importante que suas equipes de segurança monitorem ativos com software mais antigo. Você pode especificar critérios de política começando com a Conexão "Com metadados do CMDB" após o tipo de ativo de hardware para incluir as propriedades comuns listadas abaixo. Esta não é uma lista completa. Para coletar esses metadados, as propriedades devem estar disponíveis na conexão Metadados do CMDB preenchida pelos conectores do Service Graph.

- RAM
- Nome do host
- Número de série
- Domínio do SO
- Versão do SO
- Espaço em disco
- Visto pela última vez
- SO
- Visto pela primeira vez
- Contagem de CPUs
- Fabricante de MAC
- NIC
- Endereço IP
- Local
- FQDN
- Máscara de rede
- Versão do IP
- Tipo de número de série
- Service pack do SO

A partir da v3.0 de Controle de posturas de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Conexão "Com metadados do CMDB" permite que você adicione a propriedade Nome do host e use o operador regex de correspondências para ajudá-lo a digitar expressões regulares em suas condições para o tipo Ativo de hardware. Por exemplo, se você inserir "lp", poderá procurar todos os laptops com "lp" como segundo e terceiro caracteres no nome do host.

"Vistos pela primeira vez": Ativos que foram descobertos pela primeira vez por qualquer origem dentro do intervalo de tempo selecionado com a propriedade de carimbo de data/hora "Visto pela primeira vez".

"Visto pela última vez": Ativos que foram "vistos pela última vez nos últimos n dias" por qualquer origem. Insira o número de dias até 30 como um valor. Por exemplo, insira 3 como um valor para monitorar ativos por "último logon" do Active Directory nos últimos três dias.

Tipo de ativo de software: Procure fornecedores de software ou use SGCs que você instalou para importar dados de software e metadados desejados se começar com a Conexão "com detalhes de software".

Para tipos de ativos de hardware, você pode usar a Conexão "Tem informações do modelo" com a Conexão "Com metadados do CMDB" para dispositivos com base em modelos específicos e informações do modelo.

Os tipos de ativos de hardware também permitem pesquisar todos os ativos relatados por uma origem, Qualys, por exemplo, mas que não são relatados pela Descoberta do ITOM da ServiceNow.

Consulte Políticas para Controle de posturas de segurança para obter mais informações sobre Controle de posturas de segurança esquema de política.

Exceções com a aplicação Governance, Risk, and Compliance (GRC)

Uma exceção de Gestão de riscos integrada (IRM) é um ativo com uma exceção aprovada do produto Governance, Risk, and Compliance (GRC). Em uma política, você tem a opção de adicionar uma condição para uma exceção para não monitorar esses ativos e incluí-los em suas contagens.

Por exemplo, alguns ativos podem ter exceções aprovadas para determinados objetivos de controle com IRM. Para reduzir suas correspondências retornadas, as equipes de segurança da informação podem excluir esses ativos do monitoramento de controles de segurança com exceções de IRM que já foram aprovadas.

Principais informações e informações configuradas para Controle de posturas de segurança

As informações principais e configuradas (personalizadas) fornecem relatórios visuais que são criados e atualizados pelos critérios de avaliação que correspondem aos seus ativos. As informações ajudam você a monitorar métricas de controles de segurança em um painel.

Informações principais

Os critérios usados para as avaliações de seus ativos são fornecidos pelas políticas incluídas com a aplicação .

- As principais informações usam as políticas incluídas com a aplicação .
- As informações configuradas podem ser criadas usando as políticas incluídas com a aplicação, suas próprias políticas personalizadas ou uma combinação de ambas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na Página inicial (página principal) no espaço Controle de postura de segurança, a seção Informações principais abaixo da Visão geral exibe relatórios visuais que são criados e atualizados pelas políticas incluídas com a aplicação. Essas informações também estão incluídas com a aplicação e exibem as seguintes informações:

- Agente de proteção de endpoint instalado: Número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: Número de ativos gerenciados em comparação com aqueles que não são gerenciados.
- Cobertura de verificação de vulnerabilidades: Número total de ativos verificados em comparação com aqueles que não são verificados quanto a vulnerabilidades conhecidas por um verificador de vulnerabilidades de terceiros.
- Ativos com vulnerabilidades críticas: Número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: Número total de itens vulneráveis divididos por gravidade. Uma vulnerabilidade conhecida que corresponde a um ativo em seu CMDB resulta em um item vulnerável. Esta informação requer que você instale a aplicação Resposta a vulnerabilidades e pelo menos uma integração de scanner: Qualys, Rapid7 ou Integração de vulnerabilidades do Tenable. Todas essas aplicações estão disponíveis no ServiceNow® Store.
- 3 principais políticas por descobertas: Políticas que retornam a maioria das descobertas (correspondências) em seus ativos.

Informações configuradas

Você pode criar suas próprias informações se quiser que mais informações não sejam encontradas nas Informações principais. Você pode criar essas informações configuradas e usar políticas existentes ou suas próprias políticas personalizadas para avaliação. Suas informações configuradas são exibidas no módulo do painel de informações configuradas, o segundo ícone na parte superior do espaço.

Os seguintes tipos de informações podem ser configurados.

- Gráfico de comparação: Compare resultados entre várias políticas com gráficos de barras.
- Widget de contagem de correspondência de política: Exiba o número de dispositivos que correspondem a uma política.
- Gráfico de porcentagem de correspondência de política: Exiba a porcentagem de dispositivos que correspondem a uma política em um gráfico de pizza. Você pode escolher o pool de ativos total como todos os ativos monitorados pelo SPC ou os ativos que correspondem à política de base a partir da qual a política selecionada atual é criada.
- Gráfico de tendências de política: Exiba as tendências de ativos que correspondem a várias políticas.

Consulte Crie e ative uma informação configurada para o Controle de postura de segurança para obter mais informações sobre as etapas para criar uma informação configurada.

Grupos

Você deve criar ou atribuir grupos às informações configuradas ao criar novos registros no módulo Construtor de informações personalizadas. Os grupos permitem que você organize seus relatórios no painel de informações configurado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As informações podem ser organizadas em grupos. Cada grupo pode ter 21 widgets ou informações.

Usando o. Controle de posturas de segurança espaço

. Controle de posturas de segurança o espaço contém os módulos que você usa para configurar, usar e monitorar os dados importados sobre seus ativos.

Funções

Grupo de administradores do SPC

Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, incluindo informações de licenciamento. As funções granulares deste grupo incluem: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin e sn_sec_spc_core.configure].

Grupo de analistas do SPC

Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, mas não podem exibir as informações de licenciamento. As funções granulares deste grupo incluem [pa_power_user e sn_sec_spc_core.analyst].

Analista do SPC somente leitura

Os usuários neste grupo têm acesso total de leitura a todos os registros do produto, mas não podem exibir informações de licenciamento. As funções granulares deste grupo incluem [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read e cmdb_ms_user].

Funções da aplicação de suporte

As funções a seguir são exigidas pelas aplicações compatíveis com SPC e. Gestão de posturas de segurança para ativos.

- Conformidade de configurações Administrador [sn_vulc.admin] - Configura o. Conformidade de configurações a aplicação tem visibilidade de todos os registros e pode modificar propriedades. Atribui funções no Conformidade de configurações aplicação.
- Resposta a vulnerabilidades Administrador [sn_vulc.admin] - Configura a aplicação Resposta a vulnerabilidades e as calculadoras de risco de vulnerabilidade.
- MID Server [mid_server] - Configura um MID Server.

Os módulos do espaço

Para acessar o espaço, navegue até **Espaços** > **Controle de posturas de segurança** A Página inicial (página principal) é exibida. . Controle de posturas de segurança o espaço contém os seguintes módulos.

Módulos

Módulo	Descrição
Página inicial	Exiba visualizações de dados e outras informações nas seções Visão geral, Informações principais e Cobertura de caso de uso principal para ajudar você a monitorar seus ativos. As informações fornecidas nesta página permitem que você relate o status da

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos

Módulo	Descrição
	sua postura geral de segurança para TI, gerentes DE TI e segurança e outras partes interessadas importantes. Consulte Principais informações e informações configuradas para Controle de posturas de segurança e Políticas para Controle de posturas de segurança.
Informações configuradas	Exiba as visualizações de dados sobre seus ativos que você cria, configura e ativa. Consulte Principais informações e informações configuradas para Controle de posturas de segurança.
Pesquisa de ativos	PESQUISE rapidamente ativos em seu ambiente com base nas condições definidas. Verifique se você pode localizar ativos com um conjunto de condições antes de confirmar essas condições a uma política. Você pode refinar essas pesquisas para obter uma visualização dos ativos que atendem aos seus critérios de pesquisa. Quando estiver pronto, você pode salvar suas condições como uma política. Consulte Crie uma pesquisa de ativos no Controle de postura de segurança.
Perfis dos ativos	Crie e defina perfis de ativos para monitorar diferentes categorias de dispositivos com suas políticas de SPC. Incorpore seus perfis de ativos em suas políticas para que você possa executar políticas para tipos específicos de ativos. Filtre as informações no painel Informações configurado para que elas sejam baseadas em seus perfis de ativos. Consulte Crie um perfil de ativo em Controle de posturas de segurança.
Políticas e descobertas	Crie, clone, edite e ative políticas. Há políticas incluídas com a aplicação e você pode criar suas próprias. As políticas auditam seus ativos para encontrar correspondências para possíveis violações. Informações, visualizações e casos de uso dependem das políticas. Consulte Políticas para Controle de posturas de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos

Módulo	Descrição
	Os ativos que correspondem às condições da política são relatados como descobertas e são mapeados para Conformidade de configurações aplicação para correção. Consulte Controle de postura de segurança: Configurar e exibir suas descobertas.
Configuração de conectores e casos de uso	Ative e exiba o status dos Conectores do Service Graph (SGC) instalados e das integrações de API. Os Conectores do Service Graph e as integrações de API são fontes que você usa para importar dados sobre seus ativos. #Uma ampla variedade de (SGC) é compatível e está disponível no ServiceNow® Store. Configurar e monitorar os principais casos de uso. Os casos de uso são diferentes cenários que você configura para ajudar a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos em busca de possíveis violações. Consulte Casos de uso, exemplos de política e conectores do Service Graph compatíveis em Controle de posturas de segurança.
Construtor de informações personalizadas	Crie suas próprias visualizações de dados. As informações personalizadas fornecem relatórios visuais que são atualizados pelos resultados de auditoria de suas políticas e dados importados. Depois de ativá-los, suas informações personalizadas serão exibidas no painel no módulo de informações configurado. Você pode determinar onde os dados de uma informação são exibidos no painel usando grupos. Consulte Crie e ative uma informação configurada para o Controle de postura de segurança.

Usando os módulos do espaço para identificar lacunas na cobertura da ferramenta

Identificar lacunas da ferramenta de segurança requer que você execute as etapas a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Configure e ative conexões de API com qualquer uma das ferramentas que você está usando em várias categorias. Você pode usar Conectores do Service Graph para produtos que estão disponíveis na ServiceNow Store para as conexões de API necessárias. Para obter mais informações sobre os conectores do Service Graph compatíveis, consulte Conectores do Service Graph para Controle de posturas de segurança e. Conectores do Service Graph . Os conectores do Service Graph compatíveis estão disponíveis no ServiceNow® Store com assinaturas separadas.
2. Execute uma ou mais pesquisas de ativos com base em critérios específicos para obter um inventário.
3. Ative as políticas enviadas com a aplicação Controle de postura de segurança. Ou você também pode criar suas próprias políticas e ativá-las com base nos resultados de suas pesquisas de ativos.
4. Crie e ative suas próprias informações configuradas para ajudar você a monitorar seus ativos.
5. Para obter informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis com base em como as várias ferramentas de segurança são configuradas, consulte Monitoramento de controles de mitigação usando o Controle de posturas de segurança.
6. Configure regras para automatizar o fluxo de trabalho de correção na aplicação Conformidade de configuração.

Identificar lacunas da ferramenta de segurança envolve as seguintes etapas:

1. Ative as políticas enviadas com o. Controle de posturas de segurança aplicação. . Controle de posturas de segurança o produto encontra lacunas na ferramenta de segurança executando as seguintes tarefas:
   a. Identifica a lista de todos os ativos exclusivos preenchidos por vários conectores do Service Graph no CMDB.
   b. Identifica ativos que não são relatados por categorias específicas deste grupo de ativos, por exemplo, Proteção de endpoint. Os ativos são identificados com base na política ativa que está sendo avaliada.
   c. Os ativos identificados como não relatados por categorias específicas são relatados como "Descobertas" ou "Resultados de teste" em Conformidade de configurações aplicação.
2. Atribua automaticamente "descobertas" a diferentes equipes para correção com a aplicação Conformidade de configuração.

Criar suas próprias políticas

Consulte Criando suas próprias políticas no Controle de posturas de segurança aplicação para obter mais informações sobre como criar suas próprias políticas.

Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Por exemplo, políticas, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança.

Ativar uma política incluída com Controle de posturas de segurança aplicação

As políticas incluídas com a aplicação devem ser ativadas antes Controle de posturas de segurança pode monitorar os ativos que correspondem a essa política. Por padrão, nenhuma das políticas incluídas com a aplicação está ativada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Você deve verificar se todos os pré-requisitos necessários foram atendidos antes de ativar as políticas incluídas com a aplicação.

- Verifique se os Conectores do Service Graph necessários estão ativados.
- Verifique se todas as aplicações necessárias, como Resposta a vulnerabilidades, estão instaladas e ativadas, se aplicável.
- Para obter mais informações sobre políticas usadas para monitoramento de controles de mitigação, consulte Políticas de controles de mitigação.

Nota:

Não é possível editar as políticas incluídas com a aplicação, mas é possível criar novas políticas com base em seus critérios com **Política de clone** e. **Criar política secundária** recursos. Esses recursos estão disponíveis no menu Mais opções (três pontos verticais).

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Tudo**.

   Para determinar se uma política está ativada, confirme seu status (verdadeiro ou falso Na coluna Ativo.

2. Selecione um registro de política para abri-lo.
3. Você tem as seguintes opções nos registros de política incluídos com a aplicação:

Opção	Descrição
Ativar política	Ative uma política se quiser monitorar quaisquer ativos que correspondam às condições da política e gerar descobertas. Se disponível, selecione Desativar política para interromper as avaliações de ativos e a geração de descobertas para esta política.
Configurar descobertas	Selecione **Sim** no modal para gerar descobertas para a política. Selecione **Configurar regras de atribuição** Link para configurar regras de atribuição na aplicação Conformidade de configuração para atribuir descobertas à sua política para resolução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Para políticas que você cria com "Software" como o tipo de ativo, você pode salvar a política e criar informações personalizadas, mas não pode configurar descobertas do registro da política.
Clonar política	Crie uma nova política com todas as condições da política exibida como ponto de partida. Para obter mais informações, consulte Crie e ative políticas personalizadas para Controle de posturas de segurança.
Crie uma política secundária	Crie uma política secundária que herde as condições da política atual. As condições da política atual são exibidas no campo "Política de base" no novo registro e você adiciona mais condições.
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política. Esta opção de edição só está visível em registros de política ativados.
Visualizar descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são chamadas de CTRs ou registros de resultados de testes para a política.

Crie e ative políticas personalizadas para Controle de posturas de segurança

Crie suas próprias políticas personalizadas para monitorar ativos para cobertura de ferramentas e outras combinações de alto risco.

Antes de Iniciar

Para ajudar você a entender as etapas necessárias para criar uma política com mais detalhes, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança. Os exemplos orientam você pelas etapas necessárias para criar uma política de base, usar a política de base para criar uma política secundária e clonar uma política.

Por exemplo, políticas, consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança.

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Tudo**.
2. Selecione **Nova política** .
3. Selecione o ícone de lápis ao lado do nome na parte superior para modificar os metadados.

   Preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Um nome exclusivo para sua política.
Criticalidade	Selecione um na lista.
Descrição resumida	Uma descrição exclusiva para sua política.

4. Selecione **Salvar metadados** .
5. Em Tipo de ativo, selecione Ativado na lista.

Opção de entidade	Descrição da entidade
Hardware	Localize dispositivos IP que incluem dispositivos de computação pessoal, máquinas virtuais em nuvem, servidores, dispositivos de rede e outros hardwares.
Software	Localize o software instalado em dispositivos relatados por SGCS e seus scanners de vulnerabilidade.

6. **Opcional:** Escolha nenhum, um ou ambos.

Opção	Descrição
Política de base	As condições da opção de política base são herdadas na nova política.
Políticas de exclusão	Selecione todas as políticas que você deseja excluir das descobertas de ativos desta política. Todas as descobertas dessas políticas são ignoradas.

(Optional) Os campos Conexão e Entidade são exibidos.

7. Selecione um na lista para o campo Conexão.
O campo Entidade de destino é preenchido automaticamente com base em sua escolha. Um novo campo Critérios é exibido junto com os campos Propriedade, Operador e Valor. Para obter mais informações sobre tipos de ativos e o esquema para relacionamentos, consulte Políticas para Controle de posturas de segurança.
8. Selecione um na lista para Propriedade.
9. Selecione **Categoria** ou **Origem** .
10. Selecione um operador e insira uma categoria de conector, por exemplo, Gestão de endpoint ou um nome de produto de categoria (origem).
11. **Opcional:** Use o construtor de condições e adicione mais condições ou conjuntos de condições.

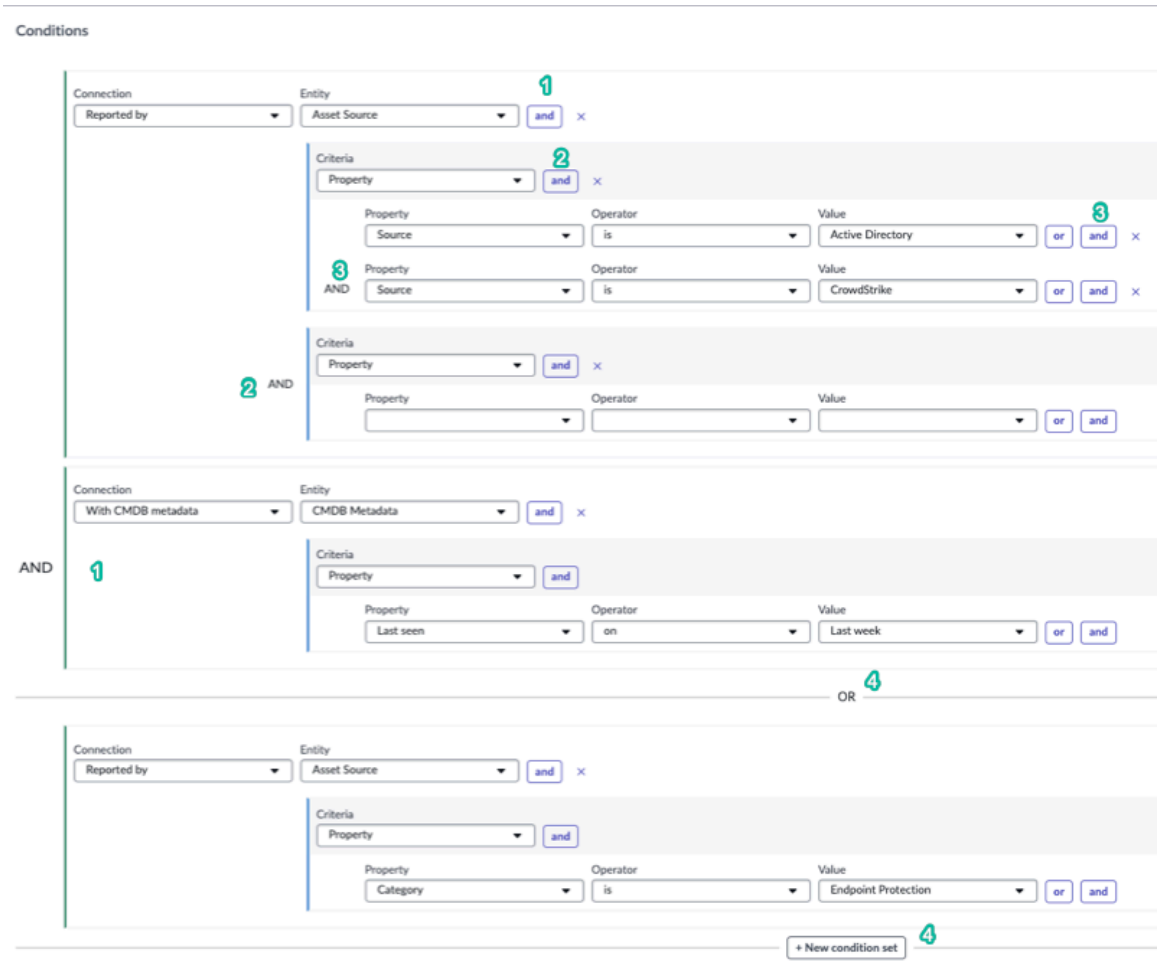
(Optional) Navegue dos tipos de ativos de nível superior para hardware e software para suas entidades secundárias usando o Construtor de condições. Dependendo das suas escolhas, os campos serão exibidos para você e você modificará ou adicionará critérios.

Os decoradores E, OU no construtor de condições permitem que você configure a lógica dos dados retornados que você deseja retornar para a política. Consulte a tabela e a imagem a seguir para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Decorador	Descrição	Número referenciado na imagem
Selecione **E.** Ao lado dos campos Conexão e Entidade superiores para o novo conjunto de condições.	Adiciona um E lógico entre os critérios de entidade de conexão atuais e novos critérios de outra entidade de conexão.	1
Selecione **E.** À direita de um campo Critérios ou Propriedade para o novo conjunto de critérios e condições de propriedade.	Adiciona um E lógico entre os critérios de entidade de conexão atuais e um novo critério na mesma entidade de conexão.	2
Selecione **E/E** À direita de um campo de propriedade para o novo conjunto de condições de propriedade.	Adiciona um OR/AND lógico entre a propriedade atual e uma nova propriedade do mesmo Connection-entity-criteria.	3
Selecione **Novo conjunto de condições** para um novo conjunto de condições.	Adiciona um OR lógico entre o conjunto de condições de todos os critérios atuais e um novo conjunto de condições.	4



12. Selecione **Salvar política** depois de terminar a edição.
    Sua política foi salva. Você pode optar por ativá-lo agora ou retornar mais tarde para ativá-lo.
13. No menu Mais opções ao lado de **Salvar política** , selecione configurar descobertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

14. Preencha os campos.

Opção	Descrição
Gerar descobertas para esta política?	Escolha **Sim** gerar descobertas para ativos correspondentes. Depois que os dados forem importados, selecione Exibir descobertas será exibido no registro da política. Escolha **Não** se você não quiser gerar descobertas.
Configurar regras de atribuição	Selecione o link para configurar regras de atribuição para atribuir descobertas para correção na aplicação Conformidade de configuração. Há uma regra de atribuição padrão na tabela [sn_vulc_assignment_rule_list] que você pode usar em Conformidade de configuração.

15. Selecione **Salvar configuração** .

Depois de salvar e ativar uma política, ele avalia os dados importados do conector do Service Graph programado na próxima execução. Se você quiser exibir os dados no painel de informações configurado no espaço, crie uma Nova informação no módulo Construtor de informações personalizadas. Depois de ativar a informação configurada, seus dados são exibidos no painel de informações configuradas no espaço .

Edite uma política ativada em Controle de posturas de segurança

Você pode editar as políticas ativadas para ajudar a personalizar as condições para corresponder melhor aos seus ativos.

Antes de Iniciar

Não é possível editar as políticas incluídas com a aplicação, mas é possível clonar e criar políticas secundárias a partir delas. Consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.

Se você editar políticas e publicar suas mudanças, as versões serão rastreadas e os números de versão serão exibidos no registro da política e nos resultados de testes relacionados.

Antes de editar uma política ativada, você pode preferir desativá-la para que a política não continue a avaliar seus ativos enquanto você edita.

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Tudo**.
2. Selecione um registro de política para abri-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Editar política** .
   Se você estiver editando pela primeira vez, dois botões desativados serão exibidos ao lado do ativo **Sair do modo de edição** botão: **Salvar mudanças** e. **Publicar mudanças** . Se você editou anteriormente esta política e a salvou como rascunho, a notificação, Você tem uma edição não publicada também é exibido.
4. Faça suas edições e escolha uma para continuar.

Opção	Descrição
Salvar mudanças	Salve suas mudanças como rascunho e retorne ao modo de edição. Suas mudanças não são publicadas neste momento e você pode retornar à política e continuar editando mais tarde.
Publicar mudanças	Publique suas mudanças como uma nova versão da política e saia automaticamente do modo de edição. Pode levar algum tempo para que as descobertas sejam exibidas em sua nova versão da política no botão Exibir descobertas da política. Se você publicar uma nova versão de uma política, terá a opção de fechar todas as descobertas existentes para a política que você alterou. Você pode preferir fechar todas as descobertas existentes da política original se quiser exibir somente as descobertas da política alterada. Se você cancelar neste momento ou sair do modo de edição, será exibida uma mensagem informando que você tem uma edição não publicada para esta política. Se você optar por fechar os resultados de testes relacionados existentes (descobertas), os estados do resultado do teste e da tarefa de correção serão transferidos de acordo com os processos de transição de estado da aplicação Conformidade de configuração. Para obter mais informações, consulte Resultado de teste e transições de estado da tarefa de correção no Controle de posturas de segurança aplicação.
Exibir histórico da versão	Para mudanças publicadas, as versões são rastreadas e os números de versão são exibidos no registro da política e nos resultados de testes relacionados.
Sair do modo de edição	Saia sem salvar suas mudanças ou salve suas mudanças e saia sem publicar. Se você salvar suas mudanças e não publicá-las, deverá publicar sua nova versão antes que ela possa criar descobertas.
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	relação a essa política. Esta opção de edição só está visível em registros de política ativos.
Visualizar descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são referidas a CTRs ou registros de resultados de testes para a política.

5. Depois de salvar a política como rascunho e sair do modo de edição, selecione uma das seguintes opções:

Opção	Descrição
Editar política	Retorne ao modo de edição.
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política. Esta opção só está visível em registros de política ativos.
Menu de mais opções	
Configurar descobertas	Selecione **Sim** no modal para gerar descobertas para a política. Consulte Controle de postura de segurança: Configurar e exibir suas descobertas.
Clonar política	Crie uma cópia do registro da política. Consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.
Criar política secundária	Crie uma nova política usando esta política como base. Consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.
Excluir política	Remova o registro de política da lista de políticas.
Visualizar descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são chamadas de registros de resultado de teste (CTRs) para a política.
Exibir registros vinculados	Para políticas publicadas, exiba informações personalizadas, se disponíveis. Veja Crie e ative uma informação configurada para o Controle de postura de segurança

Clone uma política ou crie uma política secundária em Controle de posturas de segurança

Clone uma política existente e adicione condições a ela para criar sua própria política personalizada. Você também pode criar políticas secundárias a partir de políticas existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Você pode clonar políticas para criar suas próprias políticas personalizadas. Você pode clonar uma política ou criar uma política secundária usando qualquer política como base para ajudá-lo a estender as políticas existentes sem precisar inserir as condições novamente. Todas as condições na política de base também são herdadas na política secundária. Para obter mais informações, consulte Clone uma política ou crie uma política secundária em Controle de posturas de segurança.

Você pode clonar todas as políticas incluídas com a aplicação, mas as correspondências de política não são refletidas como informações importantes no painel na página principal inicial. Somente as principais informações das políticas incluídas com a aplicação são exibidas na página principal inicial.

Depois de clonar e ativar todas as políticas criadas, você deve criar seu próprio registro de informações configurado no módulo Construtor de informações personalizadas no espaço (o último módulo no painel do navegador). Só então você poderá exibir os dados de suas políticas no painel de informações configurado (o segundo ícone de cima no espaço).

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Tudo**.
2. Selecione o registro de política que você deseja clonar.
3. Selecione um no menu Mais opções ao lado de **Ativar política** .

Opção	Descrição
Clonar política	Selecione esta opção se quiser usar as condições de uma apólice existente como ponto de partida para sua nova apólice. Uma nova guia com o registro de política clonada é exibida com "cópia" no nome. (Opcional) Selecione Política de base e adicione uma na lista para sua nova política.
Criar política secundária	Selecione esta opção se quiser criar uma nova política usando a política atual como ponto de partida. Uma nova guia com um registro de política em branco com uma política de base escolhida é exibida.

4. **Opcional:** Selecione **Política de base** e selecione uma política como base para sua nova política.

   (Optional) Você pode escolher esta opção se quiser herdar as condições de uma apólice existente como ponto de partida para sua nova apólice.

5. **Opcional:** Selecione **Políticas de exclusão** e selecione as políticas que você deseja excluir das descobertas desta política.
   Suas descobertas em sua nova política que correspondam a todas as políticas excluídas não serão incluídas em suas descobertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Para uma política clonada, edite as condições.
   Para obter mais informações sobre os relacionamentos Ativo-conexão-entidade no Construtor de condições, consulte Políticas para Controle de posturas de segurança. Para obter mais informações sobre os decoradores no construtor de condições, consulte Criando suas próprias políticas no Controle de posturas de segurança aplicação.
7. Edite e salve sua política com **Salvar mudanças** .
   Sua política é exibida na lista Todos no módulo Lista no espaço .
8. Para ativar uma política, siga as etapas descritas em Crie e ative políticas personalizadas para Controle de posturas de segurança.
9. **Opcional:** Selecione Excluir política para excluir uma política.
   A opção de exclusão não é compatível com políticas que vêm com a aplicação ou com políticas que geraram descobertas. Você só pode desativar políticas com descobertas.

Crie e ative uma informação configurada para o Controle de postura de segurança

Você pode criar suas próprias informações. As informações configuradas são informações que você pode criar usando políticas existentes ou suas próprias políticas personalizadas.

Antes de Iniciar

Você deve criar um registro de informações e ativá-lo antes de exibir seus dados no painel de informações configurado. Você pode ter até seis informações e 21 gráficos no módulo do painel de informações configurado no espaço .

Todas as políticas que você usa para obter informações personalizadas devem ser ativadas.

Para políticas que você cria com "Software" como o tipo de ativo, você pode salvar a política e criar informações personalizadas, mas não pode configurar descobertas do registro da política.

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Construtor de informações**.

   Nesta página principal, há três guias:

   Ativo

   Suas informações personalizadas ativadas. As informações personalizadas ativadas são exibidas na página principal de informações configuradas (segundo ícone a partir da parte superior do espaço).

   Inativo

   Suas informações personalizadas inativas. As informações desativadas não são exibidas na página principal de informações configuradas até que as informações e suas políticas de suporte que as apoiam sejam ativadas.

   Tudo

   Todas as suas informações configuradas ativas e inativas.

2. Selecione **Nova informação** à direita da página para criar um novo registro.
3. No campo Tipo, selecione uma informação na lista de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Gráfico de comparação	Compare contagens de ativos correspondentes para até cinco apólices.
Widget de contagem de correspondência de políticas	O número total de seus ativos que correspondem a uma política ou políticas.
Gráfico de porcentagem de correspondência de políticas	A porcentagem do total de ativos que correspondem ou não a uma política.
Gráfico de tendências de correspondência de políticas	Tendência histórica de ativos que correspondem a uma política ou políticas.

4. Selecione um.
   - Ativo de hardware ou máquina virtual em nuvem
   - Software
5. Selecione grupos para suas informações.
   Uma informação deve pertencer a pelo menos um grupo. Você deve criar ou atribuir grupos às informações configuradas ao criar novos registros no módulo Construtor de informações personalizadas. Os grupos permitem que você organize seus relatórios no painel de informações configurado.
6. Selecione as políticas e os rótulos correspondentes desejados para seus dados de informações.
7. Selecione **Save** (Salvar).
   Suas informações são salvas na guia Informações inativas.
8. Para ativar sua nova informação, abra o registro na lista Inativos e selecione **Ativar** .
   Os dados são coletados da próxima importação programada para os Conectores do Service Graph associados às políticas do insight, e os dados são exibidos no módulo do painel Informações personalizadas no espaço.

Crie um perfil de ativo em Controle de posturas de segurança

Crie um perfil de ativo com condições para agrupar ativos. Você pode usar esses perfis de ativo em suas políticas.

Antes de Iniciar

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Perfis dos ativos**.
2. Selecione **Novo**.
   O Construtor de condições é exibido. Observe que o nome inclui a data e a hora em que você criou o perfil.
3. Selecione o ícone de caneta para editar o nome do perfil com um nome exclusivo.
4. Selecione **Salvar metadados** .
5. Selecione um na lista para Conexão:

   O perfil de ativo oferece suporte a três tipos de conexão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Com metadados do CMDB** - Coleção de propriedades de IC do CMDB, como nome do host, SO, versão do SO, primeira e última exibição, por exemplo, ou conexões que têm adaptadores de rede ou software instalado.
- **Com dados agregados** - Coleção de propriedades com valores agregados relatados por diferentes origens para um determinado ativo. Um exemplo são as várias maneiras pelas quais as origens podem relatar uma versão do SO: janelas 11 , Win11 , Windows 11 e assim por diante.
- **Da classe de IC** - Coleção de classes de IC que inclui computador, servidor, instância de máquina virtual e outros.

Os operadores e a lógica deste construtor de políticas de perfil de ativo são semelhantes aos descritos em Criando suas próprias políticas no Controle de posturas de segurança aplicação.

6. Selecione **Criar**.
   Seu perfil é exibido na lista Perfis de ativo.

   Você pode associar perfis de ativo a qualquer política.
7. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Políticas e descobertas**.
8. Selecione uma política.
9. Na seção Políticas e perfis, selecione um ou mais perfis de ativo.
10. Selecione **Salvar mudanças**.
    A política audita seus ativos com base nos dados importados dos conectores do Service Graph e inclui as condições dos perfis de ativos adicionados. Você pode Crie e ative uma informação configurada para o Controle de postura de segurança e adicionar perfis de ativo como um filtro.
11. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Informações configuradas**.
    Você deve Crie e ative uma informação configurada para o Controle de postura de segurança antes que os dados sejam exibidos nesta página.

    Como as visualizações nesta página são configuradas por políticas, você pode filtrá-las com perfis de ativos. Filtre os dados das visualizações seguindo estas etapas:
12. Selecione o ícone de filtro.
13. Selecione **Selecione** .
14. Selecione e mova qualquer um dos perfis de ativo na coluna Disponível para a coluna Aplicado.
15. Selecione **Aplicar**.
    As visualizações de informações personalizadas são filtradas para mostrar dados das políticas que incluíam os perfis de ativos escolhidos. Uma mensagem no painel Filtro indica quantas informações configuradas são filtradas como resultado dos perfis de ativos adicionados. Pode haver um atraso para as atualizações dos dados de tendências, porque o trabalho programado Executar política de SPC deve ser concluído para atualizar os dados de tendências.

Exclua um perfil de ativo em Controle de posturas de segurança

Você pode excluir perfis de ativo. Você exclui perfis de ativo se eles estiverem associados a políticas para que as condições do perfil de ativo não sejam incluídas na próxima auditoria de política.

Antes de Iniciar

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Perfis dos ativos**.
2. Selecione um registro de perfil.
3. Selecione o ícone do menu Mais ações (⋮) e selecione **Excluir perfil de ativo** .
4. **Opcional:** Na caixa de diálogo, selecione **Revise as políticas** para exibir todas as políticas às quais este perfil está vinculado.
   As políticas que contêm o perfil de ativo são listadas na guia Políticas vinculadas.
5. Selecione a guia com o perfil de ativo que você deseja excluir.
6. Selecione o ícone do menu Mais ações e selecione **Excluir perfil de ativo** .
   Esta é uma exclusão definitiva. As condições do perfil de ativo são removidas de todas as políticas e não são incluídas nas próximas auditorias de política noturna para obter os resultados mais recentes.

Controle de postura de segurança: Configurar e exibir suas descobertas

Você pode exibir as descobertas geradas pela avaliação de políticas no Controle de postura de segurança no Espaço de controle de postura de segurança.

Visão geral das descobertas

Todos os ativos correspondentes são relatados como "descobertas". Você pode configurar descobertas a serem geradas a partir da execução de políticas para que essas descobertas possam ser atribuídas a várias equipes para correção ou usadas para emissão de relatórios. O Controle de postura de segurança publica essas descobertas como "Resultados de teste" no módulo Conformidade de configuração. Todos os controles administrativos na aplicação Conformidade de configuração relacionados a atribuição, agrupamento (geração de tarefa de correção), destinos de correção e exceções são compatíveis com descobertas geradas pelo Controle de postura de segurança.

Os tipos de descobertas:

Cobertura da ferramenta

Este tipo representa uma lacuna de cobertura da ferramenta de segurança. Este tipo de descoberta é aplicável a políticas que usam relacionamentos "relatado por conector" e "Não relatado por conector".

Exposição na Internet

Este tipo representa a exposição na internet de um ativo em nuvem. Este tipo de descoberta é aplicável a políticas que usam o relacionamento "has-internet-exposed-port" no CloudVM.

Combinação de alto risco

Este tipo representa um problema que tem mais de um fator de risco associado, ou seja, ativos com vulnerabilidades críticas e um agente de proteção de endpoint ausente.

Dependendo dos relacionamentos usados nas políticas, os tipos de descoberta disponíveis ficam visíveis quando você seleciona, **Configurar descobertas** . Por exemplo, se você selecionar **Configurar descobertas** Em uma política que tem mais de um fator de risco, como "Ativos em nuvem com vulnerabilidades críticas, proteção de endpoint ausente e porta SSH 22 aberta para a Internet", as seguintes opções são exibidas como tipos de descoberta que podem ser gerados.

1. Combinação de alto risco
2. Cobertura da ferramenta
3. Exposição na Internet

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode optar por gerar descobertas do tipo "Combinação de alto risco", o que cria uma descoberta por cada ativo correspondente a esta política. Como alternativa, você pode optar por criar descobertas do tipo "Cobertura de ferramentas" e "Exposição na internet", o que resultará em duas descobertas criadas por cada ativo que corresponda à política: Uma do tipo "Cobertura de ferramentas" e uma do tipo "Exposição na internet".

Usando o tipo de descobertas ou Resultado de teste, você pode escrever regras de atribuição em Conformidade de configuração para rotear esses problemas para as respectivas equipes para correção. Por exemplo, você pode enviar descobertas de "Cobertura da ferramenta" para a equipe de operações de TI e "Exposição na Internet" para a equipe de aplicações.

No entanto, se um dos responsáveis pela correção corrigir o problema, a outra descoberta será fechada automaticamente, porque essas descobertas serão geradas a partir de uma política que procura a combinação. Por exemplo, se a equipe de operações de TI fechar a descoberta "Cobertura da ferramenta" instalando o agente de proteção de endpoint, a descoberta "Exposição na Internet" gerada a partir desta política será encerrada automaticamente, mesmo que o ativo seja voltado para a internet, já que essa descoberta é gerada a partir de uma política que procura uma combinação de problemas. Se você quiser acompanhar o problema de exposição da internet nos ativos, é recomendável criar outra política que procure apenas exposição da internet nos ativos e não qualquer outro fator de risco.

Onde exibir as descobertas

Você tem essas opções para exibir as descobertas geradas pela avaliação de políticas.

- Navegar até **Espaço de controle de postura de segurança** > **Listas** > **Descobertas** > **Todos.**
- Em um registro de política, selecione **Exibir descobertas** .
- Na aplicação Conformidade de configuração, selecione **Resultados do teste** e filtrar os registros por **A origem é ServiceNow SPC** .

O painel

No Espaço de controle de postura de segurança, a página inicial (página principal) exibe estas visualizações:

Visão geral

- Ativos: O número de ativos monitorados no local e na nuvem.
- Descobertas por criticalidade: O número de descobertas críticas do total de ativos.
- Ativos monitorados pelas 5 principais origens: Os cinco principais conectores do Service Graph que relatam ativos.
- Contas de nuvem: O número de contas de nuvem monitoradas pela AWS e pelo Azure.
- Descobertas abertas versus encerradas: Uma comparação dos registros ainda em processo ou aguardando resolução e os que foram resolvidos.

Informações principais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Agente de proteção de endpoint instalado: O número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: O número de ativos gerenciados em comparação com aqueles que não são gerenciados.
- Cobertura de verificação de vulnerabilidades: O número total de ativos verificados em comparação com o número que não são verificados quanto a vulnerabilidades conhecidas por um verificador de vulnerabilidades de terceiros.
- Ativos com vulnerabilidades críticas: O número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: O número total de itens vulneráveis divididos por gravidade. Uma vulnerabilidade conhecida que corresponde a um ativo em seu CMDB resulta em um item vulnerável.
- 3 principais políticas por descobertas: As políticas que retornam a maioria das descobertas (correspondências) em seus ativos.

Cobertura de caso de uso principal

Selecione uma visualização e. **Ajudar a melhorar** para exibir quais conectores e políticas do service graph estão ativados para os principais casos de uso.

Resultado de teste e transições de estado da tarefa de correção no Controle de posturas de segurança aplicação

Os estados nas descobertas (registros de teste de configuração) e suas tarefas de correção associadas serão afetados se você modificar suas políticas na aplicação Controle de postura de segurança.

Cenários de transição de estado entre resultados de teste e tarefas de correção

Com algumas exceções, os estados geralmente fazem a transição entre suas descobertas (resultados de teste) e suas tarefas de correção associadas no Controle de postura de segurança da mesma forma que fazem a transição entre os resultados de teste e as tarefas de correção no Conformidade de configurações aplicação. No entanto, se você modificar suas políticas no Controle de postura de segurança, suas mudanças afetarão a transição dos estados nas descobertas e nas tarefas de correção associadas.

As tabelas a seguir ilustram como os estados fazem a transição em suas descobertas se você editar e publicar uma nova versão (editar), desativar ou excluir suas políticas.

Para obter mais informações sobre mudanças de estado em Conformidade de configurações, consulte Resultado de teste e transições de estado da tarefa de correção no Conformidade de configurações aplicação.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de teste	Tarefa de correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As melhorias nas auditorias de política garantem que os ativos desativados não sejam avaliados por políticas ativadas. Se o estado de um ativo fizer a transição de **Descontinuado** voltar para **Ativo** , ele está incluído na próxima avaliação de política.

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Desativado	Resultado	Mantenha os valores originais
	Estado	Encerrado
	Resolução	Obsoleto

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Editado com a opção de fechar todas as descobertas existentes selecionadas	Resultado	Mantenha os valores originais
	Estado	Encerrado
	Resolução	Resultado Inválido

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Editado com a opção de reter todas as descobertas existentes selecionadas	Resultado	Os casos de teste válidos (aprovados) retêm valores originais e os casos de teste inválidos (reprovados) são encerrados.
	Estado	Encerrado
	Resolução	Resultado Inválido

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Excluídos	Resultados	Mantenha os valores originais
	Estado	Encerrado
	Resolução	Resultado Inválido

Crie uma pesquisa de ativos no Controle de postura de segurança

Defina suas condições e pesquise ativos por produtos do conector do Service Graph específicos ou ativos que tenham dados específicos relatados por um conector.

Antes de Iniciar

Como exemplo de pesquisa, digamos que você queira identificar seus ativos que têm servidores Windows e uma versão específica encontrada em CrowdStrike detalhes dos metadados.

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Pesquisa de ativos**.
2. Escolha um.

Opção	Descrição
Ativo de hardware	PESQUISE qualquer dispositivo que inclua dispositivos de computação pessoal, servidores, dispositivos de rede, máquinas virtuais em nuvem e outros hardwares.
Software	PESQUISE o software instalado em seus ativos relatados por conectores do Service Graph, seus produtos de verificação de vulnerabilidades e o software relatado por scanners que já está contabilizado no SAM (Software Asset Management) e outros produtos da ServiceNow.

   Para este exemplo, selecione **Ativo de hardware** Para Tipo de ativo.
3. **Opcional:** Selecione **Política de base** e. **Políticas de exclusão** se você quiser usar as condições de uma política existente como início e quiser excluir ativos que correspondam às políticas existentes, respectivamente.
   As políticas selecionadas são exibidas.
4. Selecione **Com dados do conector** Para o campo Conexão.
5. Selecione **Detalhes do dispositivo CrowdStrike** Para a entidade.
6. Para Propriedade, Operador e Valor, selecione **[Versão do agente][is]** e insira a versão, por exemplo, **6.26.14003.0** .
7. Selecione o operador E à direita do campo Entidade com CrowdStrike Detalhes do dispositivo como o valor de outra condição.
8. Selecione **Com metadados do CMDB** Para o campo Conexão.
   O campo Entidade é preenchido com Metadados do CMDB.
9. Selecione **Propriedade** Para o campo Critérios.
10. Para Propriedade, Operador e Valor, selecione **[OS][Contém]** e insira **Windows Server** .
11. Selecione **Exibir ativos** .
    Alguns momentos depois, os resultados são exibidos na guia Ativos correspondentes. Se você não vir correspondências, poderá refinar sua pesquisa. Quando estiver satisfeito com a definição das condições corretamente, você pode salvar a pesquisa como uma política e ativá-la. Como outras políticas, ele pesquisa seus ativos com um trabalho em segundo plano continuamente depois que você o ativa.

Resolvendo itens de configuração duplicados em Controle de posturas de segurança

Resolver entradas duplicadas para itens de configuração (ICs) em seu Configuration Management Database garante que você obtenha auditorias precisas com o. SPC políticas.

Visão geral de itens de configuração duplicados

Em determinados casos, suas origens de descoberta de ativos, ou seja, seus produtos do conector do Service Graph (SGC), importam dados de ativos que podem criar entradas duplicadas no Configuration Management Database (CMDB) para ativos (itens de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configuração). Esses registros de IC duplicados ocorrem quando dois ou mais ativos são listados no CMDB com os mesmos nomes, mas as referências do CMDB são diferentes.

Um exemplo pode ser um ativo nomeado por seu endereço IP, 10.0.2.11 , Listado duas vezes na tabela Dados do CMDB 360 [cmdb_multisource_data]. Uma entrada para 10.0.2.11 Está listado na coluna de referência do CMDB como 10.0.2.11 e outro é listado como 10.0.65.159 . Esses ativos podem ser da mesma origem da Descoberta, um produto SGC ou podem ser de duas ou mais origens da Descoberta. Em ambos os casos, para evitar problemas com as políticas de SPC e seus inventários de ativos, você deve remover os ICs duplicados.

Identificar e remover itens de configuração duplicados

Você pode identificar ICs duplicados filtrando na coluna Nome na tabela [sn_sec_spc_core_asset_cache] e observando quais ativos têm o mesmo nome.

Se você identificar duplicatas, o Desduplicação de IC O processo incorpora um modelo de desduplicação que você deve publicar, uma propriedade do sistema que você ativa e um trabalho agendado que remove ICs duplicados na tabela Ativos em cache do SPC [sn_sec_spc_core_asset_cache]. O processo remove duplicatas e preserva o registro de IC mestre ou canônico que tem a maioria dos itens relacionados.

Resolva itens de configuração duplicados em Controle de posturas de segurança

Use este processo para remover itens de configuração duplicados na tabela Ativos em cache do SPC [sn_sec_spc_core_asset_cache]. Este processo remove registros duplicados e preserva o registro de ativo mestre ou canônico que tem a maioria dos itens relacionados.

Antes de Iniciar

Funções necessárias: sn_cmdb_user para acessar o Espaço do CMDB e sn_sec_spc_core.admin para iniciar o trabalho agendado

Procedimento

1. Navegar até **Tudo** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Localize a propriedade do sistema sn_sec_spc-core.is_ci_name_unique.

   Este é um valor configurável na propriedade que especifica se todos os itens de configuração listados na tabela CMDB ou Cache de ativos têm nomes exclusivos.

   Consulte Resolvendo itens de configuração duplicados em Controle de posturas de segurança Para obter mais informações sobre como identificar ICs duplicados.
3. Selecione o registro para abri-lo e defina o campo Valor como **verdadeiro** .
4. Atualizar o registro.
5. Navegar até **Espaço do CMDB** > **Gestão** E selecione o link da biblioteca de modelos de desduplicação em Ferramentas de gestão à direita.

   Nota: A função sn_cmdb_user é necessária para acessar o Espaço do CMDB.
6. No painel Modelos de desduplicação, expanda **Modelos de desduplicação do SPC** e selecione **Nome flip-flop** para abri-lo.
7. Selecione **Publicar**.
8. Selecione **Publicar** no modal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você publicou o modelo de desduplicação e ativou a propriedade do sistema sn_sec_spc-core.is_ci_name_unique. Você deve executar o trabalho agendado Gerar tarefa de desduplicação para gerar as tarefas que resolvem os ICs duplicados.

9. Navegar até **Tudo** > **Definição do Sistema** > **Trabalhos agendados** > **Gerar tarefa de desduplicação** e selecione o registro para abri-lo.
10. Selecione **Executar agora**.
    Verifique se o trabalho em segundo plano está enfileirado e sendo processado.
11. Navegue até **Trabalhos em segundo plano [sn_sec_cmn_background_job]** Tabela para monitorar o trabalho agendado Gerar tarefa de desduplicação.
    Quando o trabalho agendado for concluído com sucesso (concluído), você poderá iniciar o modelo publicado.
12. Navegar até **Espaço do CMDB** > **Gestão** e selecione **Exibir painel de desduplicação** .
13. Selecione **Em execução** para carregar o modelo.
14. Selecione **Concluído** para exibir as tarefas concluídas.

    Você deve verificar se as tarefas de desduplicação foram concluídas antes de verificar se há duplicatas na tabela Ativos em cache do SPC [sn_sec_spc_core_asset_cache].

    Talvez você precise atualizar sua tela para exibir as tarefas concluídas.

15. Quando o trabalho agendado for concluído com sucesso e você verificar se as tarefas de desduplicação estão concluídas, navegue até a tabela Ativos em cache do SPC [sn_sec_spc_core_asset_cache], filtre a coluna Nome e verifique se há duplicatas.
    O mestre, ou canônico, é o registro de IC que tem a maioria dos itens relacionados. Ele é preservado na tabela. Se não houver duplicatas, verifique se há duplicatas na tabela Dados do CMDB 360 [cmdb_multisource_data].
16. Navegue até a tabela Dados do CMDB 360 [cmdb_multisource_data].
17. Agrupe por Col0 e verifique se existem diferentes referências do CMDB para ativos que correspondem à coluna Nome da tabela Ativos em cache do SPC [sn_sec_spc_core_asset_cache].
    Se você encontrar duplicatas, execute o trabalho agendado Gerar tarefa de desduplicação novamente.

Monitoramento de controles de mitigação usando o Controle de posturas de segurança

Em Controle de posturas de segurança(SPC) Espaço, obtenha informações sobre quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis com base em como as várias ferramentas de segurança são configuradas.

Monitoramento de controles de mitigação

Para aplicações compatíveis com Controle de posturas de segurança E Monitoramento de controles de mitigação, consulte Explorando Controle de posturas de segurança.

. Controle de posturas de segurança a aplicação se concentra em três áreas problemáticas principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Inventário de ativos - Identificando todos os ativos empresariais que incluem ativos não gerenciados ou desconhecidos.
- Cobertura e integridade dos controles de segurança - Identificando lacunas de cobertura com seus controles de segurança
- Visibilidade da mitigação de vulnerabilidades e ameaças - Identifica quais ameaças ou vulnerabilidades aos seus ativos são mitigadas pelos controles de mitigação aplicáveis.

O monitoramento de controles de mitigação descreve os recursos do Controle de posturas de segurança que se enquadram na visibilidade de mitigação de vulnerabilidades e ameaças.

Funções necessárias:

- administrador - Instala aplicações do ServiceNow® Store E ativa plug-ins (Descoberta do ITOM).
- SPC Grupo de administração e. SPC Grupo de analistas - Os usuários deste grupo têm acesso total de leitura e gravação a todos os registros do produto e do espaço.
- SPC Analista somente leitura - Os usuários deste grupo têm acesso total de leitura a todos os registros do produto.

Monitoramento de controles de mitigação usuários e benefícios

Usuários

Usuário	Descrição
Equipes de segurança cibernética, analistas e gerentes de segurança	• Obtenha visibilidade de todos os seus ativos empresariais que incluem ativos não gerenciados ou desconhecidos. • Identifique lacunas de cobertura com seus controles de segurança, combinações tóxicas de problemas, como vulnerabilidades críticas e exposição da internet em seus ativos e desvios de seus padrões de segurança internos.
Equipes de gestão de vulnerabilidades	Obtenha informações sobre mitigações disponíveis para vulnerabilidades nos ativos e ajuste dinamicamente a pontuação de risco dessas vulnerabilidades.
Equipes de defesa contra ameaças	Obtenha informações sobre lacunas nas mitigações ou na configuração de controles de segurança em relação a técnicas de ataque específicas.

Controle de posturas de segurança e o monitoramento de controles de mitigação fluxo de trabalho

Controle de posturas de segurança Usa integrações de API com ferramentas de segurança, como firewalls de aplicações web e ferramentas de proteção de endpoint, para importar dados de configuração adicionais sobre seus ativos e analisá-los para identificar os controles de mitigação aplicáveis para um determinado ativo. Essas integrações de API são separadas das integrações do conector do Service Graph compatíveis com SPC e importar dados diferentes. Essas integrações de API são configuradas no SPC Espaço.

As integrações do Conector do Service Graph ou Descoberta do ITOM ainda são necessárias para o monitoramento dos controles de mitigação. Por exemplo, ambos CrowdStrike Conector do Service Graph e CrowdStrike Integração de API compatível com SPC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

deve ser ativado para importar informações adicionais sobre quais controles de mitigação estão habilitados pelo CrowdStrike configuração de proteção de endpoint.

Políticas de controles de mitigação

. Controle de posturas de segurança E as aplicações Controles de mitigação são necessárias para exibir os controles de mitigação e as políticas de controles de mitigação no SPC. Ambas as aplicações estão disponíveis na ServiceNow Store.

Consulte os tópicos a seguir para obter mais informações sobre como baixar e instalar aplicações do ServiceNow® Store.

- Baixar uma aplicação do ServiceNow Store pela primeira vez
- Instale um Operações de segurança integração

Para exibir as políticas de controles de mitigação, os usuários do Grupo de administradores do SPC e do Grupo de analistas do SPC podem navegar até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Tudo** em SPC Painel de navegação do espaço.

As políticas de controles de mitigação a seguir estão incluídas com a aplicação e são exibidas junto com as outras SPC políticas:

- Substituição DE SEH
- Heap spray
- CrowdStrike Alocação de página NULA
- CrowdStrike Forçar DEP
- CrowdStrike Forçar ASLR
- Microsoft Proteção de fluxo de controle do Defender
- Microsoft Defender FORCE ASLR
- Microsoft Defender ASLR obrigatório e ASLR de baixo para cima
- Controle de aplicações SentinelOne
- Arquivos de dados do SentinelOne
- Executáveis SentinelOne
- Explorações do SentinelOne
- SentinelOne IDR
- Detectar ameaça interativa do SentinelOne
- SentinelOne deteta movimento lateral
- IA estática do SentinelOne
- IA estática do SentinelOne - Suspeito
- SentinelOne aplicações potencialmente indesejadas
- SentinelOne Remote shell
- Reputação do SentinelOne

Categorias de controles de mitigação

As seguintes categorias de controles de mitigação são compatíveis no momento com SPC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Controles de mitigação e políticas necessários para controles de mitigação da Proteção contra exploração (EDR).
- Controles de mitigação da Proteção contra exploração (WAF). Você deve criar políticas para o AWS WAF. Para obter mais informações, consulte Crie uma política para AWS Integração do WAF para monitoramento de controles de mitigação.

Controles de mitigação e políticas necessários para controles de mitigação da Proteção contra exploração (EDR)

Esta categoria de controles de mitigação abrange as mitigações disponíveis em seus ativos na forma de configuração do agente de proteção de endpoint. Isso se aplica a agentes de proteção de endpoint, como CrowdStrike E SentinelOne.

Configurações de mitigação de exploração, como "Forçar randomização de layout do espaço de endereços" e "Forçar DEP", podem ser habilitadas em ferramentas de proteção de endpoint como CrowdStrike. SPC Detecta automaticamente essa configuração em dispositivos com a ajuda das políticas incluídas com a aplicação e a integração de API com ferramentas de proteção de endpoint.

Funções necessárias: SPC Grupo de administração e. SPC Grupo de analistas.

Pré-requisitos para CrowdStrike Detecção de controle de mitigação da Proteção contra exploração (EDR)

1. Verifique se você ativou o. CrowdStrike Conector do Service Graph. Esta aplicação está disponível na ServiceNow Store. As informações de instalação e configuração estão incluídas na lista de apps. Para obter mais informações, consulte Instale e configure o. CrowdStrike integrações para monitoramento de controles de mitigação.
2. Verifique se o CrowdStrike A integração de API é ativada no Controle de posturas de segurança Espaço.

Pré-requisitos para Microsoft Detecção de controle de mitigação da Proteção contra exploração (EDR)

Microsoft Credenciais do SCCM que incluem a função Autores de script. A função Autores de script fornece as permissões necessárias para criar um script necessário para importar informações de mitigação no servidor SCCM.

Você deve ativar a integração do SCCM para identificar controles de mitigação configurados no Microsoft Defender.

Para obter mais informações, consulte Instale e configure o Conector do Service Graph para Microsoft SCCM e a Integração do controle de mitigação do Microsoft Defender.

- Defender – mitigação de exploração – CFG

  Microsoft Proteção de fluxo de controle do Defender.

- Defender – mitigação de exploração – DEP

  Microsoft Prevenção de execução de dados do Defender.

- Defender - mitigação de exploração - ASLR obrigatório e ASLR de baixo para cima

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Defender FORCE ASLR.

- MITRE Táticas abordadas: Acesso inicial, execução, acesso de credencial, evasão de defesa, escalação de privilégio, movimento lateral.

1. Verifique se você ativou o Conector do Service Graph do SentinelOne.

   Esta aplicação está disponível na ServiceNow Store. As informações de instalação e configuração estão incluídas na lista de apps. Para obter mais informações, consulte Instale e configure o. Conector do Service Graph para SentinelOne E a Integração de controle de mitigação do SentinelOne.

2. Verifique se a integração da API SentinelOne está ativada no Espaço de controle de postura de segurança.

Instale e configure o. CrowdStrike integrações para monitoramento de controles de mitigação

. CrowdStrike O Conector do Service Graph e as integrações de API exigem etapas de configuração separadas. Você configura o. CrowdStrike Conector do Service Graph para importar detalhes do ativo. Você configura o. CrowdStrike Integração de API para coletar dados de mitigação sobre os ativos que são monitorados por CrowdStrike.

Antes de Iniciar

- Verifique se você instalou e ativou as aplicações Controle de postura de segurança e Monitoramento de controles de mitigação em sua instância. Essas aplicações estão disponíveis na ServiceNow Store.
- . CrowdStrike O Conector do Service Graph deve ser instalado e configurado antes de configurar o. CrowdStrike Integração de API.

Funções necessárias: administrador para instalação de plug-ins e Grupo de administradores do SPC e Grupo de analistas do SPC para configuração de integrações no espaço.

Procedimento

1. Para instalar e configurar o. CrowdStrike Integração do Conector do Service Graph, siga estas etapas:

   Nota: Se você instalou o Conector do Service Graph para CrowdStrike, prossiga para a etapa 2 para saber como configurar o. CrowdStrike Integração de API.

   a. Navegar até **Configuração de conectores e casos de uso** > **Guia Conectores do Service Graph**.

   b. Localize CrowdStrike Conector de gráfico de serviço de proteção de endpoint.

   c. Selecione o link que leva a listagem de aplicações para o Conector do Service Graph para CrowdStrike em ServiceNow® Store.

   d. Siga as instruções para instalar a aplicação.

   e. Antes de sair, baixe o guia de instalação na seção Links e Documentos de suporte da lista de apps para ajudá-lo na configuração e na ativação.

   f. Navegar até **CrowdStrike** > **Configuração** em sua instância.

   g. Siga os avisos na configuração assistida e consulte a documentação para configurar e ativar o SGC.

2. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta guia lista as origens dos controles de mitigação (CrowdStrike F5 Big IP e SCCM) e a guia será exibida no espaço somente se você tiver instalado a aplicação Monitoramento de controles de mitigação.

Nos cartões de origem, você pode exibir o status da origem de mitigação (Ativo ou Inativo e o número de controles de mitigação e suas políticas associadas que são monitorados por CrowdStrike(6). Você pode selecionar o número para exibir a lista.

Observe que a coluna Ativo em Origens é exibida, Ativo . Indica a origem (CrowdStrike SGC) está ativo, mas você deve configurar CrowdStrike Integração de API antes que você possa monitorar os controles de mitigação.

3. Selecione **Avançar**.
4. Selecione CrowdStrike Na coluna Nome.
5. Selecione Editar e preencha os campos.

Nota: Insira o mesmo CrowdStrike Informações da conta e detalhes do servidor para a integração de API que você forneceu para CrowdStrike Conector do Service Graph. Essas informações garantem que você importe dados de mitigação que correspondam aos dados do ativo importados com o conector do Service Graph.

Campo	Descrição
Nome	Nome da instância Você pode mudar esse nome para ajudar a salvar credenciais sem testá-las. Se você alterar qualquer campo no campo Nome, deverá testar a conexão antes de salvar e sair.
Limite do tamanho do ativo	Número de ativos monitorados.
ID de cliente	ID do CrowdStrike
Segredo do cliente	CrowdStrike Segredo
URL da API	URL da API, por exemplo, https://api.crowdstrike.com

6. Quando estiver pronto, selecione **Conexão de teste** .
   Se a conexão for bem-sucedida, será exibida uma mensagem.
7. Selecione **Salve e saia** .
8. Selecione **Exibir detalhes** em CrowdStrike Na guia Integrações de API do SPC, observe que a origem e a API estão ativadas e a barra de andamento da configuração está concluída.
9. **Opcional:** Se o teste de credencial não for bem-sucedido, você poderá selecionar **Reverter para credenciais anteriores** para inserir credenciais que você validou anteriormente.
10. Siga estas etapas para executar o. CrowdStrike integrações.

    a. Navegar até **Controle de mitigação do CrowdStrike** > **Integrações**.
    Há três integrações:

    - CrowdStrike Integração de política de prevenção
    - CrowdStrike Integração de política de controle de dispositivos
    - CrowdStrike Integração do Asset Insight

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As integrações são encadeadas e executadas em uma ordem específica. A conclusão bem-sucedida de uma integração inicia a próxima.

b. Selecione CrowdStrike Integração de política de prevenção na coluna Nome para iniciar as execuções de integração.

c. No registro, selecione **Ativo** marque e selecione **Executar agora** .

Você pode exibir o status de execução da integração na guia Execução de integração nos registros de integração.

Por padrão, a integração está programada para ser executada diariamente.

. CrowdStrike A integração do Asset Insight importa somente informações sobre ativos que foram alterados desde a última execução da integração. . CrowdStrike Integração de política de controle de dispositivos e CrowdStrike A integração de política de prevenção importa todos os dados de cada execução.

Instale e configure o Conector do Service Graph para Microsoft SCCM e a Integração do controle de mitigação do Microsoft Defender

O Conector do Service Graph para SCCM e a Integração do controle de mitigação do Microsoft Defender exigem etapas de configuração separadas.

Antes de Iniciar

Você deve instalar, ativar e configurar o Conector do Service Graph para SCCM para importar detalhes do ativo. Você configura a Integração de controle de mitigação do Microsoft Defender, que também usa o SCCM, para coletar dados adicionais sobre controles de mitigação configurados nos ativos para que são monitorados pelo Conector do Service Graph para SCCM.

Funções necessárias:

- administrador para instalação e ativação de plug-ins
- Grupo de administradores do SPC e Grupo de analistas do SPC para configuração de integrações no espaço
- Credenciais do Microsoft SCCM que incluem a função Autores de script. A função Autores de script fornece as permissões necessárias para criar um script necessário para importar informações de mitigação no servidor SCCM.

Nota: Esta função deve ser criada e atribuída com as seguintes permissões:

Função de autores de script

Categoria	Permissão	Estado
Coleção	Executar script	Não
Site	Leitura	Sim
Scripts de SMS	Criar	Sim
Scripts de SMS	Leitura	Sim
Scripts de SMS	Excluir	Sim
Scripts de SMS	Modificar	Sim

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Credenciais do Microsoft SCCM que incluem a função Aprovadores de script. O script criado para importar informações de mitigação requer aprovação no console do Microsoft SCCM pelo usuário com a função Aprovadores de script.

Nota: Esta função deve ser criada e atribuída com as seguintes permissões:

Aprovador de script

Categoria	Permissão	Estado
Coleção	Executar script	Não
Site	Leitura	Sim
Scripts de SMS	Leitura	Sim
Scripts de SMS	Aprovar	Sim
Scripts de SMS	Modificar	Sim

Procedimento

1. Para instalar e configurar a integração do Conector do Service Graph para Microsoft SCCM, siga estas etapas:

Nota: Se você instalou a integração do Conector do Service Graph para Microsoft SCCM, prossiga para a etapa 2 para configurar a Integração do controle de mitigação do Microsoft Defender.

   a. Navegar até **Configuração de conectores e casos de uso** > **Guia Conectores do Service Graph**.

   b. Localize a integração do Conector do Service Graph para Microsoft SCCM.

   c. Selecione o link que leva você para a lista de aplicações da aplicação no ServiceNow® Store.

   d. Siga as instruções para instalar a aplicação.

   e. Antes de sair, baixe o guia de instalação na seção Links e Documentos de suporte da lista de apps para ajudá-lo na configuração e na ativação.

   f. Navegar até **Configuração** em sua instância.

   g. Siga os avisos na configuração assistida e consulte a documentação para configurar e ativar o SGC.

2. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC** Para configurar a Integração do controle de mitigação do Microsoft Defender.

   Esta guia lista as origens dos controles de mitigação (CrowdStrike F5 Big IP e Defender) e a guia será exibida no espaço somente se você tiver instalado a aplicação Monitoramento de controles de mitigação.

   Nos cartões de origem, você pode exibir o status da origem de mitigação (Ativo ou Inativo).

   Observe que a coluna Ativo em Origens é exibida, Ativo . Indica que a origem (Conector do Service Graph para Microsoft SCCM) está ativa para recuperar dados de ativos, mas você deve configurar a Integração de controle de mitigação do Microsoft Defender que busca dados adicionais sobre as configurações do defensor nesses ativos usando o SCCM antes de monitorar os controles de mitigação.

3. Selecione **Avançar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A página Configuração do SCCM é exibida com um link de instância do Controle de mitigação do Microsoft SCCM.

4. Selecione o link da instância fornecido na coluna Nome.
5. Preencha os campos para a configuração de credenciais do SCCM do modal Integração do controle de mitigação do Microsoft SCCM.

Campo	Descrição
Nome	O campo é preenchido automaticamente com o nome da instância.
Conexão	Campo preenchido automaticamente com informações de conexão.
Host	Nome do host do servidor SCCM dentro das informações de conexão fornecidas no campo anterior.
Nome de usuário	Nome de usuário para acessar o servidor SCCM.
Senha	Senha para acessar o servidor SCCM.
MID Server	Selecione um MID Server gerenciado pela ServiceNow na lista.
Status de validação	Campo preenchido após a tentativa de validação. Se a conexão for bem-sucedida, o estado da instância de integração será **Válido** .
Conexão do conector SG	Selecione uma opção Aliases de conexão e credencial na lista do Conector do Service Graph para Microsoft SCCM. Esta conexão é configurada durante as etapas da Configuração assistida do Microsoft SCCM SGC.
Detalhe da validação	Detalhes sobre a tentativa de validação.

6. Selecione **Salvar e testar credenciais** .
. Válido uma resposta para uma conexão bem-sucedida é necessária para prosseguir para a próxima etapa.
7. Selecione **Avançar**.
Um script PowerShell é criado automaticamente para recuperar detalhes de mitigação. Um modal é exibido com a opção de validar a aprovação de script.
8. Para aprovar o script, faça login no console do Microsoft SCCM com a função Aprovador de script.

   Um script PowerShell foi gerado no Gerenciador de configuração do SCCM para recuperar detalhes de mitigação. Você deve fazer login com as credenciais apropriadas com uma função de usuário que tenha a permissão de aprovador de script para aprovar o script. Depois que for aprovado, você poderá validá-lo em seu ServiceNow AI Platform instância.

9. Em seu console, localize **ServiceNow SecOps]: Obter mitigações do sistema** script e aprove-o.

Tradução automática

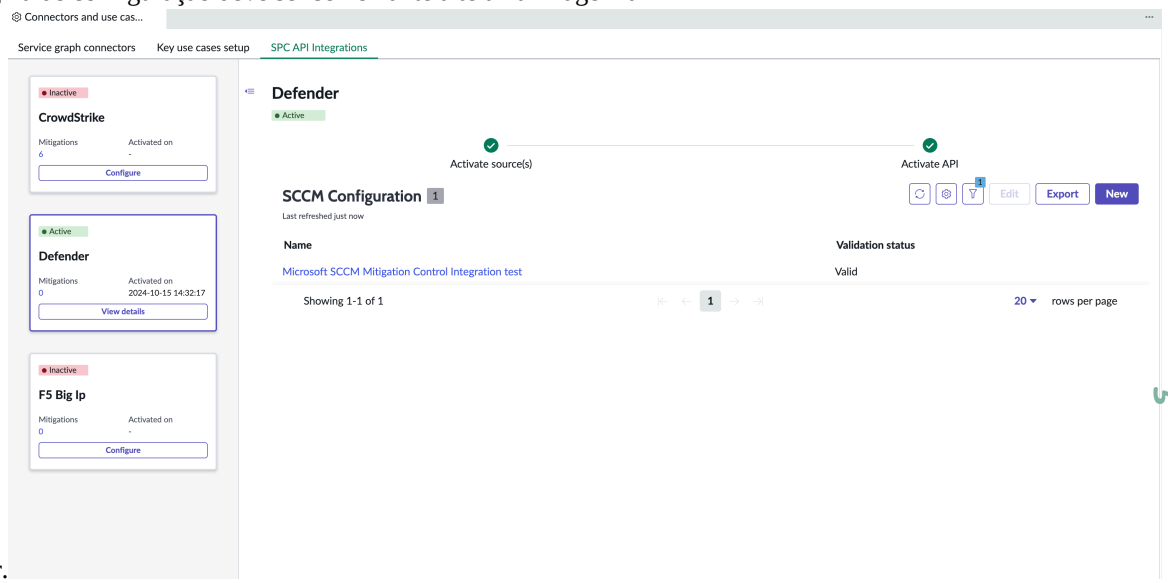
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: No gerenciador de configurações do SCCM, a seção Script está localizada na biblioteca de software. [ServiceNow SecOps]: Obtenha o script de mitigação do sistema para aprová-lo.

Este script permanece em **Aguardando aprovação** estado até que você aprove.

Você pode validar o script em seu ServiceNow AI Platform instância sem aprová-la conforme descrito acima, mas a mensagem de erro, Script não aprovado é exibido .

10. Para validar a aprovação, retorne ao ServiceNow AI Platform E no modal Aprovar script do PowerShell, selecione **Validar aprovação de script** .
11. Clique em **Done** (Concluído).
    A página de configuração deve ser semelhante à tela na imagem a seguir.



Crie várias instâncias para a Integração de controle de mitigação do Microsoft Defender

Você pode configurar várias instâncias para a Integração de controle de mitigação do Microsoft Defender.

Antes de Iniciar

Funções necessárias:

- Grupo de administradores do SPC e Grupo de analistas do SPC para configuração de novas instâncias de integração no espaço
- Credenciais do Microsoft SCCM que incluem a função Autores de script. A função Autores de script fornece as permissões necessárias para criar um script necessário para importar informações de mitigação no servidor SCCM.

Nota: Esta função deve ser criada e atribuída com as seguintes permissões:

Função de autores de script

Categoria	Permissão	Estado
Coleção	Executar script	Não
Site	Leitura	Sim
Scripts de SMS	Criar	Sim
Scripts de SMS	Leitura	Sim

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Permissão	Estado
Scripts de SMS	Excluir	Sim
Scripts de SMS	Modificar	Sim

- Credenciais do Microsoft SCCM que incluem a função Aprovadores de script. O script criado para importar informações de mitigação requer aprovação no console do Microsoft SCCM pelo usuário com a função Aprovadores de script.

Nota: Esta função deve ser criada e atribuída com as seguintes permissões:

Aprovador de script

Categoria	Permissão	Estado
Coleção	Executar script	Não
Site	Leitura	Sim
Scripts de SMS	Leitura	Sim
Scripts de SMS	Aprovar	Sim
Scripts de SMS	Modificar	Sim

Procedimento

1. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC**.
2. Selecione **Novo**.
   O modal Nova instância do Defender é exibido.
3. Insira um nome para sua nova instância e selecione **Criar instância** .
   A página Integrações de API do SPC é exibida com a instância fornecida com a aplicação e sua nova instância.
4. Selecione o link para sua nova instância.
5. Preencha os campos no modal de configuração de credenciais do SCCM para sua nova instância.

Campo	Descrição
Nome	O campo é preenchido automaticamente com o nome da instância.
Conexão	Crie uma nova conexão. **a.** Selecione **Criar conexão e alias** na parte superior do modal. **b.** No formulário Aliases de conexão e credencial, preencha os campos obrigatórios. ▪ **Nome** - Nome exclusivo ▪ **Tipo** - Conexão e credencial ▪ **Tipo de conexão** - Básico **Nota:** Não selecione **Enviar** no momento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	c. Clique com o botão direito do mouse em qualquer lugar no cabeçalho cinza e selecione **Salvar** . A página é atualizada e os links e guias relacionados são exibidos na parte inferior da página depois que você a salva. **d.** Com a guia Conexões selecionada, selecione **Novo** à direita da guia. O formulário Conexão é exibido. Preencha os campos. ▪ **Nome** - Nome exclusivo ▪ Credencial - Selecione o ícone de pesquisa. Localize as credenciais do Windows e selecione o link. No formulário Credenciais do Windows, preencha os campos. ▪ **Nome** - Nome exclusivo ▪ Nome de usuário - Nome de usuário das credenciais. Este é o nome de usuário que será referenciado para o campo Nome de usuário no modal de configuração de credenciais do SCCM depois de salvá-lo nesta página. ▪ Senha - Senha das credenciais. Esta é a senha que será referenciada para o campo de senha no modal de configuração de credenciais do SCCM depois de salvá-la nesta página. ▪ Host - Este é o host do servidor SCCM que será referenciado no campo Host no modal de configuração de credenciais do SCCM depois de salvá-lo nesta página. **e.** Selecione **Use o MID Server** caixa de seleção. Selecione MID Server específico para **Seleção DE MID** E selecione um na lista MID Server. **f.** Clique com o botão direito do mouse em qualquer lugar no cabeçalho cinza e selecione **Salvar** . Estas são as credenciais inseridas no formulário Conexão descrito acima na etapa d.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Host	Este é o Host do servidor SCCM referenciado no campo Host depois de salvá-lo na página Conexão, conforme descrito acima.
Nome de usuário	Este é o nome de usuário referenciado no campo Nome de usuário depois de salvá-lo na página Conexão, conforme descrito acima.
Senha	Esta é a senha referenciada no campo Senha depois de salvá-la na página Conexão, conforme descrito acima.
MID Server	Este é o MID Server referenciado nos campos DO MID Server depois de salvá-lo na página Conexão, conforme descrito acima.
Status de validação	Campo preenchido após a tentativa de validação. Se a conexão for bem-sucedida, o estado da instância de integração será **Válido** .
Conexão do conector SG	Selecione uma opção Aliases de conexão e credencial na lista do Conector do Service Graph para Microsoft SCCM. Esta conexão é configurada durante as etapas da Configuração assistida do Microsoft SCCM SGC.
Detalhe da validação	Detalhes sobre a tentativa de validação.

6. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC**.
7. Selecione o link para sua nova instância.
8. No modal de configuração de credenciais do SCCM, selecione a conexão na lista que você criou na etapa 5 para o campo Conexão.

   Observe que os campos listados abaixo são preenchidos automaticamente com base nas informações inseridas para sua nova conexão.

Host	Este é o Host do servidor SCCM referenciado no campo Host depois de salvá-lo na página Conexão, conforme descrito acima.
Nome de usuário	Este é o nome de usuário referenciado no campo Nome de usuário depois de salvá-lo na página Conexão, conforme descrito acima.
Senha	Esta é a senha referenciada no campo Senha depois de salvá-la na página Conexão, conforme descrito acima.
MID Server	Este é o MID Server referenciado nos campos DO MID Server depois de salvá-lo na página Conexão, conforme descrito acima.
Status de validação	Campo preenchido após a tentativa de validação. Se a conexão for bem-sucedida, o estado da instância de integração será **Válido** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conexão do conector SG	Selecione uma opção Aliases de conexão e credencial na lista.
Detalhe da validação	Detalhes sobre a tentativa de validação.

9. Selecione **Salvar e testar credenciais** .
   . Válido uma resposta para uma conexão bem-sucedida é necessária para prosseguir para a próxima etapa.
10. Selecione **Avançar**.
    O script PowerShell é criado conforme descrito em Instale e configure o Conector do Service Graph para Microsoft SCCM e a Integração do controle de mitigação do Microsoft Defender. Siga as etapas nesse tópico para aprovar os scripts para suas novas instâncias.

Instale e configure o. Conector do Service Graph para SentinelOne E a Integração de controle de mitigação do SentinelOne

. Conector do Service Graph para SentinelOne E a integração do SentinelOne para controle de mitigação exigem etapas de configuração separadas. Você instala e configura o. Conector do Service Graph para SentinelOne para importar detalhes do ativo. Você configura a Integração do SentinelOne para Integração de controle de mitigação para coletar dados de mitigação sobre os ativos que são monitorados pelo Conector do Service Graph para SentinelOne.

Antes de Iniciar

Funções necessárias:

- administrador para instalação e ativação de plug-ins.
- Grupo de administradores do SPC e Grupo de analistas do SPC para configuração de integrações no espaço.
- Credenciais do SentinelOne.

Procedimento

1. Para instalar e configurar o. Conector do Service Graph para SentinelOne integração, siga estas etapas:

   Nota: Se você instalou o Conector do Service Graph para SentinelOne, prossiga para a etapa 2 para configurar a Integração do SentinelOne para Integração de controle de mitigação.

   a. Navegar até **Configuração de conectores e casos de uso** > **Guia Conectores do Service Graph**.
   b. Localize Conector do Service Graph para SentinelOne integração.
   c. Selecione o link que leva você para a lista de aplicações da aplicação no ServiceNow® Store.
   d. Siga as instruções para instalar a aplicação.
   e. Antes de sair, baixe o guia de instalação na seção Links e Documentos de suporte da lista de apps para ajudá-lo na configuração e na ativação.
   f. Navegar até **Configuração** em sua instância.
   g. Siga os avisos na configuração assistida e consulte a documentação para configurar e ativar o SGC.
2. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC** Para configurar a Integração do SentinelOne para Integração de controle de mitigação.

   Esta guia lista as origens dos controles de mitigação: CrowdStrike F5 Big IP, Defender, SentinelOne. A guia será exibida no espaço somente se você tiver instalado a aplicação Monitoramento de controles de mitigação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nos cartões de origem, você pode exibir o status da origem de mitigação (Ativo ou Inativo).

Observe que a coluna Ativo em Origens é exibida, Ativo . Indica a origem, neste caso, o. Conector do Service Graph para SentinelOne, Está ativo para recuperar dados de ativos, mas você deve configurar a Integração do SentinelOne para Integração de controle de mitigação antes de monitorar os controles de mitigação nos ativos importados.

3. Selecione **Avançar**.
   A página Configuração do SentinelOne é exibida com um link de instância de Integração do SentinelOne para Controle de mitigação.
4. Selecione o link da instância fornecido na coluna Nome.
5. Preencha os campos da Integração do SentinelOne para Integração de controle de mitigação.

Nota:

Insira as mesmas informações de conta do SentinelOne e detalhes do servidor para a integração do SentinelOne para controle de mitigação que você forneceu para Conector do Service Graph para SentinelOne. Essas informações garantem que você importe dados de mitigação que correspondam aos dados do ativo importados com o conector do Service Graph.

Se precisar editar os campos, selecione o ícone de caneta.

Campo	Descrição
Nome da instância	O campo é preenchido automaticamente com o nome da instância.
Chave de API	Campo preenchido automaticamente com as informações da chave de API.
URL da API	Nome do host do servidor SentinelOne, por exemplo: https//usea1-na.sentinelone.net

6. Selecione **Salvar e testar credenciais** .
   . Válido uma resposta para uma conexão bem-sucedida é necessária para prosseguir para a próxima etapa.
7. Selecione **Salvar e sair** .
8. Selecione **Exibir detalhes** No cartão SentinelOne na guia Integrações de API do SPC.
   Observe que a origem e a API estão ativadas e a barra de andamento da configuração está concluída.
9. **Opcional:** Selecione **Reverter para credenciais anteriores** para inserir credenciais que você validou anteriormente.
10. Siga estas etapas para executar a Integração de importação de ativos do SentinelOne.
    a. Navegar até **Controle de mitigação SentinelOne** > **Integrações**.
       Há uma integração: Importação de ativos do SGC SentinelOne.
    b. Selecione **Integração da política de prevenção do SentinelOne** Na coluna Nome para iniciar a integração.
    c. No registro, selecione **Ativo** marque e selecione **Executar agora** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir o status de execução da integração no **Execução de integração** dos registros de integração.

Por padrão, a integração está programada para ser executada diariamente.

A Integração de importação de ativos do SentinelOne importa somente informações sobre ativos que foram alterados desde a última execução de integração.

Controles de mitigação da Proteção contra exploração (WAF)

Esta categoria de controles de mitigação abrange as mitigações disponíveis na forma de Firewall de aplicações da Web.

Proteção contra exploração (WAF)

Controle de posturas de segurança Detecta servidores que estão em execução atrás do firewall de aplicações web (WAF) usando a integração de API com ferramentas do WAF, como F5 BIG-IP(F5) e dados de tráfego de rede da Descoberta baseada em IP do ITOM, se necessário.

O controle de mitigação importa as regras de ACL da Web e todos os balanceadores de carga associados para determinar quais regras estão protegendo suas máquinas virtuais com a ajuda dos padrões de Descoberta e Mapeamento de serviços.

Funções necessárias: SPC Grupo de administração e. SPC Grupo de analistas.

Pré-requisitos para proteção contra exploração (WAF) com F5 BIG-IP

1. Verifique se você ativou a Descoberta baseada em IP do ITOM no ambiente em que F5 BIG-IP F5 WAF e os servidores de aplicações associados estão configurados.
2. Verifique se a integração da API para F5 BIG-IP F5 está ativado no Controle de posturas de segurança Espaço.

Pré-requisitos para proteção contra exploração (WAF) com Amazon Web Services AWS

Os dados desta integração são importados pela aplicação Padrões de descoberta e mapeamento de serviços [sn_itom_pattern] e pela aplicação Monitoramento de controles de mitigação [sn_sec_mit_ctrl]. Ambas as aplicações são necessárias. Siga as etapas abaixo na ordem em que estão listadas para que você possa importar todas as ACLs da Web, as regras de ACL da Web e os dados de mitigação necessários para ajudar a confirmar se uma máquina virtual está protegida. Consulte AWS descoberta usando padrões para obter mais informações sobre AWS padrões da descoberta.

1. Defina ACLs e regras da Web em seu AWS conta de serviço que você deseja usar. Consulte Uso de ACLs da web no AWS WAF para obter mais informações.

   Nota: Você pode criar suas próprias regras de ACL da Web, no entanto, você pode preferir usar o. AWS Regras gerenciadas projetadas especificamente para funcionar com suas ACLs da Web. Se você optar por criar suas próprias regras personalizadas para ACLs da Web, observe que esta integração com AWS O WAF oferece suporte somente a tipos de ataque que correspondem a ataques de injeção de SQL e contém ataques de injeção de XSS (cross site scripting). Balanceadores de carga são os ativos (recursos) compatíveis com esta integração.

2. Instale e ative a aplicação Padrões de descoberta e mapeamento de serviços [sn_itom_pattern] em sua instância para que os nomes e as ações padrão das ACLs

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da Web definidas na etapa 1 possam ser descobertos. Para obter mais informações, consulte Instale as aplicações compatíveis com o Controle de postura de segurança.

3. Verifique se a propriedade do sistema MID Server sn_itom_pattern.discover_aws_app_pool_members está definida como verdadeiro . Para ativar esta propriedade, navegue até **Tudo** > **MID Server** > **Propriedades**.
4. Verifique se você instalou e ativou a aplicação Monitoramento de controles de mitigação [sn_sec_mit_ctrl]. Esta aplicação inclui uma extensão de padrão, regras de ACL da Web e recursos associados. Esta extensão de padrão permite importar as regras reais de ACL da Web e suas associações (relacionamentos) aos seus recursos (ativos) para sua instância.

Configure o. F5 BIG-IP integrações para monitoramento de controles de mitigação

A aplicação Descoberta baseada em IP do ITOM e F5 BIG-IP As integrações de API exigem etapas de configuração separadas. Você configura a aplicação Descoberta baseada em IP do ITOM para importar detalhes do ativo. Você configura o. F5 BIG-IP Integração de API para coletar dados de mitigação sobre os ativos que são monitorados pela Descoberta baseada em IP do ITOM.

Antes de Iniciar

- A descoberta baseada em IP do ITOM deve estar em execução no ambiente em que F5 BIG-IP e todos os servidores de aplicações associados são configurados.
- Para ativos no local, você deve fornecer um MID Server.
- Ative a origem (ITOM) para coletar dados sobre os ativos que estão sendo monitorados.
- Ative a Integração de API para coletar dados de mitigação sobre os ativos.

Funções necessárias: administrador para instalação de plug-ins e criação de propriedades do sistema, e. SPC Grupo de administração e. SPC Grupo de analistas para configuração de integrações no espaço.

Procedimento

1. Para instalar e configurar a integração, siga estas etapas:

   Nota: Se você instalou e ativou o ITOM, prossiga para a etapa 2 para saber como configurar o. F5 BIG-IP(F5) Integração de API.

   a. Navegar até **Configuração de conectores e casos de uso** > **Guia Conectores do Service Graph**.

   b. Selecione F5 BIG-IP cartão.

   c. Selecione **Plug-in do ITOM** Link para ativar o plug-in ITOM.

   d. Siga as instruções.

2. Navegar até **Configuração de conectores e casos de uso** > **Integrações de API do SPC**.

   Esta guia lista as origens dos controles de mitigação (CrowdStrike F5 Big IP e SCCM) e a guia será exibida no espaço somente se você tiver instalado a aplicação Monitoramento de controles de mitigação.

   Nos cartões de origem, você pode exibir o status da origem de mitigação (Ativo ou Inativo .

3. Selecione **Avançar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observe que a origem (ITOM) está ativa, mas você deve configurar e ativar o. F5 BIG-IP Integração de API antes que você possa monitorar os controles de mitigação.

4. Selecione F5 BIG-IP Na coluna Nome.
5. Selecione Editar e preencha os campos.

Campo	Descrição
Nome	Nome da instância Você pode mudar esse nome para ajudar a salvar credenciais sem testá-las. Se você alterar qualquer campo no campo Nome, deverá testar a conexão antes de salvar e sair.
Nome do usuário	Nome do usuário F5 BIG-IP
Senha	F5 BIG-IP senha.
MID Server	Selecione um MID Server na lista.
URL da API	URL da API com porta 8443, por exemplo, https://bigip.example.com:8443.

6. Quando estiver pronto, selecione **Conexão de teste** .
   Se a conexão for bem-sucedida, será exibida uma mensagem.

   Se o erro a seguir for resultado do teste da conexão durante as etapas de configuração, A sessão não contém certificados - não confiável: A sessão não contém certificados - não confiável , defina as seguintes propriedades do sistema como `falso` :

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   Um usuário com a função de administrador deve criar essas propriedades do sistema no escopo global se elas não estiverem listadas na tabela Propriedade do sistema [sys_properties]. As propriedades do sistema são Tipo, Verdadeiro/Falso (booliano).
7. Selecione **Salve e saia** .
8. Em F5 BIG-IP Na guia Integrações de API do SPC, observe que a origem e a API estão ativadas e a barra de andamento da configuração está concluída.
9. **Opcional:** Se o teste de credencial não for bem-sucedido, você poderá selecionar **Reverter para credenciais anteriores** para inserir credenciais que você validou anteriormente.
10. Para executar as integrações de API, siga estas etapas:

    a. Navegar até **Controle de mitigação do F5 Big IP** > **Integrações**

    Há cinco integrações. As integrações são encadeadas e executadas em uma ordem específica. A conclusão bem-sucedida de uma integração inicia a próxima:

    - F5 Big IP Device Integration
    - F5 Big IP Policy Integration
    - Integração de assinatura de ataque F5 big IP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- F5 Big IP Virtual Server Integration
- Integração de membro do pool F5 big IP

b. Para iniciar a cadeia de integração, selecione **F5 Big IP Device Integration** Na coluna Nome.

c. No registro, selecione **Ativo** marque e selecione **Executar agora** .

d. Exiba o status das execuções de integração na guia Execução de integração nos registros de integração. Por padrão, a integração está programada para ser executada diariamente.

Configure o. AWS Integração do WAF para monitoramento de controles de mitigação

Determine se suas máquinas virtuais estão protegidas com AWS Integração do WAF para monitoramento de controles de mitigação.

Antes de Iniciar

Os dados são importados por duas aplicações separadas:

- A aplicação Padrões de descoberta e mapeamento de serviços importa os nomes e as ações padrão, permitir ou bloquear, das ACLs da Web que você define em seu AWS Conta de serviço. O padrão Descoberta Amazon AWS - ACL da Web (LP) é ativado com a aplicação .
- A aplicação Monitoramento de controles de mitigação importa as regras reais de ACL da Web e os relacionamentos entre os recursos associados, como um balanceador de carga de aplicações. Esta extensão está incluída como parte da aplicação Monitoramento de controles de mitigação.

Verifique se você concluiu as etapas para definir ACLs e regras da Web e ativou as aplicações necessárias para AWS Integração do WAF descrita em Controles de mitigação da Proteção contra exploração (WAF) antes de ativar as aplicações.

Funções necessárias:

- administrador para instalação de plug-ins em seu ServiceNow AI Platform® instância.
- SPC Grupo de administradores para configuração de integrações no espaço.
- AWS credenciais do AWS conta de serviço que você deseja usar.

Procedimento

1. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Configuração de conectores e casos de uso** > **Guia Integrações de API do SPC**.
2. Selecione **AWS WAF** lado a lado.
3. Selecione um.

Opção	Descrição
Exibir contas de serviço	Exiba o disponível AWS contas de serviço configuradas em sua instância. Para criar uma nova conta:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Selecione **Exibir contas de serviço** . **b.** Selecione **Novo**. **c.** Preencha os campos. ▪ Nome - Nome do seu AWS conta de serviço. Esta é a conta que você usa para sua programação e credenciais da Descoberta. ▪ ID da conta - ID da conta do seu AWS conta de serviço. ▪ Tipo de datacenter - Selecione **AWS Datacenter [cmdb_ci_aws_datacenter]** **d.** Selecione **Enviar**.
Configurar conta de serviço	Configure um AWS conta de serviço em sua instância.

4. Crie a programação da Descoberta para AWS conta de serviço que você deseja usar.

a. Navegar até **Tudo** > **Descoberta** > **Página inicial**.

b. Selecione **Exibir cronogramas ativos** .

c. Selecione **Adicionar Programação** .

d. Selecione **Adicionar Programação de nuvem** e preencha os campos.

Campo	Descrição
Provedor	AWS
Nome da programação	Insira um nome exclusivo para sua programação para ajudá-lo a diferenciá-la de outras AWS cronogramas.
Adicionar Conta	Selecione para criar uma Conta de serviço.
Selecionar Conta	Selecione para editar uma Conta de serviço existente.
ID da conta	ID da conta do seu AWS conta de serviço.
Tipo de Seleção MID	Você deve fornecer um MID Server. Selecione uma: ▪ Seleção automática DO MID Server ▪ Cluster do MID específico ▪ MID Server específico Para importar dados de regras para máquinas virtuais individuais com seu MID Server, você deve ativar uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	propriedade do MID Server. Para verificar ou definir esta propriedade, navegue até **Tudo** > **MID Server** > **Propriedades** > **sn_itom_pattern.discover_aws_app_pool_members**. Defina o valor como verdadeiro .
Credenciais	Estas são as credenciais da Descoberta para sua conta de serviço.
URL	
Nome da função de acesso	
Selecionar conta para acesso	

e. Selecione **Conta de teste** .
Você deve ter uma validação bem-sucedida antes de continuar.

f. Selecione **Avançar**.

g. Selecione os datacenters que você deseja descobrir.

h. Selecione **Descobrir VMs por endereço IP** Alterne e selecione o MID Server selecionado na etapa d na lista.

i. Selecione **Avançar**.

j. Selecione com que frequência e quando você deseja executar sua descoberta.

k. Selecione **Concluir e Executar**.

Após a execução da programação de descoberta definida, o padrão de descoberta **Amazon AWS - ACL da Web (LP)** e os dados de ambas as aplicações são importados.

Crie uma política para AWS Integração do WAF para monitoramento de controles de mitigação

Crie uma política para que você possa auditar seus ativos com base nos dados importados da integração.

Antes de Iniciar

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Tudo**.
2. Selecione **Ativo de hardware** Para Tipo de ativo.

   As propriedades também funcionam para Pesquisa de ativos e Perfis de ativos.
3. Para Conexão, selecione **Configuração do controle de segurança** .
4. Para Entidade, selecione **AWS Insight** .

   Um campo Critérios é exibido preenchido automaticamente com Conexão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Para o novo campo Conexão, selecione **Com regra gerenciada da AWS** .

   O campo Entidade é preenchido automaticamente com Regra gerenciada E um campo Critérios é exibido preenchido automaticamente com Propriedade . Os campos Propriedade em branco, Operador e Valor são exibidos.

   Se você criou uma regra da AWS personalizada, selecione **Com declaração de correspondência personalizada** . O campo Entidade é preenchido com Declaração de correspondência .

6. Selecione as propriedades na lista.

   Você pode adicionar mais de um.

   Por exemplo, para uma ACL da Web para banco de dados SQL em sua conta de serviço da AWS, você pode ver as seguintes regras:

   - SQLiExtendedPatterns_queryarguments
   - SQLiqueryARGUMNETS
   - SQLi_BODY
   - SQLi_COOKIE
   - SQLi_URIPATH

   No construtor de políticas, esta propriedade é exibida como: SQLLRuleSet-SQLi_BODY is allow. Você pode selecionar **Permitir** ou **Bloco** da lista.

7. Selecione **ou** para adicionar propriedades.
   Consulte Crie e ative políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre como usar o construtor de políticas para criar políticas.
8. Selecione **Salvar mudanças** quando você concluir sua apólice.
9. **Ativar** se você quiser exibir as descobertas.
10. Consulte Controle de postura de segurança: Configurar e exibir suas descobertas para obter mais informações sobre como exibir as descobertas da sua política.
11. Abra um registro na lista e selecione as guias Controles de mitigação Itens vulneráveis mitigados.

    A guia Itens vulneráveis mitigados lista todos os itens vulneráveis mitigados que incluem informações sobre os CVEs mitigados como resultado das regras de mitigação encontradas em seus ativos.

    - Origens verificadas - APIs da AWS, Descoberta do ITOM
    - Web Application Firewall (WAF) - Sim
    - Tipo de WAF - AWS
    - Itens vulneráveis totalmente mitigados - Número de itens vulneráveis associados mitigados.
    - Itens vulneráveis parcialmente mitigados - Número de itens vulneráveis associados em processo.
    - Regras gerenciadas categorizadas por ações - Regras gerenciadas com ações "Bloquear" e "Permitir".

      Você pode ver mais regras do que inseriu para sua política. Essas regras são identificadas com CommonRuleSet (CRS) na regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Regras personalizadas - Qualquer uma de suas regras personalizadas categorizadas por ações "Bloquear" e "Permitir".
- No painel da Página inicial, o bloco Ativos com mitigações lista os ativos protegidos pelo WAF na visualização Proteção contra exploração (WAF).

Exibir mitigações detectadas

Você deve ativar as políticas antes de exibir quais ameaças aos seus ativos são mitigadas pelos controles de mitigação disponíveis.

Antes de Iniciar

Verifique se você concluiu os requisitos listados em Instale e configure o. CrowdStrike integrações para monitoramento de controles de mitigação, Instale e configure o Conector do Service Graph para Microsoft SCCM e a Integração do controle de mitigação do Microsoft Defender e. Configure o. F5 BIG-IP integrações para monitoramento de controles de mitigação.

Funções necessárias: Grupo de administradores do SPC e Grupo de analistas do SPC.

Procedimento

Para exibir ativos com mitigações detectadas pelo Controle de postura de segurança com o widget "Ativos com mitigações DO MITRE" no painel, siga estas etapas.

a. Navegar até **Espaços** > **Controle de posturas de segurança** > **Página inicial**.

b. Na seção Principais informações, revise o widget Ativos com mitigações DO MITRE.

c. Selecione uma categoria de mitigação, **EDR (Exploit Protection, proteção contra exploração)** ou **Proteção contra exploração (WAF)** no widget.

d. Você pode ver a lista de ativos com mitigações detectadas nessa categoria de mitigação.

e. Selecione um ativo

f. Selecione **Controles de mitigação** para ver os detalhes do controle de mitigação detectado.

g. Selecione **Itens vulneráveis mitigados** para ver a lista de itens vulneráveis mitigados por este controle de mitigação.

Nota: Para que esta guia seja preenchida, o Resposta a vulnerabilidades a aplicação deve ser instalada e ativada.

Controles de mitigação para mapeamento de item vulnerável

Os dados dos controles de mitigação são mapeados para itens vulneráveis. Você pode exibir uma lista de controles de mitigação que são usados para mitigar as vulnerabilidades e as vulnerabilidades e exposições comuns (CVEs) subjacentes associadas aos itens vulneráveis.

Depois de identificar um controle de mitigação específico em um ativo, o Controle de postura de segurança identifica automaticamente todos os itens vulneráveis que são mitigados por esse controle. Por exemplo, todos os itens vulneráveis com CVEs que fazem parte de assinaturas nas políticas do Web Application Firewall (WAF) são marcados como

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

itens vulneráveis mitigados. Essa identificação pode ser útil para que as equipes de gestão de vulnerabilidades as ajudem a reduzir automaticamente as pontuações de risco de itens vulneráveis que são mitigados.

Tabela de controles de mitigação de item vulnerável

A tabela Controles de mitigação de item vulnerável [sn_vul_vulnerable_item_mitition_control] foi criada para mapear dados de controle de mitigação para Itens vulneráveis (Vits) mitigados. Esta tabela lista os Vits mitigados e os controles de mitigação detectados que foram usados para mitigar as vulnerabilidades e seus CVEs subjacentes associados aos itens vulneráveis. Os registros CVE mitigados contêm referências ao controle de mitigação usado para os ativos, por exemplo, proteção contra exploração (EDR).

Os dados de exemplo são mostrados na tabela a seguir.

Dados de controles de mitigação de item vulnerável

Existe controle de mitigação	Eficácia do controle de mitigação	Tipo de controle de mitigação detectado	CVEs mitigados	Item vulnerável
Sim/Não	Moderado	EDR (Exploit Protection, proteção contra exploração)	CVE-2009-3373	VIT0018323

Abra um registro de controle de mitigação (tipo de controle de mitigação detectado) na tabela para revisar detalhes sobre como um CVE e sua vulnerabilidade de enumeração de pontos fracos comuns (CWE) relacionada é mitigada pelo controle de mitigação associado a um ativo. O registro de controle de mitigação contém detalhes sobre os CWEs que foram mitigados, por exemplo, como uma configuração de mitigação satisfaz as vulnerabilidades especificadas em um CWE.

Calculadora de risco e regras da calculadora de risco

As informações de mitigação podem ser usadas para ajudar você a configurar regras personalizadas da calculadora de risco para ajudá-lo a recalcular as pontuações de risco em Vits que têm tipos específicos de vulnerabilidades e controles de mitigação associados a elas. Para esta regra de exemplo, que se baseia na tabela anterior, a calculadora de risco padrão calcula uma pontuação de risco de 60 para os Vits que têm o tipo de controle de mitigação, Proteção contra exploração (EDR) em ativos detectados. Esta pontuação de cálculo se deve ao risco moderado associado à vulnerabilidade com esta mitigação em vigor.

Exemplo de regra da calculadora de risco com as seguintes condições:

[Detalhes do controle de mitigação] [não está] [vazio] E. [Detalhes do controle de mitigação, tipo de controle de mitigação detectado] [IS] [Proteção contra exploração (EDR)] .

Valores:

[Pontuação de risco] [é] [60]

Para obter mais informações, consulte Defina campos e pesos para a regra de risco para Calculadoras de risco de resposta a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos de uso, exemplos de política e conectores do Service Graph compatíveis em Controle de posturas de segurança

Os casos de uso são diferentes cenários que você configura para ajudar a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos em busca de possíveis violações. Você também pode definir suas próprias políticas para ajudá-lo a atender aos requisitos de seus padrões de segurança interna específicos.

Casos de uso

A aplicação Controle de postura de segurança oferece suporte a vários casos de uso incluídos com a aplicação . Os casos de uso ajudam a identificar tipos específicos de lacunas de cobertura de ferramentas em seus ativos, exposição na internet de ativos em nuvem e combinações com vulnerabilidades. As políticas necessárias para os casos de uso compatíveis também estão incluídas com o produto.

Você pode exibir o status da cobertura de alguns dos principais casos de uso na página inicial (principal) no Espaço de controle de postura de segurança em **Espaços** > **Controle de posturas de segurança** > **Página inicial** No módulo Página inicial (página principal).

Como alternativa, você pode exibir os conectores do Service Graph compatíveis e o status de cobertura de alguns dos principais casos de uso nas guias "Conectores do Service Graph compatíveis" e "Configuração do caso de uso principal" em **Tudo** > **Espaços** > **Controle de posturas de segurança** > **Configuração de conectores e casos de uso** (o ícone de engrenagem).

Nota:

A guia Principais casos de uso nas páginas iniciais da Página inicial não lista todos os casos de uso possíveis. Ele fornece alguns casos de uso importantes que você ativa para ajudá-lo a começar a implantar o produto Controle de postura de segurança.

Antes de ativar políticas para os casos de uso compatíveis fornecidos com a aplicação, verifique se você concluiu as tarefas a seguir.

- Você instalou e configurou todos os aplicativos necessários descritos em Instale as aplicações compatíveis com o Controle de postura de segurança.
- Você atendeu a um ou mais dos seguintes pré-requisitos para cada caso de uso.

1. No momento, você está usando ou instala e ativa conectores do Service Graph para várias categorias.

   As categorias dos casos de uso incluem conectores do Service Graph que você deve ativar para obter informações iniciais e#conectores do Service Graph que você tem a opção de ativar para melhorar a cobertura dos ativos#que o Controle de postura de segurança está monitorando.

2. No momento, você está usando ou instala e ativa a aplicação Resposta a vulnerabilidades.
3. No momento, você está usando ou configura a Verificação de conta na nuvem para suas contas AWS e Azure em "Gestão de postura de segurança na nuvem".

Os requisitos específicos para cada caso de uso compatível são descritos nas seções a seguir. Além disso, você deve ativar uma ou mais das políticas enviadas com o Controle de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

postura de segurança para um caso de uso. Este conceito também é abordado nas seções a seguir.

Exemplos de políticas básicas, secundárias e clonadas

Consulte Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança e como você pode reutilizar as condições de uma política de base ao criar outras políticas. Crie políticas básicas, secundárias e políticas de clonagem existentes nesses exemplos. Esses exemplos também ajudam você a ver como o construtor de políticas funciona no módulo Políticas e descobertas.

Conectores do Service Graph compatíveis

Consulte tabelas de conectores do Service Graph compatíveis, suas categorias de ferramenta e os tipos de dados nos quais eles importam Conectores do Service Graph de hardware compatíveis com Controle de posturas de segurança e. Conectores do Service Graph de software compatíveis para Controle de posturas de segurança.

Controle de posturas de segurança Caso de uso: Detecção de ativos com proteção de endpoint ausente

Para detectar ativos sem um agente de proteção de endpoint, os seguintes pré-requisitos são necessários.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph na categoria Proteção de endpoint.
2. Ative pelo menos um Conector do Service Graph para UMA das seguintes categorias.
   a. Serviços de diretório (Microsoft Active Directory).
   b. Endpoint Management: Microsoft Intune Ou Jamf Device and Endpoint Management.
   c. Configuração e gestão de patches: Microsoft SCCM ou IBM Bigfix.
   d. Provedor de nuvem: Nuvem da Amazon AWS, Microsoft Azure, GCP.

   Nota: Se a Descoberta em nuvem estiver ativada, esses produtos do conector do Service Graph não serão necessários.

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos relatados e monitorados pelo Controle de postura de segurança.
   a. Segurança de rede
   b. Monitoramento de infraestrutura
   c. Rede
   d. Monitoramento de desempenho da aplicação#.

Depois de verificar que atendeu a esses pré-requisitos, você deve ativar a política a seguir, Ativos sem proteção de endpoint###. #Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Controle de posturas de segurança Caso de uso: Detecção de ativos perdidos pelas ferramentas de avaliação de vulnerabilidades

Para detectar ativos ausentes pelas ferramentas de avaliação de vulnerabilidades, os seguintes pré-requisitos são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem. Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph na categoria Avaliação de vulnerabilidades.
2. Ative pelo menos um Conector do Service Graph para UMA das seguintes categorias.
   a. Serviços de diretório (Microsoft Active Directory).
   b. Endpoint Management: Microsoft Intune Ou Jamf Device and Endpoint Management.
   c. Configuração e gestão de patches: Microsoft SCCM ou IBM Bigfix.
   d. Provedor de nuvem: Nuvem da Amazon AWS, Microsoft Azure, GCP.

   Nota: Se a Descoberta em nuvem estiver ativada, esses produtos do conector do Service Graph não serão necessários.

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos relatados e monitorados pelo Controle de postura de segurança.
   a. Segurança de rede#.
   b. Rede.
   c. Monitoramento de infraestrutura.
   d. Monitoramento de desempenho da aplicação#.

Depois de verificar que atendeu a esses pré-requisitos, você deve ativar a política a seguir, Ativos não verificados em busca de vulnerabilidades. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Controle de posturas de segurança Caso de uso: Detecção de ativos não gerenciados

Este caso de uso inclui duas partes, detectando ativos que não têm agentes de configuração e gestão de patches.

Para detectar ativos sem ferramentas de configuração e gestão de patches, os pré-requisitos a seguir são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph nas categorias Configuração e Gestão de patches.
2. Pelo menos um Conector do Service Graph deve ser habilitado para UMA das seguintes categorias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Serviços de diretório (Microsoft Active Directory).

b. Proteção de endpoint: CrowdStrike Ou SentinelOne.

c. Avaliação de vulnerabilidades: Qualys, Rapid7 Ou Tenable.

d. Configuração e gestão de patches: Microsoft SCCM ou IBM Bigfix.

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos relatados e monitorados pelo Controle de postura de segurança.

a. Rede.

b. Monitoramento de infraestrutura

c. Segurança de rede

d. Monitoramento de desempenho da aplicação#.

Depois de verificar que atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas a seguir. #Para qualquer política que comece com "Ativos de nuvem", os Conectores do Service Graph na categoria "Provedor de nuvem" devem estar habilitados. ##Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

- Ativos sem configuração e gestão de patches.
- Ativos em nuvem sem configuração e gestão de patches.

Controle de posturas de segurança Caso de uso: Detecção de ativos sem uma solução de gestão de endpoint

Para detectar ativos que não têm uma solução de gestão de endpoint, os seguintes pré-requisitos são necessários.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph na categoria Gestão de endpoint.
2. Pelo menos um Conector do Service Graph deve ser habilitado para UMA das seguintes categorias.

a. Serviços de diretório (Microsoft Active Directory).

b. Proteção de endpoint: CrowdStrike Ou SentinelOne.

c. Avaliação de vulnerabilidades: Qualys, Rapid7 Ou Tenable.

d. Configuração e gestão de patches: Microsoft SCCM ou IBM Bigfix.

Depois de verificar que atendeu a esses pré-requisitos, você deve ativar a política a seguir, Ativos sem solução de gerenciamento de endpoint. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Controle de posturas de segurança Caso de uso: Detecção de ativos com vulnerabilidades e lacunas na cobertura da ferramenta de segurança

Você pode identificar ativos com vulnerabilidades críticas e ferramentas de segurança críticas ausentes, como proteção de endpoint, para priorizar esses ativos para correção. O Controle de postura de segurança envia algumas políticas incluídas com o produto para oferecer suporte a este caso de uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este caso de uso requer que você instale a aplicação Resposta a vulnerabilidades e uma integração com pelo menos um produto de avaliação de vulnerabilidades, como Qualys, Rapid7 Ou Tenable.

As políticas a seguir estão incluídas com o produto Controle de postura de segurança para oferecer suporte a este caso de uso para ativos com vulnerabilidades críticas que também não têm cobertura de ferramenta de segurança.

1. Ativos com vulnerabilidades críticas e proteção de endpoint ausente.
2. Ativos com vulnerabilidades críticas e configuração ausente e gestão de patches.
3. Ativos com vulnerabilidades críticas e gestão de endpoint ausente.

Controle de posturas de segurança Caso de uso: Detecção de exposição na internet de ativos em nuvem#e combinações de alto risco

Monitorar a possível exposição na internet de ativos em nuvem (máquinas virtuais) em várias portas para garantir que as vulnerabilidades nesses ativos não sejam exploradas remotamente. Este caso de uso ajuda a identificar esses ativos.

O Controle de postura de segurança permite que você avalie a configuração de ativos em nuvem para ajudar a identificar os ativos que estão voltados para a Internet, ou seja, quais ativos podem ser acessados de qualquer lugar na Internet e de quais portas eles estão expostos.

O Controle de postura de segurança combina essas informações com lacunas de cobertura da ferramenta de segurança e dados de vulnerabilidade de scanners de terceiros, como Qualys, Rapid7 Ou Tenable para identificar combinações de alto risco.

Atualmente, este caso de uso oferece suporte à AWS e requer os seguintes pré-requisitos.

1. O Conector do Service Graph para AWS está ativado para as mesmas contas da AWS que você configurou.
2. Você ativou uma ou mais políticas incluídas com o produto no Controle de postura de segurança.
   - Ativos de nuvem com porta SSH 22 abertos para internet.
   - Ativos em nuvem com porta SSH 22 aberta para internet e proteção de endpoint ausente.
   - Ativos de nuvem com porta HTTP 80 aberta para internet e proteção de endpoint ausente.
   - Ativos em nuvem com vulnerabilidades críticas e porta SSH 22 aberta para a Internet (requer Resposta a vulnerabilidades).
   - Ativos em nuvem com vulnerabilidades críticas, proteção de endpoint ausente e porta SSH 22 aberta à Internet (requer Resposta a vulnerabilidades).
   - Ativos de nuvem com portas HTTP abertas para internet, vulnerabilidades críticas e proteção de endpoint ausente (requer Resposta a vulnerabilidades).

Conectores do Service Graph de hardware compatíveis com Controle de posturas de segurança

Conectores de gráfico de serviço de hardware compatíveis com classe de IC, origem (produto) e categorias de ferramenta. Esta lista não está completa e está sujeita a mudanças com a adição de mais produtos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para a origem da Descoberta para um conector listado, "SG", "SGO" ou "SGC" precedem o nome do produto para produtos de terceiros, por exemplo, SG-AWS, SGO-Datadog ou SGC-AD (Active Directory). Para produtos da ServiceNow, "SN" ou "ServiceNow" precedem o nome do produto, por exemplo, SNAssetManagement para ServiceNow Hardware Asset Management.

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela Conector [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os Tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_ci_computer	Active Directory	Serviços de diretório
Ativo de hardware	cmdb_ci_server	AppDynamics	Monitoramento de desempenho da aplicação
Ativo de hardware	cmdb_ci_server	Automox	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_computer	Automox	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_computer	BigFix	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_server	BigFix	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_printer	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_server	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_iot	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_hc_device	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_netgear	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_computer	Cisco Meraki	Rede
Ativo de hardware	cmdb_ci_server	CrowdStrike	Proteção de endpoint
Ativo de hardware	cmdb_ci_server	Datadog	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_server	Dynatrace	Monitoramento de desempenho da aplicação
Ativo de hardware	cmdb_ci_computer	Dynatrace	Monitoramento de desempenho da aplicação
Ativo de hardware	cmdb_ci_computer	Revelação do ExtraHop (x)	Segurança de rede
Ativo de hardware	cmdb_ci_hc_device	Revelação do ExtraHop (x)	Segurança de rede
Ativo de hardware	cmdb_ci_server	Revelação do ExtraHop (x)	Segurança de rede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_ci_iot	Revelação do ExtraHop (x)	Segurança de rede
Ativo de hardware	cmdb_ci_printer	Revelação do ExtraHop (x)	Segurança de rede
Ativo de hardware	cmdb_ci_iot	Forescout	Segurança de rede
Ativo de hardware	cmdb_ci_hc_device	Forescout	Segurança de rede
Ativo de hardware	cmdb_ci_computer	Forescout	Segurança de rede
Ativo de hardware	cmdb_ci_server	Forescout	Segurança de rede
Ativo de hardware	cmdb_ci_printer	Forescout	Segurança de rede
Ativo de hardware	cmdb_ci_server	Intune	Gestão de endpoint
Ativo de hardware	cmdb_ci_computer	Intune	Gestão de endpoint
Ativo de hardware	cmdb_ci_printer	Jamf Pro	Gestão de endpoint
Ativo de hardware	cmdb_ci_server	Jamf Pro	Gestão de endpoint
Ativo de hardware	cmdb_ci_computer	Jamf Pro	Gestão de endpoint
Ativo de hardware	cmdb_ci_server	Lansweeper	IT Asset Management
Ativo de hardware	cmdb_ci_computer	Lansweeper	IT Asset Management
Ativo de hardware	cmdb_ci_printer	Lansweeper	IT Asset Management
Ativo de hardware	cmdb_ci_hc_device	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_printer	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_server	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_vm_instance	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_iot	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_computer	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_netgear	LogicMonitor	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_server	Microsoft Defender	Proteção de endpoint
Ativo de hardware	cmdb_ci_server	New Relic	Monitoramento de desempenho da aplicação
Ativo de hardware	cmdb_ci_computer	Nexthink	Experiência do Funcionário Digital
Ativo de hardware	cmdb_ci_computer	Netskope	Prevenção contra perda de dados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_hardware_product_model	Netskope	Prevenção contra perda de dados
Ativo de hardware	cmdb_ci_network_adapter	Netskope	Prevenção contra perda de dados
Ativo de hardware	cmdb_software_instance	Netskope	Prevenção contra perda de dados
Ativo de hardware	cmdb_sam_sw_install	Netskope	Prevenção contra perda de dados
Ativo de hardware	sn_sec_sgc_netskop_client_attribute	Netskope	Prevenção contra perda de dados
Ativo de hardware	cmdb_ci_server	Telemetria aberta	Monitoramento de desempenho da aplicação
Ativo de hardware	cmdb_ci_computer	Puppet	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_server	Puppet	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_computer	Qualys	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_server	Qualys	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_vm_instance	Qualys-ServiceNow	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_server	Qualys-ServiceNow	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_hardware	Rapid7	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_computer	SCCM	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_server	SCCM	Configuração e gestão de patches
Ativo de hardware	cmdb_ci_printer	ScienceLogic	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_iot	ScienceLogic	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_server	ScienceLogic	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_computer	ScienceLogic	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_hc_device	ScienceLogic	Monitoramento de infraestrutura

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_ci_vm_instance	ScienceLogic	Monitoramento de infraestrutura
Ativo de hardware	cmdb_ci_hardware	ServiceNow HAM	Gestão de ativos de hardware
Ativo de hardware	cmdb_ci_hardware	Descoberta do ITOM da ServiceNow	Descoberta
Ativo de hardware	cmdb_ci_aws_datacenter	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_azure_datacenter	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_availability_zone	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_google_datacenter	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_cloud_service_account	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_cloud_subnet	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_compute_template	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_network	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_vm_instance	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_key_value	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_os_template	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_server	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_computer	SentinelOne	Proteção de endpoint
Ativo de hardware	sn_sec_sgc_sntlone_asset_tags	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_ip_address	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_network_adapter	SentinelOne	Proteção de endpoint
Ativo de hardware	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	Proteção de endpoint
Ativo de hardware	cmdb_ci_server	Ativo Tanium	Gestão de endpoint
Ativo de hardware	cmdb_ci_computer	Ativo Tanium	Gestão de endpoint
Ativo de hardware	cmdb_ci_ups	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_industrial_sensor	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_cnc	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_hardware	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_netgear	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_industrial_actuator	Tenable	Avaliação de vulnerabilidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_ci_ip_switch	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_hub_network	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_security	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_server	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_rtu	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_ews	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_plc	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_control	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_dcs	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_storage_server	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_hmi	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_control_module	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_industrial_robot	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_historian	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ot_industrial_drive	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_iot	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ip_firewall	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_computer	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_unclassed_hardware	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_ids_network	Tenable	Avaliação de vulnerabilidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de hardware

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Ativo de hardware	cmdb_ci_ot_ied	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_printer	Tenable	Avaliação de vulnerabilidade
Ativo de hardware	cmdb_ci_computer	VMware Workspace ONE UEM	Gestão de endpoint
Ativo de hardware	cmdb_ci_server	VMware Workspace ONE UEM	Gestão de endpoint
Ativo de hardware	cmdb_ci_printer	VMware Workspace ONE UEM	Gestão de endpoint
Ativo de hardware	cmdb_ci_vm_instance	Assistente	Plataforma de proteção de aplicações nativas na nuvem
Ativo de hardware	cmdb_ci_server	Assistente	Plataforma de proteção de aplicações nativas na nuvem
Ativo de hardware	cmdb_ci_linux_server	Assistente	Plataforma de proteção de aplicações nativas na nuvem
Ativo de hardware	cmdb_ci_win_server	Assistente	Plataforma de proteção de aplicações nativas na nuvem

Conectores do Service Graph de software compatíveis para Controle de posturas de segurança

Conectores do Service Graph de software compatíveis com classe de IC, origem (produto) e categorias de ferramenta. Esta lista não está completa e está sujeita a mudanças com a adição de mais produtos.

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela Conector [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os Tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Conectores do Service Graph de software

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Software	cmdb_ci_spkg	BigFix	Configuração e gestão de patches
Software	cmdb_ci_spkg	Dynatrace	Monitoramento de desempenho da aplicação
Software	cmdb_ci_spkg	Forescout	Segurança de rede
Software	cmdb_ci_spkg	Intune	Gestão de endpoint

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Service Graph de software

Tipo de ativo	Classe de IC	Origem do ativo	Categoria do conector
Software	cmdb_ci_spkg	Jamf Pro	Gestão de endpoint
Software	cmdb_ci_spkg	New Relic	Monitoramento de desempenho da aplicação
Software	cmdb_ci_spkg	Nexthink	Experiência do Funcionário Digital
Software	cmdb_ci_spkg	Netskope	Prevenção contra perda de dados
Software	cmdb_ci_spkg	Qualys-ServiceNow	Avaliação de vulnerabilidade
Software	cmdb_ci_spkg	SCCM	Configuração e gestão de patches
Software	cmdb_ci_spkg	Descoberta do ITOM da ServiceNow	Descoberta
Software	cmdb_ci_spkg	Ativo Tanium	Gestão de endpoint
Software	cmdb_ci_spkg	VMware Workspace ONE UEM	Gestão de endpoint

Exemplos de políticas básicas, secundárias e clonadas para Controle de posturas de segurança

Você pode criar suas próprias políticas de base que tenham conjuntos amplos de condições que podem ser usados como pontos de partida para políticas mais complexas.

Exemplos

Os exemplos a seguir ajudarão você a ver como você pode reutilizar as condições de uma política de base ao criar outras políticas criando políticas secundárias ou clonando políticas existentes. Esses exemplos também ajudam você a ver como o construtor de políticas funciona no módulo Políticas e descobertas.

Comece com o primeiro exemplo, a política de base. Os outros exemplos usam a política de base como ponto de partida.

Nota: O conector do Service Graph do CrowdStrike é usado como o conector do Service Graph nesses exemplos, mas você pode usar qualquer conector instalado. Esses exemplos permitem que você crie e ative as políticas para procurar correspondências de ativos. Você pode remover essas políticas a qualquer momento no módulo Políticas e descobertas depois de ativá-las.

Crie uma política de base para Controle de posturas de segurança(exemplo)

Um exemplo de como criar uma política de base que você pode usar para criar outras políticas.

Antes de Iniciar
Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Políticas e descobertas**.
2. Selecione **Nova política** .
3. Selecione o ícone de caneta no canto superior esquerdo e, no modal Editar metadados, preencha os campos.

Campo	Descrição
Nome	Digite Política de base - Dispositivos Windows 10.
Criticidade	Selecione **Baixo** .
Descrição resumida	Digite, **Localize dispositivos com o Windows 10 instalado** .

4. Selecione **Salvar metadados** .
5. No Construtor de condições, selecione **Ativo de hardware** Para Tipo de ativo.

   Para esta política, deixe as opções Política base e Políticas de exclusão nas configurações padrão (desativadas).

6. Para Conexão, selecione **Com dados agregados** .

   Para esta política, os dados agregados ajudam você a localizar ativos no CMDB que tenham o Windows 10 instalado. Por exemplo, alguns registros podem ter pequenas variações sobre como diferentes scanners relatam "Windows 10". Os dados agregados garantem que todas essas pequenas variações no "Windows 10" correspondam a esta política.

   Os campos Entidade e Critérios são preenchidos automaticamente com base na sua seleção no campo Conexão.

7. Para Propriedade, selecione **SO** .
8. Para Valor, digite `Windows 10` .
9. Selecione **Salvar mudanças**.
   Sua política de base é exibida na lista Todos do módulo Políticas e descobertas, mas não está ativada.
10. Selecione **Ativar política** sua política de base monitora todos os ativos que correspondem às condições da política e gera descobertas.

Crie uma política secundária a partir de uma política de base para Controle de posturas de segurança(exemplo)

Um exemplo de como criar uma política secundária usando as condições de uma política de base.

Antes de Iniciar

Esta política secundária herda as condições de uma política de base e você adicionará mais condições à política secundária para ajudá-lo a se concentrar em detalhes de ativos mais específicos. Uma nova política para monitorar todos os seus dispositivos que têm o Windows 10 instalado e que são relatados pelo CrowdStrike conector do service graph e você deseja excluir todos os dispositivos que correspondam a outra política. Para este exemplo, você excluirá ativos que foram aprovados para exceções de Gestão integrada de riscos (IRM) de suas descobertas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você não tiver CrowdStrike conector do service graph instalado, você pode usar um que tenha instalado.

Funções necessárias: Grupo de administradores do SPC ou Grupo de analistas do SPC

Procedimento

1. Navegar até **Tudo** > **Espaço de controle de postura de segurança** > **Políticas e descobertas**.
2. Na lista Ativo, localize a Política de base - Dispositivos Windows 10 que você criou no primeiro exemplo e selecione-a para abrir o registro.
3. Selecione o menu Mais opções (três pontos verticais) e selecione **Criar política secundária** .
   Uma nova guia é aberta e com um novo registro e a Política de base - Dispositivos Windows 10 é exibida no campo Política de base.
4. Selecione o ícone de caneta no canto superior esquerdo e no modal Editar metadados, preencha os campos.

Campo	Descrição
Nome	Digite, Política secundária- Dispositivos Windows com CrowdStrike .
Criticidade	Selecione **Médio** .
Descrição resumida	Digite, Localize todos os dispositivos com Windows 10 relatados pelo CrowdStrike.

5. Selecione **Salvar metadados** .
6. No Construtor de condições, selecione **Ativo de hardware** Para Tipo de ativo.
7. Selecione a alternância Política de base.
8. Selecione a política que você criou, por exemplo, 1, **Política de base - Dispositivos Windows 10** da lista.

   Esta política secundária herda automaticamente as condições da política de base.
9. Selecione a alternância Políticas de exclusão.
10. Selecione Ativos com exceção de IRM aprovada na lista.

    Nota: Se você não tiver esta política, poderá selecionar outra política na lista que deseja excluir desta política.

    Os ativos que corresponderem a esta política serão excluídos da política secundária. Observe que você pode adicionar mais políticas.
11. Selecione **Relatado por** .
12. Selecione **CrowdStrike** da lista.
13. Selecione **Salvar mudanças**.
    Sua nova política é exibida na lista Todos do módulo Políticas e descobertas, mas não está ativada.
14. Selecione **Ativar política** sua política de base monitora todos os ativos que correspondem às condições da política e gera descobertas.

Tradução automática

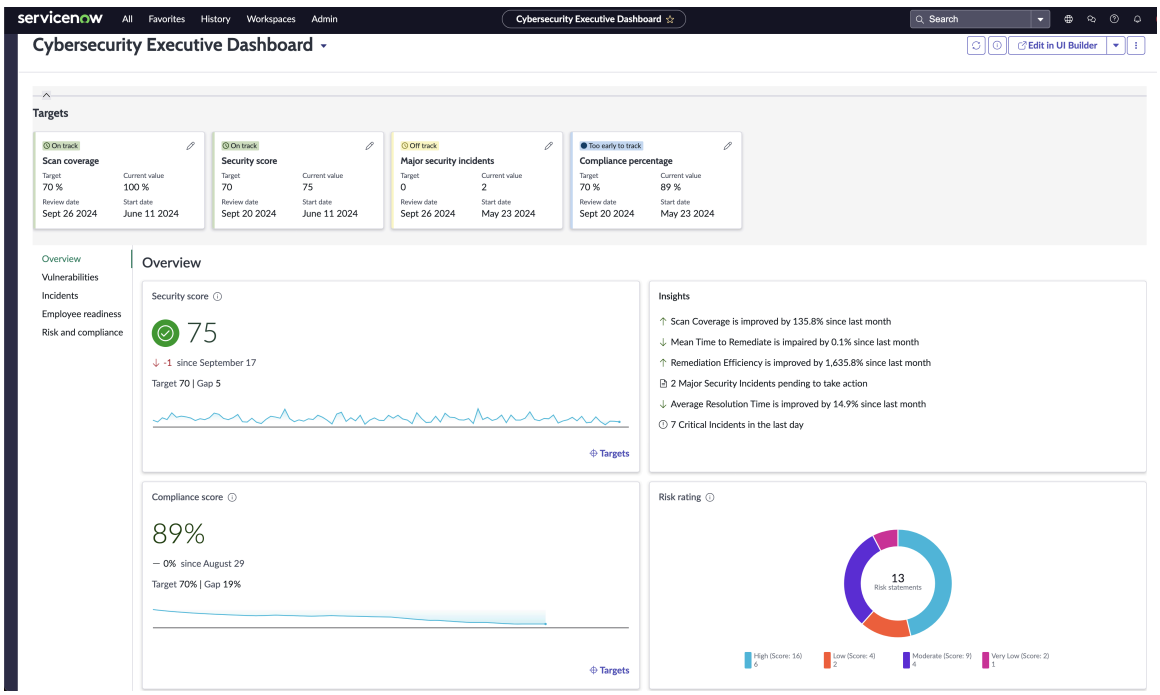
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel executivo de cibersegurança

O Painel executivo de segurança cibernética é uma solução abrangente que capacita os diretores de segurança da informação (CISOs) e os executivos de segurança cibernética com visibilidade da postura e das iniciativas de segurança da organização. O painel consolida dados de vários produtos no ServiceNow Pacote de operações de segurança e governança, risco e conformidade (GRC).

O painel fornece os seguintes recursos:

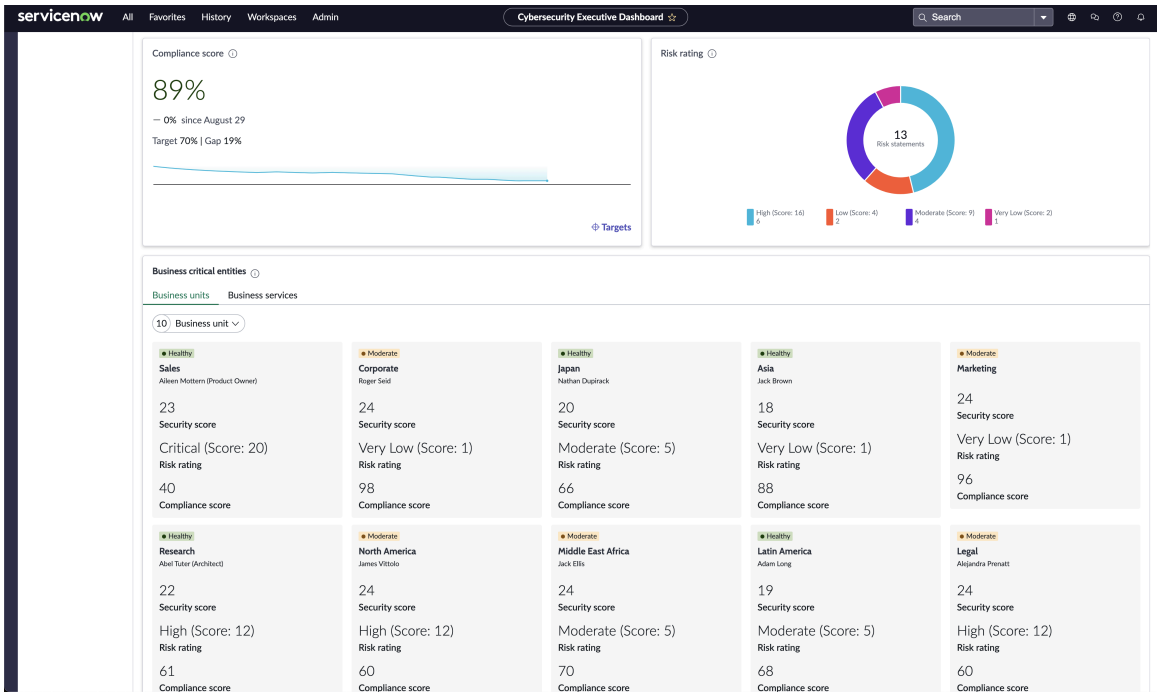
- Pontuação da postura de segurança em toda a organização
- Pontuações de segurança, risco e conformidade por unidade de negócios
- Monitoramento personalizável
- Exibição unificada do cenário de segurança de uma organização
- Benchmarking
- Interface amigável
- Visibilidade das métricas de simulação de phishing do KnowBe4 e do Microsoft Defender para Office 365



Esses recursos permitem a tomada de decisões proativa, fornecendo acesso rápido a métricas de segurança críticas. Tornando-o uma ferramenta indispensável para melhorar a resiliência e a prontidão gerais da segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Funções necessárias de ServiceNow AI Platform

- CISO (sn_bod.ciso) para exibir e compartilhar o painel.
- sn_bod.ciso_admin para exibir, compartilhar o painel e configurar pesos para classificação de postura de segurança.
- Usuário do GRC CISO (sn_grc_dashboards.grc_ciso_user) para exibir relatórios de risco e conformidade.

Acesse o Painel executivo de segurança cibernética

Para abrir o painel, navegue até **Tudo** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
CISOs (Chief Information Security Officers, diretores de segurança da informação)	CISOs obtêm informações sobre gestão de vulnerabilidades, gestão de incidentes, postura de segurança da organização, métricas de simulação de phishing e assim por diante, para suas organizações.

Visualização de dados

Nota: Para saber mais sobre um widget, selecione o ícone de informações ⓘ.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Metas

Métricas	Tipo	Descrição
Metas	Percentual	Mostra a meta definida a ser coberta para uma métrica. O status dos destinos é indicado por meio de codificação por cores. Ele mostra todos os destinos cuja data de revisão está nos últimos 30 dias ou nos próximos. Você pode definir o número de dias para exibir destinos usando `sn_bod.show_targets_from` propriedade do sistema. Esses destinos podem ser editados. Para obter mais informações, consulte Definir metas.

Métricas	Tipo	Descrição
Pontuação de segurança	Pontuação única	Pontuação geral da postura de segurança da organização considerando itens vulneráveis, incidentes de segurança, incidentes de segurança graves e configurações incorretas.
Informações	Realces	Destaques de todo o painel.
Pontuação de conformidade	Pontuação única	Fornece a postura de conformidade da organização com a ajuda da pontuação de conformidade calculada com base na porcentagem de controles em conformidade do número total de controles.
Pontuação de risco	Pontuação única	Fornece a contagem de declarações de risco com base nas classificações de risco. Ele ajuda as organizações a entender o possível impacto e a probabilidade de vários riscos, permitindo que elas priorizem e gerenciem esses riscos.
Entidades essenciais para os negócios		
Unidades de negócios	Pontuação única	Pontuação geral de segurança das unidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
		de negócios, considerando o risco associado a vulnerabilidades, configurações incorretas, vulnerabilidades de tecnologia operacional (OT), incidentes de segurança e incidentes de segurança graves. O rótulo de integridade das unidades de negócios é baseado somente na pontuação de segurança. Para ver como esses rótulos são atribuídos, navegue até a tabela Ponderações de pontuação de risco [sn_sec_cmn_risk_score_weight_list.do] e pesquise a entidade de negócios. Rótulos como "íntegro" são atribuídos com base em intervalos de valores predefinidos. Por exemplo, uma pontuação de segurança que varia de 0 a 39 é rotulada como íntegro. O código de cores desses rótulos é especificado em CISOutils Unified inclusão de script. Você pode configurar o intervalo de valores e as cores dos rótulos. Para ver como os nomes principais da unidade de negócios e da unidade de negócios são atribuídos, acesse **Tudo** > **Organização** > **Unidades de Negócios**. **Nota:** Dependendo dos plug-ins habilitados, você pode acessar a pontuação de conformidade, a pontuação de risco e a pontuação de segurança. Para exibir a pontuação de conformidade e risco, você deve ativar os plug-ins do GRC. Para exibir a pontuação de segurança, você deve ativar os plug-ins relacionados às Operações de segurança. Consulte a seção Aplicações para ativas para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Serviços de negócio	Pontuação única	Pontuação geral de segurança dos serviços de negócio, considerando o risco associado a vulnerabilidades, configurações incorretas, vulnerabilidades de tecnologia operacional (OT), incidentes de segurança e incidentes de segurança graves. Para ver como esses rótulos são atribuídos, navegue até a tabela Ponderações de pontuação de risco [sn_sec_cmn_risk_score_weight_list.do] e pesquise a entidade de negócios. Rótulos como "íntegro", "Moderado" e "Crítico" são atribuídos com base em intervalos de valores predefinidos. Por exemplo, uma pontuação de segurança que varia de 0 a 39 é rotulada como íntegro. O código de cores desses rótulos é especificado em CISOutils Unified inclusão de script. Você pode configurar o intervalo de valores e as cores dos rótulos. Para ver como a unidade de negócios e o nome principal da unidade de negócios são atribuídos, acesse **Tudo** > **Organização** > **Unidades de Negócios**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
		Nota: Dependendo dos plug-ins habilitados, você pode acessar a pontuação de conformidade, a pontuação de risco e a pontuação de segurança. Para exibir a pontuação de conformidade e risco, você deve ativar os plug-ins do GRC. Para exibir a pontuação de segurança, você deve ativar os plug-ins relacionados às Operações de segurança. Consulte a seção Aplicações para ativas para obter mais informações.

Vulnerabilidades

Métricas	Tipo	Descrição
Tempo médio para correção (mensal)	Linha	Tempo médio necessário para fechar vulnerabilidades e resultados de teste com falha em todos os ativos (hosts, contêineres e aplicações) em um mês. Ele também fornece as seguintes métricas: • Destino: Destino definido em dias para corrigir as vulnerabilidades. • Diferença: Diferença em dias entre o destino e o tempo real necessário para corrigir as vulnerabilidades. • Benchmark do setor: Média de métricas dos pares no mesmo setor. • Benchmark global: Média de métricas dos pares no mercado global Consulte Aceite pontuações de benchmark sobre como exibir as pontuações de benchmark.
Idade média das vulnerabilidades ativas (mensal)	Pontuação única	Idade média mensal dos três tipos de itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

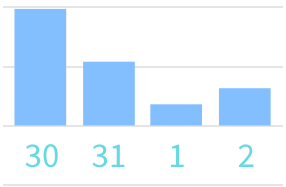
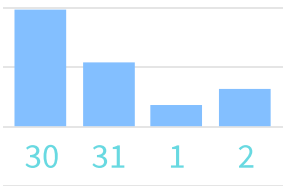
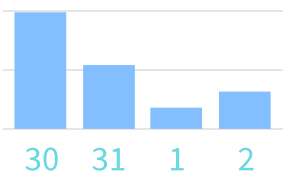
Vulnerabilidades

Métricas	Tipo	Descrição
		Ele também fornece uma comparação da idade do mês atual com o mês anterior. Ele também fornece as seguintes métricas: • Benchmark do setor: Média de métricas dos pares no mesmo setor. • Benchmark global: Média de métricas dos pares no mercado global • Destino: Destino definido em dias para corrigir as vulnerabilidades.
Eficiência de correção (mensal)	Pontuação única	Percentual de itens vulneráveis encerrados mensalmente para itens vulneráveis ativos mensais. Ele também fornece as seguintes métricas: • Mudança percentual em relação ao mês anterior. • Destino: Destino definido em porcentagem para corrigir as vulnerabilidades. • Lacuna: A lacuna entre a meta e a pontuação atual. • Benchmark do setor: Média de métricas dos pares no mesmo setor. • Benchmark global: Média de métricas dos pares no mercado global
Idade média das vulnerabilidades ativas por grupo de atribuição	Várias linhas	Idade média das vulnerabilidades ativas para cada grupo de atribuição.
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Detalhamento de vulnerabilidades ativas em hosts, contêineres e aplicações por classificação de risco e idade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades

Métricas	Tipo	Descrição
Cumprimento da meta de correção por grupo de atribuição	Barra vertical 	A proporção entre o número de vulnerabilidades e configurações incorretas encerradas no destino de correção e o número total de vulnerabilidades e configurações incorretas encerradas.
Cobertura de verificação	Percentual	Percentual de ativos verificados nos últimos 90 dias de todos os ativos no CMDB.
Ativos verificados vs. não verificado	Barra horizontal	Detalhamento de ativos verificados nos últimos 90 dias e total de ativos em CMDB Por classe de IC
Ativos verificados	Barra horizontal	Ativos verificados nos últimos 90 dias em busca de vulnerabilidades versus conformidade de configuração.
Tendência de descobertas críticas e altas ativas	Várias linhas 	Tendência diária de vulnerabilidades e configurações incorretas que têm classificação crítica e de alto risco.
Vulnerabilidades por categoria de ativo e classificação de risco	Barra vertical 	Detalhamento de vulnerabilidades ativas e configurações incorretas por categoria de ativo e classificação de risco (crítico, alto e médio).
Descobertas adiadas por motivo e grupo de atribuição	Barra vertical 	Detalhamento de vulnerabilidades ativas e configurações incorretas adiadas por motivo de adiamento e grupo de atribuição.
Tecnologia operacional (OT)		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades

Métricas	Tipo	Descrição
Tendência de vulnerabilidade crítica e alta ativa	Linha	Tendência diária de vulnerabilidades de OT ativas com classificação crítica e de alto risco.
Tempo médio para correção (mensal)	Pontuação única	Tempo médio necessário para fechar vulnerabilidades de OT. A proporção entre a idade total das vulnerabilidades de OT encerradas e o número total de vulnerabilidades de OT. Ele também fornece as seguintes métricas: • Mudança percentual em relação ao mês anterior. • Destino: Destino definido em dias para corrigir as vulnerabilidades. • Benchmark do setor: Média de métricas dos pares no mesmo setor. • Benchmark global: Média de métricas dos pares no mercado global Consulte Aceite pontuações de benchmark sobre como exibir as pontuações de benchmark.
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Detalhamento de vulnerabilidades de OT ativas por classificação de risco e idade.
Idade média das vulnerabilidades ativas (mensal)	Gráfico de linhas	Idade média mensal dos itens vulneráveis de OT. Ele também fornece uma comparação da idade do mês atual com o mês anterior.
Vulnerabilidades por estado e idade	Mapa térmico	Detalhamento de vulnerabilidades de OT ativas por estado e idade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

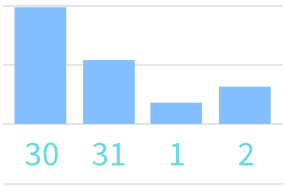
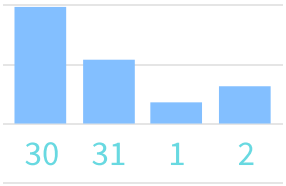
incidentes

Métricas	Tipo	Descrição
Incidentes de segurança graves	Pontuação única	Número de incidentes de segurança graves que estão ativos no momento.
Média de tempo de resolução de incidentes de segurança (mensal)	Pontuação única	Tempo médio de resolução mensal em dias de incidentes de segurança encerrados. Ele também fornece as seguintes métricas: • Mudança percentual em relação ao mês anterior. • Destino: Meta definida em dias para corrigir os incidentes de segurança. • Lacuna: A lacuna entre os dias reais necessários para resolver e o destino definido para corrigir. • Benchmark do setor: Média de métricas dos pares no mesmo setor. • Benchmark global: Média de métricas dos pares no mercado global
Tempo médio para eliminar (mensal)	Gráfico de linhas	Resolução média mensal em dias para erradicar incidentes de segurança.
Tempo médio para identificar (mensal)	Pontuação única	Resolução média mensal em dias para identificar os incidentes de segurança.
Tempo médio de contenção (mensal)	Pontuação única	Resolução média mensal em dias para conter incidentes de segurança.
Incidentes ativos por prioridade e categoria	Mapa térmico	Contagem de incidentes de segurança ativos, que são categorizados por prioridade e categoria.

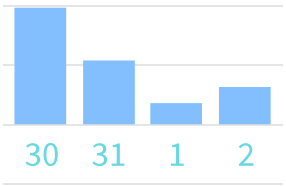
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

incidentes

Métricas	Tipo	Descrição
Tendência de incidentes encerrados e em aberto	Barra vertical 	Detalhamento de incidentes encerrados e em aberto.
Incidentes ativos por estados	Barra vertical 	Detalhamento de incidentes ativos com base em seus estados.

Prontidão do funcionário

Métricas	Tipo	Descrição
Visão geral mensal da simulação de phishing	Barra vertical 	Soma de usuários que executaram as ações, como abertos, clicados e relatados na simulação de phishing, junto com a soma do total de usuários de cada simulação nos últimos seis meses.

Risco e conformidade

Para exibir widgets de risco e conformidade, você deve ativar os plug-ins do GRC. Para obter informações sobre plug-ins GRC, consulte a seção Aplicações a serem ativadas. Para obter informações sobre widgets de GRC, consulte Painel de risco e conformidade para GRC: Metrics.

Indicadores

ANS de host - Encerrado

Este indicador é calculado diariamente. Considera a idade total de todas as vulnerabilidades de host que foram encerradas no dia anterior no momento do cálculo.

ANS de contêiner - Encerrado

Este indicador é calculado diariamente. Considera todas as vulnerabilidades de contêiner que foram encerradas no dia anterior no momento do cálculo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ANS da aplicação - Encerrado

Este indicador é calculado diariamente. Considera a idade total de todas as vulnerabilidades da aplicação que foram encerradas no dia anterior no momento do cálculo.

ANS do resultado do teste - Aprovado

Este indicador é calculado diariamente. Considera todas as vulnerabilidades de resultado de teste que foram aprovadas no dia anterior no momento do cálculo.

ANS de host – Contagem encerrada

Este indicador é calculado diariamente. Considera a contagem de todas as vulnerabilidades do host que foram encerradas no dia anterior no momento do cálculo.

ANS de contêiner – Contagem de encerrados

Este indicador é calculado diariamente. Considera a contagem de todas as vulnerabilidades de contêiner que foram encerradas no dia anterior no momento do cálculo.

ANS de aplicação – Contagem de encerrados

Este indicador é calculado diariamente. Considera a contagem de todas as vulnerabilidades da aplicação que foram encerradas no dia anterior no momento do cálculo.

ANS do resultado do teste - Contagem de aprovados

Este indicador é medido diariamente. Considera a contagem de todas as vulnerabilidades de resultado de teste que foram aprovadas pela última vez no dia anterior no momento do cálculo.

Ativos verificados

Este indicador é calculado diariamente. Considera a soma dos ICs verificados da tabela sn_vul_analytics_scan_coverage_config, que inclui os verificados pela última vez nos últimos 90 dias, em todas as classes de IC do CMDB.

Ativos verificáveis

Este indicador é calculado diariamente. Considera a soma do total de ICs da tabela sn_vul_analytics_scan_coverage_config para todas as classes de IC do CMDB presentes.

Itens vulneráveis

Este indicador é calculado diariamente. Considera a contagem de itens vulneráveis ativos no momento do cálculo.

Item vulnerável da aplicação

Este indicador é calculado diariamente. Considera a contagem de itens vulneráveis à aplicação ativos no momento do cálculo.

Item vulnerável de contêiner

Este indicador é calculado diariamente. Considera a contagem de itens vulneráveis de contêiner ativos no momento do cálculo.

Soma da idade dos itens vulneráveis

Este indicador é calculado diariamente. Considera a soma da idade dos itens vulneráveis ativos no momento do cálculo.

Soma da idade dos itens vulneráveis da aplicação

Este indicador é calculado diariamente. Considera a soma da idade dos itens vulneráveis à aplicação ativos no momento do cálculo.

Itens vulneráveis aberto

Este indicador é calculado diariamente. Considera os itens vulneráveis em aberto no momento do cálculo.

Itens vulneráveis de contêiner em aberto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Considera os itens vulneráveis do contêiner em aberto no momento do cálculo.

Itens vulneráveis de aplicação em aberto

Este indicador é calculado diariamente. Considera os itens vulneráveis à aplicação em aberto no momento do cálculo.

Resultados de testes ativos

Este indicador é calculado diariamente. Considera os resultados de testes em aberto no momento do cálculo.

VITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como item vulnerável do host.

AVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável à aplicação.

CVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável de contêiner.

Resultados de testes adiados

Este indicador é calculado diariamente. Considera os resultados do teste que estavam em um estado adiado.

Problemas de configuração em aberto – Resultados de testes

Este indicador é calculado diariamente. Ele tem uma origem de indicador como resultado de teste para o Painel de resposta unificada a vulnerabilidades.

Tempo médio para identificar

Este indicador é calculado diariamente. Considera o incidente de segurança em que a definição é o tempo de identificar no momento do cálculo.

Incidente de segurança: tempo médio de duração

Este indicador é calculado diariamente. Considera o incidente de segurança em que a definição é uma duração do estado do incidente no momento do cálculo.

Número de incidentes de segurança importantes em aberto

Este indicador é calculado diariamente. Considera incidentes de segurança graves em aberto no momento do cálculo.

Número de incidentes de segurança encerrados

Este indicador é calculado diariamente. Considera incidentes de segurança encerrados no momento do cálculo.

Itens vulneráveis da aplicação encerrados

Este indicador é calculado diariamente. Considera itens vulneráveis à aplicação encerrados no momento do cálculo.

Itens vulneráveis do contêiner encerrados

Este indicador é calculado diariamente. Considera itens vulneráveis do contêiner fechado no momento do cálculo.

Itens vulneráveis encerrados

Este indicador é calculado diariamente. Considera itens vulneráveis encerrados no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Considera a pontuação de risco máxima para itens vulneráveis no momento do cálculo.

Obter pontuação de risco máximo para item vulnerável de contêiner

Este indicador é calculado diariamente. Considera a pontuação de risco máxima para itens vulneráveis ao contêiner no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis de aplicação

Este indicador é calculado diariamente. Considera a pontuação de risco máximo para itens vulneráveis à aplicação no momento do cálculo.

Soma da pontuação de risco de VITs

Este indicador é calculado diariamente. Considera a soma das pontuações de risco dos itens vulneráveis no momento do cálculo.

Soma da pontuação de risco de AVIs

Este indicador é calculado diariamente. Considera a soma das pontuações de risco dos itens vulneráveis à aplicação no momento do cálculo.

Soma da pontuação de risco de CVIs

Este indicador é calculado diariamente. Considera a soma das pontuações de risco dos itens vulneráveis do contêiner no momento do cálculo.

Soma da pontuação de risco de configurações incorretas

Este indicador é calculado diariamente. Considera a soma das pontuações de risco dos resultados de testes no momento do cálculo.

Obter pontuação de risco máximo para incidentes de SI

Este indicador é calculado diariamente. Considera as pontuações de risco máximo dos incidentes de segurança no momento do cálculo.

Obter pontuação máxima de risco para resultados de testes de configuração incorreta

Este indicador é calculado diariamente. Considera as pontuações máximas de risco para configuração incorreta dos resultados de testes no momento do cálculo.

Obter pontuação média de risco para resultados de teste de configuração incorreta

Este indicador é calculado diariamente. Considera as pontuações médias de risco para configuração incorreta dos resultados de testes no momento do cálculo.

Número de incidentes de segurança em aberto

Este indicador é calculado diariamente. Considera incidentes de segurança em aberto no momento do cálculo.

Visão geral do phishing

Este indicador é calculado diariamente. Considera a contagem de métricas de simulação de segurança no momento do cálculo.

MTTR agregado

Calcula o tempo médio necessário para fechar vulnerabilidades (hosts, contêineres e aplicações) e o tempo necessário para fechar os resultados do teste em dias. [[ANS de host - encerrado]] [[ANS de aplicação - encerrado]] [[ANS de contêiner - encerrado]] [[ANS de resultado de teste - aprovado]]) / ([[ANS de host - Contagem de encerramento]] [[ANS de aplicação - Contagem de encerramento]]] [[ANS de resultado de teste - Contagem de aprovação]]]] [[ANS de contêiner - Contagem de encerramento]]])

Cobertura de verificação atual

Calcula a porcentagem usando a proporção entre o número de itens verificados e o número total de itens qualificados para verificação durante o mesmo período. Var ScannedItems / ScannableItems * 100;if (res > 0 100)res 0 100;res;

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Idade média dos itens vulneráveis ativos

Calcula a idade média de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) em dias. [[Soma da idade dos itens vulneráveis]] [[Soma da idade dos itens vulneráveis da aplicação]]] [[Soma da idade dos itens vulneráveis do contêiner]]) / ([[Itens vulneráveis da aplicação]]] [[Itens vulneráveis do contêiner]]]]

Ativos por idade e classificação de risco

Calcula a contagem total de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) categorizados por idade e nível de avaliação de risco. [[Abrir itens vulneráveis]] [[Abrir itens vulneráveis do contêiner]] [[Abrir itens vulneráveis da aplicação]]

Problemas adiados

Calcula a contagem total de todos os itens vulneráveis (hosts, contêineres, aplicações e resultados de testes) com o estado "Adiado". [[Adiados Vits]] [[Adiados AVITs]] [[Resultados de testes adiados]] [[Deferidos CVITs]]

Média de tempo de resolução de incidentes de segurança em aberto

Calcula o tempo médio necessário para fechar os incidentes de segurança em dias. [[Soma da duração dos incidentes de segurança encerrados]] / [[Número de incidentes de segurança encerrados]]) /24

Pontuação de Segurança

Calcula as classificações de segurança gerais diariamente. É calculado com base na pontuação de risco acumulada. Var secPostureRating: 100 - [[Pontuação de segurança]]; secPostureRating;

Pontuação de segurança (unidades de negócios)

Calcula a pontuação de risco acumulada final em que a pontuação de risco de acúmulo de itens vulneráveis, configurações incorretas, incidentes de segurança e incidentes de segurança graves são multiplicados com os respectivos pesos obtidos na tabela de acúmulo de postura de segurança. Var numMajorIncidents: [[Número de incidentes de segurança graves em aberto]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0 40) majorSIRiskScore: 100 100; else majorSIRiskScore: 0; rollUpRiskScore: ([[Pontuação de risco acumulada de vulnerabilidade e erro de configuração]] * 20% de risco acumulado de risco de vulnerabilidade]]] * 20% de risco de risco de risco de risco de 20

Pontuação de segurança (serviços de negócio)

Calcula a pontuação de risco acumulada final em que a pontuação de risco de acúmulo de itens vulneráveis, configurações incorretas, incidentes de segurança e incidentes de segurança graves são multiplicados com os respectivos pesos obtidos na tabela de acúmulo de postura de segurança. Var numMajorIncidents: [[Número de incidentes de segurança graves em aberto - Serviços]], majorSIRiskScore, rollUpRiskScore; If(numMajorIncidents > 0 40) majorSIRiskScore: 100 100; else majorSIRiskScore: 0 20; rollUpkScore: ([[Vulnerabilidade e Misconfiguration acumulou Pontuação de risco - Serviços]]] * 20 Pontuação de risco - 20]

Pontuação de risco acumulado de vulnerabilidade

Calcula a pontuação de risco acumulado de vulnerabilidade em que a pontuação de risco máxima, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis são multiplicadas com seus respectivos pesos. Var: 100; contagem de variáveis: [[ativos por idade e classificação de risco]]; var countRiskScore; if (0) countRiskScore: 0 10; else if (contagem > 10000) countRiskScore: MaxRiskScore; else if (contagem > 1000) countRiskScore: (MaxRiskScore * 0,80); else if (contagem > 0,40) Riskscore: 0,20) RiskScore: 100) RiskScore: 0,60) var vulRiskScore: ([[Obter pontuação máxima de todos os itens vulneráveis]] * 0 mais [[Pontuação média de risco de todos os itens vulneráveis]] * 100 mais countRiskScore * 0)/100; vulRiskScore;

Obter pontuação máxima de todos os itens vulneráveis

Calcula a pontuação de risco acumulado de vulnerabilidade em que a pontuação de risco máxima, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são multiplicadas com seus respectivos pesos. MaxScoreForVI: [[Obter pontuação máxima de risco para itens vulneráveis]], maxScoreForCVI: [[Obter pontuação máxima de risco para item vulnerável do contêiner], maxScoreForAVI: [[Obter pontuação máxima de risco para itens vulneráveis da aplicação]], maxScore; if (maxScoreForScoreForVI e maxScoreForScoreForScoreForVI]

Pontuação de risco médio de todos os itens vulneráveis

Calcula a pontuação média de risco de todos os itens vulneráveis (hosts, contêineres e aplicações). Var somatedRiskScore: [[Soma da pontuação de risco de vítimas]] [[Soma da pontuação de risco de AVIS]], avgRiskScore; var totalVulCount: [[Itens vulneráveis em aberto]]] [[Itens vulneráveis da aplicação em aberto]]]; if(summedRiskScore: 0) avgRiskScore: 0); 0

Pontuação de risco acumulada de configuração incorreta

Calcula a pontuação de risco acumulada de configuração incorreta usando os resultados de teste categorizados como Falha, Erro ou Desconhecido. Valor da variável: 100 0,40; contagem de variáveis: [[Problemas de configuração em aberto - Resultados de teste]]; var countRiskScore; if (0) countRiskScore: 0 10; else if (contagem > 10000) countRiskScore: MaxRiskScore; else if (contagem > 1000) countRiskScore: (MaxRiskScore * 0,80); else (contagem > 100) RiskScore: 0,20) RiskScore * 0,60) ([[Obter pontuação de risco máxima para resultados de teste de configurações incorretas]] * 0 mais [[Obter pontuação de risco média para resultados de teste de configuração incorreta]] * 100 mais countRiskScore * 0)/100; misRiskScore;

Tempo médio para eliminar

Calcula o tempo médio necessário para erradicar incidentes de segurança em dias [[SI - Tempo médio de duração > Estado do incidente de segurança: Erradicar]] / 1440

Tempo médio para identificar

Calcula o tempo médio necessário para identificar incidentes de segurança em dias. [[SI - Tempo médio para identificar]] / 1440

Tempo médio de contenção

Calcula o tempo médio necessário para conter incidentes de segurança em dias. [[SI - Tempo médio de duração > Estado do incidente de segurança contém]] / 1440

Cumprimento da meta de correção

Calcula a porcentagem mensal de adesão à meta de correção dos resultados de teste, itens vulneráveis, itens vulneráveis do contêiner e itens vulneráveis à aplicação. A adesão de destino é determinada pelo número de itens que atenderam à meta definida. ([[ANS de resultado de teste - Contagem aprovada > Status de correção (unificado): Meta atendida]]] [[ANS de contêiner - Contagem encerrada > status de correção (unificado) Destino atendido]] [[ANS de aplicação - Contagem encerrada > Status de correção (unificado) Destino atendido]]] [[ANS de host - Contagem de encerrados > Status de correção (unificado)]] [Contagem de host - ANS - Contagem de ANS - ANS - Contagem de host - ANS - Encerrado - ANS - Contagem de host - ANS - ANS - Contagem de host encerrado - ANS - ANS - Encerrado 100

Eficiência de correção mensal (todos os itens vulneráveis)

Calcula a porcentagem mensal de itens vulneráveis encerrados, itens vulneráveis de contêineres e itens vulneráveis à aplicação em contraste com os recém-identificados. Var closedItems: [[ANS de Host - Contagem Encerrada]] [[ANS de Contêiner - Contagem Encerrada]] [[ANS de Aplicação - Contagem Encerrada]] [[ANS de Resultado de Teste - Contagem Passada]];

Var newItems: [[Host Vits Opened/reabriu ontem]] [[Container Vits Opened/reabriu ontem]] [[Application Vits Opened/reabriu ontem]]] [[Resultados de testes abertos/reabertos ontem]];

Se (res > 1000) res: 0;se (newItems: 0 100) res: 1000;se (newItems: 0) res: 0; res;

VITs do host abertos/reabertos ontem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Considera os itens vulneráveis do host que foram abertos pela última vez no dia anterior no momento do cálculo.

VITs da aplicação abertos/reabertos ontem

Este indicador é calculado diariamente. Considera os itens vulneráveis à aplicação que foram abertos pela última vez no dia anterior no momento do cálculo.

VITs do contêiner abertos/reabertos ontem

Este indicador é calculado diariamente. Considera os itens vulneráveis do contêiner que foram abertos pela última vez no dia anterior no momento do cálculo.

Resultados de testes abertos/reabertos ontem

Este indicador é calculado diariamente. Considera os resultados do teste que foram vistos pela última vez no dia anterior no momento do cálculo.

Itens vulneráveis de OT

Este indicador é calculado diariamente. Considera itens vulneráveis de OT ativos presentes no momento do cálculo.

Soma da duração de OT do vulnerável encerrado

Este indicador é calculado diariamente. Considera a idade total de todas as vulnerabilidades de OT encerradas no dia do cálculo.

Itens vulneráveis fechados de OT

Este indicador é calculado diariamente. Considera os itens vulneráveis de OT que estão encerrados no dia do cálculo.

Idade média dos itens vulneráveis ativos de OT

Calcula a idade média dos itens vulneráveis a OT ([[Soma da idade dos itens vulneráveis a OT]] / [[Itens vulneráveis a OT]])

Detalhamentos

- Unidade de negócios
- Serviços de negócio
- Pontuação de risco
- Faixa etária
- Grupo de atribuição (unificado)
- Status da meta de correção (Encerrado)
- Classe de ativo
- Categoria do ativo
- Classificação de risco (unificada)
- Motivo adiado (unificado)
- Estado do Incidente de segurança
- Prioridade de Incidente de segurança
- Categoria de Incidente de segurança
- Evento de phishing
- Motivo do adiamento não encerrado (unificado)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações a serem ativadas

Você deve ativar as seguintes aplicações para preencher a pontuação nos widgets. Com base na aplicação que você está usando, você deve ativar as aplicações dependentes.

Se você estiver usando	Ativar
Resposta a vulnerabilidades	• Performance Analytics para Resposta a vulnerabilidades • Base para resposta a vulnerabilidades • Resposta a vulnerabilidades • Resposta a vulnerabilidades e Conformidade de configuração para contêineres • Conformidade de configurações
Operational Technology	Resposta a vulnerabilidades para tecnologia operacional
Integrações de phishing	• Simulação de segurança e integração de treinamento para SecOps • KnowBe4 Integration para SecOps • Integração do Microsoft Defender para Office365 para SecOps
Resposta a incidentes de segurança	• Performance Analytics para Security Incident Response • Resposta a incidentes de segurança • Gestão de incidentes graves de segurança
Governança, risco e conformidade	• GRC: elementos comuns do painel • GRC: Espaço de gestão de riscos • Risco avançado para GRC • GRC: Espaço de gestão de conformidade

Trabalhos agendados para coleta de dados

Os trabalhos agendados a seguir são executados para coletar pontuações em novos dados automaticamente.

Trabalho programado	Frequência	Descrição
Carregue as pontuações de benchmark	Sob demanda	Coleta pontuações da instância e publica na instância central. Os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Frequência	Descrição
		algoritmos de benchmark calculam as melhores pontuações do setor.
Baixe as pontuações de benchmark	Sob demanda	Baixa as pontuações de benchmark. Ele está disponível na tabela Pontuações de benchmark [sn_bm_client_score_list].

Aceite pontuações de benchmark

Obtenha pontuações de benchmark registrando sua instância no ServiceNow instância central. O último mantém informações de vários setores para fornecer a pontuação de benchmark.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre Benchmarking, consulte Explorando Benchmarks .

Procedimento

1. Para registrar sua instância com a instância central, siga estas etapas:
   a. Navegar até **Tudo** > **Propriedades do sistema** > **Todas as Propriedades**.
   b. Selecione `sn_bm_client.central_instance_url` propriedade do sistema.
   c. Em **Valor** Insira o URL da instância central do benchmark.

      Nota: Se a instância estiver provisionada, seus detalhes serão enviados automaticamente para a instância central.

   d. Selecione **Aceite** do widget para validar e estabelecer uma conexão com a instância central.
2. Para carregar sua pontuação na instância central, siga estas etapas:
   a. Navegar até **Tudo** > **Scheduler do Sistema** > **Trabalhos agendados**
   b. Selecione o `Upload the benchmark scores` trabalho agendado.
   c. Selecione **Atualizar**.
      As pontuações são carregadas na instância central. No entanto, os trabalhos agendados pela instância central são executados uma vez por mês para atualizar as pontuações nos widgets do painel.
3. Para baixar a pontuação da instância central, siga estas etapas:
   a. Navegar até **Tudo** > **Scheduler do Sistema** > **Trabalhos agendados**
   b. Selecione o `Download the benchmark scores` trabalho agendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Selecione **Executar agora**.
As pontuações estão disponíveis na tabela Pontuações de benchmark [sn_bm_client_score_list], que é refletida nos widgets do painel.

Definir metas

Defina metas em dias para corrigir as vulnerabilidades, incidentes de segurança e erros de configuração.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Selecione **Destinos** no widget ou selecione **Destinos** Ícone na página Detalhes de KPI.
2. Selecione **Para todos** botão.
3. Em **Novo valor** insira o número de dias em que você deseja atingir a meta.
4. Selecione a data de início de destino.
5. Selecione a data de revisão de destino.
6. Selecione **Atualizar**.

Simulação de segurança e integração de treinamento para operações de segurança

Fortaleça a defesa da sua organização contra ameaças de segurança cibernética importantes incorporando integrações de phishing ao Painel executivo de segurança cibernética. As Integrações de phishing aprimoram o Painel executivo de segurança cibernética incorporando perfeitamente dados de ferramentas de simulação de phishing de terceiros, como KnowBe4 e Microsoft Defender para Office 365.

As integrações a seguir aprimoram os recursos do Painel executivo de segurança cibernética, fornecendo uma perspectiva unificada sobre a postura de segurança da sua organização, a prontidão dos funcionários e a vulnerabilidade a ataques de phishing:

- Integração KnowBe4
- Integração do Microsoft Defender para Office 365

Configure a integração Knowbe4

Obtenha informações imediatas sobre a vulnerabilidade da sua equipe a ataques de phishing integrando o KnowBe4, uma plataforma líder de treinamento de conscientização sobre segurança cibernética. Por meio da integração KnowBe4, identifique tendências e áreas de melhoria em seus programas de treinamento em segurança cibernética, monitore a resiliência geral de phishing e fortaleça proativamente as medidas de segurança da sua organização.

Antes de Iniciar

Função necessária: sn_sec_phish.admin e sn_sec_phish_kb4.kb4_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Integração KnowBe4** > **Configurações do KnowBe4**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário Configuração KnowBe4

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone Pesquisa.
URL base	URL para integrar com KnowBe4.
Chave de API	Chave de API adquirida da conta KnowBe4.
Página	Número da página de onde as simulações devem ser obtidas.
Tamanho da Página	Número de simulações que devem ser incluídas.

   a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

   b. No formulário, preencha os detalhes:

Formulário Instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (KnowBe4 Integration for SecOps).
Integração	KnowBe4 é o padrão.
Ativo	O padrão é Ativado (selecionado). Se estiver desmarcada, a instância não estará ativa.
Descrição	Descrição resumida da instância de integração.

4. Selecione **Enviar**.
5. Navegar até **Tudo** > **Simulação e treinamento de segurança** > **Integrações**.
6. Selecione Integração Knowbe4.
7. Selecione **Executar agora** Para executar e coletar dados do KnowBe4.

Configure a integração do Microsoft Defender para Office 365

Obtenha informações valiosas sobre métricas de simulação de phishing diretamente no Painel executivo de segurança cibernética por meio da integração perfeita com o Microsoft Defender para Office 365.

Antes de Iniciar

Função necessária: sn_sec_phish_msatk.ms_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para saber mais sobre como simular um ataque de phishing e configurar um locatário, consulte:

- Simule um ataque de phishing com o treinamento de simulação de ataque
- Introdução ao treinamento de simulação de ataque
- Configure um locatário

Procedimento

1. Navegar até **Tudo** > **Integração de ataque da Microsoft** > **Configurações de ataque da Microsoft**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário Configuração de ataque da Microsoft

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone Pesquisa.
ID de locatário	ID do locatário da aplicação criada no portal do Microsoft Azure.
ID de cliente	ID do cliente da aplicação criada no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente da aplicação criada no portal do Microsoft Azure.
Marcador	Data a partir da qual as simulações devem ser obtidas.
URL de token	URL de base de onde o token é criado para acessar a API de simulações da Microsoft.
URL de todas as simulações	URL base da API de simulações da Microsoft.

a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

b. No formulário, preencha os detalhes:

Formulário Instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (Microsoft Defender para Office 365).
Integração	Referência de integração de terceiros (Microsoft Attack Integration).
Ativo	O padrão é Ativado (selecionado). Se estiver desmarcada, a instância não estará ativa.
Descrição	Descrição resumida da instância de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Enviar**.
5. Navegar até **Tudo** > **Simulação e treinamento de segurança** > **Integrações**.
6. Selecione Integração de ataque da Microsoft.
7. Selecione **Executar agora** Executar e coletar dados da Microsoft.

Painel de risco e conformidade para GRC: Metrics

O painel Risco e conformidade fornece aos usuários de conformidade e risco uma visão geral abrangente das informações de risco e conformidade em um único painel que ajuda em suas principais decisões.

Você pode navegar até o painel Risco e conformidade no unificado único Painel executivo de cibersegurança para exibir as métricas de risco e conformidade de Governança, risco e conformidade aplicações.

O painel fornece recursos como:

- Visão geral de conformidade
- Visão geral de risco
- Visão geral da privacidade
- Visão geral da continuidade de negócios
- Risco de terceiros
- Visão geral de auditoria

Pré-requisitos para acessar o painel Risco e conformidade

Importante: Você deve ter acesso primário ao Painel executivo de cibersegurança Para ativar o plug-in funcional Cybersecurity and Risk com o qual você pode acessar o painel Risco e conformidade.

Um novo domínio funcional é introduzido para segregar dados relacionados a segurança cibernética e riscos. Você pode ativar o plug-in de segurança cibernética e risco selecionando **Ativar** Botão de ação de IU. Por padrão, este domínio funcional está inativo.

Funções necessárias de ServiceNow AI Platform

Principal GRC A função do usuário é o sn_grc_dashboards.grc_ciso_user que pode exibir os relatórios no painel Risco e conformidade. Esta função contém:

- sn_compliance.reader
- sn_risk.reader

Nota: No entanto, você deve ter a função sn_bod.ciso para fazer login, exibir e compartilhar o Painel executivo de segurança cibernética a partir do qual você pode navegar até o painel Risco e conformidade.

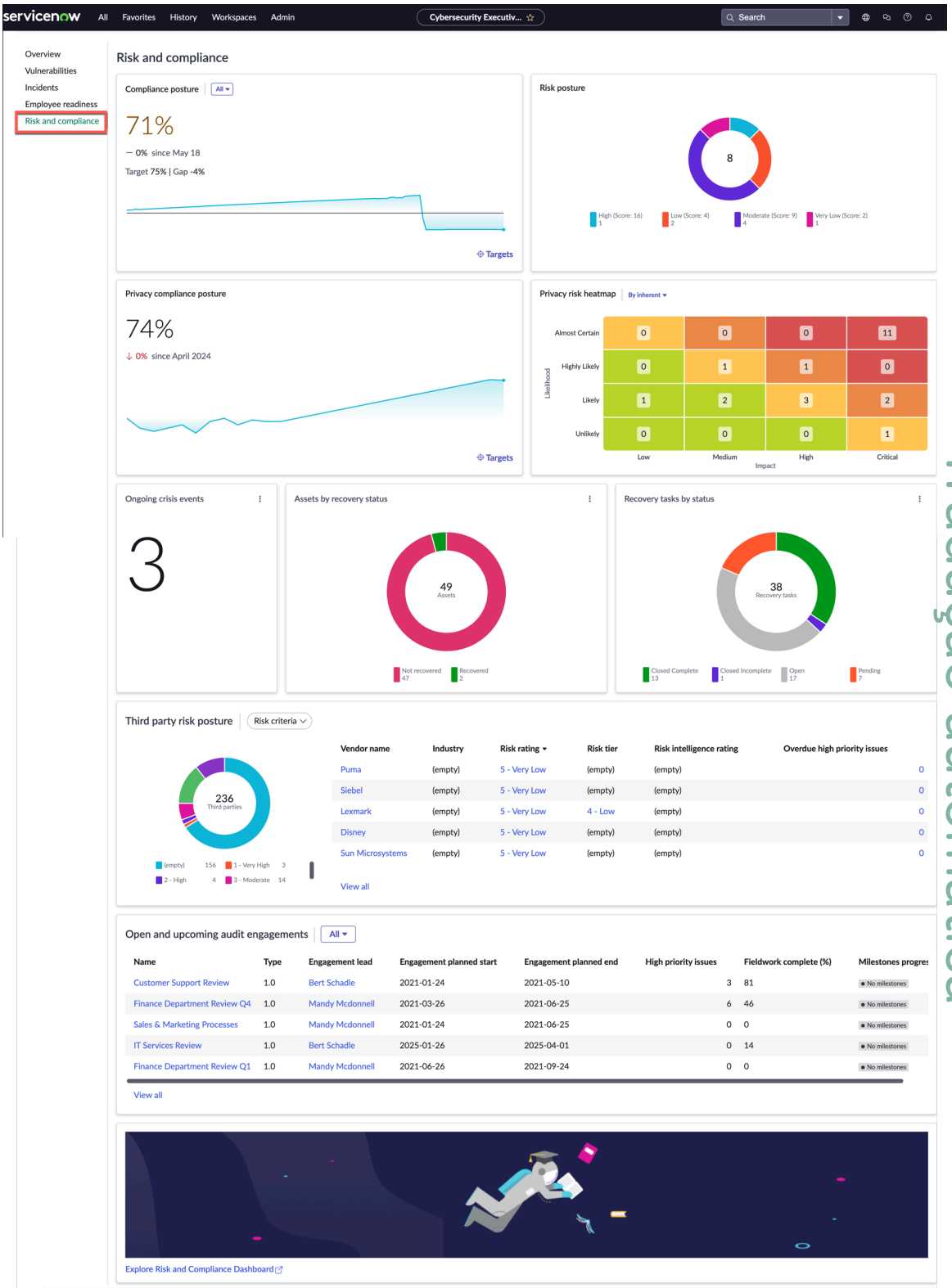
Acesse o painel Risco e conformidade

1. Para acessar o painel Risco e conformidade, navegue até **Tudo** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.
2. Selecione **Risco e conformidade** rótulo da lista à esquerda do painel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel executivo de segurança cibernética unificado para métricas de risco e conformidade



Tradução automática

3. Para visualizar seus dados e exibir os relatórios e as soluções disponíveis no painel projetado para o usuário, selecione Explorar rótulo do Painel de risco e conformidade .

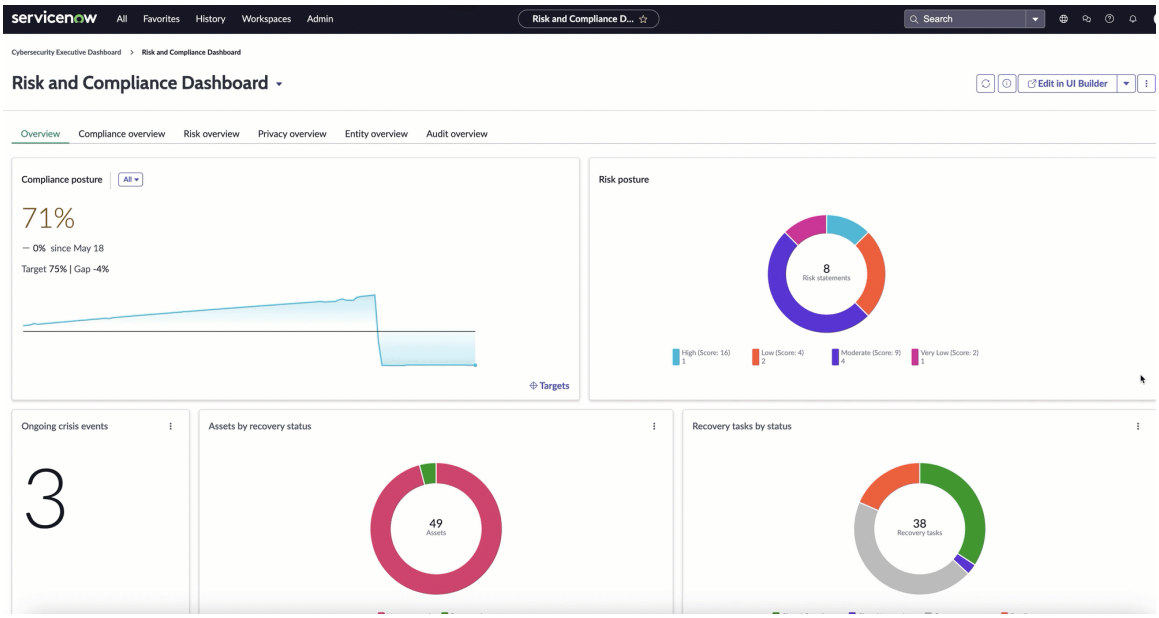
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Risco e conformidade Relatórios e soluções do painel

O painel Risco e conformidade é um painel unificado que fornece dados analíticos abrangentes de relatórios disponíveis nas principais aplicações de GRC para que o diretor de segurança da informação entenda a conformidade e a postura de risco da organização. O painel consolida dados de vários produtos no ServiceNow GRC pacote de aplicações.

Nota: Todos os relatórios estão disponíveis somente quando os espaços correspondentes estão instalados.

Painel Risco e conformidade



Funções necessárias de ServiceNow AI Platform

Para relatórios relacionados à conformidade

O usuário deve ter a função sn_grc_dashboards.grc_ciso_user e a função sn_bod.ciso.

Para relatórios relacionados a risco

O usuário deve ter a função sn_grc_dashboards.grc_ciso_user e a função sn_bod.ciso.

Para relatórios relacionados à Gestão de continuidade de negócios

O usuário deve ter as funções sn_gcn.viewer e sn_bod.ciso.

Para relatórios relacionados a risco de terceiros

O usuário deve ter a função sn_vdr_risk_asmt.vendor_assessment_revisor e a função sn_bod.ciso.

Para relatórios relacionados à Privacidade

O usuário deve ter as funções sn_privacy.analyst e sn_bod.ciso.

Para relatórios relacionados a auditoria

O usuário deve ter a função sn_audit_ws.auditor e a função sn_bod.ciso.

Acesse o Painel de risco e conformidade

Para abrir o painel, navegue até **Tudo** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Postura de conformidade

- Percentual de conformidade: Indicador de fórmula que representa a postura de conformidade.
- Todos os controles: Indicador automatizado que oferece suporte ao indicador de fórmula.
- Controles compatíveis: Indicador automatizado compatível com o indicador de fórmula.

Postura de conformidade com a privacidade

Indicador de PA: Percentual de pontuação de conformidade da atividade de processamento.

Detalhamentos

Domínio funcional.

Relatórios

Nota: Todos os relatórios estão disponíveis somente quando os espaços correspondentes estão instalados.

Guia "Visão geral"

Título	Tipo	Tabela de origem	Descrição
Postura de conformidade	Gráfico de linhas	Controle [sn_compliance_control]	Fornece segurança cibernética e risco, além de risco de TI e postura de conformidade com base na análise de dados para os gerentes de conformidade.
Postura de risco	Gráfico de rosca	As tabelas de origem são as seguintes: • Risco [sn_risk_risk] • Risco agregado detalhado [sn_risk_advanced_risk_assessment_result] (quando Risco avançado A aplicação está instalada e a Avaliação avançada de riscos está habilitada	Fornece a contagem de risco com base nas classificações de risco.
Eventos de crise em andamento	Pontuação única	Evento de recuperação [sn_recovery_event] em que o tipo de evento é real	Exibe o número total de eventos de crise em andamento que não foram aprovados nem encerrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia "Visão geral"

Título	Tipo	Tabela de origem	Descrição
Ativos por status de recuperação	Gráfico de rosca	Ativos [sn_recovery_event_asset]	Fornece o número total de ativos para eventos de crise em andamento agrupados por status de recuperação, incluindo ativos que foram recuperados e aqueles que não foram recuperados.
Tarefas de recuperação por status	Gráfico de rosca	Tarefas de recuperação [sn_recovery_event_task]	Fornece o status das tarefas de recuperação em vários estados para eventos de crise em andamento.

Guia Visão geral de conformidade

Título	Tipo	Tabela de origem	Descrição
Documentos de autoridade	Gráfico de rosca	Documento de autoridade [sn_compliance_authority_document]	Fornece dados de documentos de autoridade em conformidade e fora de conformidade no gráfico. A lista fornece detalhes dos documentos de autoridade, sua pontuação de conformidade individual em porcentagem, contagem de problemas de alta prioridade e exceções de alto risco nos documentos de autoridade e a contagem de casos de conformidade.
Políticas	Gráfico de rosca	Política [sn_compliance_policy]	Fornece a contagem de políticas em conformidade e fora de conformidade no gráfico. A lista fornece detalhes das políticas, sua pontuação de conformidade individual em porcentagem, contagem de problemas de alta prioridade e exceções de risco levantadas em cada política e a contagem de casos de conformidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
Postura de risco	Gráfico de rosca	As tabelas de origem são as seguintes: • Risco [sn_risk_risk] • Risco agregado detalhado [sn_risk_advanced_risk_assessment_result] (quando Risco avançado A aplicação está instalada e a Avaliação avançada de riscos está habilitada)	Fornece a contagem de risco com base nas classificações de risco.
Postura de risco	Lista	Status do conteúdo do GRC [sn_grc_content_reports]	Fornece a classificação de risco para cada risco organizacional para entender os resultados gerais da avaliação de risco. Essas classificações ajudam as organizações a entender o possível impacto e a probabilidade de vários riscos, permitindo que elas priorizem e gerenciem esses riscos. O cartão de postura de risco também destaca as seguintes informações para cada risco: • **Apetite de risco** Valor de apetite de risco definido. • **Problemas de alta prioridade** : O número de problemas com prioridade é definido como Alto. • **Tarefas de resposta de risco atrasadas** Número de tarefas de resposta de risco atrasadas. • **% De violação DO KRI** Percentual de KPIs (Key Risk Indicators,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
			principais indicadores de risco) que excederam seus limites predefinidos.
Postura de risco de terceiros	Gráfico de rosca	Riscos de terceiros [sn_grc_dashboards_third_party_risk]	Fornece a classificação de risco para cada terceiro. A classificação de risco é a classificação geral da avaliação que considera as pontuações e classificações de todas as avaliações realizadas para um terceiro ou fornecedor. O cartão de postura de risco de terceiros também destaca as seguintes informações para cada terceiro ou fornecedor: • **Critérios de risco** Grupo de domínios de risco (às vezes chamados de áreas de risco em outros recursos da plataforma) que se aplica a um tipo específico de terceiros. • **Nível de risco** Valor determinado com base nas respostas coletadas após a conclusão de uma avaliação de risco inerente (IRQ). • **Classificação de inteligência de risco** Agregado de todas as pontuações coletadas de provedores de inteligência de risco. • **Tarefas de resposta de risco atrasadas**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
			Número de tarefas de resposta de risco atrasadas.

Guia Visão geral da privacidade

Título	Tipo	Tabela de origem	Descrição
Postura de conformidade com a privacidade	Linha	Indicador de PA: Percentual de pontuação de conformidade da atividade de processamento [pa_indicators]	Fornece a postura de conformidade por mês e é plotada consultando a pontuação geral de conformidade em todas as atividades de processamento.
Problemas de prioridade alta atrasados	Pontuação única	Problemas [sn_grc_issue]	Fornece uma visão geral focada de todos os problemas atrasados relacionados à privacidade de alta prioridade, permitindo a rápida identificação e resolução de tarefas críticas para garantir a conformidade e a proteção de dados.
Mapa térmico de risco de privacidade	Mapa térmico	Metodologia de avaliação de risco [sn_risk_advanced_risk_assessment_methodology]	Fornece os dados de avaliação de risco de privacidade de um mapa térmico. As avaliações de risco de privacidade são avaliações detalhadas que são realizadas se a pontuação de criticidade for alta. Avalie cada risco associado à atividade de processamento e conheça a pontuação de risco agregada na atividade de processamento. Depois de avaliar os riscos de privacidade, você pode exibir a postura de risco de privacidade no mapa térmico de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da entidade

Título	Tipo	Tabela de origem	Descrição
Entidades	Lista	Status de conformidade da entidade [sn_compliance_entities_reports]	Fornece o resumo dos riscos diretamente associados à entidade que contribuem para a classificação de risco geral da entidade. A lista também exibe a pontuação de conformidade das entidades e problemas de alta prioridade e exceções de risco que são gerados como resultado dos controles fora de conformidade associados à entidade.

Guia Visão geral da auditoria

Título	Tipo	Tabela de origem	Descrição
Compromissos de auditoria abertos e futuros	Lista	Compromisso [sn_audit_engagement]	Fornece uma lista de compromissos de auditoria abertos e futuros. A lista também fornece detalhes do lead de compromisso para cada documento de autoridade, as datas de início e término planejadas de cada compromisso, problemas de alta prioridade, porcentagem de trabalho de campo concluído e os marcos em andamento.

Filtros

Nome	Tipo	Descrição
Critérios de risco	Relatório	Dependendo dos critérios de risco selecionados, o gráfico de rosca e a lista mostram os terceiros ou fornecedores que estão nessas áreas de risco.

Tradução automática

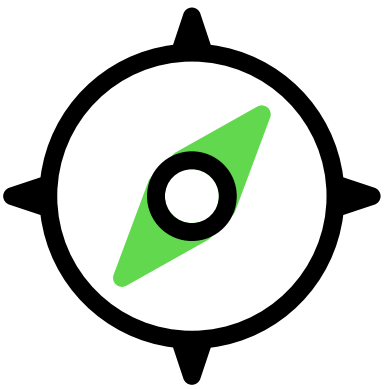
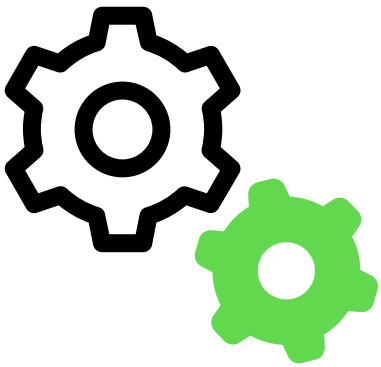
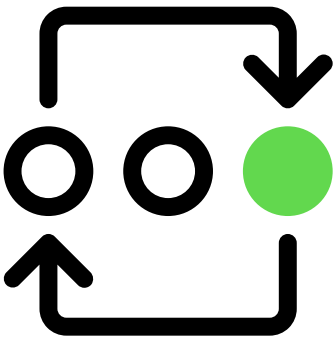
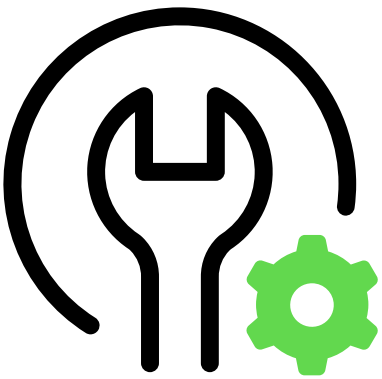
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Central de segurança de inteligência contra ameaças

. Central de segurança de inteligência contra ameaças(TISC) fornece solução de tecnologia para agregação, gestão e operacionalização da inteligência contra ameaças.

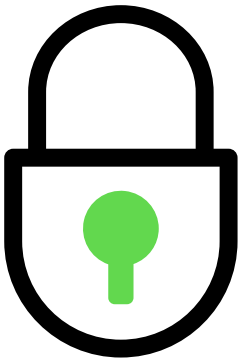
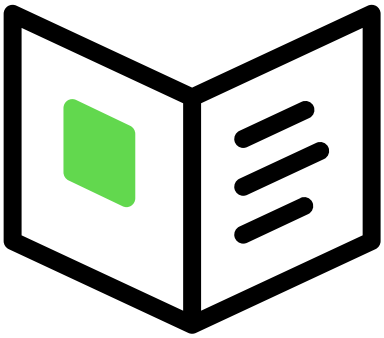
Iniciar

Clique em um bloco para começar.

Explorar	Configurar	Integrar
		
Saiba como a Central de segurança do Inteligência contra ameaças pode ajudar você com seus principais recursos e benefícios.	Instale e configure a Central de segurança do Inteligência contra ameaças para atender às suas necessidades específicas.	Integre com a Central de segurança do Inteligência contra ameaças
Administrar	Uso	Modelos de relatório
		
Gerencie e personalize sua Central de segurança do Inteligência contra ameaças.	Gerencie sua biblioteca e objetos da Central de segurança do Inteligência contra ameaças.	Gerencie e personalize seus Relatórios da Gestão de casos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Repositório do MITRE ATT&CK	TISC Arquivamento de dados Arquivamento	Referência
		
Gerenciar dados do repositório MITRE ATT&CK.	Gerenciar regras de arquivamento de dados e destruição.	Obtenha informações adicionais sobre a Central de segurança do Inteligência contra ameaças.

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Instalando Central de segurança de inteligência contra ameaças(sn_sec_tisc) instalará automaticamente todas as aplicações dependentes do ServiceNow Store.

Mais recursos

Visite Resposta a incidentes de segurança fórum em Comunidade ServiceNow.

Solucionar problemas e obter ajuda

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorando Central de segurança de inteligência contra ameaças

Central de segurança de inteligência contra ameaças(TISC) permite que você colabore com as equipes de inteligência contra ameaças e tem vários recursos para coletar e processar vários feeds de inteligência contra ameaças e um espaço para analisar, colaborar, agir e compartilhar as informações necessárias.

Assista a uma visão geral sobre Central de segurança de inteligência contra ameaças aplicação.

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

A Central de segurança da Inteligência contra ameaças foi aprimorada com recursos para gerenciar coleta de dados, processamento de dados, como DESDUPLICAÇÃO,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

normalização e agregação, análise de inteligência contra ameaças, disseminação de inteligência contra ameaças e também espaço que fornece as tarefas de administração.

Principais recursos

Central de segurança de inteligência contra ameaças oferece um pacote abrangente e robusto de recursos projetados para elevar os recursos de inteligência contra ameaças para equipes de segurança:

- **Catálogo selecionado de feeds de ameaças OSINT** : Fornece acesso a uma ampla seleção de feeds populares de inteligência contra ameaças de código aberto, garantindo ampla cobertura.
- **Integração do Feed Premium** Melhora a qualidade da inteligência contra ameaças incorporando fontes premium junto com dados OSINT.
- **Extração de observável automatizada** : Identifica e extrai automaticamente todos os observáveis relevantes dos arquivos carregados, simplificando a ingestão de dados.
- **Agregação de dados diversificada** Compatível com vários formatos de dados, incluindo STIX, MISP, JSON e outros, permitindo a consolidação do feed contínua.
- **Aprimoramento e validação** : Remove falsos positivos, atribui pontuações de confiança, valida indicadores e adiciona informações contextuais valiosas para melhorar a qualidade dos dados.
- **Mecanismo de regras de correlação** Estabelece relacionamentos automaticamente entre observáveis, permitindo informações mais detalhadas sobre os padrões de ameaça.
- **Pontuação de ameaça personalizável** : Permite o ajuste das pontuações de ameaças para uma avaliação de ameaças mais precisa e detalhada.
- **Integração de Inteligência Interna** : Combina feeds externos com dados internos de Relatórios de vulnerabilidade (VR), Resposta de incidente de segurança (SIR), Ativos, Serviços e CMDB.
- **Painéis específicos do usuário** : Adapta visualizações e exibições de dados de acordo com personas da Inteligência contra ameaças, melhorando a experiência e a relevância do usuário.
- **Ferramentas de visualização gráfica** : Facilita a compreensão de dados complexos de inteligência contra ameaças por meio de representação gráfica intuitiva.
- **Espaço dedicado do analista** : Fornece um dedicado e simplificado Inteligência contra ameaças Espaço do analista que permite que os analistas de inteligência contra ameaças se concentrem na investigação e na análise com o mínimo de distrações.
- **Busca de ameaças com Gestão de casos** Compatível com fluxos de trabalho investigativos com acompanhamento de tarefas e manipulação de casos.
- **INTEGRAÇÃO DO MITRE ATT&CK** : Permite que os usuários vinculem registros de caso com dados da estrutura MITRE ATT&CK para análise contextual aprimorada.
- **Integração SIR contínua** Garante migração de dados suave e interoperabilidade entre Inteligência contra ameaças e. Resposta a incidentes de segurança aplicações para Central de segurança de inteligência contra ameaças.
- **Notificação e regras de alerta** Estabelece alertas de gatilho para notificar as equipes com base na evolução da inteligência contra ameaças.
- **Retenção de dados e políticas de limpeza** : Permite que as organizações definam regras de gestão de dados para manter o desempenho e a conformidade da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Emissão de relatórios e colaboração** Gera relatórios de status abrangentes e resumos de investigação usando editores de rich text e modelos personalizáveis.
- **Domain Separation para MSSPs** Compatível com ambientes de vários locatários, permitindo que os provedores de serviços de segurança gerenciados (MSSPs) segregem os dados do cliente com segurança.
- **Integração extensiva de API** : Oferece API TISC para conectividade contínua com outras ferramentas e plataformas de segurança.

Terminologia da chave TISC

Os termos definidos abaixo são usados em toda a Central de segurança de inteligência contra ameaças (TISC).

Definições de terminologia

Terminologia	Definição
Processamento de dados	Uma plataforma de inteligência contra ameaças (TIP) é uma solução de tecnologia que coleta, agrega e organiza dados de inteligência contra ameaças de várias fontes e padrões. A inteligência contra ameaças são os dados coletados, processados e analisados para entender os alvos e os comportamentos de ataque dos agentes de ameaça.
Observáveis	Observáveis representam propriedades com estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes. Para obter mais informações, consulte Observáveis.
Indicadores	Os indicadores contêm um padrão que pode ser usado para detectar atividades cibernéticas suspeitas ou mal-intencionadas. Por exemplo, um Indicador pode ser usado para representar um conjunto de domínios mal-intencionados e usar a linguagem de padrão STIX para especificar esses domínios. O Indicador SDO contém uma descrição textual simples, as fases da cadeia de destruição em que ele detecta o comportamento, uma janela de tempo para quando o Indicador é válido ou útil e um obrigatório **padrão** propriedade para capturar um padrão de detecção estruturado. Para obter mais informações, consulte Indicadores.
Objetos	Define o conjunto de SDOs (objetos de domínio) do STIX, cada um dos quais corresponde a um conceito exclusivo comumente representado na Inteligência contra ameaças cibernéticas (CTI).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de terminologia

Terminologia	Definição
	Usando SDOs e SROs (objetos de relacionamento) STIX como blocos de construção, os indivíduos podem criar e compartilhar inteligência ampla e abrangente contra ameaças cibernéticas. Para obter mais informações, consulte Repositório da biblioteca TISC.
Relacionamentos	Um relacionamento é um link entre dois observáveis ou dois SDOs ou observável e SDO que descreve a maneira como os objetos estão relacionados. Os relacionamentos podem ser representados usando um objeto de relacionamento (SRO) STIX externo ou, em alguns casos, por meio de determinadas propriedades que armazenam uma referência de identificador que compreende um relacionamento incorporado. Para obter mais informações, consulte Objetos de relacionamentos.

Exibir TISC página inicial

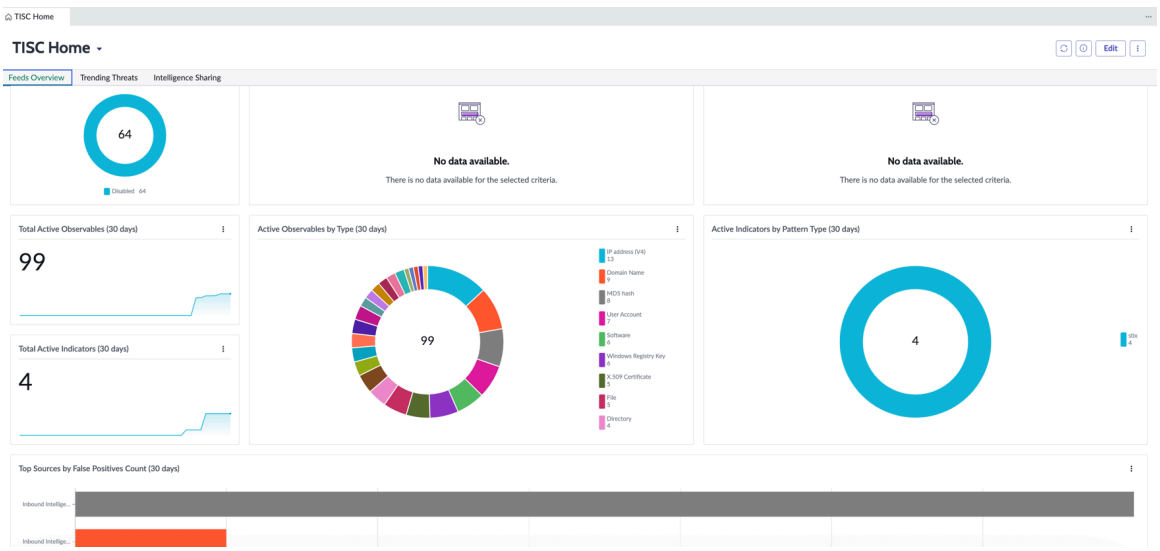
Use TISC página inicial, que é a página principal, para visualizar os dados relacionados à inteligência contra ameaças.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Central de segurança de inteligência contra ameaças**.
   . TISC A Página inicial é exibida.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Exiba TISC página inicial com diferentes dados de widgets.
   A exibição da página inicial consiste em três guias diferentes: **Visão geral dos feeds** , **Ameaças populares** e **Compartilhamento de inteligência** . O conteúdo na página inicial vem de várias fontes, como observáveis, indicadores e feeds de dados.

   a. **Visão geral dos feeds** : Esta guia fornece uma visão geral de alto nível das diferentes fontes nas quais os dados são ingeridos e as origens configuradas para a ingestão de dados.

Visão geral de feeds

Nome do widget	Descrição	Ação
Número de origens	Exibe o número de origens por status, como rascunho, habilitado e desabilitado no sistema.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Fontes ativas por tipo de origem	Exibe a distribuição de fontes ativas por tipo de origem.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Fontes ativas por formato de feed	Exibe o número de origens habilitadas por tipo de feed.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Observáveis ativos totais (30 dias)	Exibe as 10 principais origens por volume de registros de inteligência que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Observáveis ativos por tipo	Exibe o principal volume total de agregados de observáveis que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Indicadores ativos por tipo de padrão	Exibe o volume total de agregados de indicador por tipo de padrão que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Indicadores ativos totais (30 dias)	Exibe o volume total de agregados de indicador que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Principais origens por contagem de falsos positivos (30 dias)	Exibe o volume total de observáveis falso-positivos que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.

   b. **Ameaças populares** : Esta guia fornece uma visão geral de alto nível das ameaças mais populares.

Ameaças de tendência

Nome do widget	Descrição	Ação
Relatórios mais recentes (10 principais)	Exibe a lista de relatórios e links - 10 principais ordem por data de publicação.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do widget	Descrição	Ação
Feeds RSS mais recentes (10 principais)	Exibe a lista de feeds RSS e links - 10 principais ordem por data de publicação.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Observáveis ativos por intervalo de pontuação de ameaça (30 dias)	Exibe a contagem de observáveis que foram criados nos últimos 30 dias distribuídos por intervalos de pontuação de ameaça.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Observáveis ativos por reputação (30 dias)	Exibe a contagem de observáveis que foram criados nos últimos 30 dias distribuídos por reputação.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Marcadores principais (30 dias)	Exibe os principais marcadores nos registros criados nos últimos 30 dias com base na frequência de uso.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Setores mais direcionados (30 dias)	Exibe os 10 principais setores classificados por atividades relatadas que foram criadas nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.

Configuração da Central de segurança de inteligência contra ameaças

Configure os recursos, os componentes e as integrações de que você precisa para fornecer serviço e suporte aos seus clientes.

Baixe a aplicação TISC da ServiceNow Store

Antes de executar o. Central de segurança de inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow® Store e instale-o.

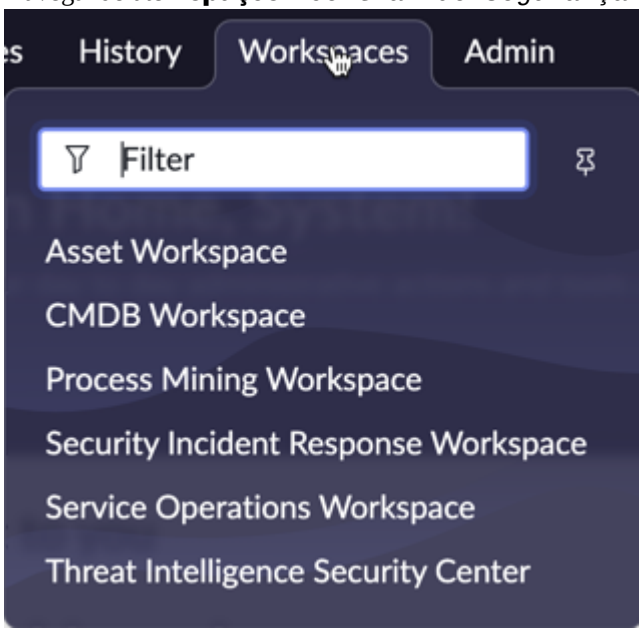
Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga as instruções para baixando uma aplicação do ServiceNow Store e instale o. **Operações de segurança da Central de segurança da Inteligência contra ameaças** aplicação.
2. Após a conclusão da instalação, você pode abrir o. Central de segurança de inteligência contra ameaças Navegando até **Espaços** > *Central de segurança de inteligência contra ameaças*



O que Fazer Depois

Depois de baixar a aplicação com sucesso, verifique se você concluiu todas as tarefas mencionadas aqui nesta seção, Configurar a Central de segurança do Inteligência contra ameaças para uma integração suave.

Configurar a Central de segurança do Inteligência contra ameaças

Antes de usar o. Central de segurança de inteligência contra ameaças, você deve baixá-lo do ServiceNow Store.

Funções instaladas

Revise as informações a seguir e verifique se você concluiu todas as tarefas para uma integração tranquila. Abaixo está a lista de diferentes personas de usuário definidas para acessar e trabalhar com a aplicação:

- Analista de inteligência contra ameaças (sn_sec_tisc.analyst)
- Administrador de inteligência contra ameaças (sn_sec_tisc.admin)

Direitos aplicáveis para funções do TISC

Configuração	Descrição
Atribua e verifique o necessário ServiceNow AI Platform E da Central de segurança do Inteligência contra ameaças.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Direitos aplicáveis para funções do TISC

Configuração	Descrição
	• Como administrador, você deve instalar a aplicação TISC do ServiceNow Armazene e atribua a função como sn_sec_tisc.admin. • Esta função sn_sec_tisc.admin executa as seguintes tarefas: ◦ Configura as Fontes de dados para ingerir os dados. Para obter mais informações, consulte Feeds de Inteligência contra ameaças. ◦ Configuradas as integrações necessárias para enriquecer os dados observáveis no TISC. Para obter mais informações, consulte Integrações de aprimoramento de TISC. ◦ Configura as funções de aprovação de importação de dados para importar dados usando o Assistente de importação. Para obter mais informações, consulte Trabalhando com importações de dados. ◦ Configura a Calculadora de pontuação de ameaças usando os critérios necessários para cálculo automático da pontuação de ameaças de observáveis. Para obter mais informações, consulte Calculadora de pontuação de ameaça. ◦ Configura as taxonomias e os valores de taxonomia necessários. Para obter mais informações, consulte Criando taxonomias. ◦ Configure o repositório MITRE ATT&CK relevante para sua organização. Para obter mais informações, consulte MITRE-ATT&CK Repositório. **Nota:** Como sn_sec_tisc.admin, você também pode atribuir a função sn_sec_tisc.analyst. • A função sn_sec_tisc.analyst executa as seguintes tarefas: ◦ Exibe a visão geral dos dados no sistema usando a página inicial da aplicação. Para obter mais informações, consulte Exibir TISC página inicial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Direitos aplicáveis para funções do TISC

Configuração	Descrição
	○ Importe dados para o sistema usando o botão Importar Inteligência na Página da Biblioteca de Ameaças. Para obter mais informações, consulte Central de segurança de inteligência contra ameaças Biblioteca. ○ ▪ Pesquisa nos dados presentes na aplicação usando a pesquisa fornecida na página Biblioteca de ameaças. ▪ Gerencia os dados ingeridos de várias fontes na Biblioteca de ameaças. ▪ Executa várias ações de aprimoramento em observáveis. ▪ Cria e gerencia casos. Para obter mais informações, consulte Criação de casos usando Workbench de analista de ameaças.

Plug-ins de dependência

Plug-in	Descrição
Estes aplicativos a seguir são necessários para a instalação desta aplicação: • Componentes do espaço comum da Gestão de casos de segurança [com.snc.escm.ws_commons] • Suporte de inteligência contra ameaças comum [com.snc.threat] • Criptografia em nível de coluna (com.glide.encryption) • JSON grande e XML Payload Builder API (com.glide.streaming_builder) • Core de suporte de segurança (com.snc.security_support.core) • Componente da experiência do mapa de nós (sn_node_map) • Componente de IU de relatório para o espaço(sn_sec_reporting) • Editor de Rich Text para operações de segurança (sn_escm_rte) • Estrutura de integração de segurança (sn_sec_int)	Verifique se o ServiceNow as principais aplicações necessárias para oferecer suporte à integração são instaladas e ativadas antes de você configurar esta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-in	Descrição
• Suporte de segurança comum (sn_sec_cmn) • Orquestração de suporte de segurança (sn_sec_cmn_orch)	

Integrar Central de segurança de inteligência contra ameaças

Use esta seção para entender Central de segurança de inteligência contra ameaças integrações.

. **Integrações** a seção inclui os seguintes submódulos.

Integrações

Nome do módulo	Descrição
Catálogo	Todos os feeds de inteligência contra ameaças e integrações de aprimoramento disponíveis são mostrados como blocos/cartões aqui. Os usuários não poderão criar um novo feed ou integração a partir desta seção.
Feeds de ameaças	Esta seção contém os detalhes relacionados somente aos feeds de Inteligência contra ameaças e os usuários poderão configurar novos feeds de inteligência contra ameaças nesta seção.
Integrações de melhorias	Esta seção contém os detalhes relacionados somente a integrações de aprimoramento e os usuários poderão configurar integrações de aprimoramento disponíveis nesta seção. **Nota:** A seção Integrações de aprimoramento só ficará visível se pelo menos um plug-in de integração de aprimoramento estiver instalado.

Central de segurança de inteligência contra ameaças Catálogo

. Central de segurança de inteligência contra ameaças O catálogo é uma lista selecionada de feeds de Inteligência contra ameaças e integrações de aprimoramento disponíveis na aplicação para você habilitá-los após adicionar as informações necessárias e programar o feed para ingerir automaticamente dados de Inteligência contra ameaças em uma frequência definida.

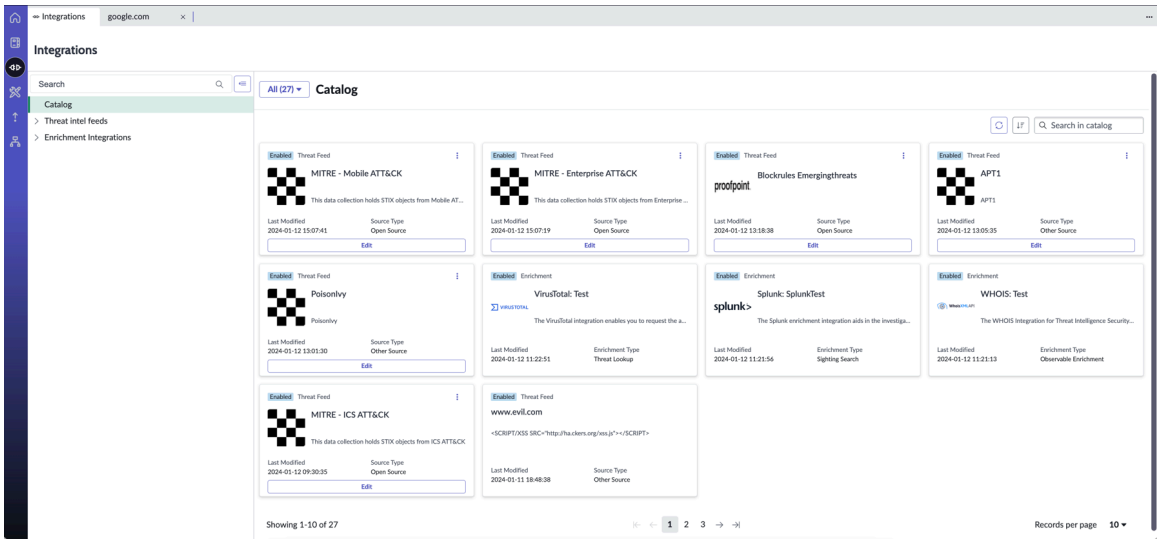
Como sn_sec_tisc.admin, você também pode pesquisar e editar as configurações de origem existentes, habilitar ou desabilitar e excluir as configurações do Catálogo. Qualquer nova fonte de dados é adicionada ao Catálogo, que aparecerá como um novo cartão de configuração no Catálogo.

Função necessária:

- sn_sec_tisc.admin (criar/atualizar)
- sn_sec_tisc.analyst (leitura)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Os cartões no catálogo são diferenciados pelo rótulo que está presente na parte superior do cartão Feed de ameaças/aprimoramento .

Ações na exibição Catálogo

A exibição Catálogo permite que você execute as ações a seguir.

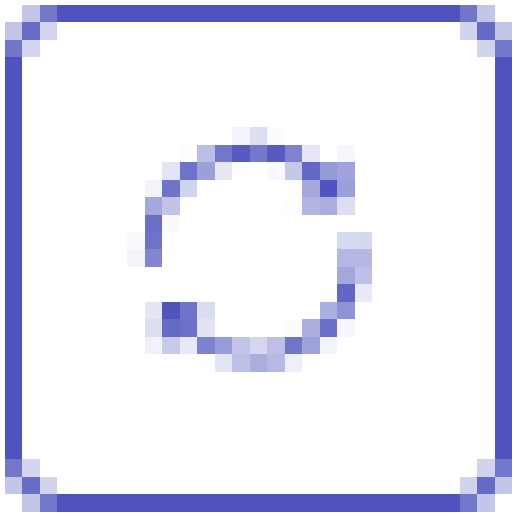
Ações na exibição Catálogo

Ação	Descrição
Tudo	Use este menu suspenso para filtrar feeds e integrações com base em seu estado atual. Você pode filtrar com base nos seguintes estados: • **Todos** : Exibe todos os feeds e integrações na página. Esta é a opção padrão. • **Habilitado** : Exibe todos os feeds e integrações que estão em um estado habilitado. • **Desabilitado** : Exibe todos os feeds e integrações que estão em um estado desabilitado. • **Rascunho** : Exibe todos os feeds e integrações que estão em um estado de rascunho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações na exibição Catálogo

Ação	Descrição
	Use esta ação para atualizar o Catálogo.
	Use esta ação para classificar todos os feeds e integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Pesquisar no catálogo	Use esta ação para pesquisar feeds/integrações com base no nome e na descrição no catálogo.

Feeds de Inteligência contra ameaças

Use Feeds de inteligência contra ameaças para adicionar, editar ou remover a fonte de dados do feed de inteligência contra ameaças.

Os feeds da fonte de dados estão disponíveis no Catálogo Intel de ameaças na seção Integrações.

O catálogo de feeds de inteligência contra ameaças foi criado para mostrar as fontes de dados do feed disponíveis na forma de blocos e tem a capacidade de filtrar, pesquisar e navegar até os detalhes da configuração de origem e executar várias ações.

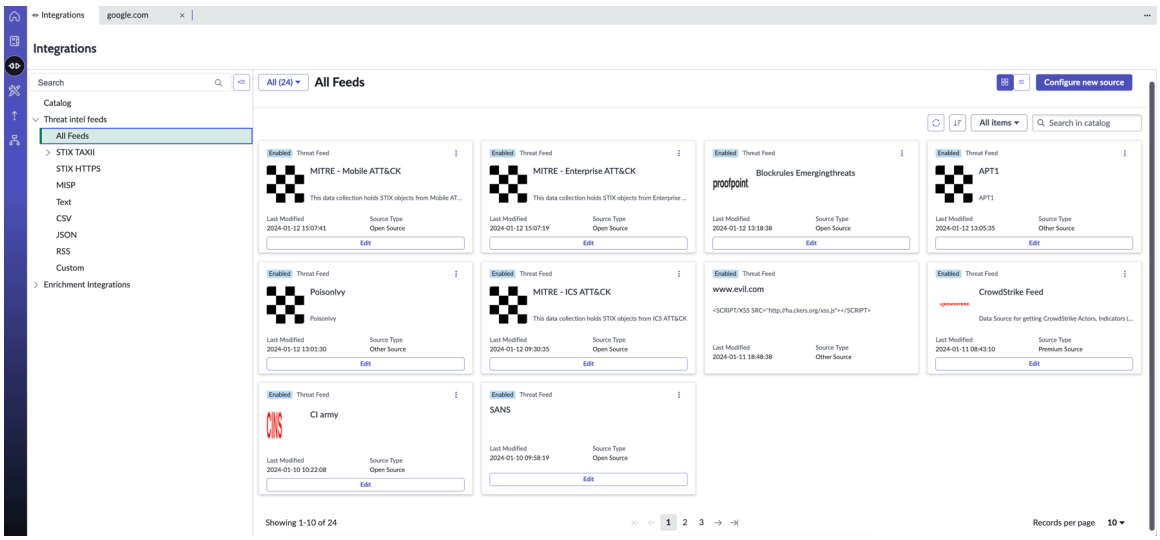
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todos os Feeds

O sistema de base inclui uma série de cartões para cada um dos feeds que você pode habilitar e usar.

Os feeds podem ser exibidos navegando até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações** > **Feeds de inteligência contra ameaça** > **Todos os Feeds**.



Ações na exibição Todos os feeds

A seção Todos os feeds permite que você execute as ações a seguir.

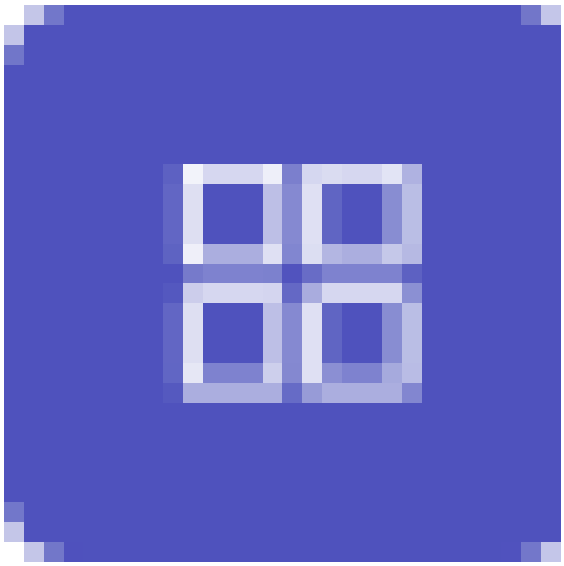
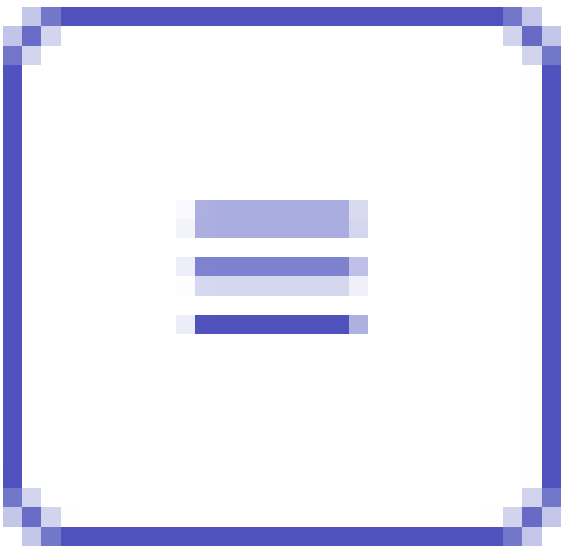
Exibição Todas as integrações

Ação	Descrição
Tudo	Use este menu suspenso para filtrar feeds com base em seu estado atual. Você pode filtrar com base nos seguintes estados: • **Todos** : Exibe todos os feeds na página. Esta é a opção padrão. • **Habilitado** : Exibe todos os feeds que estão em um estado habilitado. • **Desabilitado** : Exibe todos os feeds que estão em um estado desabilitado. • **Rascunho** : Exibe todos os feeds que estão em estado de rascunho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

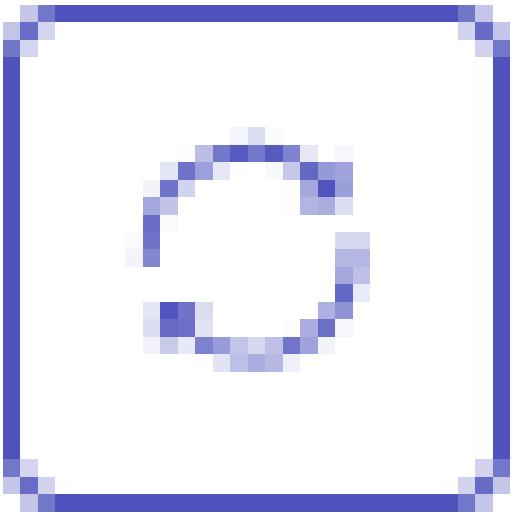
Exibição Todas as integrações

Ação	Descrição
	Use esta ação para exibir todos os feeds na forma de cartões.
	Use esta ação para exibir todos os feeds na forma de uma exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Todas as integrações

Ação	Descrição
	Use esta ação para atualizar a página.
	Use esta ação para classificar todas as integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Todos os itens	Use esta ação para filtrar e listar os blocos do feed de inteligência contra ameaças por tipo de origem ou tipo de feed. **Tipo de origem** : • Código aberto • Outra origem • Origem Premium **Tipo de feed** : • CSV • Feed personalizado • JSON

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Todas as integrações

Ação	Descrição
	• MISP • RSS • HTTPs do STIX • Texto
Pesquisar no catálogo	Use esta ação para pesquisar feeds com base no nome e na descrição no catálogo.

Tipos de feeds Intel de ameaças

Estes são os tipos de feeds de inteligência contra ameaças que podem ser configurados e habilitados:

Feeds de Inteligência contra ameaças

Tipo	Descrição
Feeds TAXII	Feeds que estão disponíveis no formato STIX/TAXII Collections.
HTTPS do STIX	Feeds de Inteligência contra ameaças no formato STIX que podem ser acessados por meio de REST APIs no protocolo HTTPS.
MISP	Feeds que estão nos Feeds do formato MISP.
Texto	Feeds que estão disponíveis como arquivos hospedados no formato de texto. **Nota:** O sistema analisará os arquivos para URL, domínio, nome de arquivo, hashes e endereço IP somente serão extraídos e nenhum outro tipo de observável será extraído.
CSV	Feeds que estão disponíveis como arquivos hospedados no formato CSV. **Nota:** O sistema analisará os arquivos para URL, domínio, nome de arquivo, hashes e endereço IP somente serão extraídos e nenhum outro tipo de observável será extraído.
JSON	Feeds que estão disponíveis como arquivos hospedados no formato JSON. **Nota:** O sistema analisará os arquivos para URL, domínio, nome de arquivo, hashes e endereço IP somente serão extraídos e nenhum outro tipo de observável será extraído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feeds de Inteligência contra ameaças

Tipo	Descrição
RSS	Feeds disponíveis no formato RSS. A aplicação armazenará os dados como registros do Feed RSS.
Personalizado	Feeds configurados usando analisadores personalizados. **Nota:** O sistema analisará os arquivos para URL, domínio, nome de arquivo, hashes e endereço IP somente serão extraídos e nenhum outro tipo de observável será extraído.

Para obter as próximas etapas do procedimento, consulte a respectiva seção para configurar cada tipo de feed específico em Feeds de Inteligência contra ameaças.

Configure um novo feed de inteligência contra ameaças

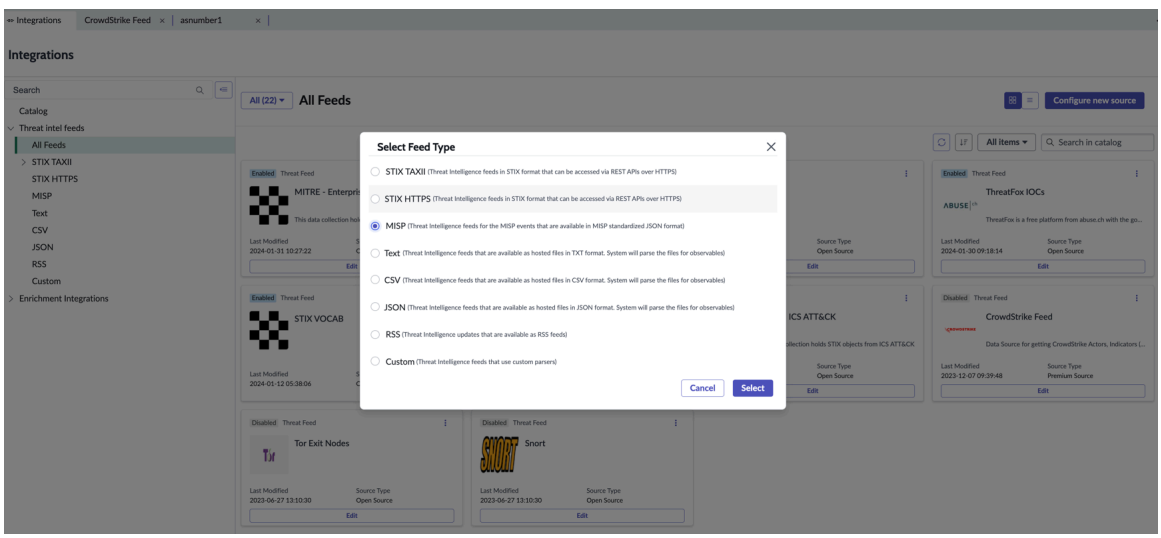
Configure o novo feed de inteligência contra ameaças.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Para configurar um novo feed de inteligência contra ameaças, siga o procedimento:

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecionar **Feeds de inteligência contra ameaça** > **Todos os Feeds**.
4. Clique em **Configurar nova origem** .
   Os vários tipos de feed são exibidos.



5. Selecione o respectivo tipo de feed.
6. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar nova origem

Campo	Descrição
Nome	Insira um nome para o feed.
Descrição	Descrição do feed.
Tipo de feed	O tipo de feed. Por exemplo, MISP. Por padrão, este valor é exibido com base no tipo de feed selecionado no Catálogo.
Logotipo	Anexe o logotipo do feed de origem. **Nota:** O tamanho deve ser 72px/72px.
Setor	Selecione a categoria do setor, como Aeroespacial, Agricultura e assim por diante, para a qual o feed é aplicável.
Tipo de Origem	Selecione o tipo de origem na lista de tipos de origem disponíveis. A lista de origens disponíveis é: ○ Governo ○ ISACs ○ Código aberto ○ Origem Premium ○ Outra origem

7. Clique em **"Selecionar"**.
8. Preencha os campos na seção Configuração, conforme apropriado.

Configuração

Campo	Descrição
Período de expiração (dias)	Insira o período de expiração do feed em dias. Por exemplo, 180 dias. **Nota:** Quaisquer que sejam os dados ingeridos da origem expirarão 180 dias após a ingestão.
Usar mensagem REST	Selecione **Usar mensagem REST** Se você precisar usar a funcionalidade Mensagem REST/ Método REST fornecida por ServiceNow AI Platform. Se esta caixa de seleção não estiver marcada, a aplicação usará o endpoint fornecido em **URL do endpoint REST** para buscar os dados do feed. Para obter mais informações, consulte Serviço web REST

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de saída ativado ServiceNow AI Platform documentação. **Nota:** Os campos Mensagem REST e Método REST são obrigatórios quando você seleciona a mensagem REST.
Mensagem REST	Selecione o registro Mensagem REST na lista de registros de mensagem REST que já estão configurados na instância. Para obter mais informações, consulte Serviço web REST de saída em ServiceNow AI Platform documentação. **Nota:** Selecione este valor quando precisar exibir cabeçalhos específicos e definir os registros relacionados AO REST usando a opção de mensagem REST.
Método REST	Selecione Método REST na lista de métodos REST disponíveis configurados para a mensagem REST selecionada. Para obter mais informações, consulte Serviço web REST de saída em ServiceNow AI Platform documentação.
Confiança	Defina a confiança para todos os registros aplicáveis que são ingeridos por meio deste feed específico. **Nota:** Defina a confiança entre 0-100 para esta origem.
Mecanismo de análise de dados	Selecione a opção de mecanismo de análise de dados apropriada. As opções disponíveis são: ○ **Extração IOC automatizada** : Esta opção é selecionada por padrão ao configurar feeds de texto, CSV ou JSON. ○ **Mapeamento de campo personalizado** : Selecione esta opção se quiser definir como os campos específicos nos dados do feed devem ser mapeados para os atributos observáveis. Uma vez selecionado, você pode configurar os mapeamentos no **Mapeamento de campo** seção. Para obter informações mais detalhadas sobre o mapeamento de campo personalizado, consulte Configurar Mapeamento de campo personalizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A opção Mecanismo de análise de dados só está disponível para feeds de texto, CSV e JSON, em que os feeds **Processador de relatório** está definido como `SimpleFeedDatasourceResponseProcessor`.
URL do endpoint REST	Insira o URL do endpoint REST em que os dados são hospedados pelo feed de inteligência contra ameaças. **Nota:** Para tipos de feed MISP, os URLs do endpoint REST que terminam com `/manifest.json` são compatíveis.
Autenticação Necessária	Marque esta caixa de seleção se a autenticação for necessária para seu novo feed de inteligência contra ameaças. **Nota:** Isso só é aplicável quando a URL do endpoint REST está sendo usada para recuperar os dados.
Tipo de autenticação	O tipo de autenticação do feed de origem. A seguir estão os tipos de autenticação configurados e provisionados no sistema de base para os usuários: ◦ ID DA API/CHAVE DE API ◦ ID DA API/SEGREDO DA API ◦ Chave de API ◦ Chave de API/Segredo da API ◦ Nome de usuário da API/Senha da API/Chave de API ◦ Autenticação básica
Cabeçalhos a serem passados com a solicitação	Quaisquer cabeçalhos a serem passados com as solicitações podem ser fornecidos no Mapeamento de cabeçalho da solicitação. ◦ O cabeçalho deve ser fornecido no par chave-valor separado por dois pontos (':'). ◦ Cada par de valor de chave de cabeçalho deve ser fornecido em uma nova linha. ◦ Para fornecer parâmetros de autenticação como valores de cabeçalho, coloque o Rótulo de autenticação necessário com " Por exemplo, x-api-key:
Avançado	Marque esta caixa de seleção para definir o script de integração personalizado e o script do processador de relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Ao marcar esta caixa de seleção, o **Script de integração** e. **Processador de relatório** os campos serão exibidos para você selecionar os scripts personalizados.
Script de integração	O script de integração invoca uma chamada para o URL do endpoint REST usando os parâmetros de autenticação e os cabeçalhos conforme configurados no feed e, em seguida, o script busca os dados que estão disponíveis no feed específico. A seguir estão as inclusões de scripts personalizados disponíveis, que são provisionadas na aplicação para os scripts de integrações: ○ MITERSourceIntegration: Usado para buscar os dados dos feeds MITRE. ○ RSSFeedDatasourceIntegration: Usado para buscar os dados de feeds RSS. ○ SimpleFeedDatasourceIntegration: Usado para buscar os dados de feeds simples sem autenticação ou autenticação básica. ○ SimpleMISPFeedDatasourceIntegration: Usado para buscar os dados de feeds MISP hospedados. O script de integração padrão é baseado no tipo de feed selecionado. Por exemplo, se você selecionar o tipo de feed MISP, que é um formato padrão para processar e buscar os dados, o script de integrações será **SimpleMISPFeedDatasourceIntegration** . **Nota:** Para os scripts de integração personalizada, você pode criar uma inclusão de script estendendo **FeedDatasourceIntegrationBase** e substituem os métodos necessários.
Processador de relatórios	O script do processador de relatório processa dados obtidos do feed usando o script de integração. O sistema de base inclui os seguintes scripts personalizados, que são provisionados na aplicação para oferecer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	suporte ao script do processador de relatórios: ○ Atom FeedDatasourceResponseProcessor: Usado para processar feeds RSS no formato Atom. ○ MITRE CollectionDataProcessor: Usado para processar feeds MITRE. ○ RSSFeedDatasourceResponseProcessor: Usado para processar feeds RSS. ○ SimpleDataplaneFeedResponseProcessor: Usado para processar feeds do plano de dados. ○ SimpleFeedDatasourceResponseProcessor: Usado para processar feeds simples usando extração de expressão regular de observáveis. ○ SimpleFeodotrakerFeedResponseProcessor: Usado para processar feeds do Feodotracker. ○ SimpleMISPFeedDatasourceResponseProcessor: Usado para processar feeds MISP hospedados. ○ TAXIIV2CollectionDataProcessor: Usado para processar dados da coleção TAXII. O processador de relatório padrão para feeds MISP é `SimpleMISPFeedDatasourceResponseProcessor`. Este processador é pré-configurado pela aplicação e não pode ser modificado ou substituído.

Tradução automática

9. Preencha os campos na seção Programação, conforme apropriado.

Programando

Campo	Descrição
Executar	Defina a frequência na qual você deseja ingerir os registros. O feed será executado e executado com base no intervalo de trabalho de programação. Os intervalos de trabalho disponíveis são: ○ Diariamente ○ Semanalmente ○ Mensalmente ○ Periodicamente ○ Uma vez

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Sob demanda ○ Calendário comercial: início da entrada ○ Calendário comercial: fim da entrada **Nota:** Por padrão, a frequência é definida como Sob demanda. Para obter mais informações, consulte Trabalhos agendados e como executar automaticamente um script de sua escolha .
Buscar dados de	A data de início a partir da qual os dados precisavam ser obtidos. Este campo deve ser definido com a hora a partir da qual os dados precisam ser ingeridos da origem correspondente. Depois que este campo for definido, a próxima execução de ingestão buscará os dados do tempo configurado e as execuções de ingestão consecutivas buscarão dados incrementais. Por exemplo, a Origem está programada para ingerir os dados a cada hora. Os conjuntos do usuário **Buscar dados de** Em 12 6:00AM de janeiro, em 12 9 de janeiro, a ingestão acionada em 12 10:00AM de janeiro buscaria os dados de 12 6:00AM de janeiro a 12 10 de janeiro. A próxima ingestão que é acionada às 11:00AM buscará somente os dados incrementais de 12 10:00AM de janeiro a 12 11 de janeiro. **Nota:** Isso significa que as execuções programadas buscarão dados incrementalmente a partir da data especificada em diante. **Importante:** Isso não se aplica a feeds de texto, CSV e JSON.

Marcadores

Campo	Descrição
Selecionar marcadores	Use os marcadores para anotar ou marcar registros que são ingeridos no sistema a partir desta origem. Comece a inserir o nome do marcador no **Pesquisa** para escolher os marcadores disponíveis na aplicação ou insira o novo nome do marcador e clique em **Adicionar** para atribuí-lo à origem.

10. Clique em **Salvar** ação para armazenar e criar o feed.
    Os detalhes fornecidos são validados e, por padrão, o status dos feeds é desabilitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. **Opcional:** Clique em **Salvar como rascunho** ação para armazenar somente as configurações do feed como rascunho.
    Os usuários não podem habilitar um feed quando ele é salvo em rascunho. Se você não tiver certeza sobre os detalhes da configuração, poderá usar **Salvar como rascunho** opção. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
12. Clique em **Habilitar** para habilitar o registro.

    Quando o registro do feed de inteligência contra ameaças estiver habilitado, você poderá executar o registro para executar a integração.

    Nota:

    - O registro do feed de inteligência contra ameaças é rotulado e indicado como **habilitado** . Da mesma forma, você pode desabilitar o feed de inteligência contra ameaças clicando em **Desabilitar** botão.
    - Você também pode habilitar, desabilitar ou excluir um feed específico usando **Ações** menu do bloco de feed necessário no **Catálogo** ou **Feeds de informações sobre ameaças** página.
13. Clique em **Excluir** para excluir o registro do feed de inteligência contra ameaças.
14. Selecione **Integrações executadas** seção para verificar os detalhes da execução.

Nota: O procedimento de configuração do feed de inteligência contra ameaças acima é o mesmo para todos os outros tipos de feed de inteligência contra ameaças, exceto para STIX TAXII. Para obter mais informações sobre como o STIX TAXII é configurado, consulte Configure um novo Feed TAXII.

Configurar Mapeamento de campo personalizado

O Mapeamento de campos permite configurar como cada campo em um feed de dados, como Texto, CSV ou JSON, é interpretado e atribuído ao observável correspondente.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Selecionar **Feeds de inteligência contra ameaça** > **Todos os Feeds** > **Texto**.
3. Selecione **Configurar nova origem** .
4. Preencha os detalhes do formulário do feed de texto conforme necessário.
   Para obter mais informações, consulte Configure um novo feed de inteligência contra ameaças.
5. Na nova exibição de formulário, faça um detalhamento até **Mecanismo de análise de dados** campo em **Configuração** seção.
   Para obter mais informações sobre o Mecanismo de análise de dados, consulte Configure um novo feed de inteligência contra ameaças.
6. Selecione **Mapeamento de campo personalizado** opção.
7. Navegue até **Mapeamento de campo** seção.
8. Selecione **Configurar** para adicionar o mapeamento de campo para a nova fonte de dados.
   Esta seção envolve três etapas, como adicionar dados de amostra, mapeamento de campo e visualizar os registros de amostra mapeados.

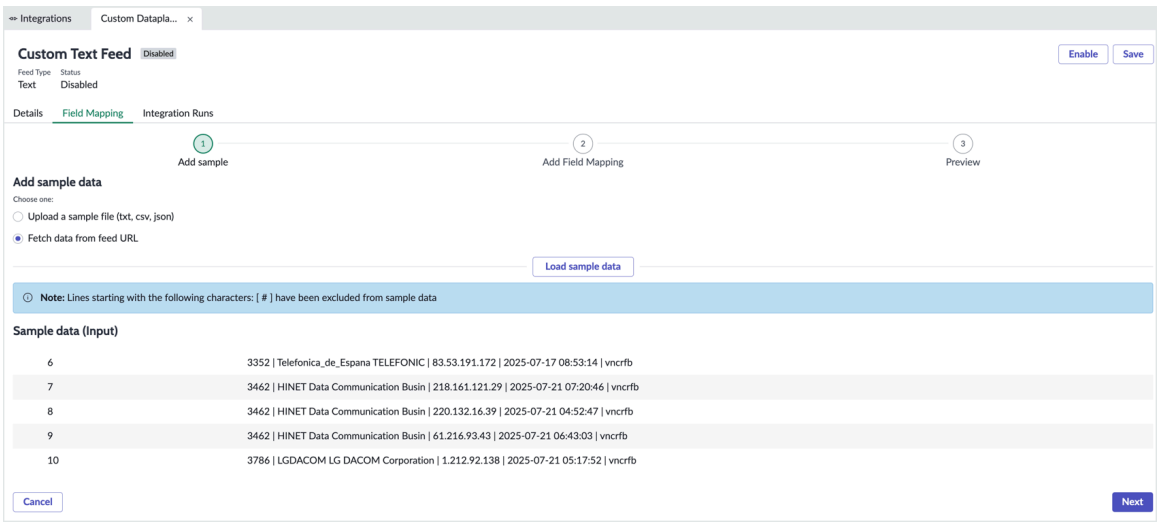
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Para adicionar os dados de amostra, selecione **Carregar dados de amostra** .
   Exibe os dados de amostra da opção selecionada, a aplicação exibe somente as linhas de dados relevantes e as linhas que começam com `Nº` são excluídos dos dados de amostra. Os identificadores de comentário podem ser modificados com a propriedade do sistema: `sn_sec_tisc.feed_comment_identificadores` .

   A aplicação buscará uma amostra dos dados de entrada de um arquivo de amostra (como .txt, .csv ou .json) ou diretamente do URL do feed configurado (o URL do feed e as credenciais inseridas no **Detalhes**). Isso permite visualizar a estrutura e o conteúdo dos dados antes de definir mapeamentos de campo.

10. Selecione uma das opções **Carregue um arquivo de amostra** ou **Feed de dados do URL do feed** .
    Esses dados de amostra buscarão os primeiros dez registros por padrão. Esse número total de registros a serem recuperados pode ser modificado com a propriedade do sistema `sn_sec_tisc.feed_field_mapping_sample_count` .



11. Selecione **Próximo** para configurar o mapeamento de campo.

12. Selecione **Defina um delimitador para analisar dados** opção na lista suspensa.
    Ao trabalhar com feeds de texto, o delimitador é essencial para analisar corretamente os dados em campos individuais.

    Nesse cenário, o feed de texto usa o operador de tubo rígido (|) como o delimitador que separa cada valor nos dados de texto de amostra em colunas distintas. Identificar e aplicar corretamente este delimitador é essencial para garantir o mapeamento de campo preciso e a ingestão de dados bem-sucedida.

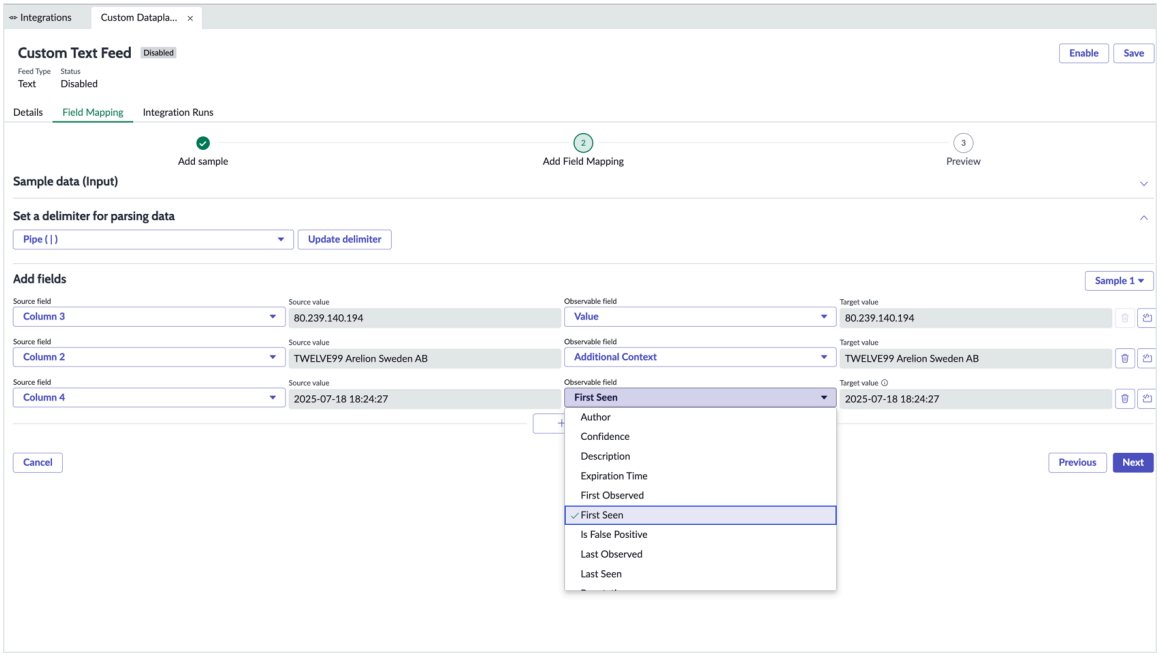
    Nota: Para feeds CSV, a vírgula (,) é o delimitador padrão e os feeds JSON não exigem nenhum delimitador.

13. Selecione **Delimitador de atualização** .
    As opções para adicionar campos para mapeamento de campo são exibidas.

14. Adicione o mapeamento de campo selecionando os valores apropriados na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



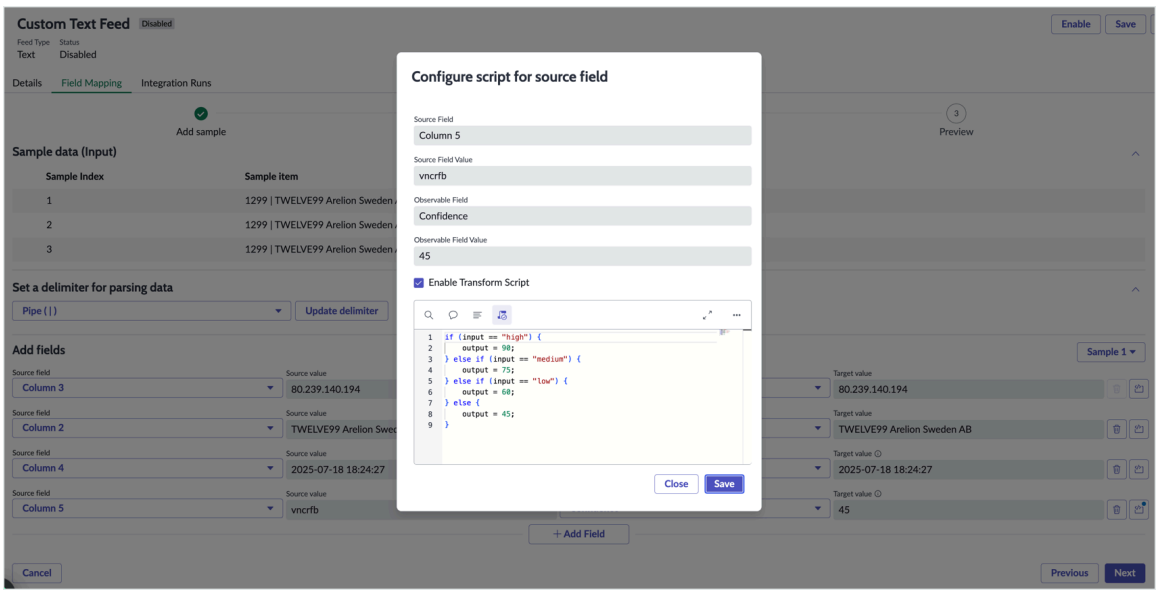
15. Use **Script de transformação** transformar e normalizar os valores de entrada antes de mapeá-los para observáveis.

    a. Selecione **Habilitar/desabilitar script de transformação** ícone para configurar o script.
    A caixa de diálogo Configurar script para campo de origem é exibida.

    b. Selecione **Habilitar script de transformação** caixa de seleção em **Configurar script para o campo de origem** caixa de diálogo.

    c. Adicione ou modifique o script.

    Por exemplo, se o campo de entrada contiver valores como baixo, médio ou alto e você quiser mapear esses valores para níveis de confiança numérica (entre 0 e 100), poderá usar o Script de transformação para converter o valor de entrada e mapeá-lo para **Confiança** campo do observável.



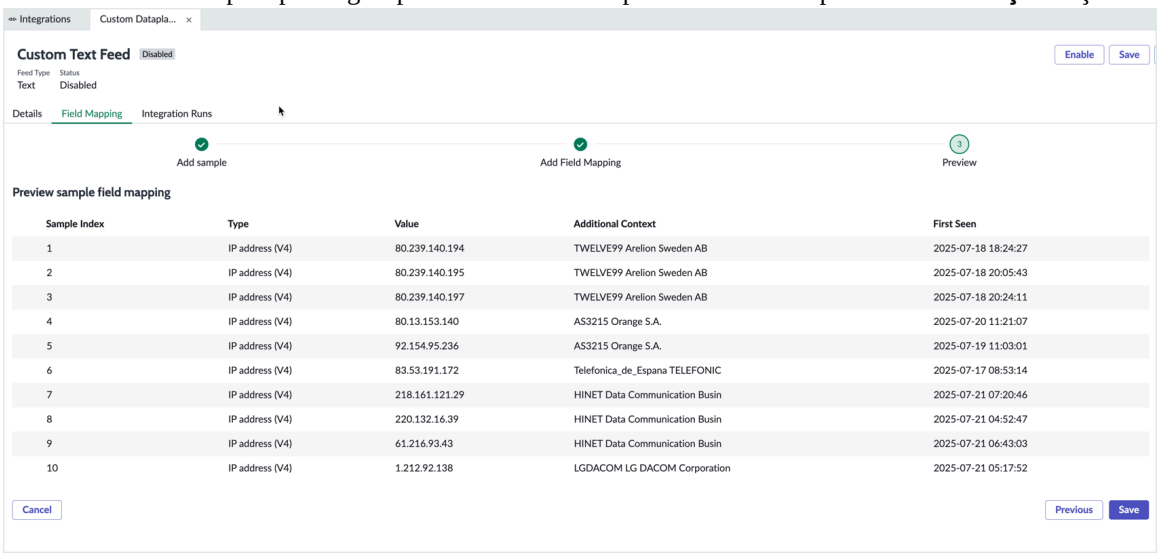
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Selecione **Salvar** para salvar o script para obter o valor de destino atualizado.

e. Fechar **Configurar script para o campo de origem** e prossiga para a próxima etapa.

16. Selecione **Próximo** para prosseguir para visualizar os mapeamentos de campo no **Visualização** seção.



17. Visualize o mapeamento de campo de amostra e selecione **Salvar** .
Uma mensagem de confirmação é exibida indicando que o mapeamento de campo foi salvo com sucesso.

Como parte do mapeamento de campo de amostra, a aplicação identifica automaticamente o tipo de observável (como endereço IP v4 e assim por diante) que o usuário mapeou a partir dos dados de amostra. Este mecanismo simplifica o processo de mapeamento e garante que os tipos de observáveis apropriados sejam atribuídos com base na entrada.

Importante: Execução de integração de mapeamento de campo: Qualquer execução de integração realizada para este tipo de feed usará a configuração de mapeamento de campo salva. Isso garante que os dados de entrada sejam consistentemente analisados e mapeados para os atributos observáveis corretos com base na estrutura definida durante a configuração.

Nota: Selecione **Editar mapeamento de campo** para editar e fazer as mudanças necessárias no mapeamento de campo, se necessário. Uma mensagem de alerta é exibida para confirmar se você deseja prosseguir com a edição. Confirme o prompt e selecione **Sim** para continuar. Faça as mudanças necessárias nos mapeamentos de campo usando os dados de amostra atualizados e salve as mudanças.

Todas as edições feitas no mapeamento de campo serão aplicadas às futuras execuções de integração para este feed.

Sempre verifique os dados de amostra após as mudanças para garantir a análise correta antes de executar a integração.

Exibir Feeds da Intel contra ameaças

Esta seção fornece os feeds de informações sobre ameaças que estão configurados no sistema de base.

Exibir feeds do STIX TAXII

Exiba os feeds STIX TAXII configurados no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **STIX TAXII** .
   Os feeds MISP no sistema de base são descritos na tabela a seguir.

Feed de ameaças	Descrição	URL
Cyware TAXII	Cyware Threat Intelligence exchange (CTIX) é uma plataforma projetada para facilitar o compartilhamento de inteligência contra ameaças cibernéticas entre as organizações.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordeFuture TAXII	Recorded Future é uma plataforma de nuvem independente de inteligência contra ameaças que permite que as organizações identifiquem e mitiguem ameaças em domínios cibernéticos, da cadeia de suprimentos, físicos e de fraude.	https://api.recordedfuture.com/taxii2
Pulsedive TAXII	Pulsedive é uma plataforma de inteligência contra ameaças que fornece uma ampla gama de serviços e ferramentas de inteligência contra ameaças cibernéticas para as organizações.	https://pulsedive.com/taxii2/api/

4. Clique em **Editar** para editar o feed.

Exibir feeds HTTPS do STIX

Exiba os feeds HTTPS STIX configurados no sistema de base.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **STIX HTTPS** .
   A tabela a seguir descreve os feeds HTTPS do STIX no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ThreatFeed	Descrição	URL
MITRE - MOBILE ATT&CK	Esta coleta de dados contém objetos STIX do Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	Esta coleta de dados contém objetos STIX do ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE - ENTERPRISE ATT&CK	Esta coleta de dados contém objetos STIX do Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Clique em **Editar** para editar o feed e fazer as atualizações necessárias.

Exibir Feeds do MISP

Exiba os Feeds do MISP configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **MISP** .
   Os feeds MISP no sistema de base são descritos na tabela a seguir.

Feed de ameaças	Descrição	URL
Feed do Intel OSINT contra ameaças digitais	Fonte de dados para buscar informações de Inteligência contra ameaças cibernéticas de código aberto do feed do DigitalSide Threat-Intel OSINT, que se baseia principalmente em análise de malware e URLs, IPs e domínios comprometidos.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLHaus IOCs	URLHUS é um projeto de abuse.ch com o objetivo de compartilhar URLs maliciosos que estão sendo usados para distribuição de malware.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
Malware Bazaar	MalwareBazaar é um projeto de abuse.ch com o objetivo de compartilhar amostras de malware com a comunidade infosec, fornecedores de AV e provedores de inteligência contra ameaças.	https://bazaar.abuse.ch/downloads/misp/manifest.json
ThreatFox IOCs	ThreatFox é uma plataforma gratuita de abuse.ch com	https://threatfox.abuse.ch/downloads/misp/manifest.json

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	o objetivo de compartilhar indicadores de comprometimento (IOCs) associados a malware com a comunidade infosec, fornecedores de AV e provedores de inteligência contra ameaças.	

Nota: Para tipos de feed MISP, os URLs do endpoint REST que terminam com `/manifest.json` são compatíveis.

4. Clique em **Editar** para editar o feed.

Exibir feeds de texto

Exiba os feeds de texto configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **Texto** opção.
   A seguir lista os feeds de texto configurados no sistema de base.

Feed de ameaças	Descrição	URL
IPs de força bruta de Haley	Fornece uma lista de endereços IP da máquina atacadora durante os últimos 2 anos classificados por endereço IP	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Emergingthreats	A Inteligência de ameaças emergentes (ET) fornece feeds de informações acionáveis sobre ameaças para identificar IPs envolvidos em atividades suspeitas e mal-intencionadas.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
POP3 Groper Web	Lista de hosts que tentaram e falharam ao fazer login no serviço pop3 em bsdly.net.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Nós de saída do TOR	Tor Exit Nodes podem ser usados para detetar tráfego vindo da rede TOR.	https://www.dan.me.uk/torlist/?exit
Lista negra de IPs do Talos Intelligence	O Talos foi formado pela combinação da equipe de pesquisa de vulnerabilidades da SourceFire, do grupo Cisco Threat Research and Communications e do Cisco Secure Applications Group. A experiência combinada é apoiada	https://www.talosintelligence.com/documents/ip-blacklist

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	por uma infraestrutura sofisticada e pela incomparável telemetria de dados da Cisco que abrange redes, endpoints, ambientes de nuvem, sistemas virtuais e tráfego diário da web e de e-mail.	
SANS	O ISC fornece um serviço gratuito de análise e aviso para milhares de usuários da Internet e organizações.	https://isc.sans.edu/feeds/topips.txt
Snort	O Snort é o mais importante Sistema de Prevenção de Intrusão (IPS) de Código Aberto do mundo. O IPS do Snort usa uma série de regras que ajudam a definir a atividade de rede mal-intencionada.	https://snort.org/downloads/ip-block-list
Exército de IC	A lista do Exército do CINS é um subconjunto do conjunto de regras do CINS Active Threat Intelligence e consiste em endereços IP que atendem a um de dois critérios básicos: 1) o fator de pontuação recente do pacote invasor do IP é muito ruim ou 2) o IP acionou um número designado de alertas "confiáveis" em um determinado número de Sentinels implantados em todo o mundo.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	IPs brutos para as listas de bloqueios de firewall. Redes de spam identificadas por Spamhaus (www.spamhaus.org), Principais atacantes listados por DShield (www.dshield.org) e Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
Greennow da lista de bloqueios	GreenSnow é uma equipe que consiste nos melhores especialistas em segurança de computadores, GreenSnow colhe um grande número de IPs de diferentes computadores localizados ao redor do mundo.GreenSnow é comparável com SpamHaus.org para ataques de qualquer tipo, exceto spam.	https://blocklist.greensnow.co/greensnow.txt
Exército de IC	A lista do Exército do CINS é um subconjunto do conjunto de regras do CINS Active Threat Intelligence e consiste em endereços IP que atendem a um de dois critérios básicos: 1) o fator de pontuação recente do pacote	https://cinsscore.com/list/ci-badguys.txt

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	invasor do IP é muito ruim ou 2) o IP acionou um número designado de alertas "confiáveis" em um determinado número de Sentinels implantados em todo o mundo.	
Lista de bloqueios	www.blocklist.de é um serviço gratuito e voluntário fornecido por um especialista em fraude/abuso, cujos servidores são frequentemente atacados via SSH-, Mail-Login-, FTP-, Webserver- e outros serviços.	https://lists.blocklist.de/lists/all.txt
Nós de saída do TOR	Tor Exit Nodes podem ser usados para detetar tráfego vindo da rede TOR.	https://www.dan.me.uk/torlist/?exit
Botscout BOT IPs	O BotScout ajuda a impedir que scripts automatizados da web, conhecidos como "bots", se registrem em fóruns, poluam bancos de dados, espalhem spam e abusem de formulários em sites.	http://botscout.com/last_caught_cache.txt
RFB do VNC do plano de dados	Endereços IP identificados como iniciando sessões de buffer de estrutura remota do VNC.	https://dataplane.org/signals/vncrfb.txt
Login TELNET do plano de dados	Endereços IP identificados como tentando fazer login via autenticação de senha TELNET.	https://dataplane.org/signals/telnetlogin.txt
Autenticação de senha SSH do plano de dados	Endereços IP identificados como tentando fazer login por meio da autenticação de senha SSH.	https://dataplane.org/signals/sshpwauth.txt
Conexão do cliente SSH do plano de dados	Endereços IP identificados como executando negociações de protocolo de cliente SSH.	https://dataplane.org/signals/sshclient.txt
Emergingthreats	A Inteligência de ameaças emergentes (ET) fornece feeds de informações acionáveis sobre ameaças para identificar IPs envolvidos em atividades suspeitas e mal-intencionadas.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Saudação SMTP do plano de dados	Endereços IP identificados como clientes SMTP que emitem comandos HELO ou EHLO não solicitados.	https://dataplane.org/signals/smtpgreet.txt
Consulta SIP do plano de dados	Endereços IP identificados como enviando consultas DE OPÇÕES SIP.	https://dataplane.org/signals/sipquery.txt
Protocolo IP do plano de dados 41	Endereços IP identificados como retransmissão do protocolo IPv4	https://dataplane.org/signals/proto41.txt

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	aberto 41 (ou seja, IPv6 sobre IPv4).	
Convite SIP do plano de dados	Endereços IP identificados como envio de operações de CONVITE SIP.	https://dataplane.org/signals/sipinvitation.txt
CH TXT do DNS do plano de dados version.bind	Endereços IP identificados como enviando consultas DNS VERSÃO.BIND do CH TXT.	https://dataplane.org/signals/dnsversion.txt
DNS TCP do plano de dados	Endereços IP identificados como enviando DNS por consultas da porta TCP 53.	https://dataplane.org/signals/dnstcp.txt
Recursão DNS do plano de dados desejada EM QUALQUER UM	Endereços IP identificados como enviando DNS recursivo EM QUALQUER consulta.	https://dataplane.org/signals/dnsrdany.txt
Recursão DNS do plano de dados desejada	Endereços IP identificados como enviando consultas DNS recursivas.	https://dataplane.org/signals/dnsrd.txt
Banco de dados de phishing do GitHub Links de phishing ativos	Fonte de dados para buscar links de phishing ativos do banco de dados de phishing disponível no Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Banco de dados de phishing do GitHub Active Domains	Fonte de dados para buscar domínios ativos do banco de dados de phishing disponível no Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Banco de dados de phishing dos IPs ativos do GitHub	Fonte de dados para buscar IPs ativos do banco de dados de phishing disponível no Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Bots de lista de bloqueios	Todos os endereços IP que foram relatados nas últimas 48 horas como tendo executado ataques nos ataques de RFI, bots de registro, bots de IRC ou BadBots.	https://lists.blocklist.de/lists/bots.txt
Ataques Apache de lista de bloqueio	Todos os endereços IP relatados nas últimas 48 horas como tendo executado ataques no serviço Apache, Apache-DDOS, RFI-Attacks.	https://lists.blocklist.de/lists/apache.txt
Lista negra de VoIP por Scopserv	Recupere a lista de ips na lista de bloqueios da lista negra de VoIP.	http://voipbl.org/update/?dm=bl
Lista de bloqueios de domínio do Threatview	Domínios mal-intencionados identificados para phishing/servir malware/comando e controle.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Lista de bloqueios de hash do Threatview MD5	Hashes MD5 de arquivos maliciosos ou associados a - malware, ransomware, ferramentas de invasão, bots etc.	https://threatview.io/Downloads/MD5-HASH-ALL.txt

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
Lista de bloqueios de URL do Threatview	URLs mal-intencionadas que servem malware, phishing, botnets e C2.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Lista de bloqueios de hash de arquivo SHA do Threatview	Hashes SHA de arquivos conhecidos ou vinculados à execução de malware.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Lista de bloqueios de IPs Threatview	Lista de bloqueios de IPs mal-intencionados para endereços IP inválidos conhecidos.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Feed de caça do Threatview C2	Infraestrutura hospedando Servidores de comando e controle encontrada durante a busca proativa pelo Threatview.io	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
Feed de ameaças do Threatview OSINT	Indicadores mal-intencionados de comprometimento coletados da origem do OSINT - Twitter e Pastebin.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Clique em **Editar** para editar o feed.

Exibir feeds CSV

Exiba os feeds CSV configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **CSV** .
   Os feeds CSV no sistema de base são explicados na tabela a seguir.

ThreatFeed	Descrição	URL
PhishStats	URLs de phishing dos últimos 30 dias do PhishStats.	https://phishstats.info/phish_score.csv
Abuse.ch Lista negra de certificados SSL	A lista negra de certificados SSL (CSV) é um CSV que contém a impressão digital SHA1 de todos os certificados SSL na lista negra SSLBL.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Botnet C2 IP blacklist	Um certificado SSL pode ser associado a um ou mais servidores (combinação de endereço IP:porta). SSLBL coleta endereços IP que estão sendo executados com um certificado SSL na lista negra SSLBL. Geralmente são	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ThreatFeed	Descrição	URL
	servidores de comando e controle de botnet (C&C). SSLBL publica uma lista negra contendo esses IPs que podem ser usados para detetar tráfego de botnet C2 de máquinas infetadas para a internet, saindo da sua rede.	
PhishTank online	N/D	https://data.phishtank.com/data/online-valid.csv

4. Clique em **Editar** para editar o feed.

Exibir feeds JSON

Exiba os feeds JSON configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **JSON** opção.
   A seguir lista os feeds JSON configurados no sistema de base.

Feed de ameaças	Descrição	URL
Hosts de C&C do Feodotracker	Fonte de dados para buscar a lista de bloqueios de IP C2 do Botnet do Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
Feodotracker	Fonte de dados para buscar a lista de bloqueios de IP C2 do Botnet do Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist.json

4. Clique em **Editar** para editar o feed.

Exibir feeds RSS

Exiba os feeds RSS configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **RSS** opção.
   A seguir lista os feeds RSS configurados no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
Feed RSS do CISO2CISO.COM	RSS Feed de dados de CISO2CISO.com	https://ciso2ciso.com/feed/
Schweier no Feed RSS de segurança	RSS Feed de dados da Schweier sobre Segurança	https://www.schneier.com/feed/atom/
RSS Feed de segurança	Dados do Feed RSS da KerbsonSecurity	https://krebsonsecurity.com/feed/
Feed RSS da Segurança Nós vivemos	RSS Feed dados de bem-vindos segurança	http://feeds.feedburner.com/eset/blog
Feed RSS da JISA Softech	Dados do Feed RSS do JISA	https://www.jisasoftech.com/feed/
Feed RSS de segurança da Cisco Newsroom	Últimas notícias de segurança da cisco.	https://newsroom.cisco.com/c/services/i/servlets/newsroom/rssfeed.json?feed=security
HelpNet Security	Notícias de segurança da informação com foco na segurança empresarial.	https://www.helpnetsecurity.com/feed/
Assuntos de segurança	Informações sobre perícia digital de mídia de nível superior.	https://securityaffairs.com/feed
Feed RSS do Volexity	RSS Feed de dados de blogs de segurança da informação da Volexity.	https://www.volexity.com/blog/feed/
Feed RSS de notícias de hackers	RSS Feed de dados de "The Hacker News	https://feeds.feedburner.com/TheHackersNews?format=xml
Feed RSS de Graham Cluley	RSS feed de dados de Graham Cluley	https://grahamcluley.com/feed/

4. Clique em **Editar** para editar o feed.

Exibir Feed personalizado

Exiba o feed personalizado que é enviado no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione **Personalizado** .
   A tabela a seguir lista Feed personalizado pronto para uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ThreatFeed	Descrição	URL
Feed do CrowdStrike	Origem para obter dados de Ator, Observável e Relatórios do CrowdStrike.	https://api.crowdstrike.com

4. Clique em **Editar** para editar o feed.

Exibir Feed de ameaças premium para CrowdStrike

O feed do CrowdStrike permite que os usuários ingerem indicadores, atores, relatórios e seu contexto associado do feed CrowdStrike Falcon Intelligence no TISC.

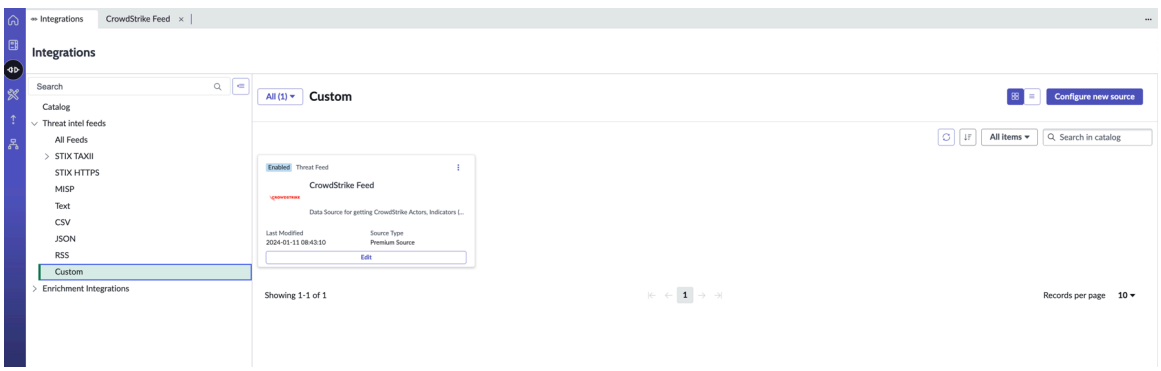
Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Selecione **Personalizado** .
3. Clique em **Editar** botão do *CrowdStrike***Feed** página de formulário.

Nota: Por padrão, o feed do CrowdStrike está desabilitado, você deve editar as configurações para habilitar o feed.



4. Detalhar até **Detalhes da configuração** seção.
5. Insira **ID do cliente** e **Segredo do cliente** .

Nota:

a. Caso não os tenha, você deve gerar o ID do cliente e o segredo do cliente. Para obter mais informações sobre o ID do cliente e o segredo do cliente, consulte Definir seu primeiro cliente de API seção.

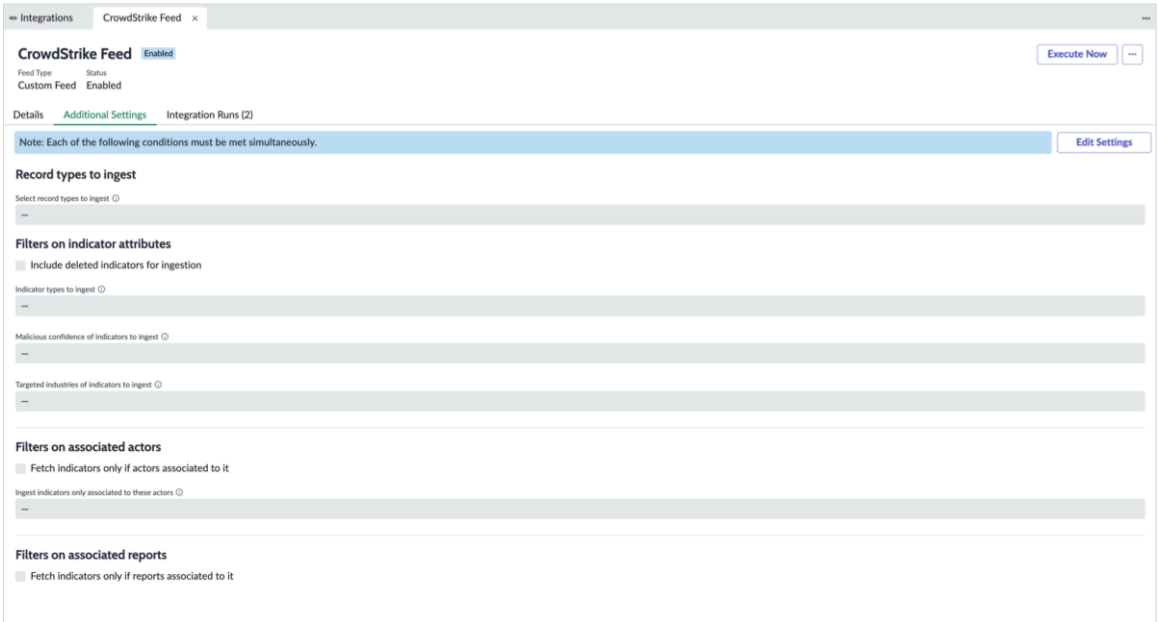
b. Obter ID do cliente e segredo do cliente de *CrowdStrike*para escopos necessários. Abaixo estão os escopos necessários para o ID do cliente e o segredo do cliente de *CrowdStrike*:

- Indicadores (Falcon Intelligence)
- Agentes (Falcon Intelligence)
- Relatórios (Falcon Intelligence)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

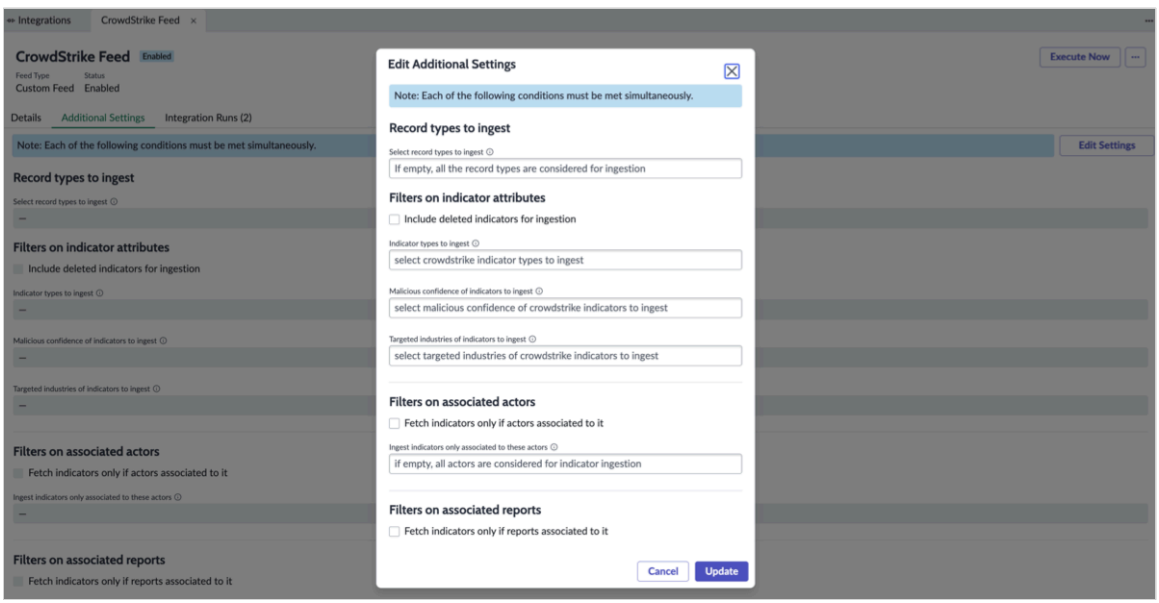
6. Navegue até **Configurações adicionais** para configurar os filtros que serão aplicados ao ingerir indicadores de CrowdStrike.



. **Configurações adicionais** a guia é usada principalmente para configurar os filtros que controlam como os dados são ingeridos na aplicação.

Esses filtros permitem personalizar o processo de integração de dados para atender aos seus requisitos específicos, garantindo que somente as informações mais relevantes sejam incluídas.

7. Clique em **Editar configurações** .



8. Selecione os filtros necessários.

Nota: Todos os filtros configurados serão aplicados em conjunto ao ingerir indicadores de CrowdStrike.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seção abaixo fornece uma explicação detalhada de cada opção disponível. Revise cada opção na tabela a seguir para entender como os filtros podem ser aplicados para otimizar os dados ingeridos na aplicação.

9. Selecione os valores necessários nos filtros disponíveis abaixo.

Editar configurações adicionais

Campo	Descrição
Tipos de registro a serem incluídos	
Selecione os tipos de registro para ingerir	Selecione os tipos de registro que você deseja ingerir. Os tipos de registro disponíveis são Indicadores, Relatórios e Atores. **Nota:** Se você selecionar Somente **Indicadores** Como o tipo de registro a ser incluído, os Relatórios e Atores relacionados associados a esses indicadores não serão ingeridos automaticamente. Para ingerir os Relatórios e Atores relacionados, você deve selecionar todos os três tipos de registro: Indicadores, Relatórios e Atores.
Filtros nos atributos do indicador	
Incluir indicadores excluídos para ingestão	Marque esta caixa de seleção para permitir a ingestão de indicadores que foram excluídos. **Nota:** Indicadores excluídos serão criados como observáveis somente se tiverem sido ingeridos anteriormente. . **Excluído no CrowdStrike** o marcador é adicionado aos indicadores que são removidos de CrowdStrike.
Tipos de indicador a serem incluídos	Selecione o específico CrowdStrike tipos de indicador que você deseja ingerir. Se nenhum for selecionado, todos os indicadores disponíveis serão recuperados por padrão.
Confiança mal-intencionada dos indicadores para ingerir	Selecione o nível de confiança mal-intencionado de CrowdStrike indicadores a serem incluídos. Se deixado em branco, todos os indicadores serão obtidos de CrowdStrike independentemente de sua confiança maliciosa.
Setores direcionados de indicadores a ingerir	Selecione os setores de destino associados a. CrowdStrike indicadores a serem incluídos. Se nenhum for selecionado, todos os indicadores serão obtidos de CrowdStrike independentemente do setor de destino.
Filtros nos atores associados	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Busque indicadores somente se os atores estiverem associados a ele	Marque esta caixa de seleção para buscar indicadores somente se eles estiverem associados a atores.
Indicadores de ingestão associados somente a esses atores	Especifique nomes de atores separados por vírgulas relacionados aos indicadores para ingestão. Se não for fornecido, todos os indicadores serão obtidos de CrowdStrike independentemente dos atores associados.
Filtros nos relatórios associados	
Buscar indicadores somente se houver relatórios associados a ele	Marque esta caixa de seleção para buscar indicadores somente se eles estiverem associados a relatórios.
Indicadores de ingestão associados somente a esses relatórios	Insira nomes de relatório separados por vírgulas associados aos indicadores para ingestão. Se deixado em branco, todos os relatórios serão incluídos no processo de ingestão. Se não for fornecido, todos os indicadores serão obtidos de CrowdStrike independentemente dos relatórios associados.
Filtros nas famílias de malware associadas	
Busque indicadores somente se famílias de malware associadas a ele	Marque esta caixa de seleção para buscar indicadores somente se eles estiverem associados a famílias de malware.
Indicadores de ingestão associados somente a essas famílias de malware	Insira nomes de famílias de malware separados por vírgulas associados aos indicadores de ingestão. Se deixado em branco, todas as famílias de malware serão incluídas no processo de ingestão. Se não for fornecido, todos os indicadores serão obtidos de CrowdStrike independentemente das famílias de malware.
Mapeamento de confiança mal-intencionada do indicador para confiança do TISC **Nota:** Os valores Alto, Médio e Baixo são o valor de origem ou confiança mal-intencionada recebida de CrowdStrike.	
Alto(a)	Insira um valor de confiança (0 a 100) para indicadores com alta confiança mal-intencionada. **Nota:** Se um mapeamento de confiança mal-intencionado correspondente for encontrado em **Configurações adicionais** . ele substituirá o valor fornecido em **Detalhes** mesmo se um valor de confiança for inserido manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Médio	Insira um valor de confiança (0 a 100) para indicadores com confiança mal-intencionada média.
Baixo(a)	Insira um valor de confiança (0 a 100) para indicadores com baixa confiança mal-intencionada.
Não verificado	Insira um valor de confiança (0 a 100) para indicadores com confiança mal-intencionada não verificada.

Nota: Com as mesmas configurações adicionais definidas acima, você pode duplicar o feed ao criar um novo.

10. Clique em **Atualização** em **Configurações adicionais** caixa de diálogo para salvar as configurações adicionais modificadas.
11. Clique em **Habilitar** para habilitar CrowdStrike Feed para ingestão.

Nota: O feed premium é o mesmo que outros feeds, exceto a resposta que é analisada durante a configuração. Uma resposta específica é analisada para CrowdStrike Adicionando o ID do cliente e o segredo do cliente.

De que tipo de dados são obtidos `CrowdStrike`:

a. Indicadores de CrowdStrike que são atualizados após o tempo de ingestão configurado e correspondem aos filtros configurados como parte das configurações adicionais. Esses indicadores de CrowdStrike em seguida, será mapeado para observáveis em TISC. Abaixo estão os tipos de indicador que são ingeridos em TISC:
   - Hash SHA256
   - Hash MD5
   - Hash SHA1
   - URL
   - Domínio
   - Endereço IP
   - Nome de mutex
   - Nome de arquivo
   - Endereço de E-mail
   - Nome do usuário
   - Bloco de endereços IP

b. Agentes de ameaça de CrowdStrike Atualizados após o tempo de ingestão configurado serão mapeados para os agentes de ameaça em TISC.

c. Relatórios de CrowdStrike atualizados após o tempo de ingestão configurado serão mapeados para relatórios de ameaças em TISC com base nos atributos correspondentes.

d. Além das entidades mencionadas acima, os seguintes dados relacionados também são obtidos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Agentes de ameaça, relatórios e indicadores relacionados aos indicadores ingeridos anteriormente.

ii. Agentes de ameaça e indicadores associados a todos os relatórios ingeridos durante o processo de ingestão atual.

Nota: Filtros configurados em **Configurações adicionais** também será aplicado ao ingerir os indicadores associados aos indicadores, relatórios ou atores ingeridos anteriormente.

12. **Opcional:** Clique em **Duplicado** para duplicar o feed.
Para obter mais informações, consulte Feeds de inteligência contra ameaças duplicados.

Propriedades do sistema do CrowdStrike

Os detalhes a seguir detalham as propriedades do sistema do CrowdStrike.

1. sn_sec_tisc.crowdstrike_ator_batch_size: Denota o número de atores a serem extraídos em uma única chamada de API. Aplicável somente quando a integração não encontrar o necessário presente no sistema.
   - Tipo: Número Inteiro
   - Valor: 250
2. sn_sec_tisc.crowdstrike_api_limit: Número de registros a serem obtidos por vez do CrowdStrike. Maior o número, mais a memória seria consumida para processar a carga.
   - Tipo: Número Inteiro
   - Valor: 1000
3. sn_sec_tisc.crowdstrike_indicator_batch_size: Denota o número de indicadores a serem extraídos em uma única chamada de API. Aplicável somente quando a integração não encontrar o necessário presente no sistema.
   - Tipo: Número Inteiro
   - Valor: 150
4. sn_sec_tisc.crowdstrike_offset_limit_total: O total permitido de deslocamento e limite da API CrowdStrike.
   - Tipo: Número Inteiro
   - Valor: 50000
5. sn_sec_tisc.crowdstrike_report_batch_size: Denota o número de relatórios a serem extraídos em uma única chamada de API. Aplicável somente quando a integração não encontrar o necessário presente no sistema.
   - Tipo: Número Inteiro
   - Valor: 50

Noções básicas do STIX TAXII

O Stix (Structured Threat Information Expression) é um formato de linguagem e serialização usado para trocar inteligência contra ameaças cibernéticas (CTI). Trusted Automated Exchange of Intelligence Information (TAXII) é um protocolo usado para trocar inteligência contra ameaças cibernéticas (CTI) por HTTPS.

Com o STIX, todos os aspetos de suspeita, compromisso e atribuição são representados como objetos e relacionamentos descritivos. As informações DO STIX podem ser visualmente representadas para um analista ou armazenadas como JSON para serem rapidamente legíveis por máquina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Inteligência contra ameaças cibernéticas (CTI) foi criada para definir um conjunto de representações de informações e protocolos para lidar com a necessidade de modelar, analisar e compartilhar inteligência contra ameaças cibernéticas. O CTI está focado principalmente no desenvolvimento e na padronização do Stix (Structured Threat Information Expression) e do Trusted Automated Exchange of Indicator Information (TAXII).

Configure um novo Feed TAXII

Você pode manter feeds TAXII para compartilhar informações no formato STIX. Cada feed do TAXII contém uma ou mais coleções do TAXII.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecionar **Feeds de inteligência contra ameaça** > **STIX TAXII** > **Feeds TAXII**.

   Nota: Configure o feed do TAXII para servir como um perfil para todas as coleções do TAXII no .

4. Clique em **Configurar nova origem** .
   A página Configurar novo Feed do TAXII é exibida.
5. No formulário, preencha os campos.

Criar nova fonte de dados

Campo	Descrição
Nome	Insira um nome para o feed.
Descrição	Descrição do feed.
Tipo de Origem	O tipo de origem, como Código Aberto, Origem Premium e assim por diante, fornecido para o feed. Os tipos de origem disponíveis são: ○ Governo ○ ISACs ○ Código aberto ○ Origem Premium ○ Outra origem
Logotipo	Anexe o logotipo do feed de origem.
Setor	Selecione a categoria do setor, como Aeroespacial, Agricultura e assim por diante, para a qual a fonte de dados do feed é aplicável.

Preencha os campos na seção Configuração, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração

Campo	Descrição
Versão de TAXII	Selecione a versão do TAXII do servidor TAXII que precisa ser configurada. As versões compatíveis são 2,0 e 2,1.
Tipo de Configuração	Forneça um tipo de configuração para buscar coleções TAXII. Os valores disponíveis são: ○ **URL do serviço da Descoberta** : Escolha a URL do serviço de descoberta para buscar coleções de todas as raízes de API disponíveis no serviço de descoberta do servidor TAXII. ○ **URL raiz da API** : Escolha o URL raiz da API para buscar coleções da raiz da API específica do servidor TAXII.
Autenticação	Se a autenticação for necessária, selecione a opção necessária na lista suspensa. As opções disponíveis são: ○ **Nenhum** : Selecione esta opção se não houver autenticação necessária. ○ **Básico** : Selecione esta opção para fornecer nome de usuário e senha. ○ **Chave de API** : Selecione esta opção para fornecer uma chave de API. ○ **Escolha uma mensagem REST** : Selecione esta opção para qualquer outro tipo de autenticação. As opções de mensagem REST são: ▪ **Usar mensagem REST** : Selecione esta caixa se você precisar de uma mensagem REST para criar uma mensagem REST de pré-compilação. Se você não selecionar, o valor no campo de endpoint será usado. Clique no ícone de pesquisa e selecione a mensagem REST na lista. ▪ **Método REST** : Selecione esta caixa se precisar de um método REST. Clique no ícone de pesquisa e selecione o método REST na lista. **Nota:** Os campos Mensagem REST e Método REST se tornam disponíveis quando a opção Mensagem REST é selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL	Insira a URL do serviço de descoberta do servidor do TAXII ou a URL raiz da API específica com base no tipo de configuração selecionado.
Seção avançada	
Avançado	Marque a caixa de seleção para escolher um script de integração e um Processador de relatório diferentes. Certifique-se de que os scripts escolhidos sejam compatíveis com a versão do TAXII selecionada. Com base na versão e na autenticação do TAXII, esses scripts são preenchidos automaticamente por padrão.
Script de integração	Invoca uma chamada para a API URL do endpoint REST usando os parâmetros de autenticação, como tipo de autenticação: Nome de usuário/senha/chave de API e os cabeçalhos a serem passados com a solicitação e, em seguida, o script busca os dados do STIX observáveis ou indicadores que estão disponíveis para o feed específico. **Nota:** Os dados obtidos são somente os dados brutos (nenhum registro é criado) que serão anexados ao processo de integração e poderão ser exibidos em **Execução de integração** seção. A seguir estão as inclusões de scripts personalizados, que são provisionadas na aplicação para os scripts de integrações: ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript O script de integração padrão é baseado no tipo de feed selecionado. As inclusões de script executam uma chamada REST simples, salva a resposta como um anexo e retorna o anexo para o processador.
Processador de relatórios	O processador de relatório invoca uma chamada para o URL do endpoint REST. No sistema de base abaixo estão as inclusões de scripts personalizados, que são provisionadas na aplicação para os scripts de integrações, **TAXIIV2CollectionDataProcessor** .

Preencha os campos na seção Programação, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programando

Campo	Descrição
Frequência de execução de coletas	O intervalo de programação que será aplicado aos registros de coleta do TAXII. A frequência de execução de uma coleção de TAXII pode ser modificada na exibição do formulário de coleta de TAXII, se necessário. **Nota:** Esta configuração será aplicada como padrão a todas as coleções TAXII obtidas. Há uma opção para substituir a configuração nas coleções TAXII, se necessário. Para obter mais informações, consulte Trabalhos agendados e como executar automaticamente um script de sua escolha .
Buscar dados de	A data de início a partir da qual os dados precisavam ser obtidos. Este campo deve ser definido com a hora a partir da qual os dados precisam ser ingeridos da origem correspondente. Depois que este campo for definido, a próxima execução de ingestão buscará os dados do tempo configurado e as execuções de ingestão consecutivas buscarão dados incrementais. Por exemplo, a Origem está programada para ingerir os dados a cada hora. Os conjuntos do usuário **Buscar dados de** Em 12 6:00AM de janeiro, em 12 9 de janeiro, a ingestão acionada em 12 10:00AM de janeiro buscaria os dados de 12 6:00AM de janeiro a 12 10 de janeiro. A próxima ingestão que é acionada às 11:00AM buscará somente os dados incrementais de 12 10:00AM de janeiro a 12 11 de janeiro. **Nota:** Isso significa que as execuções programadas buscarão dados incrementalmente a partir da data especificada em diante.

6. Clique em **Validar conexão**
   Uma mensagem informativa é exibida informando que a conexão do Feed TAXII foi bem-sucedida. Para obter as coleções, prossiga para a próxima etapa.
7. Clique em **Obter coleções TAXII** .

   Nota: Se houver erros, uma mensagem de erro será exibida informando que ocorreu um erro ao buscar coleções TAXII e verificar logs para obter mais detalhes.

   As coleções TAXII são exibidas na seção Coleções TAXII e estão desabilitadas por padrão.
8. Habilite as coleções TAXII para recuperar os objetos STIX disponíveis nessas coleções TAXII.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feeds de inteligência contra ameaças duplicados

Duplicar um feed de ameaça permite criar uma cópia exata de um feed existente, incluindo todos os observáveis, indicadores, atores e assim por diante associados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** ícone.
3. Selecione a integração desejada em **Catálogo** exibir.
   Por exemplo, selecione CrowdStrike
4. Clique em **Editar** botão para CrowdStrike cartão de feed para abrir o formulário de configuração.
5. Clique em **Mais ações** e selecione **Duplicado** .
   Uma confirmação é exibida indicando que duplicou a configuração do feed atual e criou um novo feed com o nome [integrationname Feed-copy] com um link para o novo feed duplicado. Por exemplo, CrowdStrike Feed-copy.

Integrações de aprimoramento de TISC

. Central de segurança de inteligência contra ameaças o sistema de base não inclui integrações pré-configuradas. Esta seção fornece instruções para configurar ambos ServiceNow e integrações de terceiros.

Importante:

Certifique-se de ter instalado as integrações de apps de terceiros necessárias. Você pode ver os observáveis, a pesquisa de vistas e os detalhes da pesquisa de ameaças somente para os aplicativos de terceiros instalados.

Todas as configurações de integração

Todas as integrações são aplicações separadas que precisam ser instaladas. O TISC oferece suporte a integrações com fornecedores de terceiros. Todas as integrações instaladas podem ser configuradas aqui.

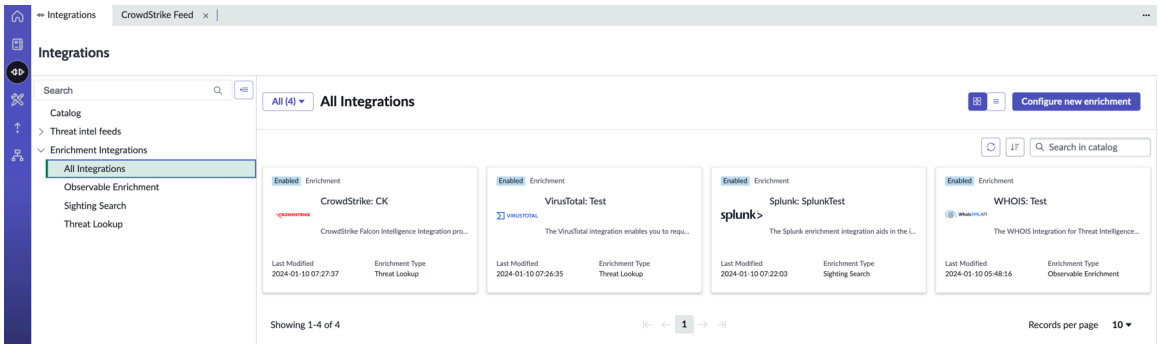
Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Cada seção de tipo de aprimoramento ficará visível somente se pelo menos uma das integrações correspondentes para esse tipo de aprimoramento estiver instalada. Por exemplo, o. **Pesquisa de ameaças** a seção estaria visível em **Integrações de aprimoramento** Pelo menos uma integração da Pesquisa de ameaças estiver instalada.

Os cartões de integração configurados podem ser exibidos navegando até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.

Tradução automática

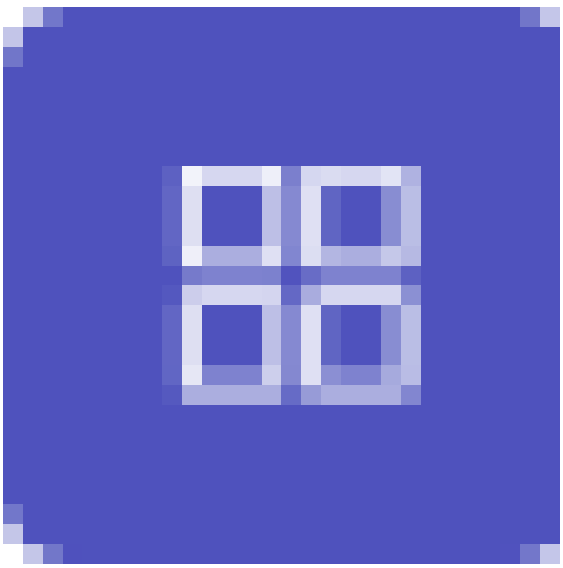
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Ações na exibição Todas as integrações

A exibição Todas as integrações permite que você execute as ações a seguir.

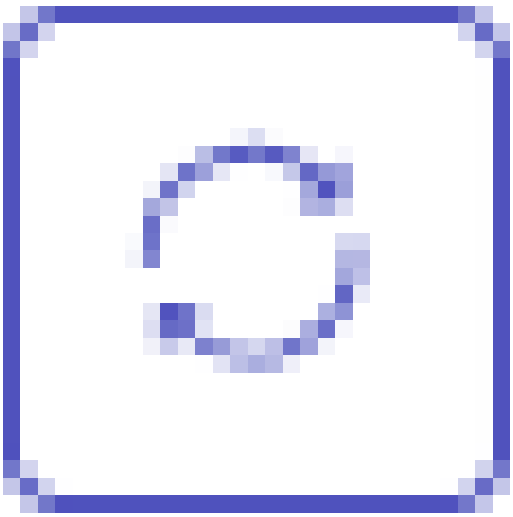
Exibição Todas as integrações

Ação	Descrição
Tudo	Use este menu suspenso para filtrar integrações com base em seu estado atual. Você pode filtrar com base nos seguintes estados: • **Todos** : Exibe todas as integrações na página. Esta é a opção padrão. • **Habilitado** : Exibe todas as integrações que estão em um estado habilitado. • **Desabilitado** : Exibe todas as integrações que estão em um estado desabilitado. • **Rascunho** : Exibe todas as integrações que estão em um estado de rascunho.
	Use esta ação para exibir todas as integrações na forma de cartões.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Todas as integrações

Ação	Descrição
	Use esta ação para exibir todas as integrações na forma de listas.
	Use esta ação para atualizar a página Todas as integrações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

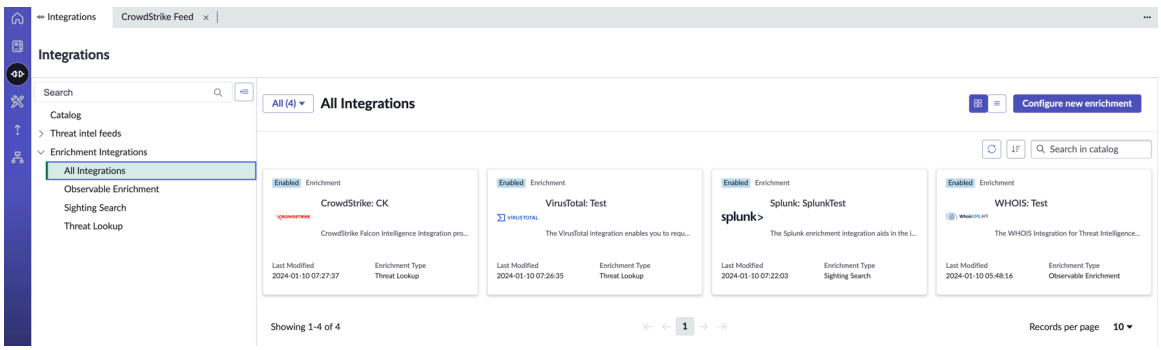
Exibição Todas as integrações

Ação	Descrição
	Use esta ação para classificar todas as integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Pesquisar no catálogo	Use esta ação para pesquisar integrações configuradas com base no nome e na descrição no catálogo.

Configure um novo aprimoramento na exibição Todas as integrações

Você pode configurar novos aprimoramentos na exibição Todas as integrações ou diretamente nas seções Aprimoramento de observável, Pesquisa de vistas ou Pesquisa de ameaças, respectivamente. Para configurar o novo aprimoramento de todas as exibições Todas as integrações, execute as etapas a seguir.

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** e selecione **Todas as integrações** seção.

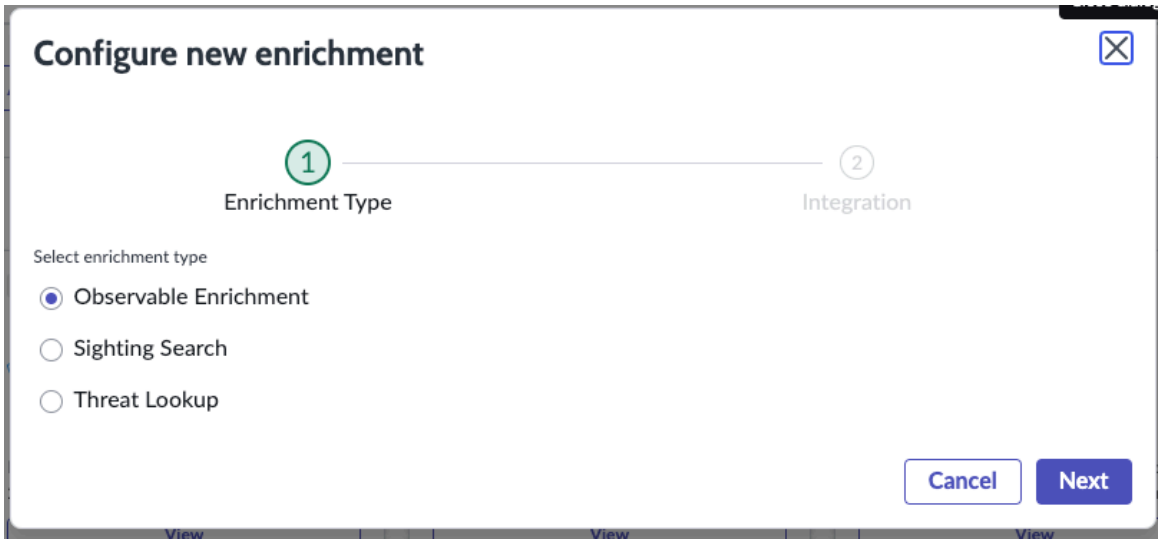


3. Clique em **Configurar novo aprimoramento** ação.

   O pop-up Configurar novo aprimoramento aparece com três tipos de aprimoramento, que são Enprimoramento observável, Pesquisa de vistas ou Pesquisa de ameaças. Você precisa escolher qual tipo de aprimoramento deseja configurar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione um tipo de aprimoramento e clique em **Próximo** .

   Você será direcionado para o pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que deseja configurar.

5. Selecione uma integração na lista de integrações disponíveis e clique em **Selecione** .

   Você será levado para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração do WHOIS.

6. No formulário Criar nova integração, preencha os campos.

Configure o novo formulário de integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `WHOIS1` .
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `WHOIS` .
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Aprimoramento de observável. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão. Os seguintes tipos de integração são compatíveis: ○ Aprimoramento de Observável ○ Pesquisa de detecções ○ Pesquisa de ameaças
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.

   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente da API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes integrações.

8. Clique em **Salvar** ação para armazenar e criar a configuração de integração de aprimoramento.

   Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento é desabilitado.

9. (Opcional) Clique em **Salvar como rascunho** ação para armazenar somente as configurações de integração como rascunho. Os usuários não podem habilitar uma integração quando ela é salva em rascunho

   Se você não tiver certeza sobre os detalhes da configuração, poderá usar **Salvar como rascunho** opção. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.

10. Para habilitar a integração de aprimoramento, clique em **Habilitar** .

    A integração de aprimoramento foi habilitada com sucesso.

11. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessária na página Catálogo ou na página Integrações de aprimoramento.

Configurar aprimoramento de observável

Você pode executar o aprimoramento da inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações executadas dependem das que você ativou.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

. Central de segurança de inteligência contra ameaças O oferece suporte ao aprimoramento de observável somente para a integração WHOIS a partir de agora. Para obter mais informações, consulte Configure e habilite a integração do Whois.

Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações compatíveis com qualquer recurso estiver instalada na aplicação.

Por Que e Quando Desempenhar Esta Tarefa

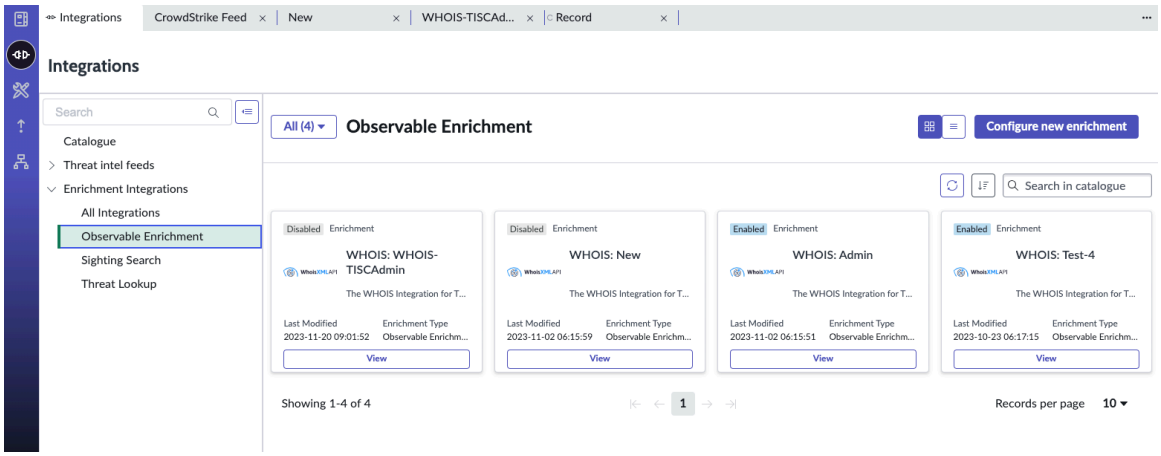
A seção Aprimoramento de observável contém somente as integrações com o tipo de integração como aprimoramento de observável. Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** e selecione **Aprimoramento de observável** seção.

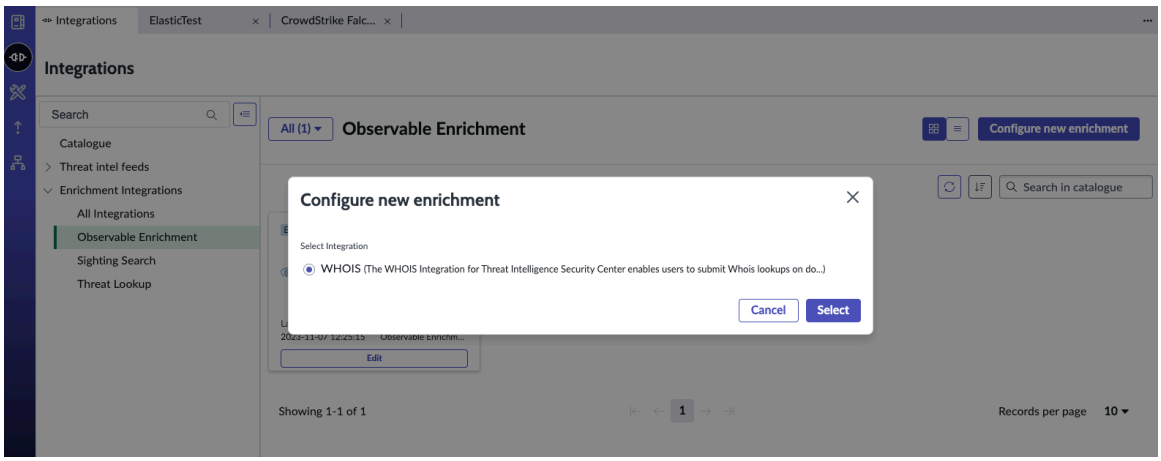
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Configurar novo aprimoramento** ação.
   Você será direcionado para o pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.

4. Selecione uma integração na lista de integrações disponíveis e clique em **Selecione** .
   Você será levado para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração do WHOIS.

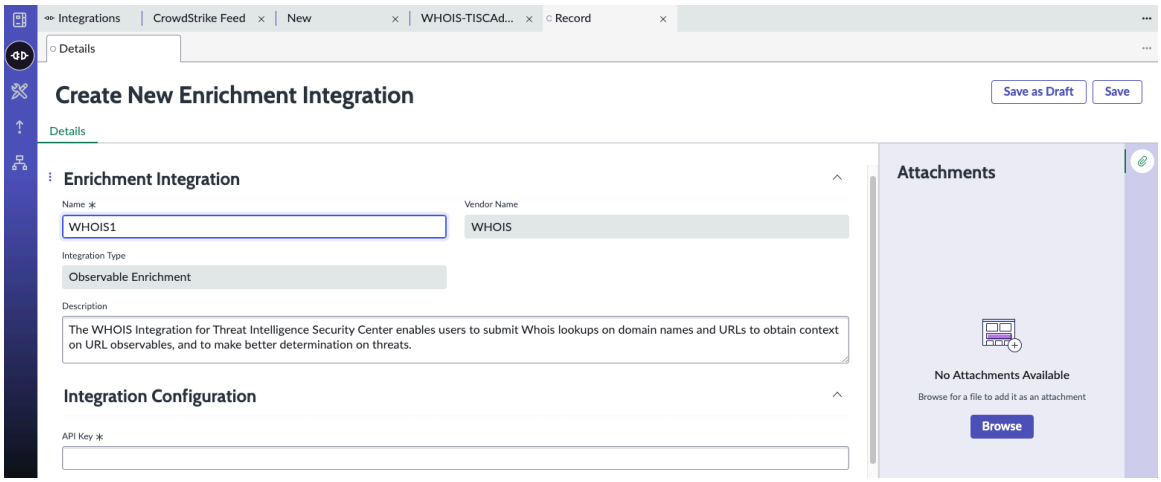


5. No formulário Criar nova integração, preencha os campos.

Campo	Descrição
Integração de aprimoramento	
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `WHOIS1` .
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `WHOIS` .
Tipo de Integração	Tipo de integração que você selecionou, que é aprimoramento observável. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente da API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.
7. Clique em **Salvar** ação para armazenar e criar a nova configuração de integração de aprimoramento.
   Depois de clicar em **Salvar** ou **Habilitar** a integração é validada usando as configurações de integração fornecidas. Por padrão, o status da integração de aprimoramento é definido como desabilitado.
8. Clique em **Salvar como rascunho** ação para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-la.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar **Salvar como rascunho** opção. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar** .
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessária na página Catálogo ou na página Integrações de aprimoramento.

Configurar Pesquisa de vistas

Você pode executar a pesquisa de vistas em um ou vários observáveis para determinar o número de vezes que os observáveis são vistos nos logs da sua organização. Você pode executar a pesquisa de vistas em observáveis dentro de um número selecionado de dias ou dentro de um intervalo de datas.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações compatíveis com qualquer recurso estiver instalada na aplicação.

. Central de segurança de inteligência contra ameaças O oferece suporte à Pesquisa de vistas somente para as seguintes integrações:

- Pesquisa do Splunk
- Elasticsearch

Por Que e Quando Desempenhar Esta Tarefa

A seção Pesquisa de vistas contém somente as integrações com o tipo de integração como pesquisa de vistas.

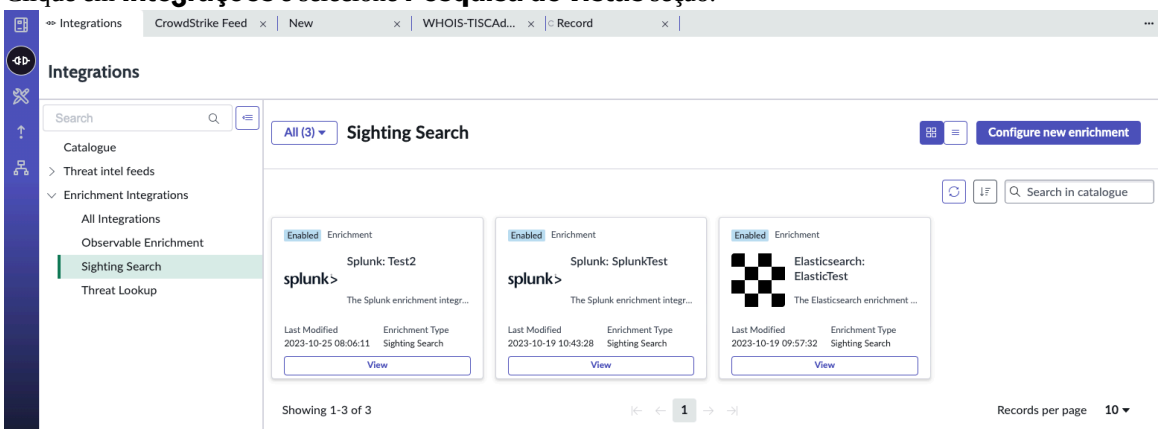
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

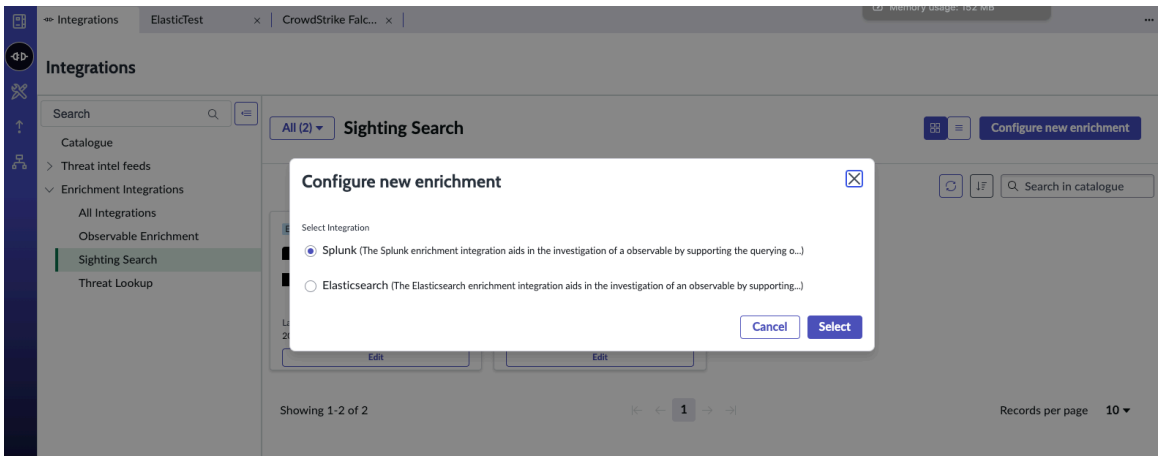
Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** e selecione **Pesquisa de vistas** seção.



3. Clique em **Configurar novo aprimoramento** ação.
   Você será direcionado para o pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.
4. Selecione uma integração na lista de integrações disponíveis e clique em **Selecione** .
   Você será levado para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, Integração do Splunk.



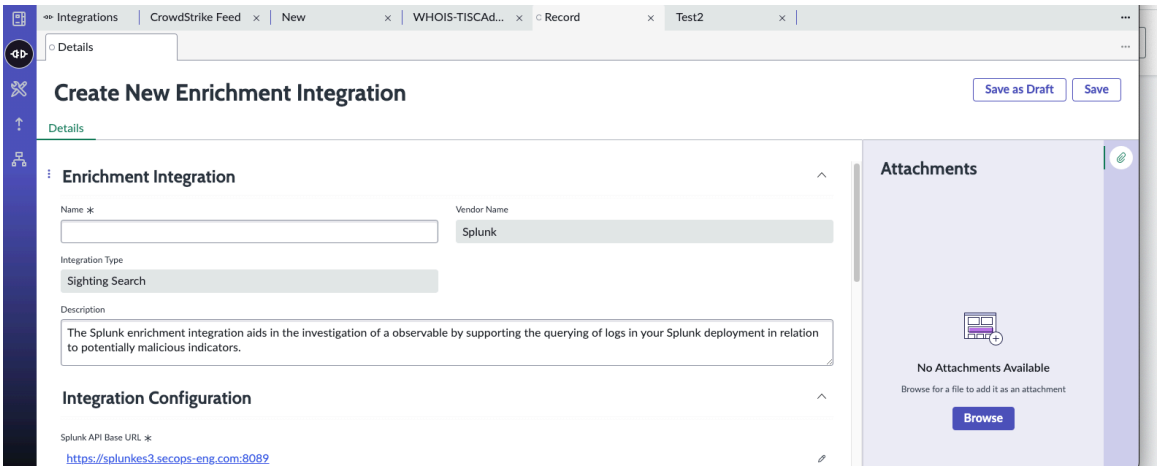
5. No formulário Criar nova integração, preencha os campos.

Campo	Descrição
Integração de aprimoramento	
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `Splunk-1` .
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `Splunk` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de Integração	Tipo de integração que você selecionou, que é Pesquisa de vistas. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente da API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.
7. Clique em **Salvar** ação para armazenar e criar a nova configuração de integração de aprimoramento.
   Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento é desabilitado.
8. Clique em **Salvar como rascunho** ação para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-la.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar **Salvar como rascunho** opção. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar** .
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessária na página Catálogo ou na página Todas as integrações.

Defina consultas para Pesquisa de vistas

Você pode usar as configurações de pesquisa de vistas para definir as consultas usadas para encontrar a prevalência de observáveis em seu ambiente como parte da investigação de observáveis.

Exibir consultas para Pesquisa de vistas

Função necessária: sn_sec_tisc.admin

Para exibir as configurações de pesquisa de vistas, execute as seguintes etapas:

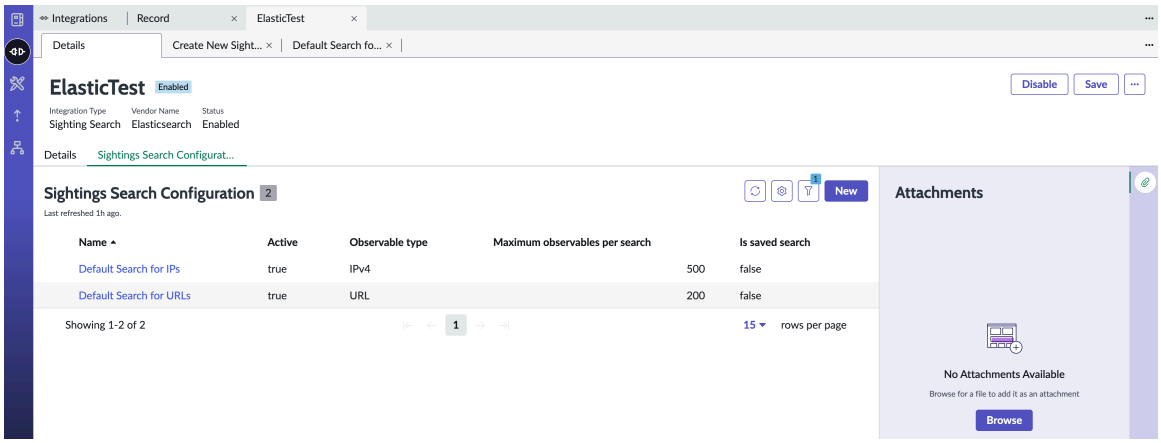
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de Vistas**.
3. Procure a integração para a qual você deseja exibir a Configuração de pesquisa de vistas e clique em **Editar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Configurações de pesquisa de vistas** guia.

   Você pode exibir a lista de configurações de pesquisa de vistas.



5. Clique na Configuração de pesquisa de vistas necessária para exibir os detalhes da configuração.
6. Para gerar uma consulta de pesquisa de detecção de teste, clique em **Gerar consulta de pesquisa de detecção de teste** ação.

   Nota: . **Gerar consulta de pesquisa de detecção de teste** a ação só funcionará se você tiver configurado parâmetros de consulta de pesquisa de vistas. Para obter mais informações, consulte Usando Parâmetros de pesquisa de vistas.

7. No pop-up Gerar consulta de pesquisa de detecção de teste, insira ou cole vários observáveis usando vírgulas, nova linha, guia ou separadores de tubo rígido para gerar uma consulta de teste.
8. Clique em **Gerar** para gerar a consulta de pesquisa de detecção de teste.
9. Você também pode executar as seguintes ações na guia Configurações de pesquisa de vistas:

   a. Para atualizar a lista de configurações de pesquisa de vistas, clique em ícone.

   b. Para executar uma ação de lista nas configurações de pesquisa de vistas, clique em ícone.

      Você pode executar as duas ações de lista a seguir:

      - **Editar colunas** : Você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.
      - **Redefinir larguras** : Você pode usar esta ação para redefinir as larguras das colunas.

   c. Para filtrar configurações de pesquisa de vistas com base em condições, clique em ícone.

      O valor 1 indica que uma condição é usada para a filtragem.

Criar configurações de pesquisa suspirantes

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

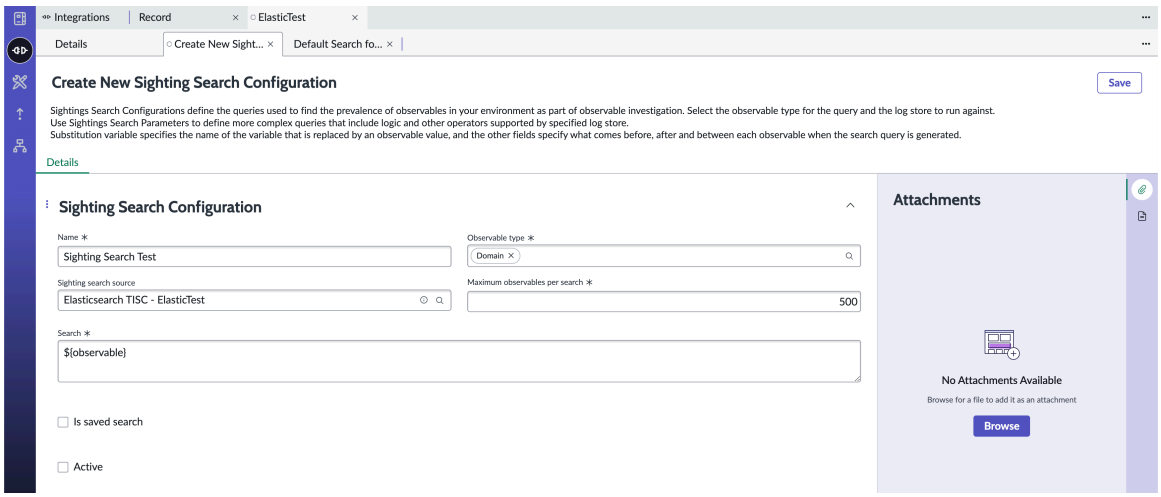
Maximum observables per search = "maximum number of observables that can be substituted in a single search query"

Search = "Search query that should be executed in sighting search source.
Search query can contain substitution variables that would be substituted with observables of specific type as configured in sighting search parameters when sighting search query is formed"

Para criar uma configuração de pesquisa de vistas, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de Vistas**.
3. Procure a integração para a qual você deseja exibir a Configuração de pesquisa de vistas e clique em **Editar** .
4. Selecione **Configurações de pesquisa de vistas** guia.

   Você pode exibir a lista de configurações de pesquisa de vistas.
5. Para criar uma configuração de pesquisa de vistas, clique em **Novo** .



6. No formulário, preencha os campos.

Crie uma configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome da configuração de pesquisa de vistas.
Tipo de observável	Define o tipo de categoria de observável.
Origem da pesquisa de detecções	Define a origem configurada para a integração.
Máximo de observáveis por pesquisa	O número de observáveis antes da consulta de pesquisa é dividido em várias consultas. Defina este valor como `500` para esta integração.
Pesquisar	Adicione uma cadeia de caracteres de pesquisa nativa para formar uma consulta. Por exemplo, `(observável)` .
Pesquisa salva	Executa uma pesquisa salva, ou seja, o campo Nome deve corresponder ao nome da pesquisa salva.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	A consulta será executada somente se a opção ativa estiver selecionada.

7. Clique em **Salvar**.

Usando Parâmetros de pesquisa de vistas

Você pode usar parâmetros de pesquisa de vistas que definem consultas mais complexas, que incluem lógica e outros operadores compatíveis com o armazenamento de logs especificado.

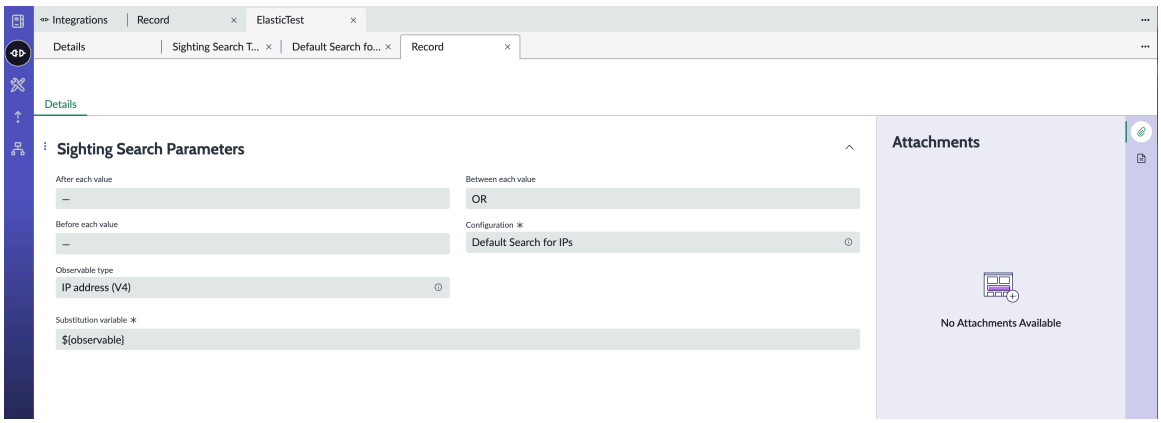
Exibir parâmetros de pesquisa de vistas

Função necessária: sn_sec_tisc.admin

Para exibir os parâmetros de pesquisa de vistas, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de Vistas**.
3. Procure a integração para a qual você deseja exibir a Configuração de pesquisa de vistas e clique em **Editar** .
4. Selecione **Configurações de pesquisa de vistas** guia.

   Você pode exibir a lista de configurações de pesquisa de vistas.
5. Clique na Configuração de pesquisa de vistas necessária para exibir os detalhes da configuração.



6. Selecione **Parâmetros de pesquisa de vistas** guia.

   Você pode exibir a lista de parâmetros de pesquisa de vistas.
7. Clique no parâmetro de Pesquisa de vistas necessário para exibir os detalhes do parâmetro.
8. Você também pode executar as seguintes ações na guia Parâmetros de pesquisa de vistas:
   a. Para atualizar a lista de parâmetros de pesquisa de vistas, clique em ícone.
   b. Para executar uma ação de lista nos parâmetros de pesquisa de vistas, clique em ícone.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Editar colunas : Você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.

c. Para filtrar os parâmetros de pesquisa de vistas com base nas condições, clique em  ícone.

O valor 1 indica que uma condição é usada para a filtragem.

Criar parâmetro de pesquisa de vistas

Exemplo de geração de consulta

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address = 192.168.10.12”
```

Para criar um parâmetro de pesquisa de vistas, execute as seguintes etapas:

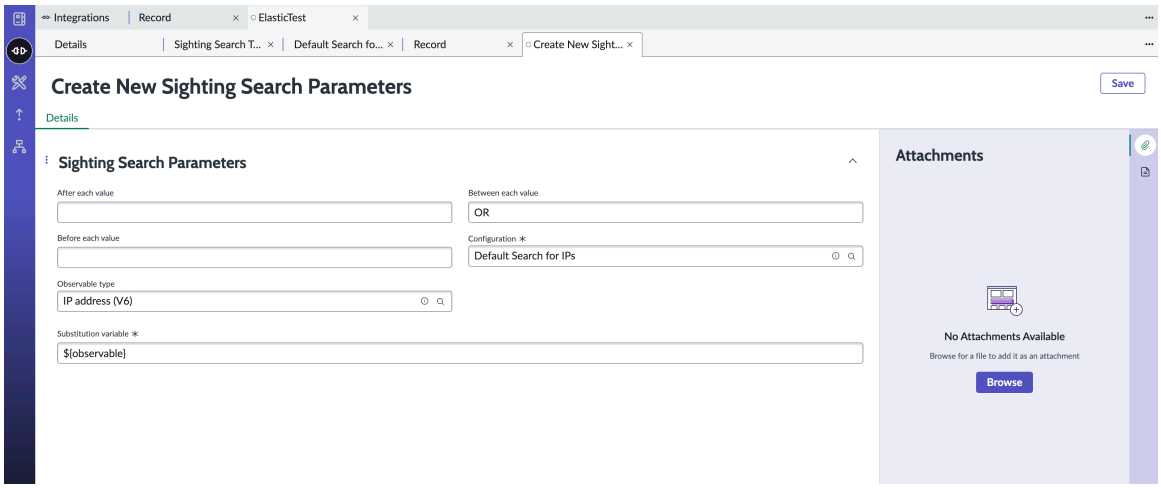
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de Vistas**.
3. Procure a integração para a qual você deseja exibir a Configuração de pesquisa de vistas e clique em **Editar** .
4. Selecione **Configurações de pesquisa de vistas** guia.

   Você pode exibir a lista de configurações de pesquisa de vistas.
5. Clique na Configuração de pesquisa de vistas necessária para exibir os detalhes da configuração.
6. Selecione **Parâmetros de pesquisa de vistas** guia.

   Você pode exibir a lista de parâmetros de pesquisa de vistas.
7. Para criar um parâmetro de pesquisa de vistas, clique em **Novo** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. No formulário, preencha os campos.

Crie um parâmetro de pesquisa de vistas

Campo	Descrição
Após cada valor	O parâmetro de pesquisa de vistas após cada observável quando a consulta de pesquisa é gerada.
Entre cada valor	O parâmetro de pesquisa de vistas entre cada observável quando a consulta de pesquisa é gerada. Por exemplo, OU.
Antes de cada valor	O parâmetro de pesquisa de vistas antes de cada observável quando a consulta de pesquisa é gerada.
Configuração	Os detalhes da configuração do parâmetro de pesquisa.
Tipo de observável	Define o tipo de categoria de observável.
Variável de substituição	Especifica o nome da variável que é substituída por um valor observável.

9. Clique em **Salvar**.

Configurar Pesquisa de ameaças

Você pode configurar a pesquisa de ameaças para executar uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pela Inteligência contra ameaças, os observáveis serão verificados em busca de malware e os resultados serão retornados. Você pode executar a pesquisa de ameaças em um ou mais observáveis para determinar a malícia de um observável.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações compatíveis com qualquer recurso estiver instalada na aplicação.

. Central de segurança de inteligência contra ameaças Oferece suporte à Pesquisa de ameaças somente para as seguintes integrações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- VirusTotal
- CrowdStrike Intelligence

Para obter mais informações, consulte Pesquisa de ameaças.

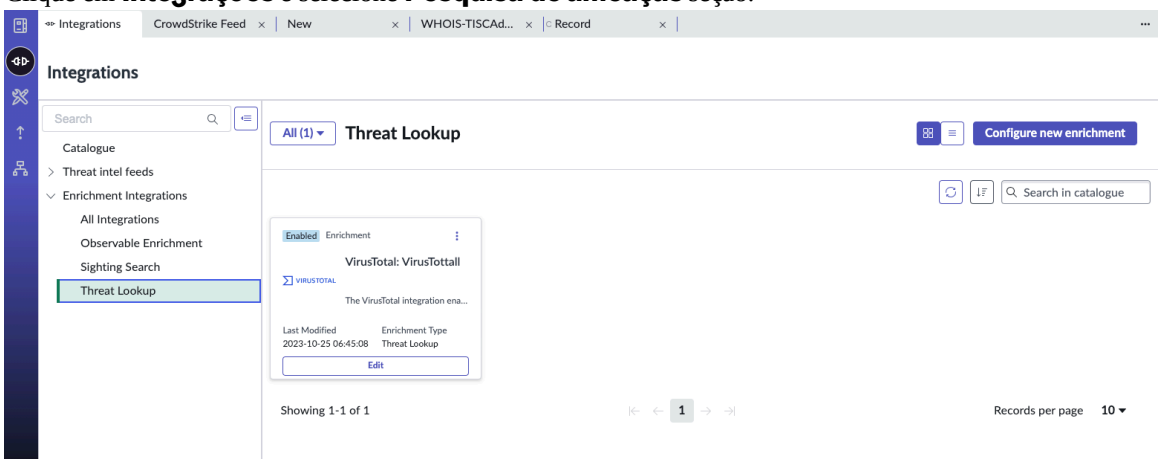
Por Que e Quando Desempenhar Esta Tarefa

A seção Pesquisa de ameaças contém somente as integrações com o tipo de integração como Pesquisa de ameaças.

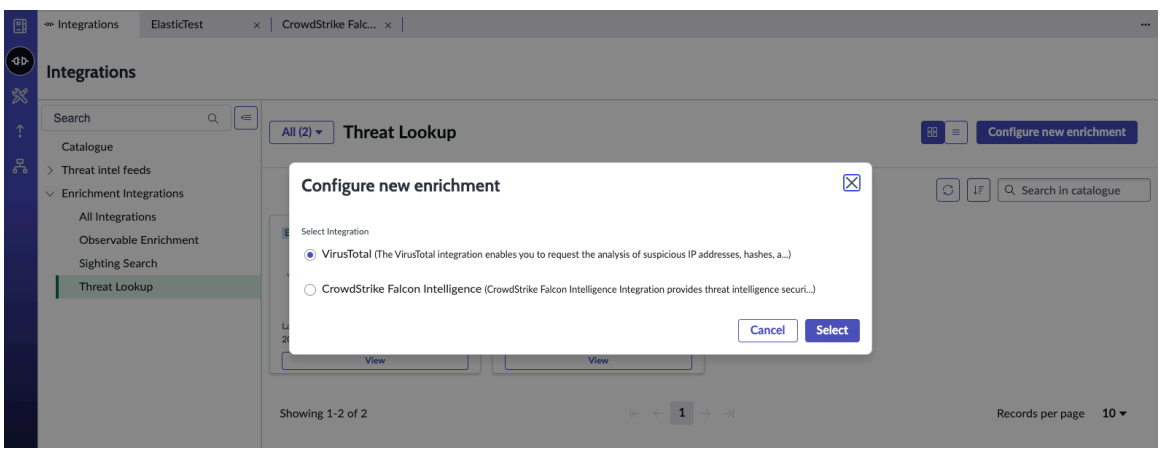
Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Integrações** e selecione **Pesquisa de ameaças** seção.



3. Clique em **Configurar novo aprimoramento** ação.
   Você será direcionado para o pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.
4. Selecione e integração na lista de integrações disponíveis e clique em **Selecione** .
   Você será levado para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, Integração VirusTotal.

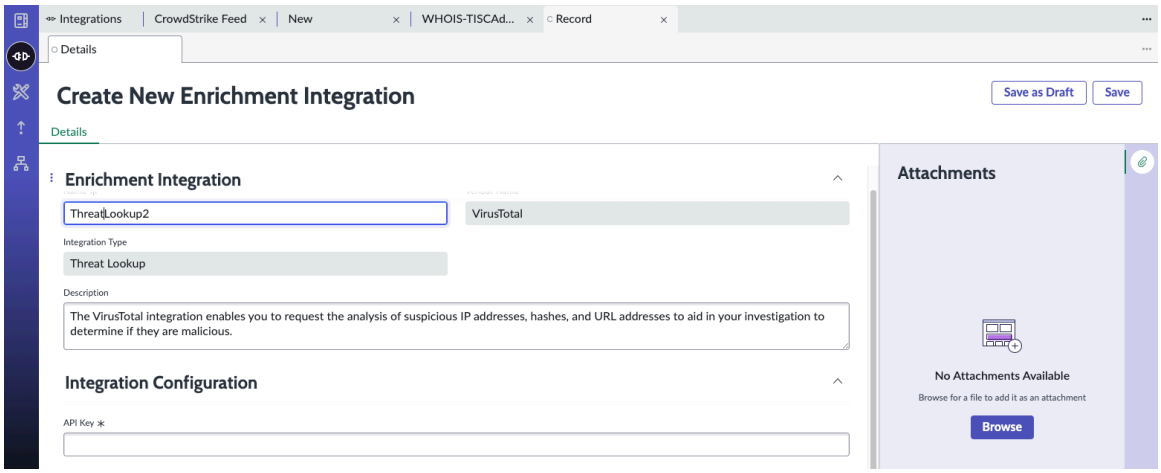


5. No formulário Criar nova integração, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `Virustotal - 1` .
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `Virustotal` .
Tipo de Integração	Tipo de integração que você selecionou, que é Pesquisa de ameaças. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente da API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.
7. Clique em **Salvar** ação para armazenar e criar a nova configuração de integração de aprimoramento.
   Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento é desabilitado.
8. Clique em **Salvar como rascunho** ação para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-la.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar **Salvar como rascunho** opção.
   Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar** .
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessária na página Catálogo ou na página Integrações de aprimoramento.

Exibir Calculadoras de reputação da Pesquisa de ameaças

Você pode exibir a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis para sua integração.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

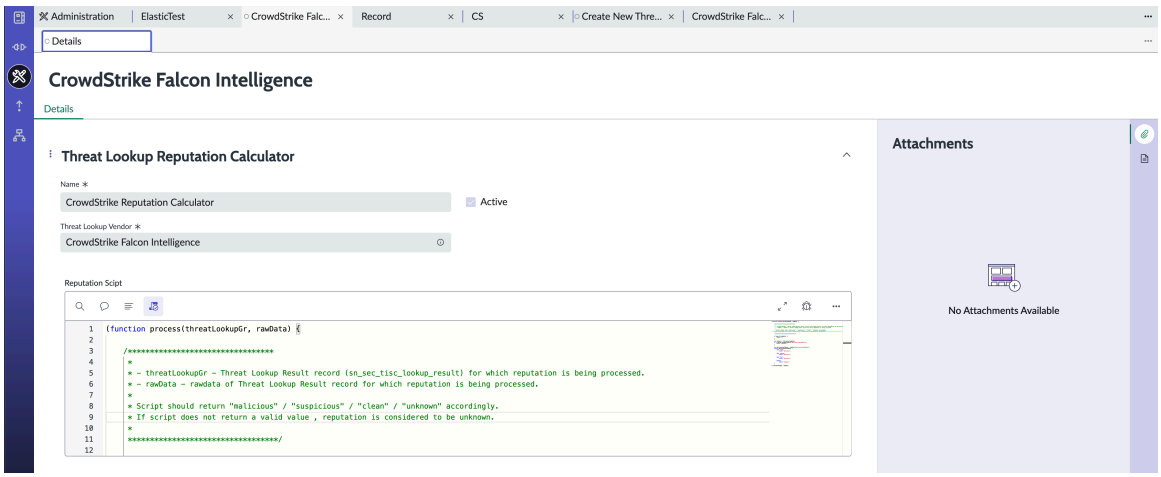
Para saber mais sobre as Calculadoras de reputação da Pesquisa de ameaças, consulte Como gerenciar a Calculadora de reputação da Pesquisa de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione **Calculadora de reputação da Pesquisa de ameaças** seção.
   Você pode exibir a lista de Calculadoras de reputação da Pesquisa de ameaças.
3. Clique na Calculadora de reputação da Pesquisa de ameaças necessária para exibir os detalhes da calculadora.



4. Você também pode executar as seguintes ações na seção Calculadora de reputação da Pesquisa de ameaças:

   a. Para atualizar a lista de Calculadoras de reputação da Pesquisa de ameaças, clique em ícone.

   b. Para executar uma ação de lista nas Calculadoras de reputação da Pesquisa de ameaças, clique em ícone.

      Você pode executar as duas ações de lista a seguir:

      - **Editar colunas** : Você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.
      - **Redefinir larguras** : Você pode usar esta ação para redefinir as larguras das colunas.

   c. Para filtrar Calculadoras de reputação da Pesquisa de ameaças com base nas condições, clique em ícone.

      O valor 1 indica que uma condição é usada para a filtragem.

Referências de API TISC

A tabela a seguir fornece as referências de endpoints de API que ajudam nos aprimoramentos.

TISC

API	Descrição
TISC - POST /sn_sec_tisc/threat_intel_data/observables	Esta API recupera os dados de observáveis, incluindo os relacionamentos entre observáveis e outros dados de inteligência contra ameaças associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC

API	Descrição
TISC - POST /sn_sec_tisc/threat_intel_data/add_observables	Esta API adiciona observáveis válidos à aplicação Central de segurança do Threat Intelligence (TISC) criando registros de origem do observável.

Para obter mais informações sobre os endpoints da API do TISC, consulte API TISC na seção de referência da REST API sobre implementação e referência de API em servicenow.com/docs.

Integrações do TISC

Esta seção fornece instruções para configurar e habilitar as integrações do Inteligência contra ameaças.

Aprimoramento de Observável

O fluxo de trabalho Enrich observable WHOIS executa o aprimoramento nos observáveis selecionados. Se os observáveis forem de um tipo reconhecido pela integração da API WhoisXML, os observáveis serão aprimorados.

Nota: A Central de segurança do Inteligência contra ameaças oferece suporte ao aprimoramento de observável somente para a integração do WHOIS.

Integração do WHOIS

A integração do Whois permite que você envie pesquisas do Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

Configure e habilite a integração do Whois

Antes de usar a integração do Whois, você deve baixá-lo na ServiceNow Store e deve ter uma conta válida do Whois.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

A Central de segurança do Inteligência contra ameaças e os plug-ins de integração do Observable do Whois são necessários.

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Aprimoramento de Observável**.
6. Em **WHOIS** cartão, clique em **Configurar Novo Aprimoramento** para configurar **WHOIS** integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, WHOIS.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, WHOIS.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento. A descrição da integração do WHOIS é, A Integração do WHOIS para a Central de segurança da Inteligência contra ameaças permite que os usuários enviem pesquisas do Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

8. Detalhar até **Configuração de integração** seção.
9. Insira (ou cole) o. **Chave de API** Adquirido no site WHOIS.
10. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status da integração do WHOIS é desabilitado.
11. Clique em **Habilitar** Para habilitar a integração do WHOIS.

Resultado
Depois de configurado, o WHOIS pode ser selecionado para executar melhorias em observáveis na Central de segurança da Inteligência contra ameaças.

Integração do Shodan

Shodan é um mecanismo de pesquisa que analisa informações de faixa de serviço de dispositivos conetados em todo o mundo.

A integração do Shodan executa o aprimoramento nos seguintes observáveis:

- Endereços IP
- URLs
- Domínios

Configurar e habilitar a integração do Shodan

Antes de usar a integração do Shodan, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Aprimoramento de Observável**.
6. Em **Shodan** cartão, clique em **Configurar Novo Aprimoramento** para configurar a integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, Shodan.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos automaticamente e, por padrão, este campo será somente leitura. Por exemplo, Shodan.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Aprimoramento de observável.
Descrição	Insira a descrição da nova integração de aprimoramento. Por exemplo, a descrição da integração do Shodan é: O Shodan ajuda você a analisar informações de faixa de dispositivos conectados em todo o mundo.

8. Detalhar até **Configuração de integração** seção.
9. Insira (ou cole) o. **Chave de API** Você adquiriu do portal Shodan.
10. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status é desabilitado.
11. Clique em **Habilitar** para habilitar a integração.

Pesquisa de Vistas

Esta seção descreve as integrações do TISC Sighting Search e Elastic Search.

Comece a usar a integração do Elasticsearch

A integração de aprimoramento do Elasticsearch pesquisa seus logs e adiciona informações de vista relevantes aos observáveis.

Configure e habilite a integração do Elasticsearch

Elasticsearch é um mecanismo distribuído de pesquisa e análise RESTful que se integra facilmente às Operações de segurança.

Antes de Iniciar

Antes de usar o Elasticsearch, você deve baixá-lo na ServiceNow Store.

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O plug-in Central de segurança do Inteligência contra ameaças deve ser instalado e ativado antes que você possa usar a integração do Elasticsearch.
- Obtenha a URL base da API Elasticsearch, a URL base do Kibana, o nome de usuário e a senha em seu perfil do Elasticsearch.

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de Vistas**

   Nota: As integrações configuradas aparecem como uma série de cartões.

6. Em **Elasticsearch** cartão, clique em **Configurar Novo Aprimoramento** para configurar **Elasticsearch** integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a configuração de pesquisa de vistas.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, Elasticsearch.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da integração do Elasticsearch. Por exemplo, a integração de aprimoramento do Elasticsearch ajuda na investigação de um observável, oferecendo suporte à consulta de logs em sua implantação do Elasticsearch.
Configuração de integração	
URL de Base da API Elasticsearch	O URL base que você adquiriu no site do Elasticsearch.
URL base do Kibana	A URL base do Kibana. [Opcional] Links para uma instância do Kibana, quando disponível.
Nome do usuário	Seu nome de usuário do Intel Elasticsearch.
Senha	Sua senha do Intel Elasticsearch.
Índice do Elasticsearch	O índice do Elasticsearch. Estes, por sua vez, conterão documentos exclusivos para cada índice. Os índices são identificados por nomes minúsculos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	que se referem a ações que são ações executadas (como pesquisar e excluir).
Campo do intervalo de datas	O carimbo de data/hora da configuração.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração na propriedade Número de linhas de dados brutos em Propriedades de resposta do incidente de segurança .
MID Server	Selecione Qualquer para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o Editor de fluxo de trabalho.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do Elasticsearch é desabilitado.
9. Clique em **Habilitar** Para habilitar a integração do Elasticsearch.

Resultado
Depois de configurado, o Elasticsearch pode ser selecionado para executar a pesquisa de vistas em observáveis na Central de segurança da Inteligência contra ameaças.

Comece a usar a integração do Splunk Search

O software Splunk pesquisa, monitora e analisa big data gerado por máquina e se integra facilmente às Operações de segurança. Antes de usar a integração do Splunk Sighting Search, você deve baixá-la na ServiceNow Store.

Configure e habilite a integração do Splunk

A integração de aprimoramento do Splunk pesquisa seus logs e adiciona informações de vista relevantes.

Antes de Iniciar
Antes de usar o Splunk Search, você deve baixá-lo na ServiceNow Store.

Função necessária: sn_sec_tisc.admin

- O plug-in Central de segurança do Inteligência contra ameaças deve ser instalado e ativado antes que você possa usar a integração do Splunk Search.
- Obtenha o Splunk e a Pesquisa Splunk e obtenha o URL base da API, o URL do link, o nome de usuário e a senha da sua instância do Splunk.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de Vistas**
   As integrações configuradas aparecem como uma série de cartões.
6. Em **Splunk Search** cartão, clique em **Configurar Novo Aprimoramento** para configurar **Splunk Search** integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a configuração de pesquisa de vistas.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, Splunk.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da integração do Splunk. Por exemplo, a integração de aprimoramento do Splunk ajuda na investigação de um observável, oferecendo suporte à consulta de logs em sua implantação do Splunk em relação a indicadores potencialmente mal-intencionados.
Configuração de integração	
URL base da API Splunk	O URL base que você adquiriu do site Splunk.
URL do Link	URL do link que vincula à interface da web do Splunk, quando disponível.
Nome do usuário	Seu nome de usuário do Intel Elasticsearch.
Senha	Sua senha do Intel Elasticsearch.
Máximo de linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados de pesquisa de avistamentos. A quantidade de dados retornados depende da sua configuração na propriedade Número de linhas de dados brutos em Propriedades de resposta do incidente de segurança .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Implantação no Local	O ambiente implantado no local.
MID Server	Selecione Qualquer para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o Editor de fluxo de trabalho.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do Splunk é desabilitado.
9. Clique em **Habilitar** Para habilitar a integração do Splunk.

Resultado

Depois de configurado, o Splunk pode ser selecionado para executar a pesquisa de vistas em observáveis na Central de segurança da Inteligência contra ameaças.

Pesquisa de ameaças

O fluxo de trabalho de inteligência Pesquisa de ameaças - VirusTotal e CrowdStrike Falcon executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo VirusTotal e pelo CrowdStrike, os observáveis serão verificados em busca de malware e os resultados serão retornados.

Integração do TISC VirusTotal

A integração do TISC VirusTotal permite que você solicite a análise de endereços IP suspeitos, hashes de arquivo e endereços de URL para ajudar na investigação e determinar se eles são mal-intencionados.

Configure e habilite a integração do VirusTotal

Antes de usar a integração do VirusTotal, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

O plug-in Central de segurança do Inteligência contra ameaças é necessário para ativar a integração do VirusTotal.

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, acesse o VirusTotal e obtenha a chave de API no seu perfil VirusTotal.
4. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
5. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
6. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de ameaças**
7. Clique em **Configurar Novo Aprimoramento** para configurar **Virustotal** integração.
8. Preencha os campos no formulário Configurar novo aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, VirusTotal.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, VirusTotal.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento.

9. Detalhar até **Configuração de integração** seção.
10. Insira (ou cole) o. **Chave de API** Adquirido do site VirusTotal.
11. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status da integração do VirusTotal é desabilitado.
12. Clique em **Habilitar** Para habilitar a integração do VirusTotal.

Resultado
Depois de configurado, o VirusTotal pode ser selecionado para executar pesquisas em observáveis na Central de segurança do Inteligência contra ameaças.

Integração do TISC CrowdStrike Falcon Intelligence

O CrowdStrike Falcon Intelligence fornece inteligência de segurança cibernética que se integra facilmente às Operações de segurança.

Nota:

O plug-in Central de segurança do Inteligência contra ameaças é necessário para implementar a integração do CrowdStrike Falcon Intelligence.

Configure e habilite a integração do CrowdStrike Falcon Intelligence

Antes de usar o CrowdStrike Falcon Intelligence, você deve baixá-lo na ServiceNow Store e adicionar o ID do cliente e o segredo do cliente apropriados.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

- A aplicação Central de segurança do Inteligência contra ameaças deve ser instalada e ativada.
- Obtenha o ID do cliente da API e o segredo do cliente da API no seu perfil do CrowdStrike Falcon Intelligence.
- Nos escopos da API do portal CrowdStrike Falcon Intelligence, habilite a configuração de leitura para indicadores (Falcon Intelligence).

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de ameaças**.
6. Clique em **Configurar Novo Aprimoramento** para configurar **CrowdStrike Falcon Intelligence** integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, CrowdStrike Falcon Intelligence.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, CrowdStrike Falcon Intelligence.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento.
Configuração de integração	
ID de cliente	O ID do cliente que você obteve do CrowdStrike.
Segredo do cliente	A chave secreta do cliente que você obteve do CrowdStrike.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do CrowdStrike Falcon Intelligence é desabilitado.
9. Clique em **Habilitar** Para habilitar a integração do CrowdStrike Falcon Intelligence.

Resultado

Depois de configurado, o CrowdStrike Falcon Intelligence pode ser selecionado para executar pesquisas em observáveis na Central de segurança da Inteligência contra ameaças.

TISC Security Tools - EDR

As integrações de EDR (Endpoint Detection and Response, detecção e resposta de endpoint) do TISC se concentram na identificação e resolução de ameaças à segurança em um nível de endpoint.

As soluções de rede EDR preveem e antecipam as ameaças emergentes e ajudam a melhorar a postura de segurança geral da organização.

Ao integrar com outras ferramentas de segurança, como EDR, o TISC permite o monitoramento proativo de ameaças em endpoints e, assim, melhora a postura geral de segurança e a resiliência contra ameaças em evolução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

CrowdStrike Integração do Falcon EDR

CrowdStrike Integração do Falcon EDR

Integração com CrowdStrike O Falcon EDR permite monitoramento contínuo e alertas em tempo real com base na inteligência do TISC.

Essa integração pode ajudar a simplificar as operações de segurança e reduzir qualquer risco potencial para os negócios da organização.

Configure a integração do Crowdstrike Falcon EDR

Antes de poder usar CrowdStrike Integração do Falcon EDR, você deve baixá-lo do ServiceNow Store Armazene e adicione o ID do cliente e o segredo do cliente apropriados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

- A aplicação Central de segurança do Inteligência contra ameaças deve ser instalada e ativada.
- Obtenha o ID do cliente da API e o segredo do cliente da API de CrowdStrike Console do Falcon.
- Em CrowdStrike Escopos da API do portal Falcon, habilite o. **IOC Management: Acesso de leitura e gravação** .

Procedimento

1. Usando sua instância, acesse **Central de segurança do Inteligência contra ameaças** .
2. Baixe a integração do ServiceNow Store.
3. Selecionar **Integrações** > **Ferramentas de segurança** > **EDR**.
4. Clique em **Configurar a nova ferramenta de segurança** para configurar CrowdStrike Integração do Falcon EDR.
5. Selecione **CrowdStrike Falcon EDR** opção.
6. Preencha os campos no formulário Configurar nova ferramenta de segurança.

Criar nova integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração da ferramenta de segurança. Por exemplo, CrowdStrike Falcon EDR.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, CrowdStrike Falcon EDR.
Descrição	Insira a descrição da nova integração da ferramenta de segurança.
Tipo de Integração	Opção que exibe o tipo de integração.
Categoria de integração	Opção que exibe a categoria de integração.
Configuração de integração	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL base	A URL base é a URL base da API do CrowdStrike. O valor padrão é https://api.crowdstrike.com . Para obter mais informações, consulte https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40 .
ID de cliente	O ID do cliente obtido de CrowdStrike. Para obter mais informações, consulte https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Segredo do cliente	A chave secreta do cliente que você obteve de CrowdStrike. Para obter mais informações, consulte https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Período de expiração em dias para qualquer tipo de observáveis	O período de expiração em dias que são aplicados a qualquer tipo de observável(s) quando eles são enviados para CrowdStrike EDR. **Nota:** Esta opção é um período de expiração de fallback quando o tempo de expiração não está definido para nenhum tipo de observável específico.
Tempo de expiração do observável de IP	O período de expiração em dias que são aplicados ao tipo de IP do observável quando eles são enviados para CrowdStrike EDR.
Tempo de expiração do Observable de domínio	O período de expiração em dias que são aplicados ao tipo de domínio do observável quando eles são enviados para CrowdStrike EDR.
Tempo de expiração do observável de hash	O período de expiração em dias que são aplicados ao tipo de hash do observável quando eles são enviados para CrowdStrike EDR.

7. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o CrowdStrike O status da integração do EDR é desabilitado.
8. Clique em **Habilitar** para habilitar o. CrowdStrike Integração de EDR.

Nota: Várias configurações são permitidas para CrowdStrike Integração do Falcon EDR.

Enviar observáveis para EDR

Enviar observáveis para a ferramenta de segurança EDR.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

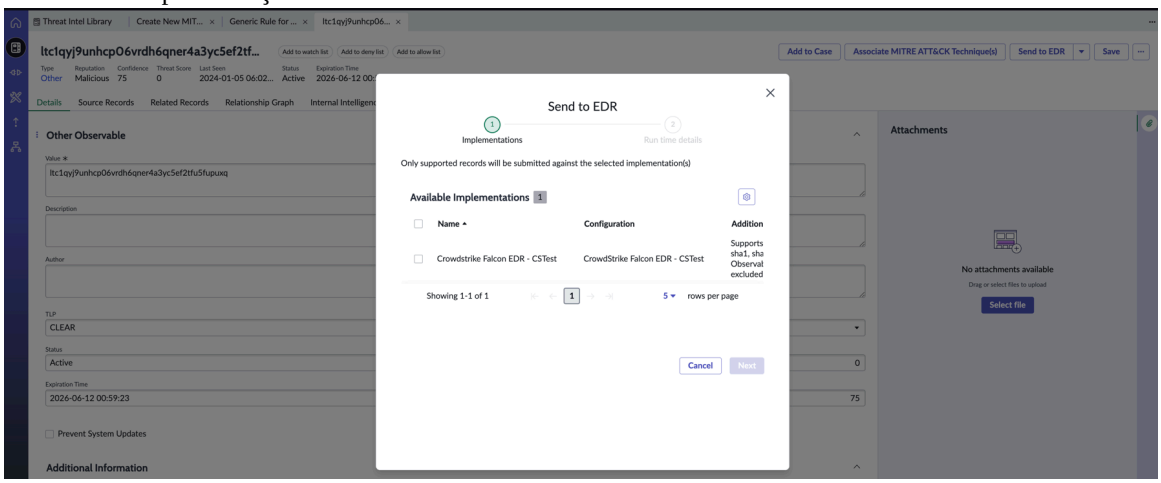
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone.

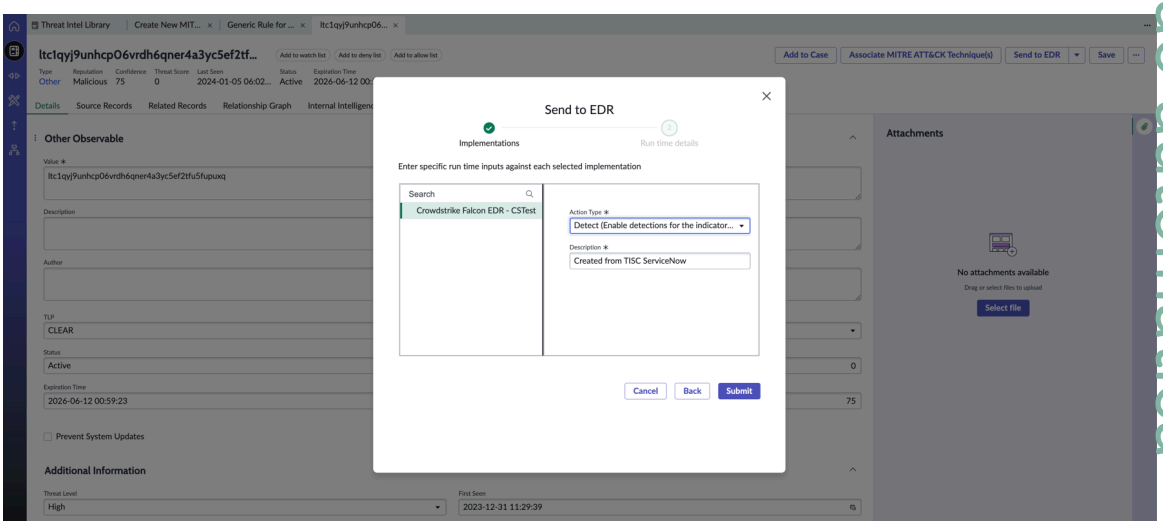
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Selecione **Enviar para EDR** .
   Enviar para EDR **Implementações** a tela modal é exibida.
6. Selecione a implementação necessária na lista.



7. Clique em **Avançar**.
8. Selecione os detalhes do tempo de execução, como **Tipo de ação** e. **Descrição** da implementação.



As opções disponíveis para CrowdStrike durante a implementação, os detalhes do tempo de execução são:

- **Nenhuma ação (Salve o indicador para uso futuro, mas não execute nenhuma ação)** : Na exibição do formulário observável, a gravidade da ameaça do observável é opcional para CrowdStrike Falcon EDR.
- **Detectar (habilitar detecções para o indicador na gravidade da ameaça do registro)** : Na exibição do formulário observável, a gravidade da ameaça é obrigatória para CrowdStrike Falcon EDR. A gravidade da ameaça do observável não deve ficar vazia para esse observável selecionado.

9. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação selecionada é executada e uma mensagem informativa é exibida A execução de Envio do Observável para EDR foi iniciada.

Nota:

- Quando a execução é iniciada ou concluída, anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.
- **Enviar para EDR** a ação também está disponível na lista de observáveis em **Artefatos** guia para um registro de caso. Para obter mais informações, consulte Adicionar artefatos a caso(s) ou tarefa(s) de caso(s).

Integração do Microsoft Defender para EDR

A integração com o Microsoft Defender para EDR permite que os analistas de Inteligência contra ameaças cibernéticas (CTI) enviem automaticamente endereços IP, domínios, hashes de arquivo e URLs maliciosos ou suspeitos para o Microsoft Defender para monitoramento contínuo e alertas em tempo real.

Registre e configure o Microsoft Defender no Microsoft Azure portal

Registre o Microsoft Defender EDR no Microsoft Azure e conceder acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: Desenvolvedor de aplicações, administrador de locatário.

Procedimento

1. Faça login no portal do Microsoft Azure.
2. Insira Registros de aplicações Na caixa Pesquisar e clique em **Clique em Novo registro** .
3. Insira um nome para sua aplicação e o URI de redirecionamento e clique em **Registre-se** .
   Um exemplo de nome é Microsoft Defender para Endpoint . O URI de redirecionamento é usado ao fornecer consentimento do administrador para a aplicação.
4. Em **Registros de aplicações** , selecione a aplicação que você registrou na Etapa 3.
5. Em Gerenciar, selecione **Certificados e segredos** .
6. Para criar um segredo do cliente, selecione **Novo segredo do cliente** .
7. Copie o segredo do cliente e salve-o.

   Caso você tenha esquecido o segredo do cliente, poderá gerar um novo segredo do cliente.
8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique em **Adicione uma permissão** .
10. Na janela Solicitar permissões da API, clique em **APIs que minha organização usa** guia.
11. PESQUISE e selecione **WindowsDefenderATP** .
12. Em Permissões WindowsDefenderATP, selecione **Permissões da aplicação** .
    Habilitar esta permissão garante que a aplicação seja executada como um serviço em segundo plano ou daemon sem um usuário conectado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

13. Adicione a seguinte permissão de nível de aplicação e conceda o consentimento do administrador para a permissão de API recém-adicionada.

Permissão	Nome de exibição da permissão
ReadWrite.All	Indicadores de leitura e gravação

Instale e configure o Microsoft Defender para integração EDR

Instale e configure a integração do Microsoft Defender para EDR na ServiceNow Store.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

- Central de segurança de inteligência contra ameaças A aplicação deve ser instalada e ativada na ServiceNow Store.
- Obtenha o ID do locatário da API, o ID do cliente e o segredo do cliente no console do Microsoft Defender para EDR.

Procedimento

1. Baixe a integração do Microsoft Defender para EDR na ServiceNow Store e instale-a.
2. Usando sua instância, acesse `Central de segurança de inteligência contra ameaças`.
3. Baixe a integração do ServiceNow Store.
4. Selecionar **Integrações** > **Ferramentas de segurança** > **EDR**.
5. Clique em **Configure a nova integração da ferramenta de origem** .
6. Selecione **Microsoft Defender para EDR** opção.
7. Clique em **"Selecionar"**.
8. No formulário, preencha os campos a seguir.

Configure o Microsoft Defender para integração EDR

Campo	Descrição
Nome	Nome da nova configuração de integração da ferramenta de segurança. Por exemplo, integração do Microsoft Defender para EDR.
Categoria de integração	Opção que exibe a categoria de integração.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão.
Tipo de Integração	Opção que exibe o tipo de integração.
Descrição	Insira a descrição da nova configuração de integração da ferramenta de segurança.
Configuração de integração	
URL base	A URL de base é a URL de base da API do Microsoft Defender para EDR. O valor padrão é https://api.securitycenter.microsoft.com/ .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID de locatário	O ID do locatário que você obteve do Microsoft Defender.
ID de cliente	O ID do cliente que você obteve do Microsoft Defender.
Segredo do cliente	A chave secreta do cliente que você obteve do Microsoft Defender.
Título pré-preenchido (usado durante o envio)	O título preenchido previamente define o título padrão usado durante o envio de observáveis para o Microsoft Defender. Esses detalhes são exibidos por padrão, portanto, você não precisa inseri-los novamente sempre que enviar para o EDR.
Descrição pré-preenchida (usada durante o envio)	A descrição pré-preenchida define o título padrão usado durante o envio de observáveis para o Microsoft Defender. Esses detalhes são exibidos por padrão, portanto, você não precisa inseri-los novamente sempre que enviar para o EDR.
Período de expiração em dias para qualquer tipo de observáveis	O período de expiração em dias que é aplicado para observáveis quando eles são enviados para o Microsoft Defender EDR. **Nota:** Esta opção é um período de expiração de fallback quando o tempo de expiração não está definido para nenhum tipo de observável específico.
Período de expiração em dias para o tipo de IP de observáveis	O período de expiração em dias que é aplicado ao tipo de IP do observável quando eles são enviados para o Microsoft Defender EDR.
Período de expiração em dias para o tipo de domínio de observáveis	O período de expiração em dias que é aplicado ao tipo de domínio de observável quando eles são enviados para o Microsoft Defender EDR.
Período de expiração em dias para o tipo de hash de observáveis	O período de expiração em dias que é aplicado ao tipo de hash do observável quando eles são enviados para o Microsoft Defender EDR.

9. Clique em **Salvar** depois de adicionar as informações de configuração necessárias.
10. Clique em **Habilitar** Para habilitar a configuração, depois de salvar a nova integração do Microsoft Defender EDR.
    Uma mensagem de confirmação é exibida informando que a integração de aprimoramento foi habilitada com sucesso.

Resultado

Depois que a integração estiver configurada, você poderá selecionar qualquer tipo de observável compatível com o Microsoft Defender EDR na Biblioteca Intel de ameaças e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

enviar observáveis para o EDR. Para obter mais informações, consulte Enviar observáveis para EDR.

Propriedades do sistema do Microsoft Defender EDR

Os detalhes a seguir detalham as propriedades do sistema do Microsoft Defender EDR.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Catálogo de propriedades do Glide** > **Propriedades do Glide**.
2. PESQUISE propriedades do Microsoft Defender.

Propriedade	Descrição
sn_tisc_defender.rate_limiter.minute	Isso permite que os usuários limitem a taxa de envio de EDR para o MS Defender minuciosamente. ○ Tipo: Número Inteiro ○ Valor: 100
sn_tisc_defender.rate_limiter.hour	Isso permite que os usuários limitem a taxa de envio de EDR para o MS Defender por hora. ○ Tipo: Número Inteiro ○ Valor: 1500

Enviar observáveis para EDR

Enviar observáveis para a ferramenta de segurança EDR.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Selecione **Enviar para EDR** .
   Enviar para EDR **Implementações** a tela modal é exibida.
6. Selecione a implementação necessária na lista.
   Por exemplo, selecione a implementação associada ao Microsoft Defender EDR.
7. Clique em **Avançar**.
8. Selecione os detalhes do tempo de execução, como **Título** e. **Descrição** da implementação.
9. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação selecionada é executada e uma mensagem informativa é exibida A execução de Envio observável para EDR foi iniciada e os resultados dessa execução estarão disponíveis no Fluxo de atividades após a conclusão da execução.

Nota: Quando a execução é iniciada ou concluída, anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário e você pode verificar o andamento da execução de acordo.

TISC Security Tools - Firewall

TISC Security Tools - Firewall impede o acesso não autorizado à rede. A integração do Palo Alto com o TISC ajuda a bloquear endereços IP, URLs e domínios mal-intencionados usando recursos de Lista dinâmica externa (EDL) com ServiceNow Dados da Inteligência contra ameaças.

No TISC, integrando com outras ferramentas de segurança, como Palo Alto Networks aprimora a segurança de rede geral da organização.

Integração da Palo Alto Networks

Uma vez configurada, a integração da Palo Alto Networks permite que o analista de ameaças adicione endereços IP, URLs e domínios mal-intencionados à Lista dinâmica externa (EDL) ou remova essas entradas da EDL depois de confirmadas como não mal-intencionadas ou limpas.

Um EDL é um arquivo de texto hospedado em um servidor web externo. Para esta integração, este servidor web é seu ServiceNow AI Platform Instância, que permite que o Firewall da Palo Alto Networks importe objetos incluídos na lista, endereços IP, URLs e domínios.

Criar novo EDL para Palo Alto Networks

Crie uma nova lista dinâmica externa (EDLs) para a Palo Alto Networks. Depois de criar EDLs, você pode começar a criar entradas para esses EDLs.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Depois de salvar a configuração do Palo Alto NGFW recém-configurada, navegue até **EDLs** seção.
2. Clique em **Novo** Para criar uma nova Lista dinâmica externa (EDLs).
3. No formulário, preencha os campos.

Formulário Lista dinâmica externa do firewall da Palo Alto Networks

Campo	Descrição
Nome	Nome da lista dinâmica do firewall da Palo Alto Networks.
Tipo de Observável	Selecione um tipo de observável que este EDL aceita na lista de seleção: IP (incluindo CIDR), URL ou domínio.
Período de expiração (dias)	Período de expiração do EDL. 0 (o padrão) indica que a entrada EDL nunca expira. Se você mudar este valor, esta entrada ficará ativa para o número de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	dias que você inserir. Você pode inserir um valor mínimo de 1 e não há valor máximo. Por exemplo, se você inserir 30 Às 2:01 PM em 1 de novembro, o EDL expirará às 2:01 PM em 30 de novembro. Em seguida, todas as entradas neste EDL herdam este valor por padrão, a menos que você substitua o valor na base de entrada individual.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em seu ServiceNow AI Platform Que estão anexadas ao registro EDL. A solicitação de mudança é usada para configurar o URL de recuperação da lista EDL no servidor Firewall de última geração da Palo Alto Networks. Esta opção é recomendada se o administrador do firewall também estiver usando o. ServiceNow AI Platform para mudanças de regra ou política de firewall. Se você criar uma solicitação, depois que ela for fechada, a lista EDL será ativada automaticamente.
Descrição	Lista dinâmica de firewall da Palo Alto Networks. Geralmente, o nome contém os tipos de locais e observáveis que você esperaria estar neste EDL, e você pode usar este campo para obter mais detalhes.
Solicitação de Mudança	Quando a caixa de seleção Criar solicitação de mudança é marcada, o número da solicitação de mudança é exibido no ServiceNow AI Platform Uma vez que o EDL é salvo. Quando a caixa de seleção para **Criar solicitação de mudança** está limpo, este campo não é exibido.
Combine endereços IP e de sub-rede em uma entrada única	Opção para combinar endereços IP e endereços de sub-rede em uma única entrada. Se você marcar esta caixa de seleção e o IP do tipo CIDR for adicionado, ele removerá automaticamente as entradas existentes que estão no intervalo CIDR. Por exemplo: Se houver uma entrada no EDL com o valor 192.168.1.1 e se um valor de CIDR 192.168.1.0/24 for adicionado ao mesmo EDL, a entrada de endereço IP inicial será removida, já que

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	está dentro do intervalo de CIDR da nova entrada. **Nota:** Esta opção é exibida somente quando você seleciona **Tipo de observável** IP.
URL de recuperação da EDL	O link da URL que o administrador do firewall da Palo Alto Networks usa para configuração no firewall da Palo Alto Networks é gerado e exibido automaticamente.

4. Crie e adicione mais EDLs conforme necessário.
   Os EDLs são exibidos na lista Listas dinâmicas externas da Palo Alto Networks.

Tópicos relacionados

Regras de aprovação de EDL de Palo Alto

Regras de aprovação de EDL de Palo Alto

As regras de aprovação permitem que os usuários ativem o fluxo de trabalho de aprovação necessário para aprovar ou rejeitar as entradas de EDL.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

O administrador do TISC define essas regras de aprovação para conceder consentimento nas solicitações de aprovação. Como administrador do TISC, você também pode definir vários níveis de aprovação aqui.

Procedimento

1. Depois de salvar a configuração do Palo Alto NGFW recém-configurada, navegue até **Regras de aprovação de EDL** seção.
2. Clique em **Novo** para criar uma nova regra de aprovação.
   As regras a seguir são as regras pré-configuradas no sistema de base para a integração do Palo Alto NGFW.

Regras de aprovação de EDL pré-configuradas

Nome	Descrição	Ação de EDL
Regra de aprovação para adicionar ao EDL	Esta regra de aprovação permite que os usuários ativem o fluxo de trabalho de aprovação para adicionar entradas ao EDL.	Adicionar à EDL
Regra de aprovação para remover do EDL	Esta regra de aprovação permite que os usuários ativem o fluxo de trabalho de aprovação para remover entradas do EDL.	Remover da EDL

3. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar novas regras de aprovação de EDL

Campo	Descrição
Nome	Nome da regra de aprovação.
Ação de EDL	Opção para adicionar ou remover a entrada EDL.
EDLs	Selecione os EDLs que exigem aprovação. Se você deixar este vazio, ele incluirá todos os EDLs.
Descrição	Insira a descrição da regra de aprovação.
Selecione Usuário ou Grupos que requerem aprovação	
Usuário(s)	Selecione o(s) usuário(s) que requer aprovação.
Grupo(s)	Selecione o(s) grupo(s) que requer aprovação.
Selecionar aprovadores	
Usuário(s)	Selecione o(s) usuário(s) para aprovação.
Grupo(s)	Selecione o(s) grupo(s) para aprovação.
Notificações	
Notificar solicitante sobre aprovação	Marque esta caixa de seleção para notificar o solicitante sobre a aprovação de EDLs.
Notificar solicitante sobre rejeição	Marque esta caixa de seleção para notificar o solicitante sobre a rejeição de EDLs.

4. Clique em **Salvar** validar e salvar a regra de aprovação.
5. Clique em **Habilitar** para habilitar a regra de aprovação.

Adicionar observáveis ao EDL

Adicione observáveis como IPs, domínios e hashes à Lista dinâmica externa (EDLs).

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique em **Adicionar ao EDL** .
   A tela modal Adicionar ao EDL é exibida.

Remover observáveis do EDL

Remover observáveis do EDL.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique em **Remover do EDL** .
   A tela modal Remover do EDL é exibida.

Aprovar entradas de EDL para Palo Alto Networks

A aprovação de entradas da Lista dinâmica externa (EDL) faz parte da pré-configuração. Você deve aprovar as entradas de EDL antes que as entradas sejam ativadas nos EDLs para que o firewall recupere a entrada e aplique a política de segurança.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada de EDL não é ativada ou desativada no EDL até que seja aprovada.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Workbench do analista de ameaça**.
2. Detalhar até **PAN NGFW** E selecione o registro EDL para aprovação.
3. Vá para **Minhas aprovações** .
4. Selecione o(s) registro(s) EDL(s) para aprovação.
5. Clique em **Aprovar**.
6. Em **Minha aprovação** , clique em um item no **Estado** coluna para abri-la.
7. Escolha a opção para aprovar a entrada de EDL.

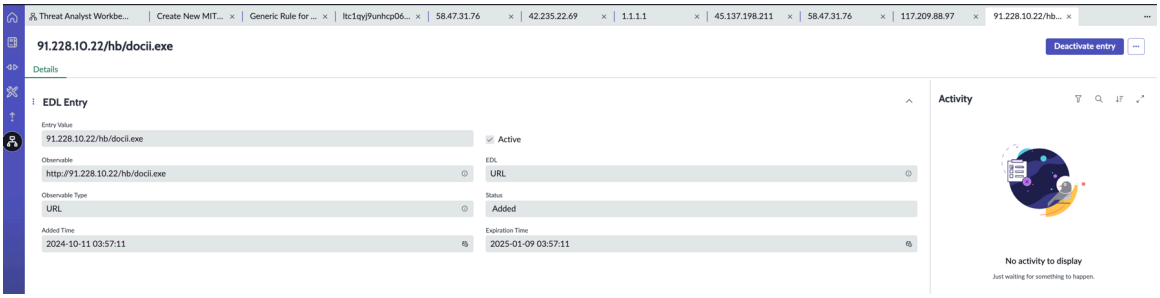
Opção	Descrição
Aprovar	No registro de entrada, **Status** o campo muda para Adicionado e **Ativo** a caixa de seleção está marcada. . **Desativar** o botão é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada EDL foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para **Rejeitado** e **Ativo** a caixa de seleção está desmarcada indicando que a entrada não está bloqueada no firewall. As anotações de trabalho mostram que a solicitação da entrada EDL foi rejeitada.

Depois de aprovar a entrada de EDL e ela ser ativada, a Palo Alto Networks recupera a entrada de EDL após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

partir desse ponto em diante. Na figura a seguir, observe que **Ativo** Está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.



Complemento do TISC para visão geral do Splunk

Central de segurança de inteligência contra ameaças (TISC) para Splunk O app oferece integração entre o TISC e Splunk Que permite que os usuários importem perfeitamente a inteligência contra ameaças mais recente do TISC para Splunk para monitorar e enriquecer alertas. Os usuários podem configurar coleções de indicadores, executar pesquisas e utilizar painéis para analisar correspondências de pesquisa e coleções de indicadores com eficácia.

Integração do TISC com Splunk

A integração entre Central de segurança de inteligência contra ameaças(TISC e. Splunk permite que os usuários filtrem e extraiam dados observáveis relevantes de inteligência contra ameaças para Splunk. Em Splunk, os usuários podem usar esses dados para gerar alertas de segurança.

Função necessária: administrador do Splunk

Usando o. TISC aplicação complementar, você pode configurar o intervalo no qual pode extrair observáveis de ServiceNow TISC instância.

Este intervalo determina com que frequência a aplicação pode fazer solicitações ServiceNow e recuperam os dados de observáveis. Além disso, você pode definir e aplicar filtros para especificar os observáveis que você deseja extrair do ServiceNow TISC instância.

Depois que os observáveis são extraídos de ServiceNow, os dados observáveis são armazenados em Splunk KV Store (armazenamento de chave-valor) e você pode escrever ainda mais as regras de correlação sobre o conjunto de observáveis que foram extraídos.

Criando usuários na ServiceNow TISC instância

Você pode criar usuários no ServiceNow TISC instância com qualquer função de usuário válida: sn_sec_tisc.api_obs_read_access.

Instalar TISC App de complemento no Splunk

Para obter mais informações, consulte Atribua uma função a um usuário .

Função necessária: Splunk administrador.

1. Faça login em *Splunk*.
2. Navegar até **Apps** > **Gerenciar apps** ou clique em **Gerenciar** ícone de engrenagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. PESQUISE *Central de segurança de inteligência contra ameaças* **para** *Splunk* e instale-o.
4. Uma vez instalada, a aplicação ficará visível na lista de aplicações.

Configurando TISC complemento em Splunk

Siga este procedimento abaixo para configurar a aplicação.

Antes de Iniciar
Função necessária: administrador do Splunk

Por Que e Quando Desempenhar Esta Tarefa
O procedimento abaixo descreve a configuração do complemento TISC no Splunk.

Procedimento

1. Pesquisar **Central de segurança de inteligência contra ameaças para Splunk** aplicativo na navegação à esquerda.
2. Clique em **Configurar** em **Ações** coluna.
   . **Configuração** é exibida e você pode configurar seu ServiceNow TISC conta.
3. Selecione **Adicionar**.
4. No formulário, preencha os campos.

Campo	Descrição
Adicionar Contas	
Nome	Um nome exclusivo para a conta.
Nome de usuário	Forneça seu ServiceNow nome de usuário da conta. Você pode usar o mesmo nome de usuário usado para os usuários criados durante a criação da função sn_sec_tisc.api_obs_read_access na etapa acima.
Senha	Fornecer ServiceNow senha da conta.
URL da Instância	Forneça o. ServiceNow Endereço da URL da instância.

5. Clique em **Adicionar**.
   . ServiceNow a conta de instância é adicionada ao Splunk.
6. Navegue até **Entradas** página para criar coleções gerencie suas entradas de dados para seu ServiceNow conta.
7. Clique em **Criar nova entrada** .
   . **Adicionar entrada** a caixa de diálogo é exibida para você adicionar as entradas ao seu ServiceNow conta.

   Depois que o conjunto de entradas é definido, a aplicação envia as informações para TISC instância para recuperar um número específico de observáveis que atendem aos critérios.
8. Preencha os detalhes de entrada, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Um nome exclusivo para sua entrada. Por exemplo, lista de IPs mal-intencionados.
Conta	Forneça seu ServiceNow nome de usuário da conta. Você pode usar o mesmo nome de usuário usado para os usuários criados com a função `sn_sec_tisc.api_obs_read_access` na etapa acima.
Intervalo	Defina o intervalo de tempo em segundos para recuperar os dados TISC.
Período de vencimento (em dias)	Opção para definir o período de expiração em dias. **Nota:** A expiração da amostra é definida como 30 dias. Por exemplo, quando os dados são extraídos em uma data específica, um conjunto de 10 000 registros pode ser recuperado. Esses registros serão armazenados no armazenamento KV (Key-Value) em Splunk. A partir da data de ingestão, os registros serão retidos por 30 dias. No 31º dia, eles serão excluídos automaticamente do armazenamento do KV.
Nunca expira	Escolha esta opção se você não quiser expirar os registros ingeridos.
Atributos Adicionais	Permite adicionar atributos adicionais da lista de opções recomendadas para incluir no armazenamento de KV. Os atributos devem ser separados por vírgulas. Uma lista de atributos permitidos é fornecida na tabela após a tabela Atributos obrigatórios.
Filtros	Defina as condições com base nas quais os dados que devem ser importados serão filtrados. Para definir as condições do filtro, você pode definir os critérios com base nos campos, como pontuação de ameaça, nível de confiança e tipo. Para condições de filtro simples, você pode usar esta opção de filtragem. No entanto, se as condições de filtro forem mais complexas e para qualquer filtragem avançada, você poderá optar por adicionar filtros JSON. ○ Os operadores inteiros permitidos são: "=", "!=", ">", "<", ">=", "<="

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Os operadores de cadeia de caracteres permitidos são: "", "!", "IN" **Abaixo está um exemplo de um filtro simples** : {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	Os filtros baseados em JSON permitem definir condições mais complexas. O status do objeto JSON deve ser Ativo. Selecione **JSON** Caixa de seleção Filtros para alternar para filtros avançados em que um JSON pode ser usado para aplicar a condição de filtro.

Filtro avançado de amostra :

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}
```

Nota: As contas estão ativas por padrão, mas as entradas estão inativas por padrão. Você deve ativá-las para começar a importar os dados. Para obter possíveis filtros, consulte a seção observable_filters em Adiciona registros de origem observáveis à Central de segurança de inteligência contra ameaças (TISC) aplicação.

9. Clique em **Adicionar** para adicionar as entradas.
10. Clique em **Clone** ou copiar para copiar e criar uma nova conta com base na conta existente. Certifique-se de que a entrada esteja desativada antes da clonagem para evitar a criação de entradas duplicadas ao importar dados usando os mesmos critérios.
11. Depois que os dados forem extraídos, as seguintes informações serão recuperadas e armazenadas no armazenamento de KV em Splunk Junto com os registros extraídos do TISC:

Campo	Descrição
confiança	Indica o nível de confiança associado à precisão da pontuação de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
kvlookup_created_time	Indica a hora de criação do registro no armazenamento de valor de chave.
kvlookup_days_till_expiration	Indica o número de dias após os quais o registro será excluído do armazenamento do KV.
instance_url	Indica ServiceNow Endereço da URL da instância.
reputação	Indica a reputação da entidade envolvida.
source_reported_score	A pontuação de origem relatada de TISC.
sys_id	Sys ID do registro que está chegando TISC.
threat_level	Indica o nível de gravidade da ameaça.
threat_score	A pontuação que indica o nível de ameaça associada a um registro.
threat_severity	Indica a gravidade da ameaça do observável.
tipo	Indica o tipo de observáveis.
updated_by	Fornece as informações sobre quem atualizou o registro pela última vez.
kvlookup_updated_time	Indica o carimbo de data/hora em que o registro foi atualizado pela última vez no armazenamento de valor de chave.
valor	Valor do registro. Por exemplo, IP, hash e assim por diante.

Atributos Adicionais

Campo	Descrição
adicional_context	Forneça qualquer contexto adicional, conforme necessário.
attack_phases	Indica fases de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
autor	Forneça o nome do autor.
comentários	Adicione comentários adicionais conforme necessário.
criado(a)	Indica quando o observável foi criado.
descrição	Forneça a descrição.
expiration_time	Especifica o tempo de expiração do registro observável.
extensões	Indica as extensões de um observável.
first_observed	A primeira vez em que os dados foram observados.
first_seen	A primeira vez que este registro foi visto realizando atividades mal-intencionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
historicamente_significativo	Indica se o observável é considerado historicamente significativo. Este sinalizador do sistema TISC é usado para excluir o observável do arquivamento.
id	Identificador exclusivo atribuído ao observável pelo sistema TISC.
_defanged	Sinalizador que indica se o valor do observável foi depurado.
é_falso_positivo	Um sinalizador booliano que indica se o observável é identificado como falso positivo.
idioma	Indica o idioma do conteúdo de texto neste objeto.
last_observed	A última hora em que os dados foram observados.
last_seen	A hora em que este objeto foi visto pela última vez executando atividades mal-intencionadas.
anotações	Adicione anotações adicionais para um registro observável.
número	Número gerado pelo sistema atribuído ao observável pelo TISC.
security_type	Especifica se o observável pertence à Lista de permissões ou à Lista de proibições.
_de_origens	Representa o número de fontes exclusivas que contribuíram para o observável.
origens	Especifica a origem da ameaça a partir da qual este registro é criado.
status	Insira o status do observável se ativo ou inativo.
tisc_tags	Selecione os marcadores TISC associados a um observável.
taxonomias	Selecione a taxonomia associada a um observável.
tlp	Valor exclusivo que indica a configuração de confidencialidade de dados por TLP.
atualizado	Indica quando o registro do observável foi atualizado pela última vez
usage_categories	Categorias nas quais o observável se enquadra, como botnet ou phishing.
watch_list	Sinalizador que especifica se o observável está incluído na lista de observação.

, esses campos, juntamente com quaisquer outros definidos por seus critérios, estarão disponíveis em Splunk e podem ser exibidos, pesquisados e analisados por meio da guia de pesquisa.

Armazenamento de dados em Splunk

Esta seção descreve como TISC Utiliza pesquisas durante a integração no armazenamento de chave-valor do Splunk para armazenamento de dados. Ele detalha como essas pesquisas são configuradas e recuperadas em Splunk.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisar	Descrição da pesquisa
tisc_store_lookup	Nome da pesquisa de KV a ser usada para pesquisar os registros de entrada.
tisc_kv_store	Nome do armazenamento de KV onde os dados residem.
inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup	Consulta para pesquisar registros no armazenamento do KV.

TISC - Integração do Microsoft Sentinel

Central de segurança de inteligência contra ameaças O para Microsoft Sentinel oferece vários recursos, incluindo a importação de observáveis do TISC Para o Sentinel, enriquecendo os incidentes do Sentinel com detalhes de observáveis relacionados e também permita exportar observáveis do Sentinel para TISC.

Nota: No Microsoft Sentinel, observáveis são chamados de entidades.

Pré-requisitos

Dependências

. **Inteligência contra ameaças** A solução do Microsoft Sentinel Content Hub deve ser instalada.

Funções e permissões

Aplicação	Funções e permissões	Descrição
Funções específicas do Microsoft Sentinel	1. Colaborador do aplicativo lógico 2. Colaborador do Microsoft Sentinel	1. Para instalar os playbooks necessários em um nível de Grupo de recursos. 2. Interaja com os playbooks do Microsoft Sentinel. Para obter mais informações, consulte Funções e permissões No Microsoft Sentinel.
Central de segurança de inteligência contra ameaças	sn_sec_tisc.api_azure_sentinel_solution	O usuário configurado no Conector personalizado do TISC deve ter esta função para permitir acesso às APIs do TISC.

Modelos de playbook do TISC

Esta seção descreve os modelos de playbook que são enviados com a solução TISC Sentinel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos de uso do Playbook

A tabela a seguir descreve os vários casos de uso do playbook.

Caso de uso	Playbook	Descrição
Importação de observáveis do TISC para o Sentinel	Batch_Indicator_Uploader	Fornece mecanismo em lote para exportar observáveis do TISC usando a API de indicadores de carregamento fornecida pelo Microsoft Sentinel.
	Import_observables_Batch	Habilita a exportação programada de observáveis do TISC.
Exporte entidades do Sentinel para o TISC	Export_Incident_Entities	Exporte todas as entidades de um incidente do Sentinel.
	Export_Hash_Entity	Exporte entidades de hash de arquivo do incidente do Sentinel.
	Entidades Export_Domain_Entity	Exporte entidades de domínio do incidente do Sentinel.
	Export_ip_entity	Exporte entidades IP do incidente do Sentinel.
	Export_url_entity	Exportar entidades de URL do incidente do Sentinel.
Enriquecer incidentes do Sentinel	Incident_RICHRICH	Habilita o aprimoramento de incidentes do Sentinel buscando detalhes relacionados a entidades associadas a ele e publicando informações na forma de comentários sobre o incidente.

Nota: Todos os playbooks usam o Conector personalizado do TISC internamente para usar as APIs do TISC.

Criar playbooks a partir de modelos

1. Navegue até T **Solução ISC** página de conteúdo do **Hub de conteúdo no Espaço do Sentinel** .
2. Para cada playbook mostrado na página de conteúdo, faça o seguinte:
   a. Selecione o modelo do playbook, um painel de contexto será exibido no lado direito da tela, clique em **Configuração** .
   b. Leia a descrição do modelo de playbook e passe por **Pré-requisitos** e. **Pós-implantação** etapas mencionadas na descrição.
   c. Clique em **Implantar conector personalizado** (se você ainda não implantou o conector personalizado).

      Adicione **URL da instância da ServiceNow** em **Configuração de implantação** página.

   d. Clique em **Criar Playbook** você será levado para a tela de configuração da implantação
   e. Na tela Criar configuração do playbook:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecione o grupo de recursos apropriado.
- Modifique o nome do playbook ou use o nome padrão.
- Forneça o. **nam do conector personalizado** E (certifique-se de corresponder ao nome do conector implantado na etapa anterior) na seção Parâmetros.
- Clique em **Revise e crie** .

Configure o playbook Import_Observables_Batch

Certifique-se de criar o playbook Batch_Indicator_Uploader antes de criar o playbook Import_Observables_Batch.

1. Navegar até **Designer de aplicações lógicas** para editar o playbook.
2. Atualize o tempo de recorrência (em horas) conforme necessário.
3. No componente Conector personalizado do TISC no playbook, atualize os parâmetros que são enviados para a API do TISC.

Nome do Parâmetro	Descrição
Tipo de Observável	A seguir estão os tipos compatíveis, selecione um ou mais: ○ IP ○ Hash de Arquivo ○ Domínio ○ URL
Pontuação de ameaça	Insira a pontuação de ameaça para observáveis. O valor da pontuação de ameaça DEVE ser um número no intervalo de 0 a 100.
Confiança	Insira a confiança para observáveis. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Reputação	A seguir estão os valores compatíveis, selecione um ou mais: ○ Limpar ○ Mal-intencionado ○ Suspeito ○ Desconhecido
Gravidade da ameaça	A seguir estão os níveis de gravidade compatíveis, selecione um ou mais: ○ Crítico ○ Alto(a) ○ Média ○ Baixo(a)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Parâmetro	Descrição
Nível de ameaça	A seguir estão os níveis de ameaça compatíveis, selecione um ou mais: ○ Alto(a) ○ Média ○ Baixo(a)
Delta atualizado pela última vez em horas	A hora da última atualização (em horas) dos observáveis.

Configure o playbook Export_Incident_Entities

Este playbook usa a API de adição de observáveis do TISC. Usando o Designer de aplicativo lógico, você pode editar os parâmetros que são enviados para a API do playbook. Para obter mais informações, consulte TISC - POST /sn_sec_tisc/threat_intel_data/add_observables .

Você pode seguir o mesmo procedimento para todos os playbooks listados abaixo que exportam diferentes tipos de entidades:

- Export_Hash_Entity
- Export_Domain_Entity
- Export_ip_entity
- Export_url_entity

Configure o playbook Incident_Enrichment

Este playbook usa a API Observables TISC. Usando o Designer de aplicativo lógico, você pode editar os parâmetros que são enviados para a API do playbook. Para obter mais informações, consulte TISC - POST /sn_sec_tisc/threat_intel_data/observables .

Executar playbooks

A tabela a seguir descreve como você pode executar os playbooks a seguir.

Playbook	Ação
Import_observables_Batch	Este playbook é executado automaticamente com base na hora programada mencionada no gatilho de recorrência.
Export_Incident_Entities	Em um incidente do Sentinel, selecione **Ações de incidente** > **Executar Playbook** para execução.
Export_Hash_Entity	Em um incidente do Sentinel, selecione **Entidade de hash de arquivo** > **Executar Playbook** para execução.
Export_Domain_Entity	Em um incidente do Sentinel, selecione **Entidade de domínio** > **Executar Playbook** para execução.
Export_ip_entity	Em um incidente do Sentinel, selecione **Entidade IP** > **Executar Playbook** para execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook	Ação
Export_url_entity	Em um incidente do Sentinel, selecione **Entidade de URL** > **Executar Playbook** para execução.
Incident_RICHRICH	Em um incidente do Sentinel, selecione **Ações de incidente** > **Executar Playbook** para execução.

Administração do Central de segurança de inteligência contra ameaças

Usando a navegação à esquerda para navegar até o módulo Administração em Central de segurança de inteligência contra ameaças e exibem os seguintes módulos de TISC administração de dados, para definir ainda mais regras de filtragem, regras de aprovação, definir pontuação de ameaça e gerenciar notificações.

Administração de dados

Módulo	Descrição
Mecanismo de regras	Esta seção consiste nas seguintes regras necessárias durante o gerenciamento de dados: 1. **Regras de aprovação de importações de dados** : Defina as regras de aprovação e integre o fluxo de aprovação na seção Inteligência de importação após enviar a importação de dados. 2. **Regras de filtragem de entrada** : Crie regras de filtro para filtrar os dados de registros de origem de entrada. 3. **Regra de pontuação de ameaça** : Personalize a calculadora de pontuação de ameaça que atribui pontuação de ameaça aos observáveis.
Listas de controle de segurança	Este módulo ajuda você com os controles de segurança: 1. **ListaPermissões** 2. **ListaRecusas** 3. **Lista de observadores**
Taxonomias	Este módulo ajuda você a criar taxonomias para os registros da fonte de dados.
Notificações	Este módulo define como gerenciar notificações por e-mail.
Modelos	Este módulo descreve como criar modelos de relatório no tempo de design e na experiência de tempo de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir regras de aprovação de importações de dados

Use esta seção para definir as regras de aprovação e integrar o fluxo de aprovação na seção Inteligência de importação após enviar a importação de dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Administração** ícone no espaço.
3. Ir para **Mecanismo de regras** > **Regras de aprovação de importações de dados**.
4. Selecione **Regra de aprovação para importações de dados** .

   No sistema de base, **Regra de aprovação para importações de dados** é a regra de aprovação padrão provisionada para permitir que os usuários ativem o fluxo de trabalho de aprovação.

5. Insira pelo menos um nome de usuário ou grupo de usuários para cada um **Selecione Usuário ou Grupos que exigem aprovação** e. **Selecionar aprovador(es)** seção.
6. Clique em **Habilitar** botão para habilitar o fluxo de aprovação para as importações de dados.

   Quando habilitadas, as importações de dados estarão na fila de aprovação para que o aprovador aprove ou rejeite o processamento de dados. O aprovador revisará as mudanças feitas pelo analista e aprovará ou rejeitará a solicitação de importação de dados.

   Nota: Uma notificação por e-mail é enviada para os usuários ou grupos de usuários informando que o trabalho de importação foi processado e aprovado ou rejeitado.

Definir regras de expiração

Defina regras de expiração para vários observáveis ou uma combinação de vários objetos de origem ou origem de indicadores criados no TISC.

Antes de Iniciar

Cada origem criada na aplicação tem um período de expiração. Os feeds de dados usam as técnicas, como o período de expiração baseado em tempo, para impulsionar a ingestão de dados. No TISC, as regras de expiração definem o tempo de expiração para um conjunto específico de fontes de dados ou conjunto de tipos de objetos ou tipos de observáveis.

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Regras de expiração**.
   A página Regras de expiração é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome para a regra de expiração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Insira uma descrição para a regra de expiração.
Período de expiração (dias)	Especifique o tempo após o qual os dados ingeridos devem expirar ou ser considerados desatualizados. Insira o período de vencimento do observável em dias. Por exemplo, 100 dias. **Nota:** Quaisquer que sejam os dados ingeridos da origem expirarão 100 dias após a ingestão.
Fontes de dados	Indica a regra de expiração da fonte de dados atual. Selecione a lista de fontes de dados na pesquisa. **Nota:** Não selecione este campo e deixe-o em branco se quiser selecionar todas as fontes de dados. Se você quiser selecionar o indicador como um objeto, selecione o objeto e, em seguida, selecione **Tipo de registros** valor como **Indicador** . **Nota:** Por padrão, uma regra de expiração de amostra sn_sec_tisc_m2m_entity_rules é provisionada para os usuários no sistema de base. Para observáveis, esta regra de expiração de amostra estará no estado desabilitado. Você deve habilitar e ativar a regra. Para aplicar a regra nos registros de origem, você deve habilitar a regra.
Categoria	Indica o tipo de categoria de regra de expiração para a fonte de dados atual. Selecione o tipo de categoria na lista suspensa, como observável ou objeto.
Tipo de registros	Selecione o tipo de registros.

4. Clique em **Habilitar** para habilitar a regra de expiração depois de criar uma nova regra.
Se você não habilitar a regra de expiração, a regra não será aplicada ao registro de origem.

Nota:

- Sempre que você habilita uma regra de expiração, uma verificação de duplicação acontece em segundo plano para verificar se há alguma regra duplicada no sistema com a mesma combinação de fontes de dados e Tipo de registros. Em caso afirmativo, a aplicação exibirá uma mensagem informativa informando que a regra já contém a mesma combinação de fonte de dados e categoria de objeto e você deve modificar a combinação existente para habilitar a regra.
- Uma regra de expiração de amostra é provisionada para os usuários no sistema de base e isso **Regra de expiração de amostra** o observable estará no estado desabilitado por padrão e você deve habilitar e ativar a regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Salvar**.
6. Clique em **Excluir** se você deseja excluir qualquer regra de expiração.

Regras de expiração para registros de origem

Basicamente, as regras de expiração são úteis para definir o tempo de expiração dos registros de origem. O registro agregado herda o tempo de expiração mais alto de seus registros de origens correspondentes.

Como as regras são aplicadas

Example: O tipo de registro de origem de entrada é Malware do tipo de fonte de dados CrowdStrike

Processo de avaliação de regra com base nas regras fornecidas para aplicar tempos de expiração aos registros de origem:

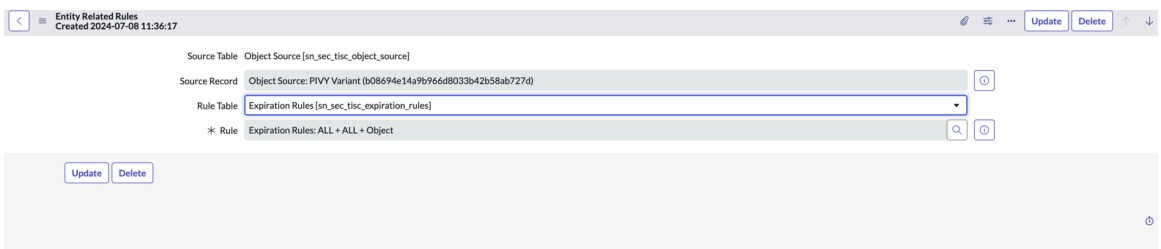
1. **Buscar todas as regras habilitadas:** A aplicação é iniciada verificando todas as regras que estão habilitadas no momento.
2. Verificar se há uma combinação de regra específica:

   Procure uma regra que corresponda especificamente à combinação de:

   - **Tipo de fonte de dados** CrowdStrike
   - **Tipo de registros** : Malware
3. **Prioridade baseada nas combinações de regras correspondentes:**

   Se houver uma regra em que o tipo de fonte de dados seja **CrowdStrike** e o tipo de registro é **Malware** esta regra tem precedência. O tempo de expiração especificado nesta regra será aplicado.

4. **Regras de fallback:**
   a. Se nenhuma regra corresponder a. **CrowdStrike e Malware** , o sistema verifica se há uma regra em que o tipo de fonte de dados é **CrowdStrike** e o tipo de registro é **Todos** .
   b. Se nenhuma regra ainda for encontrada, ele procurará uma regra em que o tipo de fonte de dados seja **Todos** e o tipo de registro é **Malware** .
   c. Por fim, se nenhuma das regras acima existir, o padrão será uma regra em que o tipo de fonte de dados e o tipo de registro são **Todos** .
5. Se nenhuma dessas regras existir no sistema, nenhuma regra de expiração será aplicada aos registros de origem. Nesse caso, navegue até a tabela abaixo (mostrada na captura de tela) para verificar a combinação de regras que foram aplicadas aos objetos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. **Exclusão de fontes de dados:**

   Se uma fonte de dados que tem as regras de expiração associadas a ela for excluída, a exclusão poderá ser restrita ou não permitida até que essas regras sejam resolvidas. Isso garante que não haja inconsistências na aplicação de políticas de expiração.

Criar regras de exclusão de dados de entrada

Crie regras de exclusão de dados de entrada para filtrar qualquer tipo de dados ou qualquer tipo de dados de registros de origem de entrada.

Antes de Iniciar

O aplicativo oferece suporte à integração de vários feeds de inteligência contra ameaças, incluindo fontes de dados STIX. Para garantir que somente dados relevantes sejam ingeridos, regras de exclusão personalizáveis devem ser aplicadas.

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

As regras de exclusão são criadas e aplicadas em um registro de origem para processar outras etapas. O sistema de base fornece o. **Regra de filtragem de amostra** para os usuários com uma regra predefinida filtrarem observáveis, dados de indicadores ou entidades/objetos ingeridos.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Detalhar até **Mecanismo de regras** > **Regras de exclusão de dados de entrada**.
3. Clique em **Novo** para definir regras de exclusão.
   A página Criar novas regras de exclusão de dados de entrada é exibida.
4. No formulário, preencha os campos.

Definir Regras de Exclusão

Campo	Descrição
Nome	Nome da nova regra de exclusão.
Descrição	Descrição resumida da regra de exclusão.
Ordem	A prioridade da regra de exclusão. Este campo indica a ordem na qual as regras de exclusão são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de exclusão com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100 para a regra de exclusão do sistema de base.
Fontes de dados	Selecione os feeds para os quais a regra de exclusão deve ser aplicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela	Selecione o tipo de tabela à qual você deseja aplicar o filtro. Por exemplo, Origem do observável, Origem do indicador e Origem do objeto.
Tipo de filtro (somente quando a tabela selecionada é Origem de observáveis)	Os tipos de filtro contêm duas opções com base nas quais você pode aplicar o filtro. ○ Filtrar com base nas condições ○ Filtro com base em lista
Tipo de filtro (filtro baseado na condição)	Condições de filtro no construtor de condições. Essas condições são baseadas na tabela de origem. Por exemplo, Origem do indicador e Origem do objeto têm somente o tipo de filtro: Filtro baseado na condição. Para adicionar mais condições, clique em **E.** ou **OU** . Se **E.** selecionado, todas as condições devem ser correspondidas. Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novo conjunto de condições** .
Tipo de filtro (filtro baseado na lista)	Se os observáveis de entrada corresponderem às entradas na lista selecionada, serão filtrados. **Nota:** Essas regras de exclusão não se aplicam às importações de dados usando o Inteligência de importação e as opções disponíveis são Lista de permissão, Lista de negação e Lista de observação.

Os registros excluídos pela regra de exclusão podem ser exibidos nas seções a seguir.

a. **Registros observáveis filtrados** : Filtra e lista os registros de observáveis.

b. **Registros de indicadores filtrados** : Filtra e lista os registros de indicadores.

c. **Registros de objeto filtrados** : Filtra e lista os registros de objeto.

Nota: Para aplicar as regras de exclusão com base em marcadores que são adicionados aos registros de origem, selecione *TISC***marcadores** No construtor Condições de filtro.

Calculadora de pontuação de ameaça personalizada no TISC

A Calculadora de pontuação de ameaça personalizada permite definir e calcular uma pontuação de gravidade de ameaça de um observável com base nos critérios definidos pelo usuário, o que fornece uma pontuação de inteligência transparente de observáveis. A pontuação de ameaça é calculada automaticamente para registros observáveis.

Calculadora de pontuação de ameaça

Defina pontuação de ameaça para os registros observáveis gerados com base nos parâmetros definidos pelo usuário. O sistema de base é provisionado com uma regra de pontuação de ameaça, que pode ser personalizada e habilitada de acordo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: Por padrão, a regra de pontuação de ameaça ficará inativa, você precisa habilitar a regra para ver a pontuação de observáveis.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Ir para **Regra de pontuação de ameaça**.
   A página Calculadora de pontuação de ameaças é exibida.

Importante:

- No aplicativo, no sistema de base, há uma regra de pontuação que é provisionada para os usuários exibirem, editarem ou modificarem a pontuação de ameaça, mas o usuário não pode criar uma nova regra ou excluir a regra de pontuação de ameaça predefinida.
- As mudanças serão aplicadas a todos os novos observáveis ou atualizações nos observáveis a partir desse ponto em diante. Para redefinir pontuações históricas, eles devem usar a opção recalcular.

3. No formulário, os campos a seguir contêm os valores predefinidos.

Padrão de Calculadora de pontuação de ameaça

Campo	Descrição
Nome	Nome do valor de pontuação da ameaça. Por exemplo, Calculadora de pontuação de ameaça.
Descrição	Descrição do registro de pontuação de ameaça. Por exemplo, calcula a pontuação de ameaça com base na soma ponderada das pontuações de critérios predefinidos.
Ponderação geral (aplicável ao construtor de critérios)	Este campo não é editável e exibe a ponderação geral calculada pelo sistema com base no peso correspondente aos critérios habilitados.
Critérios de pontuação	Indica os critérios de pontuação para um observável. Estas são as duas opções disponíveis para definir os critérios de pontuação de ameaça: ○ **Construtor de critérios** : Use esta opção para adicionar, editar ou remover e habilitar e desabilitar critérios que contribuem para o cálculo da pontuação de ameaça e garantir que a ponderação agregada total seja de 100%. ○ **Usar script (Avançado)** : O recurso de script é um recurso avançado para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	criar um script personalizado que deve retornar a pontuação de ameaça dentro do intervalo de 0 a 100.

Abaixo estão as opções disponíveis para definir o. **Critérios de pontuação** :

- Criador de critérios
- Usar script (Avançado)

Este é o procedimento para Construtor de critérios:

Nota: Você pode editar ou modificar os critérios existentes ou adicionar novos critérios.

a. Selecione o tipo de critério.
Por exemplo, Adicionar um novo critério.

b. Selecione **Tabela** para o qual os critérios estão configurados.
A lista de valores na lista suspensa é Observáveis, Agente de ameaça, Campanha, Local, Identidade, vulnerabilidade, Evento de ameaça, Incidente de segurança e Agregados. Quando você seleciona uma dessas opções na lista suspensa, uma condição é aplicada. Esta condição garante que somente registros relacionados ao valor selecionado sejam exibidos ou calculados.

Nota:

- Se o observável selecionado, a condição será aplicada no registro do observável para o qual a pontuação de ameaça será calculada. Se a tabela selecionada não for observável, a condição será aplicada somente se os registros estiverem relacionados ao observável para o qual a pontuação de ameaça será calculada.
- Uma tabela de agregados adicional é adicionada para definir as pontuações com base no número de relações associadas aos observáveis. Por exemplo, selecione a Tabela: Agregados e o valor do campo: Agentes de ameaça e, em seguida, para um observável, se houver mais de dois agentes de ameaça, defina a pontuação e aplique as condições conforme aplicável.
- Por exemplo, se você quiser definir uma pontuação para um ou mais agentes de ameaça associados a um observável, selecione o campo como Não de agentes de ameaça, defina a pontuação desejada e aplique as condições conforme aplicável.

c. Selecione **Campo** da tabela selecionada acima.

d. Insira **Ponderação** dos critérios entre 0-100.
A ponderação geral de todos os critérios deve ser de 100%.

e. Insira o nome e a descrição resumida dos critérios.

f. Selecione **Habilitar critérios de pontuação** caixa de seleção para habilitar os critérios de pontuação.

g. Defina **Condições** e definir a pontuação para as condições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

h. Você também pode adicionar novas condições usando **Nova condição** e exclua a condição usando **Excluir critérios** ícone.

i. Clique em **Adicionar** para adicionar os critérios configurados.

Este é um exemplo de definição de uma condição para uma pontuação de ameaça:

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Clique em **Recalcular Histórico** botão para recalcular a pontuação da ameaça.
Se houver mudanças na regra de pontuação de ameaça, você deverá aplicar novamente a regra de pontuação aos observáveis que têm a pontuação de ameaça já calculada no passado, use **Recalcular o histórico** botão para acionar o trabalho de recálculo.

Nota:

- Uma mensagem de confirmação será exibida para você executar a ação, Este é um processo de longa execução que é executado em segundo plano. Você não poderá fazer mudanças até que o processo seja concluído. Tem certeza de que deseja executar esta ação?
- Para quaisquer eventos de atualização gerados para observáveis como parte de **Recalcular Histórico** , o processamento de webhooks está desabilitado e, caso você queira habilitar, modifique esta propriedade do sistema `webhook_ignore_threat_score_reaplicar` .

5. Clique em **OK**.

Importante: Esta ação acionará um trabalho de longa execução e o sistema não permitirá que você faça mais mudanças na regra de pontuação de ameaça até que o trabalho seja concluído. Para obter mais informações sobre como a configuração do trabalho em segundo plano é configurada, consulte Configuração da estrutura de trabalho em segundo plano de Resposta a vulnerabilidades .

A seguir está **Usar script (Avançado)** Script: Use este script para criar um script personalizado que deve retornar a pontuação de ameaça dentro do intervalo de 0 a 100.

O campo de script avançado é preenchido automaticamente com uma função que usa os parâmetros **atual** e. **agregados** e esta função deve retornar a pontuação de ameaça no intervalo de 0 a 100.

Aqui, o parâmetro atual é o objeto GlideRecord da entidade (observável) para a qual a pontuação de ameaça está sendo calculada. Para observáveis, corresponde ao GlideRecord da tabela sn_sec_tisc_observable. O parâmetro Agregados é um objeto GlideRecord do sn_sec_tisc_agregados registro de tabela que é usado para acessar as contagens de registros dos vários tipos de registro associados (como campanhas ou identidades) para a entidade principal (observável).

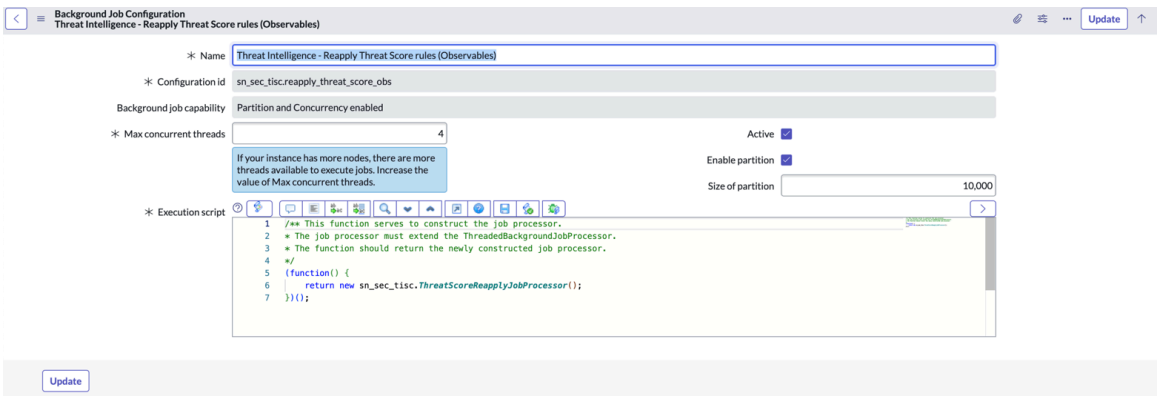
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de exemplo do script na opção avançada:

```
answer = (function threatScoreCalculator(current, aggregates) {

   // return the threat score in the range of 0-100
   var threatSeverity = current.getValue("threat_severity");
   if(threatSeverity == "high")
    return 80;
   else {
      let associatedCampaigns = aggregates.getValue("num_of_campaigns");
      if(associatedCampaigns > 0)
         return 50;
   }
   return 0;

})(current, aggregates);
```

Abaixo está a captura de tela que mostra o processo de configuração do trabalho em segundo plano de pontuação de ameaça.



Regras de extração de técnica do MITRE ATT&CK

Extraia técnicas DO MITRE automaticamente de observáveis ou objetos ingeridos de várias fontes de dados e também extraia técnicas DO MITRE dos resultados da pesquisa de ameaças no registro do observável.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: Certifique-se de verificar se os dados do repositório MITRE ATT&CK estão disponíveis na instância que você está usando. Se os dados não estiverem disponíveis, a aplicação não executará a extração.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Ir para **Mecanismo de regras** > **Regras de extração de técnica do MITRE ATT&CK**.
   A página Regras de extração da técnica MITRE ATT&CK é exibida.
3. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome para a regra de extração de técnica MITRE ATT&CK.
Descrição	Insira uma descrição para a regra de extração de técnica MITRE ATT&CK.
Tipo de Integração	Indica a regra de extração da técnica MITRE ATT&CK para as fontes de dados ou resultados da pesquisa de ameaças. Selecione a lista de fontes de dados na pesquisa. Estas são as opções disponíveis para Fontes de dados: ○ **Fontes de dados - Todas** : O que significa que a regra é aplicável a todos os tipos de fontes de dados, como Feeds da Intel contra ameaças, registros da Inteligência de importação, origens de API (por exemplo, observáveis criados a partir da API), enviados do SIR (observáveis enviados do SIR) e várias entidades criadas manualmente pelos usuários na biblioteca de Inteligência contra ameaças. ○ **Fontes de dados - Feeds da Intel contra ameaças** Corresponde às regras de extração que são aplicáveis somente aos feeds de inteligência contra ameaças. ○ **Fontes de dados - Fontes de API** Corresponde às regras de extração que são aplicáveis somente para origens de API. ○ **Integrações da Pesquisa de ameaças** : Para este tipo de opção, a regra de extração é aplicável a todas as integrações de pesquisa de ameaças, como Virustotal. **Nota:** ▪ Ao selecionar esta opção, você deve inserir o nome do fornecedor para a pesquisa de ameaças. Os nomes dos fornecedores são preenchidos automaticamente somente quando as integrações de pesquisa de ameaças são instaladas do ServiceNow store. ▪ Para as fontes de dados de inteligência contra ameaças, as regras de extração são compatíveis somente com os tipos STIX, MISP e Feed personalizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Integrações de aprimoramento de observável** : para este tipo de opção, a regra de extração é aplicável a todas as integrações de aprimoramento observável.
Tipo de feed de ameaça	Estas são as opções disponíveis para o Tipo de feed de ameaças: ○ **STIX (TAXII/HTTPS)** Opção para filtrar os feeds de ameaças do tipo de feed STIX TAXII ou HTTPS e selecionar os feeds associados na pesquisa. ○ **MISP** : Opção para filtrar os feeds de ameaça do tipo de feed MISP e selecionar os feeds associados pesquisando usando o ícone de pesquisa. ○ **Feed personalizado** : Opção para filtrar os feeds de ameaça do tipo de feed personalizado e selecionar os feeds associados pesquisando usando o ícone de pesquisa.
Feeds	Selecione uma ou mais integrações de feed de ameaças para o tipo de feed selecionado. **Nota:** Se este campo for deixado em branco, todas as integrações de feed de ameaças para o tipo de feed selecionado serão consideradas automaticamente para a extração.
Método para extrair táticas e técnicas do MITRE ATT&CK	Opção para selecionar o método Extrair táticas e técnicas DO MITRE ATT&CK. Os dois métodos disponíveis são: **a.** Usar Regex **b.** Usar script
Método de extração - Use Regex	Este método usa uma expressão regular que permite que os analistas de ameaças definam um padrão com uma sequência de caracteres para executar o método de extração.
Regex de tática	Opção para fornecer expressão regular para a extração de IDs de tática MITRE ATT&CK.
Regex de técnica	Opção para fornecer expressão regular para a extração de IDs de técnica MITRE ATT&CK.
Método de extração - Use script	Este método usa um formato de script para executar a extração na origem do observável ou na origem do objeto ou na origem do indicador ou nos resultados da pesquisa de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ○ Este método de script pode ser usado para extrair táticas e técnicas DO MITRE do registro de origem da entidade e vincular as táticas e técnicas ao próprio registro de origem da entidade. ○ Este método de script pode ser usado para extrair táticas e técnicas DO MITRE dos resultados da pesquisa de ameaças e vincular as táticas e técnicas ao registro da entidade. O script de amostra é mostrado abaixo para sua referência: `(function process(lookupResultRawData, recordGr, ruleGr, lookupResultGr) { /********** * - threatLookupResult: The raw data of the threat lookup result in stringified JSON format. * - recordGr: The GlideRecord of the observable record. * - ruleGr: GlideRecord of matched MITRE extraction rule * * Once you extracted MITRE tactic IDs and technique IDs, * then you can use this method to link the tactics and techniques to the observable record. **********/ var utils = new MITREExtractionUtils(); var parsedRawData =JSON.parse(lookupResultRawData); var mitreDataField = parsedRawData.mitre_data; var response = utils.extractMITREDataUsingRegex(mitreDataField,'TA[0-9][0-9][0-9][0-9]','T[0-9][0-9][0-9][0-9].[0-9][0-9][0-9]|T[0-9][0-9][0-9][0-9]'); utils.addTacticTechniquesForLookup(response.tacticIds, response.techniqueIds, recordGr, ruleGr.getUniqueValue(), lookupResultGr);` `})(lookupResultRawData, recordGr, ruleGr, lookupResultGr);` Here is a sample script example for

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Habilitar** Para habilitar a regra de extração de técnica MITRE ATT&CK após criar uma nova regra.
   Se você não habilitar a regra de extração de técnica MITRE ATT&CK, a regra não será aplicada ao registro.

   Nota:

   a. Fontes de dados: Sempre que você habilitar a regra de extração, a combinação de fontes de dados e o tipo de integração não deve corresponder a nenhuma das regras de extração habilitadas existentes e, em caso afirmativo, a aplicação exibirá uma mensagem de erro para você modificar as combinações existentes e habilitar novamente a regra.

   b. Pesquisa de ameaças: Sempre que você habilitar a regra de extração, o nome do fornecedor não deve corresponder a nenhuma das regras de extração habilitadas existentes e, em caso afirmativo, a aplicação exibirá uma mensagem de erro para você modificar o nome do fornecedor e habilitar novamente a regra.

   c. Um exemplo de regras de extração da técnica MITRE ATT&CK são provisionadas para os usuários no sistema de base e essas regras estarão no estado desabilitado por padrão e você deve habilitar e ativar a regra.

Campo	Descrição
Regra genérica para ingestão de fontes de dados	Esta é uma regra genérica para ingestão de todos os tipos de fontes de dados, incluindo Inteligência de importação e criação manual.
Regra genérica para Pesquisa de ameaças	Esta é uma regra genérica para qualquer integração de pesquisa de ameaças.
Regra genérica para integrações de aprimoramento de observável	Esta é uma regra genérica para qualquer integração de aprimoramento de observável.

5. Clique em **Duplicado** para criar uma cópia da regra de extração.
6. Clique em **Desabilitar** para desabilitar a regra de extração.

   Nota: Quando estiver desabilitada, a regra não será mais considerada para a extração de dados DO MITRE.

7. Clique em **Salvar**.
8. Clique em **Excluir** Se você deseja excluir qualquer regra de extração de técnica MITRE ATT&CK.

Método de extração da técnica MITRE ATT&CK

O método de extração da técnica MITRE ATT&CK descreve como os métodos de extração são realizados e as técnicas associadas são verificadas.

1. As regras de extração para fontes de dados (pesquisas de ameaça não são aplicáveis) são processadas sempre que um registro de origem de entidade (por exemplo, origem observável ou origem de objeto) é criado.
2. As regras são aplicáveis a todos os campos no registro de origem da entidade (exceto data, campos numéricos e Categoria de uso e fases de ataque).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. As técnicas DO MITRE extraídas são associadas ao registro de entidade correspondente e você exibe os registros na lista relacionada Técnicas DO MITRE no **Registros relacionados** guia.

> **Nota:** Primeiro, as técnicas MITRE são extraídas e associadas ao registro de origem da entidade, em seguida, as associações de técnicas são desduplicadas e agregadas ao registro da entidade primária.

Exibir técnicas MITRE

1. Navegar até **Biblioteca de informações sobre ameaças**qualquer registro de entidade (observável ou objeto) usando .
2. Clique em **Registros relacionados** guia.
3. Selecione **Técnicas MITRE** e exibem as técnicas associadas que são extraídas.
4. Clique no ID da técnica MITRE para exibir e acessar o registro de associação da técnica MITRE. . **Origens** A coluna exibe todas as origens (também separadas por uma vírgula se houver uma ou mais origens) associadas ao registro de origem da entidade no qual a extração DO MITRE é realizada.

> **Nota:** Se os mesmos IDs de tática e técnica forem extraídos de várias fontes, somente um registro de associação de tática e técnica será exibido e o **Origens** a coluna exibe todas as origens extraídas.

5. Para solução de problemas, você pode exibir a regra de extração DO MITRE, que foi responsável pela extração das associações de tática e técnica navegando até **Relações de origem da técnica** .

> **Nota:** Certifique-se de adicionar **Regra de extração** coluna usando **Listar ações** Caso você não veja a coluna Regra de extração.

As regras de extração para pesquisas de ameaças são processadas sempre que o registro de resultado da pesquisa de ameaças é criado para qualquer observável para o qual **Executar pesquisa de ameaças** a ação é acionada e a extração é realizada somente na carga de dados brutos (campo raw_data) que está disponível no registro de resultado da pesquisa de ameaças.

Nota:

- Se não houver ID de tática presente na origem da entidade extraída (observável ou objeto) ou no resultado da pesquisa de ameaça para qualquer técnica MITRE ATT&CK, as associações de técnica serão criadas para todas as táticas associadas à técnica correspondente no repositório MITRE.
- Se houver qualquer ID de tática presente na origem da entidade extraída (observável ou objeto) ou no resultado da pesquisa de ameaça para qualquer técnica MITRE ATT&CK, as associações de técnica serão criadas especificamente somente para todas as táticas extraídas associadas à técnica correspondente no repositório MITRE.

Definir listas de controle de segurança

Use este recurso para adicionar ou remover observáveis em massa.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Ir para **Listas de controle de segurança**.
   Por exemplo, adicionar observáveis à lista de permissões e vá para a opção de lista de permissões.
3. Selecione **Lista de permissões** .
4. Selecione o tipo de observáveis, como Endereço IP, Arquivo e assim por diante, para adicionar à lista de permissões.
5. Clique em **Adicionar**.
   . **Selecione observáveis para a lista de permissões** é exibido.
6. Selecione todos os observáveis que precisam ser adicionados à lista de permissões.
7. Clique em **Adicionar à Lista de permissões** .
   Os observáveis selecionados são adicionados.
8. Da mesma forma, selecione **Adicionar à lista de proibições** para adicionar os observáveis à lista removida.
9. Selecione **Adicionar à lista de observação** para adicionar os observáveis à lista de observação.

   Nota: Você pode adicionar diretamente os observáveis à lista de permissões, à lista de proibições ou à lista de observação diretamente na página de exibição do formulário de observáveis, que estão disponíveis acima da faixa do formulário.

10. Para verificar, navegue até **Biblioteca Intel de ameaças** .
11. Selecione o tipo de observável que foi adicionado à lista de permissões.
    O observável é indicado como adicionado à lista de permissões.

    Nota: A lista de permissões e a lista de proibições são mutuamente exclusivas e o sistema garantirá automaticamente que um observável na lista de permissões não faça parte da lista de proibições e vice-versa.

Criando taxonomias

Crie taxonomias para os registros da fonte de dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração** > **Taxonomias**.
2. Clique em **Nova**.
3. Insira **Nome** .
4. Habilite ou desabilite a taxonomia **Status** Habilitar ou desabilitar ações de formulário.

   Nota: Taxonomias desabilitadas não estarão disponíveis para seleção de registros em que as taxonomias sejam aplicáveis.

5. Vá para **Valores de taxonomia** seção para adicionar valores de taxonomia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Novo** Para abrir a nova exibição do formulário de valor de taxonomia e insira **Taxonomia** e. **Valor** .
7. Clique em **Salvar**.
8. Por exemplo, navegue até **Biblioteca de informações sobre ameaças** > **Observáveis** para verificar as taxonomias do registro de observáveis.
9. Navegue até **Marcadores e taxonomias** em qualquer página de formulário observável e selecione a taxonomia recém-criada.

Nota: Você também pode adicionar marcadores e taxonomias na exibição de lista da biblioteca de informações sobre ameaças.

Taxonomias de importação em massa

Importe os registros de taxonomia.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode importar as taxonomias usando os dados da planilha. Isso permite importar vários registros em massa.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração** > **Taxonomias**.
2. Selecione **Importação** botão.
   Esta ação abre uma ação para importar o arquivo de dados no formato XLSX ou CSV. você também pode baixar o arquivo de amostra para entender o formato a ser importado. O formato de arquivo contém dois valores que incluem Taxonomia e Valor de taxonomia.
3. Clique em **Adicionar arquivo** link.
4. Selecione o arquivo e. **Upload** .
5. Clique em **Concluído**.
   Uma mensagem de confirmação exibe que os dados do arquivo anexado foram importados com sucesso. Você pode clicar no link para exibir o resumo da importação. Ao clicar no link, o registro é aberto em uma nova guia. Você pode exibir a contagem de taxonomias e valores de taxonomia criados e, se houver algum erro registrado, ele será registrado na seção Erros de importação.

   Nota: Por padrão, todas essas taxonomias e valores de taxonomia são criados com o status Habilitado. Se você quiser desabilitar, você sempre pode fazer isso na exibição de lista.

6. Em **Taxonomias** , você pode clicar em qualquer registro, esta ação mostrará os valores de taxonomia como uma guia separada e você poderá ver os dois valores de taxonomia que são importados com sucesso, e esses valores de taxonomia estarão no status habilitado.
7. Além disso, para exibir qualquer uma das importações de taxonomia, você sempre pode navegar até **Importações** , as taxonomias importadas são exibidas em **Importações de taxonomia** seção.
8. Clique em **Todas as importações** para exibir todas as importações de taxonomia criadas por diferentes usuários na aplicação.
9. Clique em **Minhas importações** para ver as importações de taxonomia do usuário conectado no momento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como gerenciar a Calculadora de reputação da Pesquisa de ameaças

Você pode usar a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis com base nas respostas recebidas do fornecedor de pesquisa de ameaças.

Você pode criar uma Calculadora de descoberta de pesquisa de ameaças para sua integração e usar um script para determinar como você deseja identificar as várias descobertas observáveis. A Calculadora de descoberta de pesquisa de ameaças inclui um script de amostra que vem com o sistema de base, que você pode usar para identificar as descobertas observáveis ou modificar esse script de acordo com seus requisitos.

Para integrações de terceiros que fornecem os resultados calculados, a Calculadora de descoberta da pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema de base.

Resultados da pesquisa de ameaças de acúmulo

Quando você tem vários resultados de pesquisa de ameaças para um observável de vários fornecedores de integração, os resultados recentes da pesquisa de ameaças de todos os fornecedores são considerados e as descobertas gerais do observável são marcadas da seguinte forma:

Acúmulos de descobertas da Pesquisa de ameaças

Descoberta observável mais recente	Descoberta observável geral
Mal-intencionado	Se um dos fornecedores de integração relatar o observável como mal-intencionado, a descoberta geral do observável será marcada como mal-intencionada.
Suspeito	Se nenhum dos fornecedores de integração relatar o observável como mal-intencionado, um deles o relatará como suspeito e a descoberta geral do observável será marcada como suspeita.
Limpar	Se todos os fornecedores de integração relatarem o observável como limpo, a descoberta geral do observável será marcada como limpa.
Desconhecido	Se nenhum dos fornecedores de integração relatar o observável como mal-intencionado ou suspeito e um deles relatar como Desconhecido, a descoberta geral do observável será marcada como Desconhecido.

Exibir Calculadoras de reputação da Pesquisa de ameaças

Você pode exibir a Calculadora de descoberta de pesquisa de ameaças para determinar como a reputação do observável é calculada com base na resposta do fornecedor de pesquisa de ameaças específico.

Função necessária: sn_sec_tisc.admin

Para exibir a Calculadora de reputação da Pesquisa de ameaças, execute as seguintes etapas:

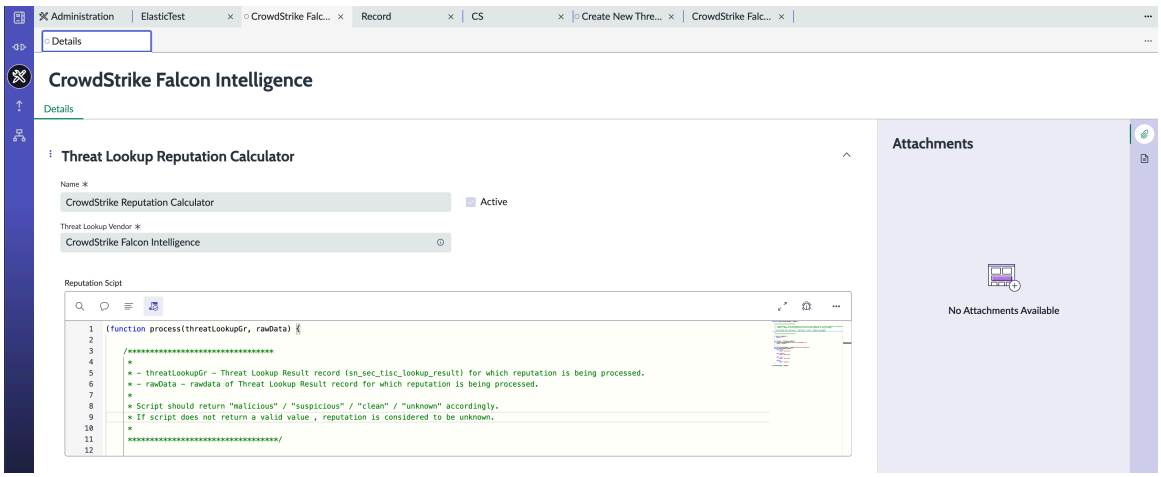
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione **Calculadora de reputação da Pesquisa de ameaças** seção.

   Você pode exibir a lista de Calculadoras de reputação da Pesquisa de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique na Calculadora de reputação da Pesquisa de ameaças necessária para exibir os detalhes da calculadora.



Calculadora de reputação da Pesquisa de ameaças

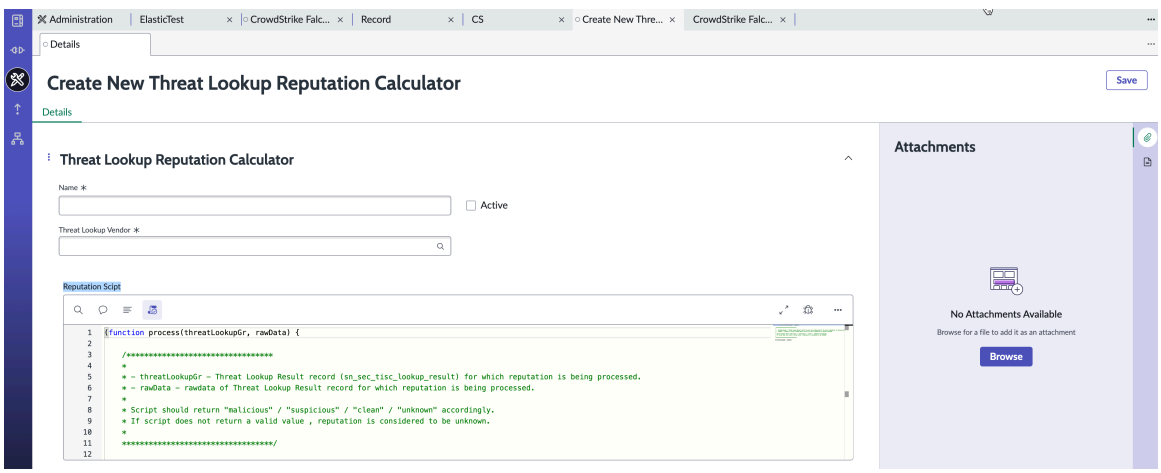
Função necessária: sn_sec_tisc.admin

Nota: Apenas uma calculadora de pesquisa de ameaças pode estar ativa a qualquer momento por fornecedor de pesquisa de ameaças.

Para criar uma Calculadora de reputação da Pesquisa de ameaças, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione **Calculadora de reputação da Pesquisa de ameaças** seção.

   Você pode exibir a lista de Calculadoras de reputação da Pesquisa de ameaças.
3. Para criar uma Calculadora de reputação da Pesquisa de ameaças, clique em **Novo** .



4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma Calculadora de reputação de Pesquisa de Threat

Campo	Descrição
Nome	Calculadora de reputação da Pesquisa de ameaças.
Ativo	O cálculo da Pesquisa de ameaças será executado somente se a opção Ativo estiver selecionada.
Fornecedor da pesquisa de ameaças	Nome do fornecedor da Pesquisa de ameaças. Por exemplo, CrowdStrike Falcon Intelligence .
Script de reputação	Editor de script para determinar como você deseja identificar as várias descobertas observáveis. Cada integração de pesquisa de ameaças vem com um script de base para calcular a reputação da pesquisa de ameaças.

5. Clique em **Salvar**.

Gerenciar notificações por e-mail

Usar ServiceNow Notificações para criar e gerenciar notificações por e-mail do sistema e exibir logs de e-mail.

Notificações por e-mail

Use notificações por e-mail para enviar notificações por e-mail de usuários selecionados sobre tarefas específicas na aplicação, como atualizações de observáveis/indicadores/ vários outros objetos.

Função necessária: administrador

Nota: Como administrador do sistema, você pode exibir, criar ou editar os detalhes da regra de notificação por e-mail na exibição clássica da aplicação.

Central de segurança de inteligência contra ameaças fornece notificações por e-mail orientadas por regras que são enviadas para endereços de e-mail individuais ou uma lista de endereços de e-mail. Normalmente, a disseminação de informações de informações sobre ameaças para usuários internos é enviada normalmente na forma de e-mail. O processo envolve a entrega dos dados de inteligência contra ameaças aos usuários de acordo com o formato e as linhas de tempo especificados.

As notificações por e-mail permitem que os administradores especifiquem:

- Quando enviar a notificação
- Quem recebe a notificação
- Qual o conteúdo da notificação

Nota: Se você quiser fazer mudanças, precisará configurar para quem o e-mail deve ser enviado, modificando as regras do sistema de base com base em seus requisitos.

Para obter mais informações, consulte Crie uma notificação por e-mail seção ativada Administração do ServiceNow AI Platform documentação.

A tabela a seguir detalha as regras de notificação por e-mail provisionadas no sistema de base.

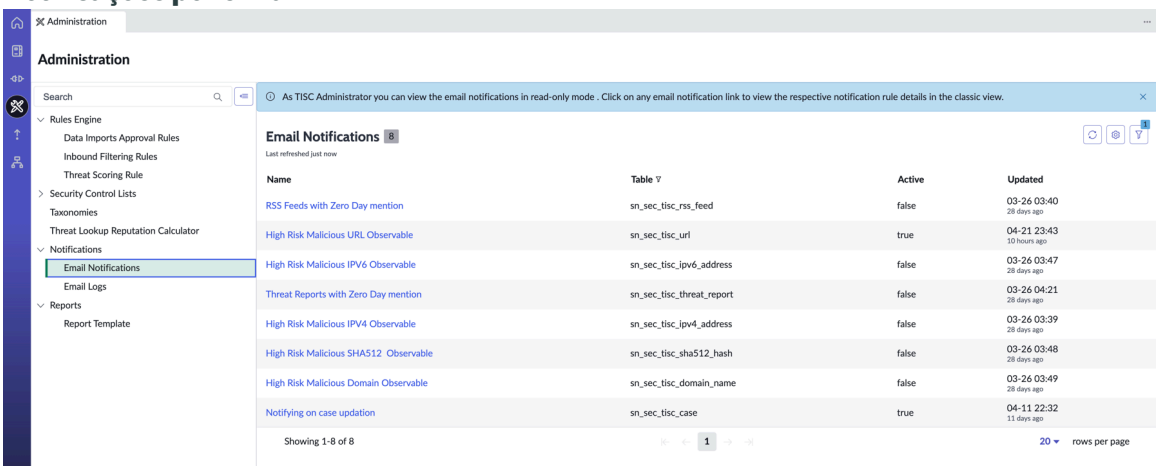
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificações por e-mail

Nome	Tabela
RSS feeds com menção de dia zero	sn_sec_tisc_rss_feed
Observável de URL mal-intencionada de alto risco	sn_sec_tisc_url
Observável IPV6 mal-intencionado de alto risco	sn_sec_tisc_ipv6_address
Relatórios de ameaças com menção de dia zero	sn_sec_tisc_threat_report
Observável IPV4 mal-intencionado de alto risco	sn_sec_tisc_ipv4_address
Observável SHA512 malicioso de alto risco	sn_sec_tisc_sha512_hash
Observável de domínio mal-intencionado de alto risco	sn_sec_tisc_domain_name
Notificando sobre a atualização do caso	sn_sec_tisc_case

Notificações por e-mail



Nota: Clicar em cada notificação por e-mail levará você para a IU clássica, para que você possa tomar as ações necessárias, como exibir, editar ou criar as notificações.

Logs de e-mail

Esta seção fornece uma visibilidade clara para os administradores do TISC sobre os e-mails que são enviados usando as regras de notificação por e-mail configuradas.

Notificações por e-mail e finalidade de logs

O TISC fornece finalidades diferentes para acessar, exibir ou modificar notificações por e-mail e logs com base em personas diferentes.

Nota:

Persona	Níveis de acesso
TISC (sn_sec_tisc.admin)	Como sn_sec_tisc.admin, você só pode exibir as notificações por e-mail configuradas para o TISC. **Nota:** Clique nos hiperlinks dos logs de e-mail para navegar até a IU clássica e exibir essas notificações.

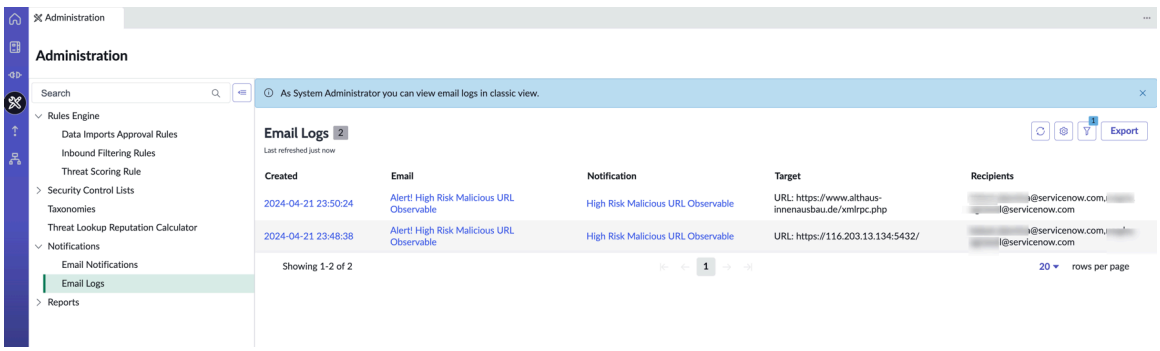
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona	Níveis de acesso
Administrador do sistema (admin)	Como administrador, você pode criar, exibir e editar as notificações na IU clássica. **Nota:** Clique nos hiperlinks dos logs de e-mail para navegar até a IU clássica para exibir e criar essas notificações.

Nota: O administrador do TISC e o administrador do sistema podem usar os filtros e pesquisar os logs de e-mail.

Logs de E-mail



Modelos de relatório

Define a capacidade de reutilizar os modelos de relatório que podem ser compartilhados no grupo de usuários para gerar relatórios de forma rápida e consistente.

Use este recurso para criar diferentes tipos de modelos de relatório, que podem ser aplicados a casos que fornecem o status da investigação em andamento em relevância para qualquer ameaça à sua organização e ajudam na geração de relatórios do mesmo.

Esta seção explica como implementar a emissão de relatórios de CTI em um nível de caso e também fornece experiências de administrador (design de modelo) e analista (tempo de execução).

Você pode adicionar campos de formulário de tarefa de caso personalizados ou listas relacionadas ao modelo de relatório que podem ser verificados com pontos. Além disso, você pode formatar e configurar o relatório com base em seus requisitos usando vários elementos de relatório.

Função necessária: sn_sec_tisc.admin

A tabela a seguir explica alguns modelos de relatório provisionados no sistema de base.

Modelo de relatório

Nome	Descrição
Relatório de status do caso — Perfil do agente da ameaça	O relatório foi projetado para fornecer um status sobre a investigação de caso em andamento relacionada a um agente de ameaça que tenta entender o contexto e a relevância da ameaça para a organização, comportamento do adversário e objetivos em potencial, aprimoramento do IOC, malware e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de relatório

Nome	Descrição
	ferramentas associados, TTPs observados, diferença dos TTPs existentes - novos recursos líquidos, pequenas modificações e assim por diante.
Resumo executivo	O Relatório foi projetado para informar os tomadores de decisão sênior sobre um risco específico. O foco está no público executivo e em apoio a problemas estratégicos explicando por que e como, em vez de o que e quando. Quaisquer detalhes técnicos e apêndices em apoio à escrita narrativa longa não serão incluídos neste relatório.
Resumo pós-investigação — Perfil do agente da ameaça	O Relatório foi projetado para fornecer contexto e relevância da ameaça para a organização; comportamento do adversário e objetivos potenciais; enriquecimento do IOC; malware e ferramentas associadas; TTPs observados; diferença dos TTPs existentes – novos recursos líquidos, pequenas modificações e assim por diante.

Nota: Por padrão, esses relatórios estão no estado Publicado e estarão no modo somente leitura. Como os modelos de relatório estarão no modo somente leitura, os usuários não poderão fazer edições nos modelos e os analistas não poderão gerar os relatórios, pois os modelos de relatório serão desabilitados.

Crie um novo Modelo de Relatório

Crie um novo modelo de relatório de caso de acordo com as necessidades de negócios da sua organização.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
   Esta seção exibe os modelos disponíveis no sistema de base e também os modelos publicados. Você pode escolher qualquer modelo desejado para trabalhar com os relatórios.

   Nota: Nesta seção, você também pode excluir os modelos, se necessário.

3. Clique em **Nova**.
4. Insira o nome e a descrição do modelo.
5. Clique em **Salvar**.
   A seção Conteúdo do modelo é exibida.

   Nota: Sempre que você criar um novo modelo de relatório, o modelo estará no estado de rascunho, o que significa que a criação do modelo é Trabalho em andamento e qualquer outro usuário não poderá exibir o modelo de relatório até que ele seja concluído.

6. Expanda **Conteúdo do modelo** Para inserir os campos desejados no corpo do modelo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- O modelo que você está editando permite definir o corpo do modelo e selecionar as variáveis necessárias para adicionar à seção do editor de modelos. Os modelos são compatíveis com o editor de rich text (RTE) para que você possa controlar várias funções disponíveis, como recuo, tamanho da fonte, criar tabelas, adicionar imagens e vários outros recursos de formatação.
- Você também pode inserir imagens em seus modelos de relatório, para isso, você precisa copiar e colar a imagem diretamente no modelo. Ao adicionar uma imagem, essa imagem é carregada como um anexo.
- Você pode carregar ou anexar uma imagem de até 698 pixels. Se a imagem estiver acima do tamanho definido, ela será ajustada automaticamente para o tamanho original. Esta restrição de tamanho de pixel ajudará a geração do relatório em PDF a ser exibida em um formato adequado e as imagens não serão truncadas no relatório.

7. Adicione os elementos necessários do caso.
8. Clique em **Salvar conteúdo** para salvar o conteúdo do seu novo modelo de relatório.
9. Clique em **Visualização** para visualizar o formato do relatório e também ver como um relatório é gerado quando você gera qualquer relatório de caso.

Nota:

- **Campos de Caso** : Sempre que você modificar seus modelos de relatório, visualize o conteúdo adicionado ao modelo. Por exemplo, quando você está gerando um relatório de caso e deseja adicionar um campo chamado Descrição resumida, selecione esse campo nos campos de caso e esse campo é adicionado como uma variável no modelo de relatório. Quando um relatório é gerado para o analista, qualquer que seja a descrição resumida do caso, essa descrição será exibida no relatório.
- **Registros** : No modelo de relatório, você também pode adicionar os registros relacionados desse caso específico que são exibidos como artefatos do caso. Por exemplo, se você quiser ver observáveis mal-intencionados no relatório das listas relacionadas de observáveis, poderá adicioná-los ao seu modelo de relatório. Esses registros relacionados são exibidos no formato de tabela
- **Scripts** : Sempre que você quiser ver a data e a hora do relatório, adicione o. **Data e hora atual** Seu modelo de relatório, e isso adicionará a data e a hora de criação do relatório.
- **MITRE ATT&CK** : Exibe as técnicas associadas ao cartão MITRE em seu relatório.

Depois de adicionar todos os campos obrigatórios relacionados ao caso ao seu modelo de relatório, você precisa publicar seu modelo de relatório.

10. Clique em **Publicar** para publicar o modelo.
Uma mensagem de confirmação será exibida se você deseja publicar o modelo de relatório.

Nota: Quando você publica um modelo de relatório, esse modelo é habilitado para todos os usuários. Se ele estiver desatualizado e você quiser restringir a exibição do relatório para os usuários, poderá desabilitar o relatório publicado, o que significa que o modelo de relatório ficará oculto para os usuários. Você precisa habilitar novamente o relatório publicado para que os usuários o vejam e o usem até que ele fique oculto para exibição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Clique em **Excluir** para excluir o modelo de relatório caso você não queira esse modelo de relatório.
Se você quiser renomear seu modelo de relatório, clique em **Editar** e modifique os campos desejados.

Propriedades do sistema para Relatórios

As propriedades do sistema para relatórios são explicadas abaixo.

Propriedade	Descrição	Valor
sn_sec_reporting.max_list_columns_allowed	Limite o número de colunas que podem ser adicionadas ao renderizar listas em pdfs de relatório. As colunas serão usadas desde o início da exibição até o limite permitido.	5
sn_sec_reporting.report_default_style_object	Use esta propriedade para controlar o CSS de campos de formulário livre, painel esquerdo, listas de relatório.	(Objeto JSON)
sn_sec_reporting.load_all_records	Carrega todos os registros das listas no relatório criado a partir de um modelo. “Verdadeiro” carrega todos os registros e “falso” carrega o número específico de registros definidos pela propriedade sn_sec_reporting.reporting_list_records_count.	Falso(a)
sn_sec_reporting.reporting_list_records_count	Carrega um número específico de registros no editor de relatórios.	20
sn_sec_tisc.sn_sec_tisc_case.defang_control_list_urls	Controla se os URLs das listas serão corrigidos ou não.	Verdadeiro(a)
sn_sec_tisc.show_all_tactics_reporting	Se verdadeiro, mostrará todas as táticas (incluindo aquelas sem técnicas associadas ao caso) para as listas do MITRE renderizadas no relatório.	Falso(a)
sn_sec_tisc.reporting_email_template_sys_id	SYS ID do modelo de cliente de e-mail para a tabela Caso (sn_sec_tisc_case) que será usada no relatório de compartilhamento.	b55e22c5444021060eee0ea78b8f2df
sn_sec_tisc.sn_sec_tisc_case.excluded_fields	Campos excluídos do caso nas opções de menu de relatório/ modelo para substituir um campo.	(Lista de todos os campos de casos excluídos
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	Esta propriedade é usada para obter o registro de mensagem de IU correspondente para o rótulo de campos de caso nas opções de menu de relatório/modelo.	sn_sec_tisc_case_reporting_ctx_menu_field_header

Edite um modelo de relatório publicado

Use esta seção para editar um modelo de relatório publicado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
3. Selecione o modelo de relatório necessário.
4. Selecione **Editar** Botão que é exibido no Modelo de relatório.

Nota:

Uma mensagem de confirmação é exibida indicando que você está editando um modelo publicado e deve republicar o modelo para disponibilizá-lo em Relatórios de caso. Continuar editando? Isso significa que você precisa republicar o modelo editado depois de fazer as mudanças necessárias.

5. Selecione **Editar** na caixa de diálogo de confirmação.
6. Adicione os campos de conteúdo obrigatórios ou a lista relacionada para fazer as mudanças necessárias.
7. Selecione **Salvar conteúdo** .
8. Selecione **Publicar** botão para publicar as mudanças.
   Depois de publicar o modelo de relatório, uma mensagem de confirmação será exibida indicando que o modelo de relatório foi publicado com sucesso.

Nota:

- Você também pode visualizar o conteúdo do modelo de relatório antes de publicar o modelo de relatório.
- Se você quiser excluir o modelo de relatório, selecione **Excluir** para excluir o modelo de relatório.

Duplicar um modelo de relatório

Se quiser adicionar atualizações incrementais, você poderá criar uma cópia do modelo de relatório.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
3. Selecione o modelo.
4. Clique em **Duplicar**.
   O conteúdo do modelo selecionado é duplicado e a cópia desse modelo é exibida. Novamente, o modelo ficará no estado Rascunho, você poderá personalizar o conteúdo e renomear o modelo conforme necessário.
5. Edite ou modifique o conteúdo do modelo copiado.

Nota: Caso não precise mais deles, você também pode excluir os modelos de relatório e criar novos modelos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhar com webhooks

Webhook é uma solicitação HTTP, acionada por um evento no sistema de origem (TISC) e enviada para um sistema de destino (onde a URL do endpoint está presente), com uma carga de dados do evento.

Estes webhooks no Central de segurança de inteligência contra ameaças são úteis para notificar a aplicação de destino sempre que ocorrem eventos.

No TISC, você pode fazer o seguinte:

- Configurar webhooks
- Gerenciar gatilhos
- Mecanismo de nova tentativa
- Executar validação
- Gerenciar assinaturas

Propriedades do sistema para webhooks

As propriedades do sistema para webhooks são explicadas abaixo.

Nome da Propriedade	Descrição	Tipo	Valor
sn_sec_tisc.webhook_ignore_event_rule	Ignorar eventos de webhook acionados pela pontuação de ameaça recalcular histórico.	Verdadeiro/Falso	Verdadeiro(a)
sn_sec_tisc.webhook_max_event_batch_size	Número máximo de eventos a serem enviados como parte de uma solicitação de webhook. O tamanho do lote será limitado a 2000 mesmo se um valor maior for definido nesta propriedade.	Inteiro	1000
sn_sec_tisc.webhook_retry_count	Número de vezes que uma solicitação com falha deve ser tentada novamente antes de marcá-la como erro e passar para o próximo lote de eventos. A contagem de novas tentativas será limitada a 10 mesmo se um número maior for definido nesta propriedade.	Inteiro	5
sn_sec_tisc.webhook_retry_interval	Número de segundos de espera antes de tentar novamente um lote com falha.	Inteiro	30

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição	Tipo	Valor
	Isso aumentará exponencialmente com base na contagem de novas tentativas. Por exemplo, se retry_count for 3 e retry_interval for 30, as novas tentativas serão disparadas após 30, 60 e 120 segundos. O intervalo de novas tentativas inicial será limitado a 300 segundos, mesmo se um valor mais alto for definido nesta propriedade.		

Configurar webhooks

Configure um webhook para assinar eventos na Central de segurança do Inteligência contra ameaças.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

Os webhooks do TISC fornecem a capacidade de integração com ferramentas de segurança, como o SIEM. Os usuários podem assinar vários eventos relacionados a diferentes artefatos, como observáveis ou indicadores, malware ou agentes de ameaça. O TISC notifica as ferramentas de segurança (como SIEM) quando uma nova inteligência contra ameaças está disponível ou qualquer dado de inteligência contra ameaças existente é atualizado ou excluído no TISC.

Por exemplo, sempre que um novo observável é adicionado à inteligência contra ameaças, uma solicitação de carga é enviada para a configuração de URL do webhook. Essa solicitação de carga geralmente coleta as informações observáveis e as fornece como informações adicionais para ferramentas de segurança (como SIEM).

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome de webhook.
Descrição	Adicione a descrição do webhook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Detalhes da Configuração	
Usar Mensagem REST	Selecione **Usar mensagem REST** Se você precisar usar a funcionalidade Mensagem REST/Método REST fornecida por ServiceNow AI Platform. Se esta caixa de seleção não estiver marcada, a aplicação usará o endpoint fornecido na URL do webhook para enviar as informações do evento. Para obter mais informações, consulte Serviço web REST de saída ativado ServiceNow AI Platform documentação.
Mensagem REST	Selecione o registro Mensagem REST na lista de registros de mensagem REST que já estão configurados na instância. Para obter mais informações, consulte Serviço web REST de saída em ServiceNow AI Platform documentação. **Nota:** Os campos Mensagem REST e Método REST são obrigatórios quando você seleciona a mensagem REST.
Método REST	Selecione Método REST na lista de métodos REST disponíveis configurados para a mensagem REST selecionada. Para obter mais informações, consulte Serviço web REST de saída em ServiceNow AI Platform documentação. **Nota:** Os métodos REST POST são compatíveis com webhooks.
URLs do Webhook	Um endpoint do webhook é um URL que recebe notificações de evento do webhook.
Autenticação Necessária	Marque esta caixa de seleção se a autenticação for necessária. **Nota:** Aplicável somente quando o URL do webhook está sendo usado para recuperar os dados.
Tipo de autenticação	O tipo de autenticação do webhook. **Nota:** A partir de agora, somente o tipo de autenticação básica é compatível.
Nome do usuário	Forneça um nome de usuário para seu tipo de autenticação.
Senha	Forneça uma senha para seu tipo de autenticação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Cabeçalhos a serem passados com a solicitação	Quaisquer cabeçalhos a serem passados com as solicitações podem ser fornecidos no Mapeamento de cabeçalho da solicitação. O cabeçalho deve ser fornecido no par chave-valor separado por dois pontos (':'). Cada par de valor de chave de cabeçalho deve ser fornecido em uma nova linha. Para fornecer parâmetros de autenticação como valores de cabeçalho, coloque o Rótulo de autenticação necessário com " Por exemplo, nome de usuário:

4. Clique em **Validar e Salvar** .
   Se os detalhes da configuração estiverem incorretos, o sistema validará automaticamente a conexão se os detalhes da configuração forem alterados e, em seguida, a aplicação exibirá uma mensagem de aviso de que a validação do webhook falhou e você precisará verificar os detalhes da configuração e modificá-los de acordo.

Nota:

- Para a validação do webhook, a carga de solicitação vazia é enviada para o endpoint e o usuário precisa garantir que o endpoint envie o código de resposta bem-sucedido (200) quando a solicitação vazia é passada para o endpoint do webhook configurado.
- Por padrão, qualquer webhook criado estará no estado desabilitado, você precisa habilitar o webhook e ativá-lo. Um webhook de amostra é provisionado no sistema de base como uma referência aos usuários.

Gatilhos de assinatura

Exiba a lista de todos os gatilhos de webhook inscritos para o webhook atual.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
   A seção Gatilhos assinados é exibida.
4. Clique em **Assinar** Botão na seção Gatilho assinado.
   A exibição de lista mostra todos os gatilhos de webhook habilitados na instância.
5. Selecione os gatilhos de webhook desejados e clique em **Assinar** Na caixa de diálogo Gatilhos do webhook.
   Uma mensagem de confirmação é exibida informando que o webhook foi inscrito com sucesso nos gatilhos selecionados. A partir daqui, você também pode criar diretamente um novo gatilho e assinar o webhook.

Nota: Você também pode **Cancelar assinatura** o webhook dos gatilhos selecionados.

Exibir logs de erros do webhook

Use esta seção de logs de erro para exibir todas as entradas de auditoria marcadas como erro no status de um webhook específico.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Os logs de auditoria permitem que os usuários investiguem, depurem a execução e identifiquem a causa raiz da falha de execução.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
4. Vá para **Logs de erros** .
5. Exiba os logs de erro.
   A exibição de lista mostra todos os logs de erro de um webhook específico.
6. Vá para **Lote** coluna.
7. Clique em qualquer um **ID do lote** .

   Nota: Cada log de erros está associado a um lote e, usando o ID do lote (na coluna Lote), você pode exibir o registro do lote associado. Clique em qualquer um dos IDs do lote e isso será aberto em uma guia separada. Cada ID de lote contém o número de lote do webhook, a mensagem de erro, o código de status da resposta, a contagem de novas tentativas, os dados reais da carga, e a lista de eventos que serão enviados para o webhook.

8. Clique em **Lote de novas tentativas** para repetir os lotes com falha.
   Quando você clica neste botão, envia uma carga de solicitação (dessas informações de lote específicas) para o endpoint do webhook configurado.

   Nota: Esta ação está disponível somente para os registros em lote que têm erros de execução ou concluídos com sucesso e os registros que estão no estado de nova tentativa serão tentados automaticamente.

Exibir lotes de webhook

Um registro em lote do webhook é criado para cada execução do webhook.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Para reduzir o número de chamadas de API enviadas para os endpoints do webhook, o lote de eventos é implementado nos webhooks. Para cada webhook, se houver vários eventos acionados quase durante o mesmo tempo, todos esses eventos serão enviados como parte da mesma solicitação para o endpoint do webhook.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
4. Vá para **Logs de erros** .
5. Exiba os logs de erro.
   A exibição de lista mostra todos os logs de erro de um webhook específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Vá para **Lote** coluna.
7. Clique em qualquer um **ID do lote** .
   A página Lote do webhook é exibida.

Nota: Todos os lotes são armazenados na tabela `sn_sec_tisc_webhook_batch` .

Abaixo está o formato de carga de amostra que o endpoint do webhook recebe:


```
{
  "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
  "events": [
    {
      "record": "Observable",
      "record_fields": {
        "is_false_positive": "false",
        "reputation": "malicious",
        "sys_updated_on": "2024-07-22T14:31:26.000Z",
        "type": "url",
        "sys_updated_by": "admin",
        "sys_created_on": "2024-07-04T06:45:20.000Z",
        "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
        "is_defanged": "false",
        "sys_created_by": "SecCommon.System",
        "tags": "Enriched",
        "taxonomies": "T1: V1",
        "domain": "urlhaus.abuse.ch",
        "status": "active",
        "source_count": "1",
        "threat_score": "20",
        "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
        "value": "https://urlhaus.abuse.ch/url/2578255/",
        "confidence": "89",
        "expiration_time": "2025-10-07T07:13:18.000Z",
        "tlp": "CLEAR"
      },
      "trigger": {
        "name": "Observable Update",
        "type": "UPDATE",
        "trigger_time": "2024-07-22T14:31:26.000Z",
        "trigger_fields": [
          {
            "field_name": "reputation",
            "previous_value": null,
            "current_value": "malicious"
          }
        ]
      }
    },
    {
      "record": "Observable",
      "record_fields": {
        "is_false_positive": "false",
        "reputation": "malicious",
        "sys_updated_on": "2024-07-22T14:31:19.000Z",
        "type": "url",
        "sys_updated_by": "admin",
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
            "sys_created_on": "2024-07-04T06:45:20.000Z",
            "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
            "is_defanged": "false",
            "sys_created_by": "SecCommon.System",
            "tags": "Enriched",
            "taxonomies": "T1: V1",
            "domain": "urlhaus.abuse.ch",
            "status": "active",
            "source_count": "1",
            "threat_score": "20",
            "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
            "value": "https://urlhaus.abuse.ch/url/2578264/",
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
        },
        "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:19.000Z",
            "trigger_fields": [
                {
                    "field_name": "reputation",
                    "previous_value": null,
                    "current_value": "malicious"
                }
            ]
        }
    }
  ]
}
```


A tabela a seguir lista a estrutura de carga em lote e seus atributos que serão enviados aos usuários como carga do webhook:

Parâmetros na carga em lote	Tipo	Descrição
batch_id	Cadeia de caracteres	Especifica o identificador exclusivo para um lote.
eventos	Matriz de objetivos	Contém uma matriz de eventos que são acionados como parte desse webhook. Cada evento conterá o snapshot dos valores de campo no momento da geração do evento e também conterá as informações do gatilho. **Nota:** Para obter mais informações sobre como exibir os parâmetros no objeto Evento, consulte Gatilhos de webhook.

Nota:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Lote de novas tentativas** botão para repetir o lote com falha.

> **Nota:** Você também pode acionar o lote de novas tentativas para os lotes concluídos.

Gatilhos de webhook

Os gatilhos do webhook são usados para filtrar as entidades de inteligência contra ameaças que precisam ser rastreadas para quaisquer mudanças de evento, como Criar, Atualizar e Excluir.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de webhooks** > **Gatilhos**.
   A página Gatilhos de webhooks é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome de gatilho de webhook.
Descrição	Adicione a descrição do gatilho do webhook.
Tabela	Selecione a tabela para o gatilho do webhook.
Tipo de gatilho	Define se o gatilho de webhook configurado é criar/atualizar/excluir evento na tabela especificada. **Campos do gatilho** : Isso é exibido quando você seleciona **Tipo de gatilho: Atualização** . Esta é a lista de campos no registro para os quais o evento de atualização precisa ser rastreado. Se estiver vazio, o evento será considerado para qualquer mudança de campo no registro. Por exemplo, se os campos do gatilho forem **Confiança** e. **Reputação** para **Observáveis** , este gatilho é considerado somente quando os campos confiança ou reputação são atualizados. **Nota:** Os campos selecionados nos Campos de exclusão não estarão disponíveis na seleção de Campos do gatilho. **Excluir** : Se o **Tipo de gatilho: Excluir** Os Campos de exclusão não ficam visíveis.
Campos de exclusão	Este é o conjunto de campos que são excluídos da carga útil do gatilho do webhook.
Condições do filtro	Condições opcionais que podem ser aplicadas para filtrar os registros de correspondência para qualquer gatilho de evento. Por exemplo, se a Severidade da

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ameaça for alta e o Tipo de gatilho for definido como Atualizar na Tabela observável, somente os observáveis alterados e onde a Severidade da ameaça for alta serão enviados para o URL do webhook.

4. Clique em **Salvar**.
   Por padrão, o gatilho é criado no estado desabilitado.
5. Clique em **Habilitar** para habilitar o gatilho e este gatilho estará disponível para assinatura dos webhooks.

   Nota: Clique em **Desabilitar** desabilitar o gatilho habilitado e desabilitá-lo cancelará a assinatura de todos os webhooks associados deste gatilho.

6. Clique em **Exibir carga útil de amostra** para selecionar o registro.
   Exiba a carga de amostra desse gatilho de webhook específico. Com base na tabela selecionada, os registros dessa tabela especificada serão preenchidos em **Selecione Registro** lista suspensa. Selecione o registro para exibir a carga de amostra. A carga de amostra é mostrada no formato JSON. Os campos na carga estão listados abaixo.
7. Selecione o tipo de registro na lista suspensa.
   A carga será alterada automaticamente com base no registro selecionado.


```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
  "trigger": {
    "name": "Observable Update",
    "type": "UPDATE",
    "trigger_time": "2024-07-26T07:27:29.000Z",
    "trigger_fields": [
      {
        "field_name": "confidence",
        "previous_value": "30",
        "current_value": "50"
      }
    ]
  }
}
```

Lista de parâmetros na carga do gatilho

Parâmetro na Carga do gatilho	Tipo	Descrição
registro	Cadeia de caracteres	Especifica o tipo de registro, como Observável ou Indicador.
record_fields	Objeto	Especifica o snapshot dos campos de registro quando o evento é gerado. Para obter a lista de campos compatíveis, consulte a tabela na seção abaixo.
gatilho	Objeto	Especifica as informações do gatilho correspondentes.
trigger.name	Cadeia de caracteres	Especifica o nome do gatilho
gatilho.type	Cadeia de caracteres	Especifica o tipo de gatilho. Os valores válidos são CREATE, UPDATE, DELETE.
gatilho.trigger_time	Data (no formato ISO com fuso horário UTC)	Especifica a hora em que o evento ocorreu no registro.
trigger_fields	Matriz de objetivos	Disponível somente para o tipo de gatilho de ATUALIZAÇÃO. Especifica a lista de campos do gatilho que foram alterados como parte do evento ocorrido. Os parâmetros dentro **trigger_fields** : ○ **field_name** : fornece o nome do campo que foi alterado ○ **previous_value** : fornece o valor anterior do campo. ○ **current_value** : fornece o valor atual do campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de campos compatíveis para Criar e atualizar gatilhos

Tabela	Nome da Coluna	Rótulo da Coluna
Campanha	aliases	Aliases
Campanha	descrição	Descrição
Campanha	first_seen	Visto pela primeira vez
Campanha	last_seen	Visto pela última vez
Campanha	nome	Nome
Campanha	objetivo	Objetivo
Indicador	adicional_context	Contexto adicional
Indicador	attack_phases	Fases de ataque
Indicador	autor	Autor
Indicador	confiança	Confiança
Indicador	descrição	Descrição
Indicador	expiration_time	Tempo de expiração
Indicador	first_detected	Detectado pela primeira vez
Indicador	first_observed	Observado pela primeira vez
Indicador	first_seen	Visto pela primeira vez
Indicador	id	ID
Indicador	indicator_types	Tipos de Indicador
Indicador	ioc_classification	Classificação IOC
Indicador	last_observed	Última observação
Indicador	last_seen	Visto pela última vez
Indicador	nome	Nome
Indicador	padrão	Padrão
Indicador	pattern_type	Tipo de padrão
Indicador	pattern_version	Versão do padrão
Indicador	plataformas	Plataformas
Indicador	revogado	Revogado
Indicador	source_count	Nº de origens
Indicador	spec_version	Versão de especificação
Indicador	status	Status
Indicador	marcadores	Marcadores de TISC
Indicador	taxonomias	Taxonomias
Indicador	threat_level	Nível de ameaça
Indicador	threat_severity	Gravidade da ameaça

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Indicador	tlp	TLP
Indicador	usage_categories	Categorias de uso
Indicador	valid_from	Válido de
Indicador	valid_until	Válido Até
Malware	aliases	Aliases
Malware	attack_phases	Fases de ataque
Malware	descrição	Descrição
Malware	executable_process_archetectures	Arquiteturas de processo
Malware	first_seen	Visto pela primeira vez
Malware	implementation_languages	Idiomas de implementação
Malware	is_family	É família
Malware	last_seen	Visto pela última vez
Malware	malware_capabilities	Capacidades do malware
Malware	malware_types	Tipos de malware
Malware	nome	Nome
Objeto (Campos de objeto comum)	adicional_context	Contexto adicional
Objeto (Campos de objeto comum)	confiança	Confiança
Objeto (Campos de objeto comum)	expiration_time	Tempo de expiração
Objeto (Campos de objeto comum)	id	ID
Objeto (Campos de objeto comum)	revogado	Revogado
Objeto (Campos de objeto comum)	source_count	Nº de origens
Objeto (Campos de objeto comum)	spec_version	Versão de especificação
Objeto (Campos de objeto comum)	status	Status
Objeto (Campos de objeto comum)	marcadores	Marcadores de TISC
Objeto (Campos de objeto comum)	taxonomias	Taxonomias
Objeto (Campos de objeto comum)	threat_level	Nível de ameaça
Objeto (Campos de objeto comum)	threat_severity	Gravidade da ameaça

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Objeto (Campos de objeto comum)	tlp	TLP
Observável	adicional_context	Contexto adicional
Observável	attack_phases	Fases de ataque
Observável	autor	Autor
Observável	confiança	Confiança
Observável	descrição	Descrição
Observável	expiration_time	Tempo de expiração
Observável	first_observed	Observado pela primeira vez
Observável	first_seen	Visto pela primeira vez
Observável	id	ID
Observável	_defanged	Está danificado
Observável	é_falso_positivo	É falso-positivo
Observável	last_observed	Última observação
Observável	last_seen	Visto pela última vez
Observável	reputação	Reputação
Observável	source_count	Nº de origens
Observável	status	Status
Observável	marcadores	Marcadores de TISC
Observável	taxonomias	Taxonomias
Observável	threat_level	Nível de ameaça
Observável	threat_score	Pontuação de ameaça
Observável	threat_severity	Gravidade da ameaça
Observável	tlp	TLP
Observável	tipo	Tipo
Observável	usage_categories	Categorias de uso
Observável	valor	Valor
Agente da ameaça	aliases	Aliases
Agente da ameaça	descrição	Descrição
Agente da ameaça	first_seen	Visto pela primeira vez
Agente da ameaça	objetivos	Objetivos
Agente da ameaça	last_seen	Visto pela última vez
Agente da ameaça	nome	Nome
Agente da ameaça	personal_motivations	Motivações pessoais
Agente da ameaça	primary_motivation	Motivação primária
Agente da ameaça	resource_level	Nível de recurso

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Agente da ameaça	secondary_motivations	Motivações secundárias
Agente da ameaça	sofisticação	Sofisticação
Agente da ameaça	threat_actor_roles	Funções de agente da ameaça
Agente da ameaça	threat_actor_types	Tipos de Agente da Ameaça
Relatório de ameaças	descrição	Descrição
Relatório de ameaças	nome	Nome
Relatório de ameaças	publicado	Publicado
Relatório de ameaças	report_types	Tipos de relatório
Vulnerabilidade	affected_software	Software afetado
Vulnerabilidade	descrição	Descrição
Vulnerabilidade	exploalization_status	Status de exploração
Vulnerabilidade	exploit_exists	Explorar Itens Existentes
Vulnerabilidade	nome	Nome
Vulnerabilidade	publicado	Publicado
Vulnerabilidade	record_last_modified	Última modificação do registro
Vulnerabilidade	severidade	Gravidade

Abaixo está a lista de campos do sistema aplicáveis que são comuns a cada entidade, e eles são compatíveis com a Carga do gatilho do webhook para criar e atualizar gatilhos.

- Sys_id (SYS ID)
- Sys_created_on (criado)
- Sys_created_by (Criado por)
- Sys_updated_on (Atualizado)
- Sys_updated_by (Atualizado por)

Nota: Para Excluir, somente o sys_id (SYS ID) é enviado para a URL do endpoint do webhook como parte da carga útil e outros campos do sistema não são compatíveis.

Lista de campos compatíveis para Excluir gatilho

Tabela	Nome da Coluna	Rótulo da Coluna
Observável	tipo	Tipo
Observável	valor	Valor
Indicador	nome	Nome
Indicador	padrão	Padrão
Indicador	pattern_type	Tipo de padrão
Indicador	valid_from	Válida de
Campanha	nome	Nome
Malware	is_family	Família

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Malware	nome	Nome
Agente da ameaça	nome	Nome
Relatório de ameaças	nome	Nome
Relatório de ameaças	publicado	Publicado
Vulnerabilidade	nome	Nome
Vulnerabilidade	severidade	Gravidade

Configurar dicas de ferramentas para mapas de nós

Use esta seção para configurar dicas de ferramentas para relacionamentos de mapa de nós na tela de investigação.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração** > **Controles de Nodemap** > **Configuração de dica de ferramenta**.
2. Selecione o objeto desejado na lista.
   Por padrão, os três registros a seguir são provisionados no sistema de base.
   a. Observáveis
   b. Indicadores
   c. Objetos
3. Selecione **Observável** como um registro de exemplo.
4. Adicione um ou mais valores ao registro observável, se necessário.
   Da mesma forma, adicione valores a indicadores e outros objetos.

   Nota: Cada objeto oferece suporte a no máximo seis valores.

5. Selecione **Salvar** para aplicar as mudanças.
6. Vá para **Tela de investigação** e selecione **Atualizar** ícone.
   Os mesmos valores configurados no **Configuração de dica de ferramenta** a página será exibida em cada mapa de nó.

Trabalhar com fluxos automatizados

Use estas etapas definidas para saber como você pode usar os fluxos automatizados no TISC e seus recursos.

Crie fluxos que são executados com funções do TISC. No TISC, os fluxos são criados para o seguinte:

- Aprimoramento de IOC automatizado
- Analisar, avaliar e disseminar sobre os COIs relacionados à ameaça
- Analise, avalie os IOCs relacionados à ameaça e crie um incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Suporte à Gestão de vulnerabilidades.
- Acompanhamento de vulnerabilidades de dia zero.

Nota: Todos os fluxos são modelos que são enviados no estado de rascunho para os usuários personalizarem ou copiarem de acordo com suas próprias necessidades.

Ações reutilizáveis

Ação de fluxo	Descrição
Adicionar marcador à entidade	Adicionar marcador a uma entidade compatível com ele (observável/indicador/objeto).
Remover marcador da entidade	Removendo marcador para uma entidade compatível com ele (observável/indicador/objeto).
Verificar se o endereço IP está no intervalo CIDR	Verificando se um endereço IP está dentro de um intervalo CIDR.
Verificar se o endereço IP está no intervalo	Verificando se um endereço IP está entre o intervalo De e Para.

Aprimoramento de IOC automatizado

Saiba como automatizar o aprimoramento de IOCs usando fluxos quando eles corresponderem a um determinado critério.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Automatizar o aprimoramento dos gatilhos do IOC somente quando:

- O tipo de observável é um nome de domínio, endereço IPv4 ou endereço IPv6.
- o observável está em um estado processado.
- O observável não tem os marcadores aprimorados ou Ignorar aprimoramento.

Procedimento

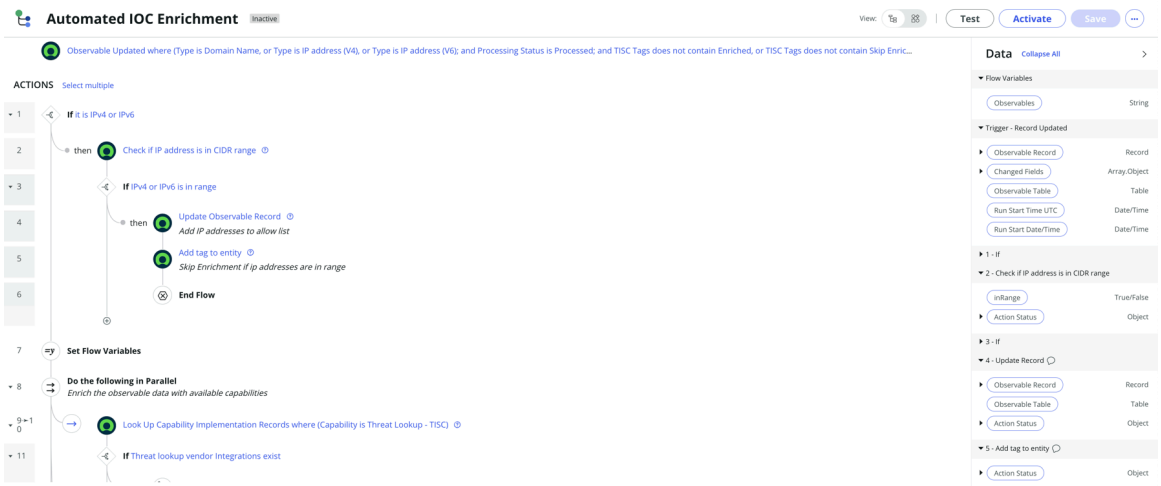
1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos automatizados**.
3. Selecione **Aprimoramento de IOC automatizado** link de ação para exibir os respectivos detalhes da regra no flow designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

   Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched, or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Se o observável for um endereço IPv4 ou IPv6 e estiver dentro de um intervalo CIDR permitido, então:**
   a. Adicione o observável à lista de permissões.
   b. Atualize os marcadores de observáveis para Ignorar aprimoramento.
   c. Encerre o fluxo deste observável.
6. **Caso contrário, enriqueça os dados observáveis com os recursos disponíveis:**
   a. Execute a pesquisa de ameaças e a pesquisa de detecções para coletar informações adicionais sobre o observável.
   b. Atualize o observável com dados aprimorados.
   c. Adicione um marcador **Enriquecido** Indicar que o IOC foi processado.
7. **Além disso, se a reputação do observables estiver limpa, então:**
   a. Marcar observável como falso positivo e desativar.
8. **Caso contrário, se a reputação do observável for desconhecida**
   a. Adicionar marcador **Ameaça potencial e enriquecida** indicar que não é uma ameaça.



Analisar, avaliar e disseminar observáveis

Saiba como analisar e disseminar observáveis relacionados a ameaças.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um aprimoramento de pesquisa de avistamentos é solicitado, ele retorna sem avistamentos.

Procedimento

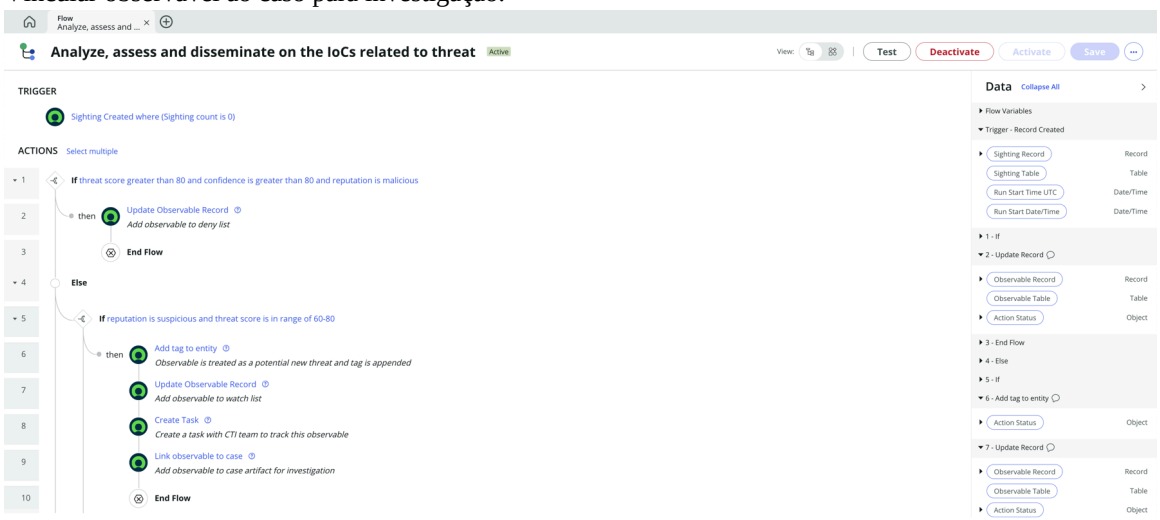
1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos automatizados**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Analisar, avaliar e disseminar nos IOCs relacionados à ameaça** link de ação para exibir os respectivos detalhes da regra no flow designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

   Sighting Created where (Sighting count is 0)

5. **O observável tem uma pontuação de ameaça maior que 80, confiança maior que 80 e reputação mal-intencionada:**
   a. Adicione o observável à lista de proibições.
   b. Encerre o fluxo deste observável.
6. **Caso contrário, a reputação do observável é suspeita e a pontuação de ameaça está no intervalo de 60 a 80:**
   a. Adicione um marcador chamado Potential New Threat.
   b. Adicione o observável à lista de observação.
   c. Crie uma tarefa de caso com a equipe de CTI para rastrear este observável e analisar melhor.
   d. Vincular observável ao caso para investigação.



Analisar e avaliar IOCs de ameaça

Saiba como analisar IOCs que são uma ameaça e notificar a equipe de incidentes de segurança.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um aprimoramento de pesquisa de vistas é solicitado:

- se o observável for avistado (contagem > 0) e.
- A reputação do observável é mal-intencionada e.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A pontuação de ameaça observável é > 80 e.
- Confiança do Observável > 80

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos automatizados**.
3. Selecione **Analisar, avaliar os IOCs relacionados à ameaça e criar incidente** link de ação para exibir os respectivos detalhes da regra no flow designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

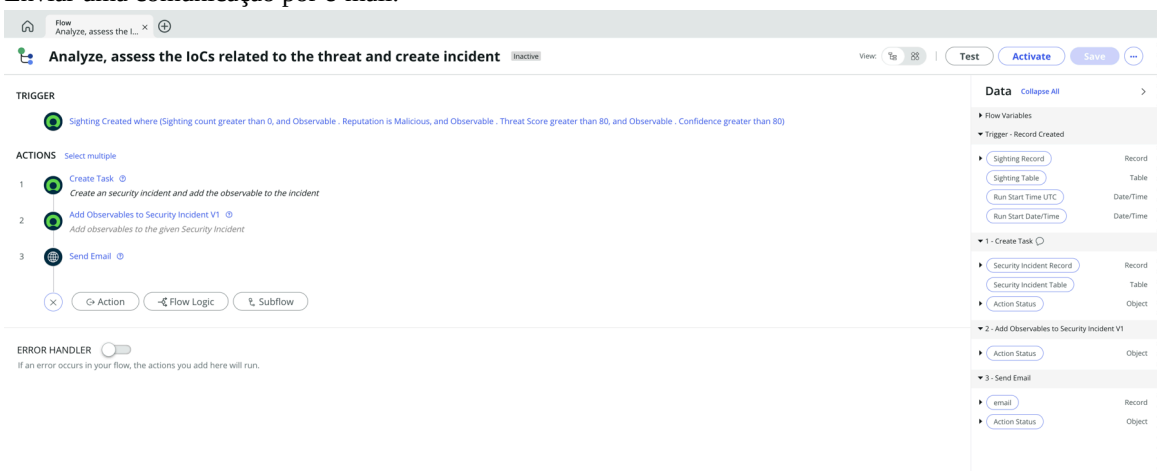
   ```
   Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)
   ```

5. **Se a vista foi criada em (contagem de vistas maior que 0 e observável. A reputação é mal-intencionada e observável. Pontuação de ameaça maior que 80 e observável. Confiança maior que 80), então:**

   a. Crie um incidente de segurança e adicione o observável ao incidente.

   b. Adicionar observáveis ao Incidente de segurança V1.

   c. Enviar uma comunicação por e-mail.



Suporte à Gestão de vulnerabilidades

Saiba como uma nova vulnerabilidade é criada no TISC com uma vulnerabilidade relacionada em VR.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Quando uma nova vulnerabilidade é criada no TISC e há uma vulnerabilidade relacionada no VR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

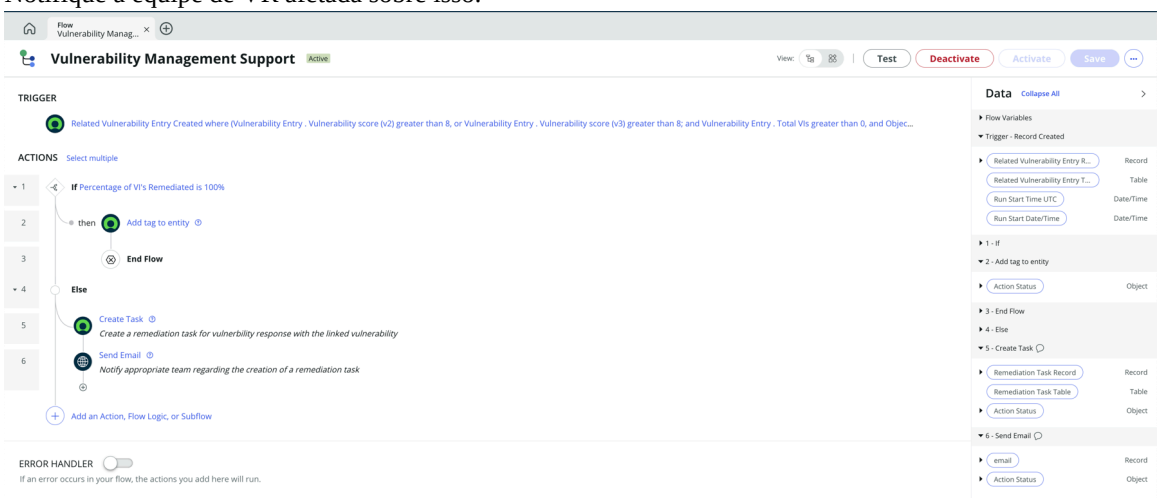
- Se a pontuação de vulnerabilidade de VR (v2) for > 8 OU a pontuação de vulnerabilidade de VR (v3) for > 8.
- O total de IVs associados a ele é maior que 0.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos automatizados**.
3. Selecione **Suporte à Gestão de vulnerabilidades** link de ação para exibir os respectivos detalhes da regra no flow designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

   When new vulnerability is created in TISC and there is a related vulnerability in VR.

5. **Se a porcentagem do total de VIs corrigidos associados a essa vulnerabilidade for 100%, então:**
   a. Adicione um marcador chamado Corrigido ao observável.
6. **Caso contrário, enriqueça os dados observáveis com os recursos disponíveis:**
   a. Crie uma tarefa de correção para VR.
   b. Notifique a equipe de VR afetada sobre isso.



Acompanhamento de vulnerabilidades de dia zero

Saiba como analisar feeds RSS que entram no sistema.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um novo Feed RSS é criado no sistema e ele tem uma menção a "Dia zero" no título ou na descrição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos automatizados**.
3. Selecione **Acompanhamento de vulnerabilidades de dia zero** link para exibir os respectivos detalhes da regra no flow designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

   ```
   RSS Feed Created where (Title contains zero day, or Description contains zero day, or Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or Description contains zero-day)
   ```

5. **Se o observável for um endereço IPv4 ou IPv6 e estiver dentro de um intervalo CIDR permitido, então:**
   a. Crie um caso para a equipe do TISC, junto com uma tarefa de correção para a equipe de VR.
   b. Notifique as equipes de TISC e as equipes de VR envolvidas.

Tabelas de fluxos automatizados

As tabelas a seguir ajudam a entender as tabelas de relacionamento entre entidades e tabelas de aprimoramento que são usadas em fluxos automatizados.

Tabelas de relacionamento entre entidades

Tabela	Entidade
Observável de indicador relacionado	sn_sec_tisc_m2m_indicator_observable
Indicador relacionado	sn_sec_tisc_m2m_indicator
Observável relacionado	sn_sec_tisc_m2m_observable
Relacionamento objeto-objeto	sn_sec_tisc_m2m_object
Objeto do indicador relacionado	sn_sec_tisc_m2m_object_indicator
Relacionamento objeto-observável	sn_sec_tisc_m2m_object_observable

Tabela de aprimoramento

Tabela	Entidade
Resultados da Pesquisa de ameaças	sn_sec_tisc_lookup_result
Detecções	sn_sec_tisc_sighting
Resultados de Aprimoramento do Observável	sn_sec_tisc_observable_enrichment_result

Referência do Central de segurança de inteligência contra ameaças

Os tópicos de referência fornecem informações adicionais sobre Central de segurança de inteligência contra ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações de referência	Links para tópicos
Domain Separation e. Central de segurança de inteligência contra ameaças	Domain Separation e Central de segurança da Inteligência contra ameaças
Componentes instalados com Central de segurança de inteligência contra ameaças aplicação	Componentes instalados com a Central de segurança do Inteligência contra ameaças

Domain Separation e Central de segurança da Inteligência contra ameaças

A separação de domínio é compatível com Central de segurança de inteligência contra ameaças. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui todos os aspectos de **Básico** suporte de nível.
- As propriedades da aplicação reconhecem domínio conforme necessário.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

Domain Separation está habilitada para todos os recursos do Central de segurança de inteligência contra ameaças.

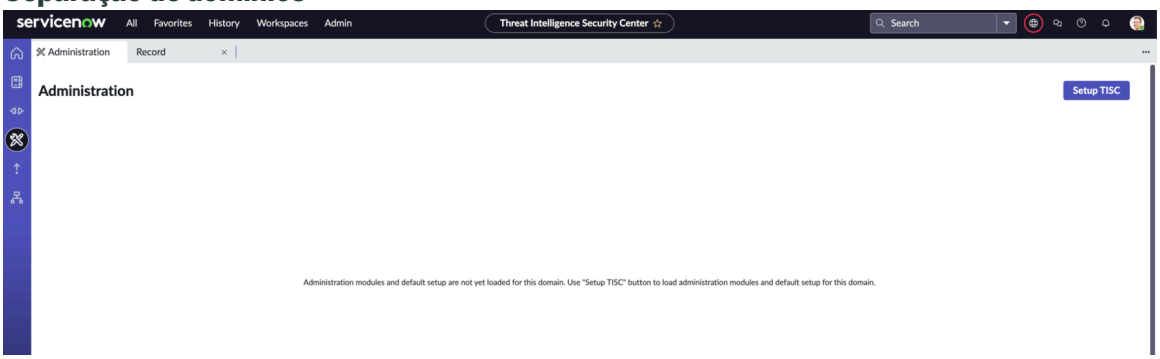
Como o Domain Separation funciona no Central de segurança de inteligência contra ameaças

- Todos os registros relacionados à configuração provisionados no sistema de base são enviados no domínio global. Caso a instância seja separada por domínio, os usuários verão um botão explícito **TISC** em **Administração** Módulo do espaço do TISC. Clique neste botão para clonar as configurações de domínio global provisionadas pelo sistema de base nos respectivos domínios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Separação de domínios



Nota: Os usuários só devem habilitar ou modificar registros de configuração específicos do domínio e não devem habilitar ou modificar registros de configuração no domínio global.

- Algumas regras de notificação da plataforma (sysevent_email_action) são provisionadas no sistema de base. Essas regras de notificação devem ser clonadas nos domínios obrigatórios e somente as regras de notificação específicas do domínio precisam ser habilitadas.

  Nota: Para obter mais informações sobre as notificações de regras, navegue até **Notificação do Sistema** > **Notificações** e filtram todas as regras de notificação de domínio global definidas nas tabelas que começam com o nome `sn_sec_tisc` para entender como os usuários podem identificar as regras de notificação de base que são provisionadas no sistema de base.

- Todas as configurações e dados ingeridos serão específicos para cada domínio, o que significa que os usuários de um domínio não poderão acessar dados de outro domínio.
- Configure um ambiente separado por domínio com esta aplicação instalando Domain Support - Instalador de extensões de domínio plug-in.
- Há colunas de domínio adicionadas para todas as tabelas de aplicações do sistema de base.
- Usando a funcionalidade fornecida pela plataforma, os domínios de locatário gerenciam seus próprios dados de aplicação.
- A lógica de negócios e os processos que podem ser separados por domínio pelo proprietário da instância são iguais aos compatíveis com a plataforma.
- A lógica de negócios e os processos que podem ser administrados pelo domínio do locatário são os mesmos compatíveis com a plataforma.
- Você pode acessar a página Configuração na seção Administração. Clique no link fornecido na seção Administração para exibir a exibição Domain Separation.
- Para oferecer suporte à separação de domínio para os widgets que usam indicadores de PA (Performance Analytics) no painel inicial do TISC, consulte o artigo da base de conhecimento KB1647990 para obter o procedimento detalhado.

Tabelas separadas por domínio

Todas as tabelas são separadas por domínio.

Casos de uso

Todos os recursos desta aplicação são separados por domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Domain Separation para provedores de serviço

Componentes instalados com a Central de segurança do Inteligência contra ameaças

Vários tipos de componentes são instalados quando você baixa e ativa o. Central de segurança de inteligência contra ameaças aplicação, incluindo funções e propriedades do usuário.

Propriedades instaladas

Função necessária: sn_sec_tisc.admin

Usuários com a função Administrador de segurança [sn_sec_tisc.admin] podem modificá-los.

Propriedade	Uso
Propriedades da Central de segurança de inteligência contra ameaças	
Todas as regras de correlação serão desabilitadas. Se só precisarmos desabilitar as regras de correlação selecionadas, use o campo "ativo" na regra de correlação. sn_sec_tisc.disable_correlation_rules	• **Tipo**: verdadeiro | falso • **Valor-padrão**: falso
Esta propriedade é usada para habilitar/desabilitar o processamento de agregados no recurso da calculadora de pontuação de ameaça. sn_sec_tisc.agregados_for_calculator	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
O número de linhas de dados brutos que serão salvas quando uma Pesquisa de vistas for realizada. Intervalo de 0 a 100 sn_sec_tisc.sighting_search_raw_data_rows	• **Tipo**: inteiro • **Valor padrão**: 50
Associe resultados da pesquisa de detecções a ICs no CMDB. sn_sec_tisc.associate_ci_with_sighting_search	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
Isso controlará se os URLs das listas serão danificados ou não sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	• **Tipo**: verdadeiro | falso • **Valor-padrão**: falso
Esta propriedade permitirá que as técnicas MITRE sejam acumuladas automaticamente para casos dos incidentes de segurança ou objetos associados. sn_sec_tisc.auto_rollup_mitre_data	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
Se verdadeiro, mostrará todas as táticas (incluindo aquelas sem técnicas associadas ao caso) para as listas do MITRE renderizadas no relatório.	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_sec_tisc.show_all_tactics_reporting	
SYS ID do modelo de cliente de e-mail para a tabela Caso (sn_sec_tisc_case) que será usada no relatório de compartilhamento. sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	• **Tipo**: cadeia de caracteres • **Valor padrão** b55e22c5444021060eee0ea78b8f2df
O nível de TLP padrão é aplicado ao criar um novo registro. Se não for definido manualmente no formulário, este valor será usado. sn_sec_tisc.tlp_default_value	• **Tipo**: lista de seleção • **Valor padrão** 955c9e5543d35110baf06e434ab8f2fb
Nível de registro em log: depurar, informativo, aviso, erro sn_sec_tisc.logging.detalhamento	• **Tipo**: lista de seleção • **Valor padrão**: info
Propriedades de feeds de inteligência contra ameaças	
Tempo máximo em segundos que uma conexão HTTP de saída aguarda para obter dados de coleta de TAXII sn_sec_tisc.taxii.http.max_timeout	• **Tipo**: inteiro • **Valor padrão**: 300
Número máximo de objetos recuperados em uma chamada REST de um servidor TAXII (aplicável somente para TAXII versões 2.0 e 2.1) sn_sec_tisc.taxii.max_page_size	• **Tipo**: inteiro • **Valor padrão** : 5000
Número máximo de novas tentativas para um TAXII2 com falha. X chamada REST sn_sec_tisc.taxii2.retry_count	• **Tipo**: inteiro • **Valor padrão**: 3
Número máximo de objetos recuperados em uma chamada REST do servidor Cyware TAXII sn_sec_tisc.cyware_taxii.max_page_size	• **Tipo**: inteiro • **Valor padrão**: 1000 **Nota:** Especifica o tamanho da página usado ao buscar dados de coleções TAXII relacionadas ao Feed do Cyware TAXII. Para todas as outras coleções TAXII, o tamanho da página recuperado da coleção TAXII é padronizado para o valor definido na propriedade correspondente: sn_sec_tisc.taxii.max_page_size .
Número de registros a serem obtidos por vez do CrowdStrike. Maior o número, mais a memória seria consumida para processar a carga.	• **Tipo**: inteiro • **Valor padrão**: 1000

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_sec_tisc.crowdstrike_api_limit	
Denota o número de indicadores a serem extraídos em uma única chamada de API. **Nota:** Aplicável somente quando a integração não encontra o necessário presente no sistema. sn_sec_tisc.crowdstrike_indicator_batch_size	• **Tipo**: inteiro • **Valor padrão**: 1000
Denota o número de atores a serem extraídos em uma única chamada de API. **Nota:** Aplicável somente quando a integração não encontra o necessário presente no sistema. sn_sec_tisc.crowdstrike_ator_batch_size	• **Tipo**: inteiro • **Valor padrão**: 1000
Denota o número de relatórios a serem extraídos em uma única chamada de API. **Nota:** Aplicável somente quando a integração não encontra o necessário presente no sistema. sn_sec_tisc.crowdstrike_report_batch_size	• **Tipo**: inteiro • **Valor padrão**: 50
O total permitido de deslocamento e limite da API do CrowdStrike. sn_sec_tisc.crowdstrike_offset_limit_total	• **Tipo**: inteiro • **Valor padrão** : 50000
Propriedades para REST APIs	
Define o tamanho máximo da página (número máximo de observáveis retornados como parte da resposta) para a API Obobservables Fetch. Aumentar para um valor alto, pois isso pode afetar o tempo de resposta da API. sn_sec_tisc.api_maximum_page_size_limit	• **Tipo**: inteiro • **Valor padrão**: 1000
Define o número máximo de observáveis que podem ser enviados no corpo da solicitação para a API de adição de observáveis. Aumentar para um valor alto, pois isso pode afetar o tempo de resposta da API. sn_sec_tisc.add_obs_api_max_records	• **Tipo**: inteiro • **Valor padrão**: 100
Propriedades dos webhooks	
Número máximo de eventos a serem enviados como parte de uma solicitação de webhook. O tamanho do lote será limitado a 2000 mesmo se um valor maior for definido nesta propriedade. sn_sec_tisc.webhook_max_event_batch_size	• **Tipo**: inteiro • **Valor padrão**: 100

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
Número de vezes que uma solicitação com falha deve ser tentada novamente antes de marcá-la como erro e passar para o próximo lote de eventos. A contagem de novas tentativas será limitada a 10 mesmo se um número maior for definido nesta propriedade. sn_sec_tisc.webhook_retry_count	• **Tipo**: inteiro • **Valor padrão**: 100
Número de segundos de espera antes de tentar novamente um lote com falha. Isso aumentará exponencialmente com base na contagem de novas tentativas. Por exemplo, se retry_count for 3 e retry_interval for 30, as novas tentativas serão disparadas após 30, 60 e 120s. O intervalo de novas tentativas inicial será limitado a 300 segundos, mesmo se um valor mais alto for definido nesta propriedade. sn_sec_tisc.webhook_retry_interval	• **Tipo**: inteiro • **Valor padrão**: 30
Ignorar eventos de webhook acionados pela reaplicação da pontuação de ameaça sn_sec_tisc.webhook_ignore_threat_score_reaplicar	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
Propriedades da tela de investigação	
Definir o valor como verdadeiro adiciona novos nós ao canto superior esquerdo, enquanto definir como falso os adiciona ao centro da tela. sn_sec_tisc.canvas_suspend_reLayout	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
Propriedades para exportação em formatos CTI	
Número máximo de linhas que podem ser exportadas para um arquivo STIX 2.1 sn_sec_tisc.stix_export_limit	• **Tipo**: inteiro • **Valor padrão** : 10000
Incluir campos de tipo de Diário no arquivo de exportação. sn_sec_tisc.export_journal_fields	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro

Tradução automática

Trabalhos agendados

A tabela a seguir descreve os trabalhos agendados:

Trabalho	Descrição
Registros de origem do indicador agregado	Agrega registros de origem do indicador.
Agregar registros de origem de objeto	Agrega registros de origem do objeto.
Agregar registros de origem do observável	Agrega registros de origem observável.
Limpeza de importações obsoletas	Limpa registros de trabalho de importação obsoletos.
Limpeza de novos nós não utilizados da tela	Limpa novos nós não utilizados da tela.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Limpar registros de download de arquivo seguro	Limpa registros de download seguro de arquivos.
Registros de origem do indicador de desduplicação	Registros de origem do indicador desduplicados.
Registros de origem de objeto de desduplicação	Registros de origem de objeto desduplicados.
Desduplicar registros de origem do observável	Desduplica registros de origem observável.
Desativar indicadores expirados	Desativa registros de indicador expirados.
Desativar objetos expirados	Desativa registros de objeto expirados.
Desativar observáveis expirados	Desativa registros observáveis expirados
Migrar dados de TI para o TISC	Processa registros de execução de trabalho de migração pendentes
Preencha registros agregados para registros de origem do indicador	Identifica o registro agregado primário para registros de origem de indicador recém-criados
Preencha registros agregados para registros de origem de objeto	Identifica o registro agregado primário para registros de origem de objeto recém-criados.
Preencha registros agregados para registros de origem do observável	Identifica o registro agregado primário para registros de origem observável recém-criados.
Preencher Referência de TISC no TI	Preenche a referência do observável agregado do TISC no registro do observável de TI.
Importações aprovadas de processo	Processa trabalhos de importação aprovados.
Processar registros de fila importados do MISP DSM	Registros de fila de ingestão do feed MISP em fases processados.
Processar registros importados da fila de importação do indicador MISP	Processa dados do MISP em fases ingeridos da inteligência de importação
Processar registros importados da fila de importação do STIX	Processa dados do STIX em fases ingeridos da inteligência de importação
Processar registros importados da fila de importação do STIX - Ingestão	Processa dados do STIX em fases ingeridos de feeds de ameaças.
Processar migração de artefatos de caso pendentes	Migra artefatos de caso da aplicação de inteligência contra ameaças para a central de segurança Inteligência contra ameaças.
Processar registros pendentes da fila de ingestão de origem da ameaça	Processa registros de fila de ingestão de origem pendentes.
Processar entidades enfileiradas para a Calculadora de pontuação de ameaça	processa entradas de fila da calculadora de ameaças pendentes
Processar registros de fila do MISP DSM enfileirados	Processa dados MISP enfileirados ingeridos do feed de ameaças
Processar registros da fila de importação do indicador MISP na fila	Processa dados de MISP enfileirados ingeridos da inteligência de importação
Processar registros da fila de importação do STIX enfileirados - Ingestão	Processa dados do STIX enfileirados ingeridos de feeds de ameaças.
Processar registros da fila de importação do indicador STIX na fila	Processa dados do STIX enfileirados ingeridos da inteligência de importação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Fila do webhook de processo	Processa registros de fila de webhook pendentes.
Agregar novamente os registros de origem	Agrega novamente os registros de origem dos quais os registros agregados são excluídos.
Remover registro de origem filtrado	Limpa registros de origem filtrados
Retomar o Verificação de processo de integração do CrowdStrike/Reprocessar registros de origem do CrowdStrike	Reinicia as execuções de integração de feed do CrowdStrike aguardando limite de taxa/registros de origem de relatório para agregar relacionamentos
Contagem de observáveis falso-positivos de sincronização	Sincroniza contagens de falsos positivos observáveis com contagens positivas de flase por origem
TISC Criar lotes de webhook	Lotes criados para entradas de fila de webhook enfileiradas para processamento
Webhooks do TISC Fire	Executa lotes de webhook pendentes
Atualizando coluna Arquivada de Relacionamento	Atualiza o status de arquivamento dos registros de origem e destino do relacionamento

Como usar o Central de segurança de inteligência contra ameaças

Usar Central de segurança de inteligência contra ameaças Para gerenciar registros da biblioteca Inteligência contra ameaças, importar dados de ameaças externas e simplificar a gestão de casos. Ele ajuda as equipes de segurança a centralizar os dados de inteligência, aprimorar a análise e responder de forma mais eficaz às ameaças, integrando as informações relevantes nas investigações em andamento.

Integração do TISC com o SIR Workspace

A integração do TISC com o SIR anexa automaticamente o contexto nos observáveis no espaço Incidente de segurança para os Analistas de segurança. Novos observáveis do SIR podem ser enviados para o TISC para análise adicional pela equipe de CTI usando as ações de IU fornecidas nas telas.

Todos os resultados de aprimoramento produzidos a partir de integrações disponíveis somente no SIR também podem ser enviados usando as ações de IU fornecidas no espaço.

Trabalhando com importações de dados

As importações de dados permitem que você exiba todos os registros que estão sendo processados para o trabalho de importação e também lista os trabalhos de importação que estão aguardando aprovações.

Exibindo todas as importações

Use esta seção para exibir todos os registros importados que são exibidos na exibição de lista para todos os usuários.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Todas as importações**
   Esta página exibe todos os registros que estão sendo processados para o trabalho de importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra qualquer registro para exibir o status do processo de importação.

> **Nota:** Você também pode clicar em **Nova importação** para criar um novo registro de importação. Depois de clicar neste botão, a aplicação direcionará você para **Inteligência de importação** página. Para obter mais informações sobre como criar novos registros, consulte Importar Inteligência em TISC e prossiga com o respectivo tipo de importação.

Exibindo minhas importações

Use esta seção para exibir os registros de importação criados pelo usuário conectado.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Minhas importações**
   Esta página exibe todos os registros de importação que são categorizados para processo adicional para o trabalho de importação.
3. Abra qualquer registro para exibir o status do processo de importação.

> **Nota:** Você também pode clicar em **Nova importação** para criar um novo registro de importação. Depois de clicar neste botão, a aplicação direcionará você para **Inteligência de importação** página. Para obter mais informações sobre como criar novos registros, consulte Importar Inteligência em TISC e prossiga com o respectivo tipo de importação.

4. Exiba o resumo dos registros de importação.

> **Nota:** Se algum dos trabalhos de importação não for enviado, você poderá **Enviar** os registros para processamento posterior e enviá-los para aprovação. Se a aprovação não for necessária para esse trabalho de importação específico, esses registros serão processados automaticamente.

Exibindo minhas aprovações

Use esta seção para revisar e aprovar os registros de trabalho de importação.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Minhas aprovações**
   Esta página exibe todos os registros de importação que estão aguardando aprovação do usuário conectado.
3. Abra qualquer registro para aprovar ou rejeitar o registro de importação.
4. Clique em **Aprovar** para aprovar o registro do trabalho de importação.
   . **Aprovar importação** é exibida e uma mensagem de confirmação é exibida se as importações selecionadas devem ser aprovadas.

> **Nota:** Uma notificação por e-mail é enviada para os respectivos usuários informando que o trabalho de importação que estava em andamento agora foi aprovado. Para obter mais informações sobre regras de aprovação, consulte Definir regras de aprovação de importações de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Aprovar** na caixa de diálogo.
   Uma notificação por e-mail é enviada para o usuário que criou o trabalho de importação e o trabalho de importação que estava em andamento agora é aprovado.
6. Clique em **Rejeitar** para rejeitar um registro.

Nota:

- Você pode revisar e reenviar o trabalho de importação rejeitado. Adicione comentários para rejeição.
- Uma notificação por e-mail é enviada ao usuário que criou o trabalho de importação quando o trabalho de importação que estava em andamento é rejeitado.
- Uma notificação por e-mail é enviada aos aprovadores que solicitam a aprovação.

Importar Inteligência em TISC

Use este recurso para importar manualmente dados de inteligência contra ameaças para o repositório, permitindo que os analistas ingerem as informações relevantes de fontes externas conforme necessário.

Os seguintes formatos são compatíveis com a importação de dados de inteligência contra ameaças:

Formato de importação	Descrição	Registros compatíveis
Importar do arquivo estruturado	Baixe o arquivo de amostra usando o link Visualizar e carregue seus dados estruturados em um formato compatível, como CSV, XLS ou XLSX.	• Observáveis • Indicadores
Importar do formato padrão	Os tipos de arquivo compatíveis incluem os formatos JSON STIX 2.x e JSON MISP.	• **STIX 2,1** Observáveis, indicadores • **MISP** Observáveis
Importar de texto simples	Analise a entrada como texto bruto para importar observáveis. O limite máximo de caracteres para a entrada é de 10 000 caracteres.	Observáveis
Importar do arquivo (não estruturado)	A aplicação analisará automaticamente o arquivo carregado para extrair observáveis. Tipos de arquivo compatíveis: Txt, CSV, JSON, XLS e XLSX.	Observáveis

Para entender melhor cada formato de importação e os tipos de registros compatíveis, consulte a seção Informações relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

- Importar dados usando arquivo estruturado
- Importe dados usando o formato padrão
- Importe dados usando texto bruto
- Importe dados usando o formato de arquivo não estruturado

Importar dados usando arquivo estruturado

Carregue os dados estruturados nos formatos de arquivo compatíveis, como CSV, XLSX ou XLS.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca Intel de ameaças é exibida.
2. Clique em **Inteligência de importação** .
3. Clique em **Importar do arquivo estruturado** cartão.

> **Importante:** Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou Arquivo Estruturado, o tamanho do arquivo é limitado a 5 MB. O limite de caracteres para texto bruto é limitado a 10 000.

4. No formulário, preencha os campos.

Campo	Descrição
Escolha uma opção	Selecione a opção necessária na lista suspensa, como observáveis ou indicadores. ○ **Observáveis** : Selecione os dados observáveis a serem importados. **Nota:** Se você estiver importando dados de observáveis. Também não modifique os cabeçalhos de coluna no arquivo. Os campos Obrigatórios são Valor e Tipo, e outros são opcionais. Insira a data/hora no formato AAAA-MM-DDThh:mm:ssZ. ○ **Indicadores** : Selecione os dados dos indicadores a serem importados. **Nota:** Selecione esta opção se você estiver importando dados de indicadores. Também não modifique os cabeçalhos de coluna no arquivo. Os campos obrigatórios para indicadores são Padrão, Tipo de padrão e Válido de e outros são opcionais. Insira a data/hora no formato AAAA-MM-DDThh:mm:ssZ.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visualizar e baixar arquivo de amostra para Indicadores	Use este link para baixar o arquivo de amostra usando o link Visualizar e carregar os dados estruturados em um formato de arquivo compatível, como CSV, XLS ou XLSX. **Nota:** Os cabeçalhos das colunas devem corresponder exatamente aos cabeçalhos. Os campos Valor, Tipo são obrigatórios para cada observável no arquivo. Os campos restantes são opcionais em que Como visto pela primeira vez, Visto pela última vez deve estar em números e são o tempo de época em milissegundos.
Carregar arquivo	Clique neste link para carregar os dados do arquivo no formato de arquivo de estrutura recomendado. **Nota:** Você só pode carregar um arquivo de cada vez. Para adicionar um novo arquivo, você deve remover o existente e adicionar um novo arquivo.
Definir definições	
TLP	Selecione o indicador Protocolo de semáforo (TLP) na lista suspensa a ser aplicado aos registros importados. TLP está em TISC é rotulado com cores diferentes para garantir que os dados confidenciais sejam compartilhados com os usuários pretendidos. ○ LIMPAR: As informações podem ser compartilhadas sem restrições. ○ VERMELHO ○ E ESTRITO ○ ÂMBAR ○ VERDE
Confiança (0–100)	Defina o valor de confiança entre 0-100 para os registros importados.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Adicionar observáveis(s) à Lista de controle de segurança	Selecione esta opção para adicionar observáveis à lista de controle de segurança apropriada. Esta opção permite adicionar diretamente os observáveis a uma lista de controle de segurança durante a importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	As opções disponíveis na lista suspensa são: ○ Lista de permissões ○ Lista de proibições ○ Nenhum(a) A opção padrão é **Nenhum** .
Marcadores	
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador no **Pesquisa** para escolher os marcadores disponíveis no sistema ou insira o novo nome do marcador e clique em **Adicionar** para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia dos dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência contra ameaças. Por exemplo, nomenclatura do CAPEC. Para obter mais informações, consulte Criando taxonomias. **Nota:** As opções de valor de taxonomia mudam com base na taxonomia selecionada.
Substituir valor de origem	Marque esta caixa de seleção se quiser substituir os valores de origem para TLP, Confiança, Expiração, Marcadores e taxonomias pelos valores configurados. Se você não marcar esta caixa de seleção, os valores configurados serão aplicados se não estiverem vazios.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

Nota: A revisão de registros importados não é compatível com a opção STIX.

Depois de clicar em **Próximo** , você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo fornece todos os registros que precisam ser importados.

O usuário pode executar qualquer tipo de atividade e os vários usuários podem colaborar usando a seção de comentários que está disponível no menu contextual direito. A lista de registros importados será renderizada quando o arquivo inteiro ou o texto bruto for processado. O processamento de importação de arquivos grandes levará mais tempo e, enquanto estiver sendo processado, você também pode verificar o status, revisar e enviar na página de registro de importação.

Nota: Todos os registros que falharem nas validações serão ignorados do processo de importação e esses registros não serão exibidos na página Revisar e enviar para processamento posterior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Tipo de atualização** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

> **Nota:** Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não exigir o processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente durante o envio da solicitação.

10. Clique em **Exibir status** para exibir o status do registro de importação ou clique em **Concluído** .
    O registro exibe o status Processado depois que os dados são importados para processamento.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Importe dados usando o formato padrão

Carregue os dados padrão nos formatos de arquivo compatíveis, como STIX 2.x JSON, MISP JSON.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca Intel de ameaças é exibida.
2. Clique em **Inteligência de importação** .
3. Clique em **Importar do arquivo padrão** cartão.

> **Importante:** Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou Arquivo Estruturado, o tamanho do arquivo é limitado a 5 MB. O limite de caracteres para texto bruto é limitado a 10 000.

4. No formulário, preencha os campos.

Campo	Descrição
Formato do arquivo	Selecione a opção necessária na lista suspensa, como STIX 2.x JSON ou MISP JSON. ○ **STIX 2.x JSON** : Selecione o formato no STIX 2.x JSON a ser importado. **Nota:** Somente observáveis e indicadores serão importados do arquivo STIX carregado. Todos os outros tipos de objeto serão ignorados durante o processo de importação. ○ **JSON MISP** : Selecione o formato no formato JSON MISP a ser importado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Carregar arquivo	Clique neste link para carregar os dados no formato de arquivo padrão.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de pesquisa para escolher os marcadores disponíveis no sistema ou insira o novo nome do marcador e clique em Adicionar para atribuí-lo à origem.
Adicionar observáveis(s) à Lista de controle de segurança	Selecione esta opção para adicionar observáveis à lista de controle de segurança apropriada. Esta opção permite adicionar diretamente os observáveis a uma lista de controle de segurança durante a importação. As opções disponíveis na lista suspensa são: ○ Lista de permissões ○ Lista de proibições ○ Nenhum(a) A opção padrão é **Nenhum** .
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia dos dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência contra ameaças. Por exemplo, nomenclatura do CAPEC. Para obter mais informações, consulte Criando taxonomias.
Selecione Valores de taxonomia	Indica os valores de taxonomia associados à taxonomia.
Substituir valor de origem	Marque esta caixa de seleção se quiser substituir os valores de origem para TLP, Confiança, Expiração, Marcadores e taxonomias dos valores configurados. Se você não marcar esta caixa de seleção, os valores padrão serão aplicados.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A revisão de registros importados não é compatível com a opção STIX.

Depois de clicar em **Próximo**, você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo fornece todos os registros que precisam ser importados.

O usuário pode executar qualquer tipo de atividade e os vários usuários podem colaborar usando a seção de comentários que está disponível no menu contextual direito.

Nota: Todos os registros que falharem nas validações serão ignorados do processo de importação e esses registros não serão exibidos na página Revisar e enviar para processamento posterior.

7. Clique em **Tipo de atualização** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

Nota:

Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não exigir o processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente durante o envio da solicitação.

10. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído**.
    O registro exibe o status Processado depois que é processado.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Importe dados usando texto bruto

Importe os dados observáveis copiando e colando texto bruto ou inserindo o texto livre.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca Intel de ameaças é exibida.
2. Clique em **Inteligência de importação**.

Importante:

- Todos os caracteres de depuração serão limpos como parte da análise e extração de observáveis.
- Para esta opção de texto colado, somente URL, domínio, nome de arquivo, hashes e endereço IP serão extraídos e nenhum outro tipo de observável será extraído para a importação de dados e, no caso de observáveis como registro, tipos de diretório, esses serão ignorados da importação.

3. Clique em **Importar do texto bruto** cartão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Ao importar os dados de inteligência contra ameaças no formato de texto bruto, os caracteres são limitados a 10 000. A opção de texto bruto pode ser usada como uma solução alternativa para extrair os observáveis do PDF.

4. No formulário, preencha os campos.

Campo	Descrição
Caixa de texto de dados brutos	Insira ou copie e cole o texto bruto aqui nesta caixa de texto. **Nota:** Você só pode inserir ou colar o texto bruto em 10 000 caracteres.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Adicionar observáveis(s) à Lista de controle de segurança	Selecione esta opção para adicionar observáveis à lista de controle de segurança apropriada. Esta opção permite adicionar diretamente os observáveis a uma lista de controle de segurança durante a importação. As opções disponíveis na lista suspensa são: ○ Lista de permissões ○ Lista de proibições ○ Nenhum(a) A opção padrão é **Nenhum** .
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Digite o nome do marcador na barra de pesquisa para escolher os marcadores disponíveis no sistema ou insira o novo nome do marcador e clique em Adicionar para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia dos dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência de ameaças. Por exemplo, nomenclatura do CAPEC. Para obter mais informações, consulte Criando taxonomias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

   Depois de clicar em **Próximo** , você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo fornece todos os registros que precisam ser importados.

   O usuário pode executar qualquer tipo de atividade e os vários usuários podem colaborar usando a seção de comentários que está disponível no menu contextual direito.

   Nota: Todos os registros que falharem nas validações serão ignorados do processo de importação e esses registros não serão exibidos na página Revisar e enviar para processamento posterior.

7. Clique em **Tipo de atualização** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

   Nota: Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não exigir o processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente durante o envio da solicitação.

10. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído** .
    O registro exibe o status Processado depois que é processado.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Importe dados usando o formato de arquivo não estruturado

Carregue os dados em um formato não estruturado compatível com os formatos de arquivo como TXT, CSV, JSON, XLS, XLSX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca Intel de ameaças é exibida.
2. Clique em **Inteligência de importação** .

   Importante:

   - Todos os caracteres de depuração serão limpos como parte da análise e extração de observáveis.
   - Para esta opção de formato de arquivo não estruturado, somente URL, domínio, nome de arquivo, hashes e endereço IP serão extraídos e nenhum outro tipo de observável será extraído para a importação de dados e, no caso de observáveis como registro, tipos de diretório, esses serão ignorados da importação.

3. Clique em **Importar do arquivo (não estruturado)** cartão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou Arquivo Estruturado, o tamanho do arquivo é limitado a 5 MB.

4. No formulário, preencha os campos.

Campo	Descrição
Carregar arquivo	Clique neste link para carregar os dados no formato de arquivo padrão.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de vencimento dos observáveis associados. **Nota:** Este é um campo obrigatório.
Adicionar observáveis(s) à Lista de controle de segurança	Selecione esta opção para adicionar observáveis à lista de controle de segurança apropriada. Esta opção permite adicionar diretamente os observáveis a uma lista de controle de segurança durante a importação. As opções disponíveis na lista suspensa são: ○ Lista de permissões ○ Lista de proibições ○ Nenhum(a) A opção padrão é **Nenhum** .
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de pesquisa para escolher os marcadores disponíveis no sistema ou insira o novo nome do marcador e clique em **Adicionar** para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia dos dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência contra ameaças. Por exemplo, nomenclatura do CAPEC. Para obter mais informações, consulte Criando taxonomias.

5. Revise os dados antes do envio para processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de clicar em **Próximo** , você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo fornece todos os registros que precisam ser importados.

O usuário pode executar qualquer tipo de atividade e os vários usuários podem colaborar usando a seção de comentários que está disponível no menu contextual direito.

Nota: Os formatos compatíveis para importar os dados são TXT, CSV, JSON, XLS e todos os registros que falharem nas validações são ignorados do processo de importação e esses registros não são exibidos na página Revisar e enviar para processamento.

6. Clique em **Tipo de atualização** e selecione o tipo para atualizar qualquer tipo de registros importados.
7. Clique em **Excluir** para excluir qualquer tipo de registros importados.
8. Clique em **Enviar**.

Nota: Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não exigir o processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente durante o envio da solicitação.

9. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído** .
   O registro exibe o status Processado quando o envio é bem-sucedido.
10. Clique em **Cancelar** para anular o processo de importação.
11. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Workbench do analista de ameaça

A página Workbench do analista de ameaças consiste em casos e tarefas de caso que estão em Analistas de ameaças e sua equipe.

Use **Gestão de casos** recurso para criar e rastrear as investigações de ameaças e as atividades de análise.

Durante as investigações de ameaças, os analistas coletam os dados de registros de inteligência interna, como observáveis, agentes de ameaça, campanhas e assim por diante.

Visão geral do workbench

A página Visão geral do Workbench consiste nas tarefas do caso e nos casos que estão sob análise de ameaças e sua equipe.

A visão geral lista todos os casos em aberto e seus status, o que ajuda os analistas a gerenciar sua carga de trabalho e priorizar suas investigações.

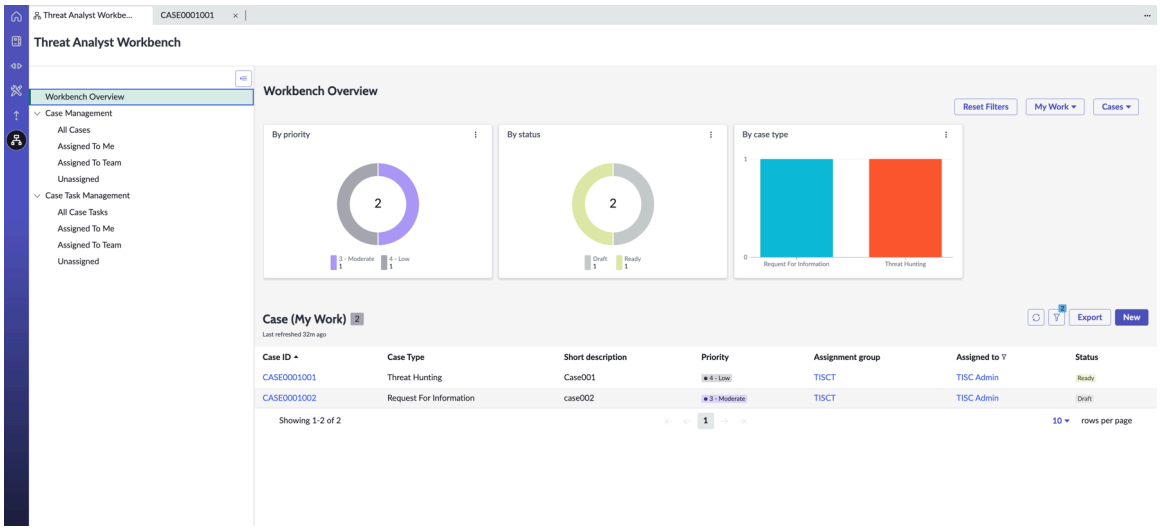
Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Depois que o caso for criado, os analistas atribuirão as tarefas do caso a outros analistas ou equipes para investigação adicional e também colaborarão com eles para compartilhar informações e informações.

Cada filtro é agrupado por prioridade, status e tipo de caso, que estão nas filas dos analistas de ameaças e na fila da equipe de analistas de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando filtros são aplicados nos widgets, a metade inferior da página de visão geral é preenchida com os casos ou tarefas de caso correspondentes apresentados como itens de lista. Para remover os filtros aplicados, clique em **Redefinir filtros** para redefini-lo para a exibição original.

Usando esta página, os analistas e administradores de ameaças podem exibir seu trabalho, o trabalho das equipes e qualquer trabalho não atribuído. Você pode navegar até a lista suspensa. As opções disponíveis são:

- Meu trabalho: Selecione esta opção para exibir o trabalho atribuído a você.
- Trabalho da minha equipe: Selecione esta opção para exibir o trabalho da sua equipe atribuído a todos os grupos dos quais você faz parte.
- Trabalho não atribuído: Selecione esta opção para exibir o caso ou a tarefa de caso que não estão atribuídos. Para atribuir o caso ou a tarefa do caso, você deve ir para a exibição do formulário e atribuir o(s) usuário(s) ou grupo(s) de usuários ao caso e às tarefas do caso.

Você também pode exibir casos e tarefas de caso diretamente na Visão geral do Workbench que são atribuídos a você. Por padrão, a exibição do caso é exibida. Você pode usar o menu suspenso e selecionar as tarefas do caso se quiser exibir as tarefas do caso por prioridade e status.

Criação de casos usando Workbench de analista de ameaças

Os casos são usados para rastrear informações sobre uma campanha ou agente de ameaça que ameaça sua organização. Depois que um caso é criado, você pode adicionar artefatos que permitem revisar e analisar todas as informações relacionadas de um único caso ou tarefa de caso.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha os campos, se for o caso.

Criar novo caso

Campo	Descrição
ID do caso	Um identificador exclusivo do caso. Este é o ID gerado pelo sistema.
Descrição Resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Descrição	Uma descrição detalhada, incluindo todas as informações relevantes sobre o caso, como histórico, qual análise é necessária, resultados esperados.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado. As opções possíveis para a investigação são: ○ Busca de ameaças ○ Solicitação de informações ○ Caso de gestão de vulnerabilidade ○ Caso de conformidade ○ Caso de resposta do incidente ○ Caso de colaboração ○ Outros
Prioridade	Uma avaliação da gravidade da solicitação ou problema.
Grupo de atribuição	O grupo atribuído responsável por trabalhar no caso.
Status	O status atual do caso.
Atribuição a	O analista responsável por trabalhar em um caso.
Data de vencimento	A data e a hora em que a tarefa deve ser concluída ou encerrada.
Colaboradores	A lista de designados acumulada de tarefas e deve ser possível adicionar sobre ela.
TLP	Valor exclusivo que indica a configuração de confidencialidade de dados por TLP.
Participantes da lista de observação	Quando um usuário é adicionado à lista de observação, a pessoa receberá notificações por e-mail sobre mudanças de status e prioridade.
Impor restrição	Marque esta caixa de seleção para modificar membros do grupo permitido e membros permitidos. Para obter mais informações, consulte Restrições impostas para caso(s).

6. Preencha os campos na seção Informações, conforme apropriado.

Tradução automática

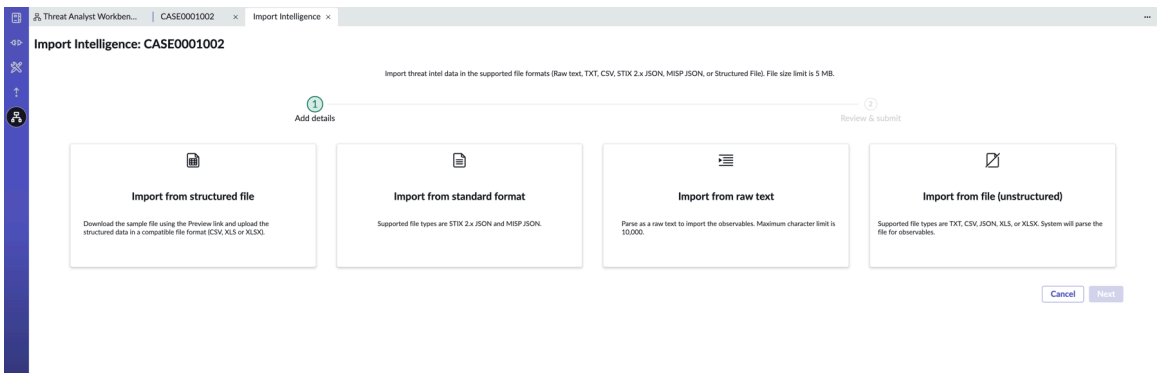
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Quaisquer anotações adicionais relacionadas à investigação de ameaça.
Recomendações ou ações	Todas as recomendações ou ações relacionadas à investigação de ameaça.
Análise e descobertas	Insira a análise e as descobertas relacionadas à investigação de ameaça.
Resumo do fechamento	Adicione o resumo de fechamento das descobertas.

7. Clique em **Salvar**.
   Depois que o registro for salvo, você pode clicar em **Inteligência de importação** para importar os dados de inteligência contra ameaças usando **Inteligência de importação** recurso.

   Nota: Se você estiver importando e processando dados do Gestão de casos, um exclusivo será associado ao registro de importação.



Restrições impostas para caso(s)

Use este recurso para restringir um caso e fornecer uma lista de grupos e usuários que podem acessá-lo.

Função necessária:

- sn_sec_tisc.analyst
- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

Principais considerações

1. Restringir um caso e fornecer uma lista de grupos/usuários que podem acessá-lo.
2. Impor campo Restrição na página do formulário Caso.
3. Modifique membros do grupo permitido e membros permitidos.
4. Quando um caso é marcado como restrito, somente membros de grupos permitidos, membro da lista de usuários permitidos e usuário com a função sn_sec_tisc.admin podem acessar este caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Conceda acesso ao analista (sn_sec_tisc.restriction_access_manager com esta função) que precisa acessar o campo Impor restrição.
6. O analista e analista assigned_to existentes que o marcou como restrito também perderão o acesso se não forem adicionados aos grupos ou membros permitidos.
7. A restrição de caso na equipe de CTI é implementada por caso. Membros permitidos podem acessar casos restritos se estiverem na lista permitida. Colocá-los em uma das listas de casos permitidos não implica que eles possam acessar todos os outros casos restritos.
8. Se o caso estiver marcado como restrito e membros permitidos ou o grupo permitido for deixado em branco, somente sn_sec_tisc.admin poderá acessar esses casos restritos.
9. Somente os grupos que têm a função de analista (sn_sec_tisc.analyst) atribuída são permitidos na lista Membros permitidos e Grupos permitidos.

Nota: Uma anotação de trabalho será publicada se um caso estiver marcado como restrito.

Controles de acesso para um caso

Permitir controles de acesso específicos a um caso.

A tabela a seguir descreve as funções e os controles de acesso.

Função	Acesso	Descrição
sn_sec_tisc.restriction_access_manager	Acesso de leitura	Os usuários externos adicionados aqui terão acesso para exibir o formulário do caso, mas não poderão editar nenhum campo no caso ou executar nenhuma ação.
	Acesso privilegiado	Os usuários externos adicionados aqui terão acesso para editar qualquer campo no formulário Caso, mas não terão permissão para executar orquestrações.
sn_sec_tisc.special_access_read_manager	Acesso de leitura	Os usuários externos adicionados aqui terão acesso para exibir o formulário do caso, mas não poderão editar nenhum campo no caso ou executar nenhuma ação.
sn_sec_tisc.special_access_write_manager	Acesso privilegiado	Os usuários externos adicionados aqui terão acesso para editar qualquer campo no formulário Caso, mas não terão permissão para executar orquestrações.

Acesso de usuário externo para tarefas de caso

Esta seção descreve o acesso do usuário externo para tarefas de caso.

Atribuição de tarefas de caso a usuários externos

As tarefas de caso são atribuídas aos usuários com a função externa, mesmo que eles não tenham acesso à função sn_sec_tisc.analyst.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Qualquer usuário externo atribuído com uma tarefa de caso só pode exibir o módulo de tarefa de caso e terá o privilégio de editar a tarefa de caso.
2. O usuário externo só pode exibir as tarefas de caso atribuídas a esse usuário específico ou aos grupos aos quais o usuário pertence.
3. O usuário externo deve ser capaz de reatribuir a tarefa no grupo ao qual o usuário pertence.

Associe técnicas MITRE a um caso

Associe uma ou mais técnicas DO MITRE a um caso.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Clique em **Associar técnica MITRE** botão.
6. Clique em **Adicionar matriz** Para associar a técnica MITRE.
   . **Associe a técnica MITRE ao caso** a caixa de diálogo é exibida.
7. Selecione **Matriz** .
   Todas as matrizes habilitadas serão exibidas para você selecionar a Matriz.
8. Selecione a tática nas listas suspensas.
   Todas as táticas associadas a uma matriz serão exibidas.

   Nota: Se você quiser adicionar mais táticas, clique **Adicionar tática** . As táticas selecionadas anteriormente não serão mais exibidas na lista suspensa se você estiver adicionando uma nova tática.

9. Selecione **Técnica** .
   Todas as técnicas associadas à tática selecionada serão exibidas. Se você estiver adicionando mais táticas, poderá selecionar as técnicas associadas a essas táticas selecionadas.
10. Clique em **Salvar**.
    Se você quiser excluir todos os dados associados à matriz, clique em **Excluir matriz** Esta ação removerá somente os dados de matriz associados, mas a matriz permanecerá no Repositório MITRE ATT&CK.

    O registro de dados de matriz associado é exibido na seção Cartão MITRE ATT&CK. Na exibição de cartão:

    Nota: Você pode alternar entre várias matrizes na lista suspensa Matriz.

    a. A primeira linha da exibição do cartão exibe todas as táticas associadas à matriz selecionada atual.
    b. Cada cartão de tática mostra o nome da tática e o número de técnicas dessa tática mapeada para o registro do caso atual.
    c. Todas as técnicas associadas a esse caso são mostradas verticalmente em cada tática. Você pode clicar em qualquer técnica para exibir a exibição do formulário de técnica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Clique em **Mostrar ID** Mostrará os IDs de todas as técnicas associadas.

    Nota: Cada cartão de técnica mostra o nome da técnica e o ID da técnica somente quando **Mostrar ID** habilitado.

12. Clique em **Atualizar** para atualizar a exibição do cartão.
    Você pode exibir o carimbo de data/hora da última atualização da matriz selecionada.

    Nota: Clique no ícone Pop-out para exibir o cartão de matriz associado em uma nova guia.

Acúmulo de associações de técnicas MITRE

Acúmulo de associações de técnicas MITRE de observáveis, indicadores, objetos e incidentes de segurança vinculados ou desvinculados de um registro de caso.

Antes de Iniciar

Nota:

- O acúmulo de associações de técnicas MITRE para incidentes de segurança acumulará os dados associados à técnica MITRE de incidentes de segurança para a gestão de casos no TISC.
- Por padrão, esta propriedade sn_sec_tisc.auto_rollup_mitre_data está habilitada para as técnicas MITRE, a serem acumuladas automaticamente para os casos dos objetos associados ou incidentes de segurança.
- Se você quiser executar o acúmulo sob demanda de associações de técnicas MITRE, navegue até Mais ações em **Exibição do formulário Caso** e selecione **Acumular técnicas MITRE** opção. Esta operação acontecerá de forma assíncrona e você poderá verificar **Fluxo de atividades** seção para as atualizações na atividade de acúmulo.

Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa

- Sempre que qualquer entidade, como um observável ou indicador, estiver vinculada a qualquer caso, todas as associações de técnica MITRE presentes para essa entidade serão automaticamente acumuladas para o caso.
- Sempre que qualquer entidade, como um observável ou indicador, for desvinculada e removida do caso, todas as associações de técnica MITRE acumuladas do caso que estão presentes para essa entidade serão removidas automaticamente e acumuladas no caso.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Abra qualquer caso.
5. Vá para **Artefatos** guia.
6. Selecione **Observáveis** na lista relacionada artefatos.
7. Selecione **Link** botão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione os observáveis que você pode querer vincular ao caso.
9. Clique em **Link** para vincular os observáveis.
   Depois de vincular os observáveis a um caso, as técnicas MITRE associadas a esse observável específico são acumuladas automaticamente e a contagem da lista de técnicas MITRE na seção Artefatos é atualizada automaticamente.
10. Clique em **Desvincular** para desvincular os observáveis do caso.
    Depois de desvincular os observáveis a um caso, as técnicas MITRE associadas a esse observável específico são removidas automaticamente e a contagem da lista de técnicas MITRE na seção Artefatos é atualizada automaticamente.

Criando tarefa de caso usando o Workbench de analista de ameaças

Crie tarefas de caso para associar a caso(s).

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de tarefas do caso** > **Tarefas de todos os casos**.
   Todas as tarefas do caso são exibidas.
4. Clique em **Nova**.
5. Preencha os campos, se for o caso.

Criar nova tarefa de caso

Campo	Descrição
ID da tarefa	Um identificador exclusivo para a tarefa do caso. Este é o ID gerado pelo sistema.
Descrição Resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Descrição	Uma descrição detalhada, incluindo todas as informações relevantes sobre a tarefa do caso, como histórico, qual análise é necessária, resultados esperados.
ID do caso primário	Selecione o ID do caso primário na pesquisa.
Prioridade	Uma avaliação da gravidade da solicitação ou problema.
Grupo de atribuição	O grupo atribuído responsável por trabalhar na tarefa do caso.
Status	O status atual da tarefa do caso.
Atribuição a	O analista responsável por trabalhar em uma tarefa de caso.
Data de vencimento	A data e a hora em que a tarefa do caso deve ser concluída ou encerrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
TLP	Valor exclusivo que indica a configuração de confidencialidade de dados por TLP.
Impor restrição	Como sn_sec_tisc_admin, marque esta caixa de seleção para modificar os membros do grupo permitido e os membros permitidos. Para obter mais informações, consulte Restrições impostas para caso(s).

6. Preencha os campos na seção Informações, conforme apropriado.

Informações

Campo	Descrição
Anotações	Quaisquer anotações adicionais relacionadas à investigação de ameaça.
Fechamento	Adicione o resumo de fechamento das descobertas.

7. Clique em **Salvar**.
Sua tarefa de caso será associada ao seu caso.

Nota: Depois de salvar a tarefa de caso, você pode adicionar marcadores e taxonomias à tarefa. Para obter mais informações, consulte Criando taxonomias.

Trabalhar com a tela de investigação

A tela de investigação é um recurso significativo importante, que fornece informações mais valiosas para os analistas de Inteligência contra ameaças (TI). Ele fornece uma estrutura estruturada mapeando relacionamentos um para um ou um para muitos e visualizando informações relacionadas a observáveis, indicadores de comprometimento (IOCs) ou entidades.

Ao usar a tela de investigação, os analistas de ameaças podem efetivamente:

- **Mapear relacionamentos** : Visualize conexões de nó entre várias entidades, como observáveis, indicadores de comprometimento (IOCs), agentes de ameaça, padrões de ataque, ativos afetados e muito mais. Cada objeto na tela de investigação é representado por uma cor específica, junto com seu tipo de objeto, tipo de nó e status. O status reflete a reputação do objeto, como **Suspeito** , **Baixo** ou **Crítico** para observáveis e outros tipos de objeto. Os indicadores são exibidos com a severidade da ameaça associada para ajudar a priorizar a análise.
- **Vincular casos ou telas de pintura** Vincule um caso ou tela para aprimorar a análise e fornecer uma exibição mais abrangente do cenário de ameaças na gestão de casos.
  - O recurso de vinculação permite que os analistas adicionem ou removam nós dinamicamente. Isso também preenche os relacionamentos existentes entre os nós para a tela.
  - Gráficos de relacionamento temporários salvando relacionamentos separadamente no contexto da tela de investigação.
- **Associações de técnicas MITRE** Associe ou remova técnicas DO MITRE com nós diretamente na tela e forneça análise no cartão de cadeia de inutilização DO MITRE.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontos de entrada para a tela de investigação

1. **Primeiro ponto de entrada: Nova tela em branco** : Este ponto de entrada deve permitir que os analistas abram uma tela nova e em branco sem nós ou links.
2. **Segundo ponto de entrada: Abrir tela na investigação de caso** :
   a. Este ponto de entrada abre um caso de investigação existente e permite editar, modificar e renomear a tela.
   b. Uma nova tela com artefatos existentes como nós.

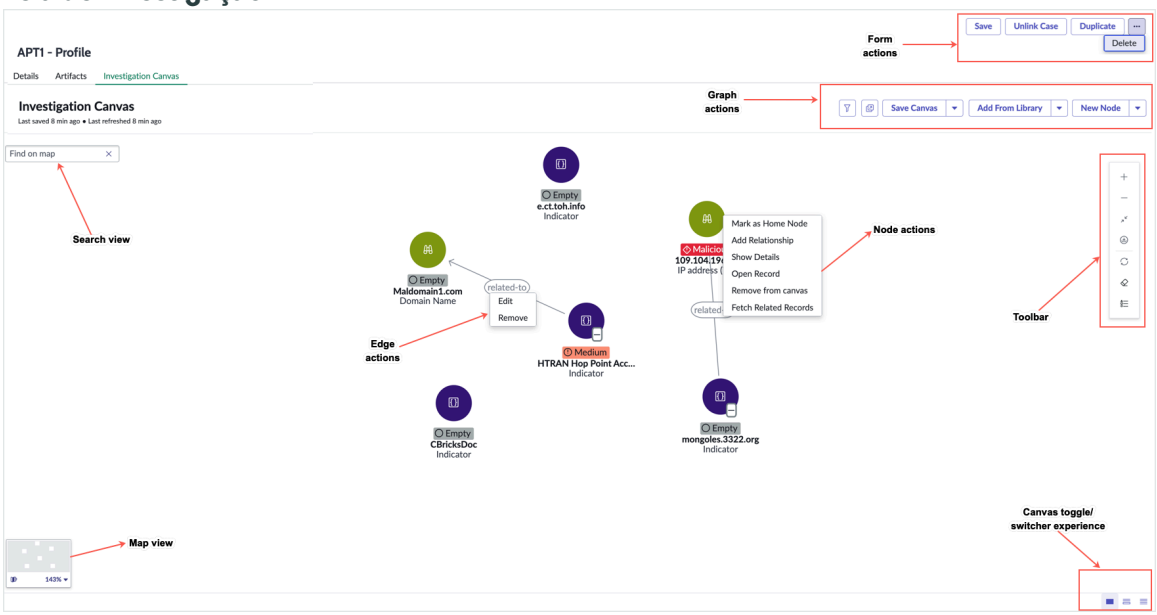
Trabalhar com ações na tela de investigação

Esta seção descreve as várias ações que você pode executar na tela de investigação.

A tela de investigação inclui:

1. Ações de formulário
2. Ações do gráfico
3. Ações de nó
4. Ações de borda
5. Ações da barra de ferramentas

Tela de investigação



Ações do formulário da tela de investigação

Ação	Operação
Vincular caso	Permite vincular o caso na tela de investigação.
Desvincular caso	Permite desvincular o caso na tela de investigação.
Salvar	Opção para salvar o registro do caso.
Duplicar	Opção para duplicar os nós na tela de investigação.
Excluir	Opção para excluir a tela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do gráfico da tela de investigação

Ação	Operação
Localizar no mapa	Permite pesquisar diferentes nós e bordas.
Filtro de tela	. **Filtro** a funcionalidade ajuda a refinar sua exibição na tela de investigação. Por exemplo, se você filtrar um tipo de registro, como Campanha, ele será removido temporariamente da exibição da tela. Ao aplicar filtros, você pode controlar quais tipos de entidades ou registros são mostrados no mapa, permitindo uma experiência de investigação mais limpa e focada. **Nota:** Use filtros para destacar somente os nós mais relevantes, como observáveis ou agentes de ameaça, ocultando temporariamente informações menos críticas na tela.
Salvar tela	Permite salvar a tela de investigação.
Adicionar dados à biblioteca	Esta opção permite que você estabeleça um novo relacionamento entre dois nós diferentes na tela de investigação. Todas as mudanças feitas na tela, incluindo os novos nós, novos links entre nós e quaisquer rótulos de borda editados ou modificados, serão salvos na biblioteca. Atualmente, todos os nós presentes na tela serão adicionados como artefatos ao caso vinculado. Uma mensagem de confirmação será exibida quando os dados forem salvos com sucesso na biblioteca.
Adicionar da biblioteca	Esta ação adicionará os dados da biblioteca de inteligência contra ameaças e também estabelecerá o relacionamento entre o novo nó importado da biblioteca de inteligência contra ameaças e os nós existentes na tela de investigação.
Adicionar dos artefatos do caso	Permite adicionar dados de artefatos de caso correspondentes vinculados à tela.

Ações do nó da tela de investigação

Ação	Operação
Marcar como nó inicial	Esta opção permite marcar um nó específico como o nó inicial na Tela de investigação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do nó da tela de investigação

Ação	Operação
	Ao girar durante a análise, a aplicação destaca e centraliza automaticamente o nó inicial, colocando-o em foco no centro da tela. O nó em foco é visualmente enfatizado por meio de: • Uma borda distinta • Destaque • Uma animação de movimento circular subtil Isso facilita a identificação e a exploração dos dados da tela relacionados ao foco primário da sua investigação.
Adicionar Relacionamento	Esta opção permite adicionar relacionamentos personalizados entre nós na tela de investigação. Você pode definir tipos de relacionamento, como: • Um para muitos • Muitos para um • Muitos para muitos Isso ajuda a representar associações complexas entre entidades.
Exibir Detalhes	Esta opção permite exibir informações detalhadas sobre o nó selecionado na Tela de investigação, incluindo seus atributos e quaisquer observáveis ou relacionamentos associados.
Abrir Registro	Esta opção permite que você abra o registro selecionado em uma nova guia do navegador para facilitar a referência e a multitarefa.
Remover da tela	Esta opção permite remover o nó selecionado da tela de investigação, excluindo-o efetivamente da exibição atual.
Buscar registros relacionados	Esta opção permite buscar registros relacionados para um nó específico e adicioná-los diretamente à tela de investigação usando **Selecione Tipos de entidade** caixa de diálogo. Selecione **Adicionar tudo** opção para incluir automaticamente todos os tipos de registro relacionados a objetos na caixa de seleção fornecida. Por exemplo, se houver de 5 a 10 tipos diferentes de registros relacionados, você

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do nó da tela de investigação

Ação	Operação
	terá que selecionar manualmente cada tipo de objeto. . **Adicionar tudo** o recurso simplifica esse processo preenchendo todos os registros relevantes de uma só vez, melhorando a experiência do usuário. Depois de adicionar registros, você pode removê-los ou selecionar **Expandir** opção para exibir os nós relacionados. No entanto, para aprimorar a usabilidade, agora você pode selecionar **Expandir tudo** para expandir instantaneamente todos os registros relacionados vinculados a um nó, em vez de adicionar ou expandir manualmente os registros.

Ações de borda da tela de investigação

Ação	Operação
Editar	Esta opção permite editar e modificar o rótulo de uma borda na Tela de investigação, permitindo uma representação mais clara dos relacionamentos entre nós.
Remover	Esta opção permite remover uma borda da tela de investigação, excluindo efetivamente a conexão visual entre dois nós.

Ícones da barra de ferramentas da tela de investigação

Ação	Operação
Ampliar	Opção para ampliar a tela de investigação para se concentrar facilmente em áreas específicas da tela.
Reduzir	Opção para diminuir o zoom da tela de investigação para se concentrar facilmente em áreas específicas da tela.
Ajustar à tela	Opção para ajustar a tela de investigação ao tamanho da tela.
Exportar mapa	Opção para exportar a tela de investigação como PDF para melhor exibição.
Atualização	. **Atualizar** A opção permite atualizar e recarregar os dados da biblioteca na tela de investigação. **Nota:** Todas as mudanças não salvas na tela serão perdidas se você atualizar sem salvar. É recomendável salvar sua tela antes de atualizar para evitar perda de dados.

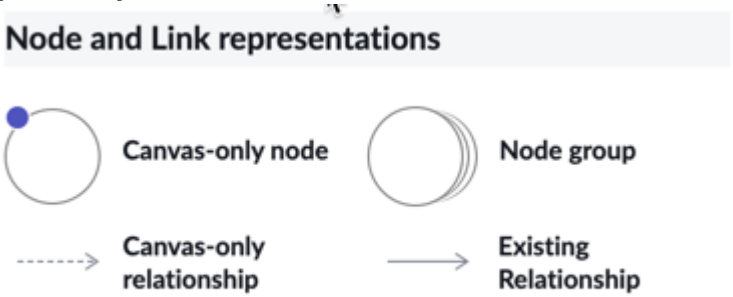
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ícones da barra de ferramentas da tela de investigação

Ação	Operação
Limpar Tela	Permite limpar a tela. Esta seleção removerá temporariamente os nós da tela de investigação. Uma mensagem de confirmação é exibida, solicitando que você confirme se deseja limpar a tela. Confirme a mensagem para prosseguir. **Nota:** Depois de fazer mudanças na tela de investigação, você deve **Salvar** a tela. Se as mudanças não forem salvas e você atualizar a tela, ela será revertida para o estado anterior e todos os nós ou modificações não salvos serão perdidos.
Legenda	Esta opção fornece uma representação visual dos nós e entidades exibidos no momento na Tela de investigação. A legenda inclui duas exibições principais: • **Representação de nó e link** : Exibe como diferentes tipos de nó aparecem na tela e como eles são conectados por meio de bordas. Isso ajuda você a entender rapidamente a estrutura e o relacionamento entre os vários elementos na investigação. • **Representação de entidades** : Mostra os tipos de entidades presentes no momento na tela (observáveis, indicadores e objetos). A seguir ilustra as legendas das representações de nó, link e entidade:

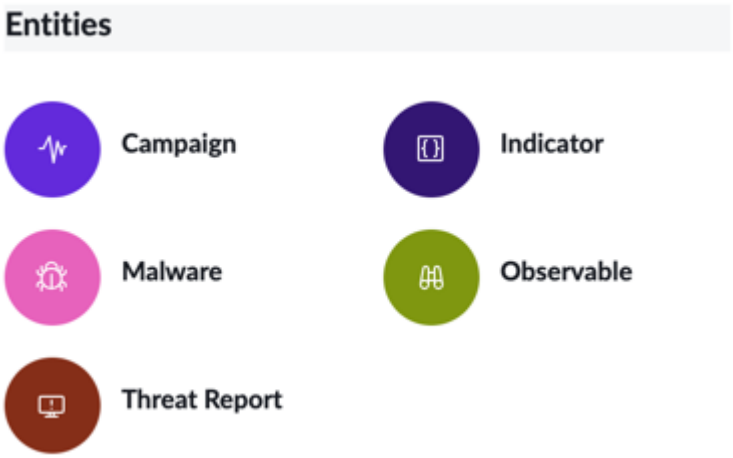
Representação de nó e link



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Representação de entidades



Agrupando ou desagrupando registros da tela de investigação

O recurso de grupo permite agrupar nós para facilitar a análise. Um botão de agrupamento foi adicionado ao lado dos nós que podem ser agrupados. Por padrão, este botão exibe um ícone de menos (-) na tela, indicando que o nó conectado pode ser recolhido ou agrupado.

Qualquer nó externo seria considerado para um grupo.

Nota: O ícone de grupo foi introduzido para reduzir a desordem na tela e simplificar a navegação durante investigações críticas. Para nós sem bordas adicionais (conexões), o botão de agrupamento não é exibido, pois não há nós relacionados disponíveis para agrupar.

A tabela a seguir explica as diretrizes ao agrupar ou desagrupar os nós:

Ação	Resultado
Agrupando um nó	• Todos os nós secundários com apenas um primário (mesmo em vários níveis) serão ocultos no grupo. • Os nós com vários primários permanecem visíveis, mas as conexões do grupo com eles ficarão ocultas.
Desagrupando um nó	• Revela todos os nós ocultos anteriormente com um primário e suas conexões. • Se nós com vários primários já estiverem visíveis, suas conexões ocultas também serão restauradas.
Importando registros relacionados a nó/busca	Expande automaticamente um grupo recolhido se o novo nó se conectar a um nó oculto dentro dele.
Ações permitidas	Os nós agrupados são compatíveis somente com **Mostrar detalhes** ação, que mostrará detalhes do nó primário. Outras ações estão desabilitadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação	Resultado
Filtrar	Filtragem **nós não agrupados** segue o comportamento de filtragem padrão, respeitando as regras de agrupamento. Filtrando um **nó agrupado** oculta o grupo inteiro e seu nó secundário.
Outras ações	Ações como remover um nó ou modificar bordas seguem todas as regras e comportamentos de agrupamento.

Vincular um caso existente da tela de investigação

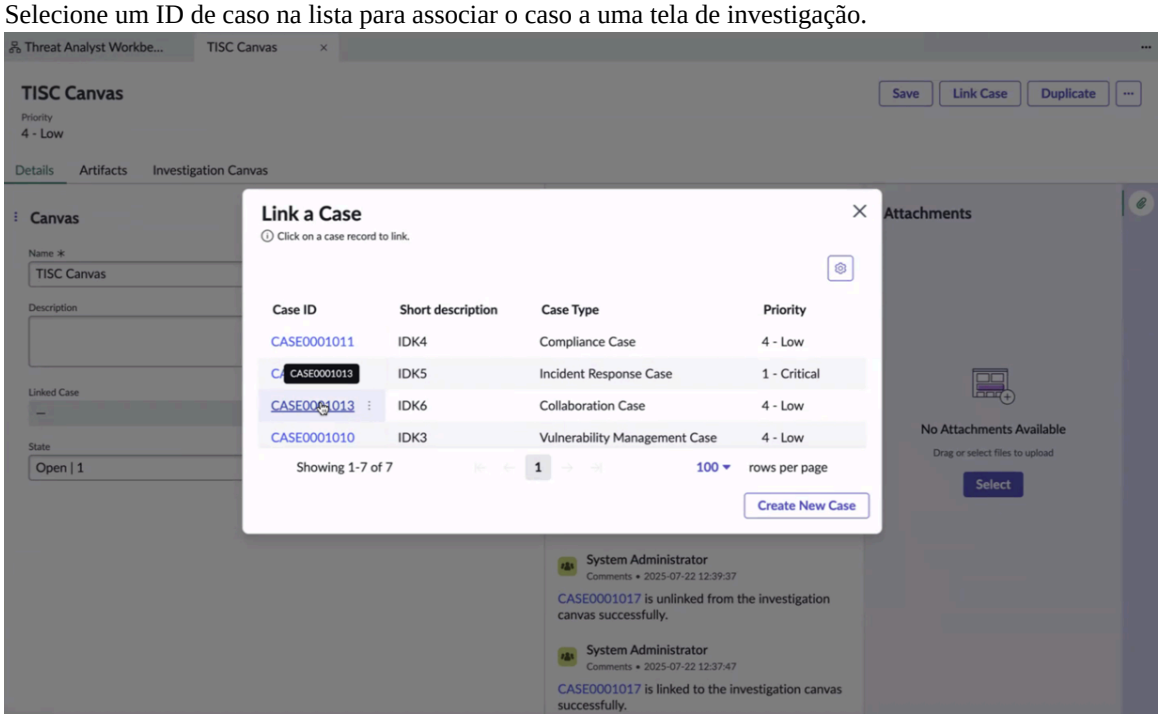
Use esta seção para vincular um caso existente da tela de investigação.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Selecione **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Exibe todos os casos.
4. Selecionar **Gestão de casos** > **Todos os Casos**
5. Abra qualquer registro de caso na exibição de lista.
6. Selecione **Vincular Caso** em **Detalhes** seção.
   A caixa de diálogo Vincular um caso é exibida.
7. Selecione um ID de caso na lista para associar o caso a uma tela de investigação.



Uma mensagem de confirmação é exibida confirmando que o caso foi vinculado com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se nenhum caso estiver disponível para vincular à tela de investigação, você poderá criar um novo caso para iniciar e organizar seu contexto de investigação. Para obter mais informações sobre como criar um novo caso, consulte Criar um caso e vincular a partir da tela de investigação

.

8. Para remover um caso vinculado, selecione **Desvincular** botão.

Tópicos relacionados

Criando uma tela de investigação

Criar um caso e vincular a partir da tela de investigação

Use esta seção para criar e vincular um caso(s) a partir de uma tela de investigação.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Selecione **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Exibe todos os casos.
4. Abra qualquer registro de caso na lista.
5. Selecione **Vincular Caso** em **Detalhes** seção.
   A caixa de diálogo Criar e vincular caso é exibida.
6. Selecione um caso na lista para associá-lo a uma tela de investigação.
7. Selecione **Criar nova tela** .
   A caixa de diálogo Criar novo caso é exibida.
8. Preencha os campos de formulário, se for o caso.

Campo	Descrição
ID do caso	Um identificador exclusivo do caso. Este é o ID gerado pelo sistema.
Descrição resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado. As opções possíveis para a investigação são: ○ Busca de ameaças ○ Solicitação de informações ○ Caso de gestão de vulnerabilidade ○ Caso de conformidade ○ Caso de resposta do incidente ○ Caso de colaboração ○ Outros

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prioridade	Indica a prioridade de um caso.
Grupo de atribuição	O grupo atribuído responsável por trabalhar no caso.
Status	O status atual do caso.
Atribuição a	O analista responsável por trabalhar em um caso.

9. Selecione **Criar e vincular** para criar um novo caso e vinculá-lo diretamente à tela de investigação.

   Uma confirmação é exibida confirmando que o caso foi criado e vinculado à tela de investigação com sucesso.

   Nota: Esta opção é útil quando nenhum caso existente está associado à tela de investigação.

10. Para remover um caso vinculado, selecione **Desvincular** botão.
    Para obter mais informações sobre como vincular diretamente um caso existente à tela de investigação, consulte Vincular um caso existente da tela de investigação.

Tópicos relacionados

Criando uma tela de investigação

Vincular tela de um caso

Use esta seção para vincular uma tela de um caso.

Antes de Iniciar

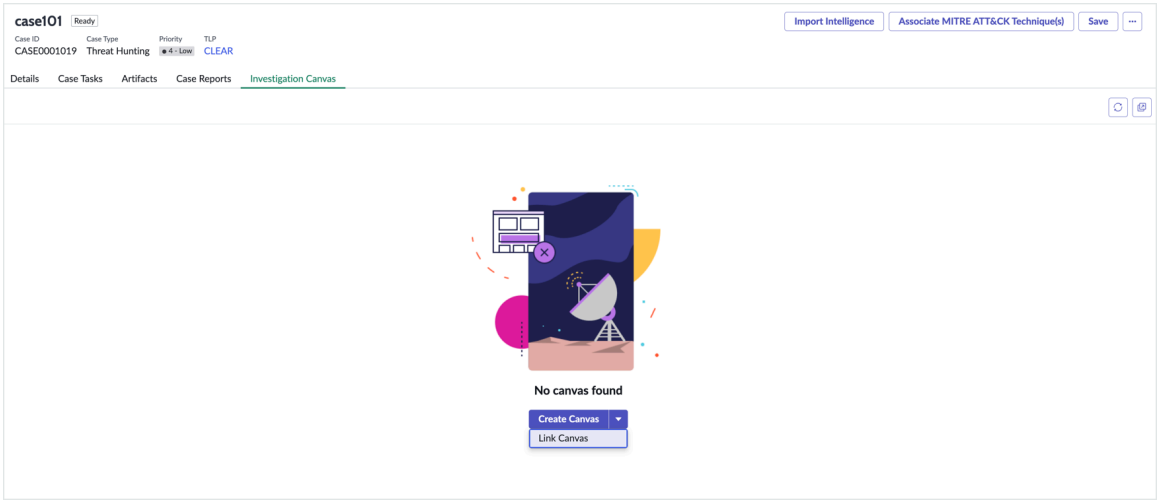
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Telas de investigação** > **Todas as telas**.
4. Em **Todos os casos** exibição de lista, selecione um caso que não esteja vinculado à tela.
5. Vá para **Tela de investigação** seção.
6. Selecione **Vincular Caso** na lista suspensa na página da tela vazia (a opção é mostrada na captura de tela a seguir).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Selecione a tela.
8. Selecione **Link** botão para vincular a tela a um caso.

   Uma mensagem informativa é exibida indicando que os dados da tela foram atualizados com sucesso.

Criando uma tela de investigação

Crie uma tela para adicionar observáveis da biblioteca de inteligência contra ameaças.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Telas de investigação** > **Todas as telas**.
4. Clique em **Nova**.
5. Preencha os campos, se for o caso.

Criar nova tela

Campo	Descrição
Nome	Insira o nome da tela.
Descrição	Adicione a descrição da tela.
Caso vinculado	Esta opção exibe uma lista de casos que não têm telas de pintura associadas a eles. O campo é preenchido dinamicamente com base na ausência de uma tela vinculada para cada caso, permitindo que os usuários identifiquem facilmente casos que podem precisar de contextos de investigação criados ou vinculados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prioridade	Selecione a prioridade da tela.
Estado	Selecione o estado da tela.

6. Clique em **Salvar**.
   As duas novas seções são exibidas **Artefatos** e. **Tela de investigação** . Quando você cria uma nova tela, a tela não inclui nenhum nó. Você deve adicionar nós da biblioteca do Inteligência contra ameaças ou artefatos por meio da opção de adicionar da biblioteca.
7. Vá para **Tela de investigação** .
8. Clique em **Adicionar da biblioteca** .

   Nota: Há duas opções disponíveis para adicionar os nós. Você pode selecionar qualquer um **Importação** para importar todos os observáveis ou selecione **Adicionar da biblioteca** opção para adicionar os observáveis da biblioteca de inteligência contra ameaças.

   . **Nó de importação da Biblioteca** é exibida a caixa de diálogo.
9. Selecione **Tipo de nó** na lista suspensa.
   Por exemplo, selecione o tipo como observáveis se você estiver adicionando observáveis à tela de investigação.
10. Selecione o número necessário de observáveis.
11. Clique em **Importar**.
    Depois de importar observáveis, os nós são adicionados à tela de investigação. Quaisquer que sejam os nós adicionados à tela, são adicionados temporariamente à tela e não serão persistentes na tela.
12. Selecione **Salvar tela** .
    Se você quiser processar os dados dos nós para a tela, salve os dados para mantê-los permanentemente.

    Nota: Se você não executar **Salvar tela** opção em seguida, você pode perder os dados sempre que atualizar a tela.

13. Selecione **Adicionar dados à biblioteca** para criar qualquer novo relacionamento entre dois nós diferentes.
    O relacionamento entre os dois nós é indicado com a linha pontilhada, o que significa que os nós são temporários. Se você quiser mover os dados dos nós para os relacionamentos, selecione **Salve dados na biblioteca** e adicionar dados à biblioteca. Depois de executar esta operação, a linha pontilhada se transformará em uma linha de borda sólida indicando que o nó agora faz parte da biblioteca.
14. Use **Filtro** ícone para exibir o tipo de observáveis e objetos que estão presentes na tela e você pode escolher seletivamente o tipo de dados a serem mostrados na tela de investigação.
15. Além disso, selecione o ícone pop-out para exibir ou executar qualquer operação nos nós da tela de investigação em um espaço maior.
16. Selecione **Vincular Caso** para vincular o caso à tela de investigação.
    a. Selecione **ID do caso** .
    b. Clique em **Link** botão.
17. Clique em **Duplicado** para duplicar os dados da tela e os nós na tela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Trabalhar com ações na tela de investigação

Vincular tela de um caso

Criar um caso e vincular a partir da tela de investigação

Adicionando um novo nó à tela

Use esta seção para criar e adicionar novas entidades, incluindo observáveis ou objetos, diretamente da tela de investigação.

Antes de Iniciar

Este recurso permite o aprimoramento rápido da tela sem precisar sair da exibição atual.

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Selecione **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
4. Abra qualquer registro de caso.

   Nota: Ao criar um caso, você precisa criar uma tela ou vincular uma existente. Após a vinculação, as ações da tela, incluindo a opção de adicionar novos nós, estarão disponíveis automaticamente na interface do usuário.

5. Selecionar **Tela de investigação** > **Novo nó**.
   - Você também pode exibir **Novo nó** da lista suspensa do vazio **Tela de investigação** Seção do caso.
   - Outra opção para exibir **Novo nó** a funcionalidade deve ser exibida na página da tela de investigação diretamente.
6. Para criar um nó, selecione o apropriado **Categoria da entidade** e. **Tipo de entidade** .

Campo	Descrição
Categoria da entidade	Selecione a categoria da entidade, como Observável ou Objeto.
Tipo de Entidade	Selecione o tipo de entidade nas opções disponíveis com base na categoria selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ○ Quando um tipo de entidade é selecionado, o formulário de objeto correspondente é exibido automaticamente, mostrando os campos-chave, como Nome e Descrição, juntamente com todos os campos obrigatórios necessários para identificar a entidade primária. ○ Se você tentar criar uma entidade duplicada, o que significa que se selecionar uma entidade existente na aplicação e tentar criar uma com o mesmo valor, uma mensagem de erro será exibida indicando que a entidade já existe na Biblioteca de Inteligência contra ameaças com o mesmo valor e tipo.

7. Preencha os detalhes do objeto necessários, como nome e descrição.
8. Selecione **Adicionar** para adicionar o novo nó.
   Este processo adiciona automaticamente o nó à tela de investigação.

   Os nós recém-adicionados são visualmente diferenciados com um ponto



   no nó, eles são importados por meio da biblioteca ou artefatos de caso.

   Importante: Os nós recém-adicionados são temporários e não são salvos na biblioteca de inteligência contra ameaças ou na tela. Se você atualizar a tela antes de salvar, esses nós serão perdidos. Certifique-se de salvar a tela depois de adicionar novos nós para manter suas mudanças.

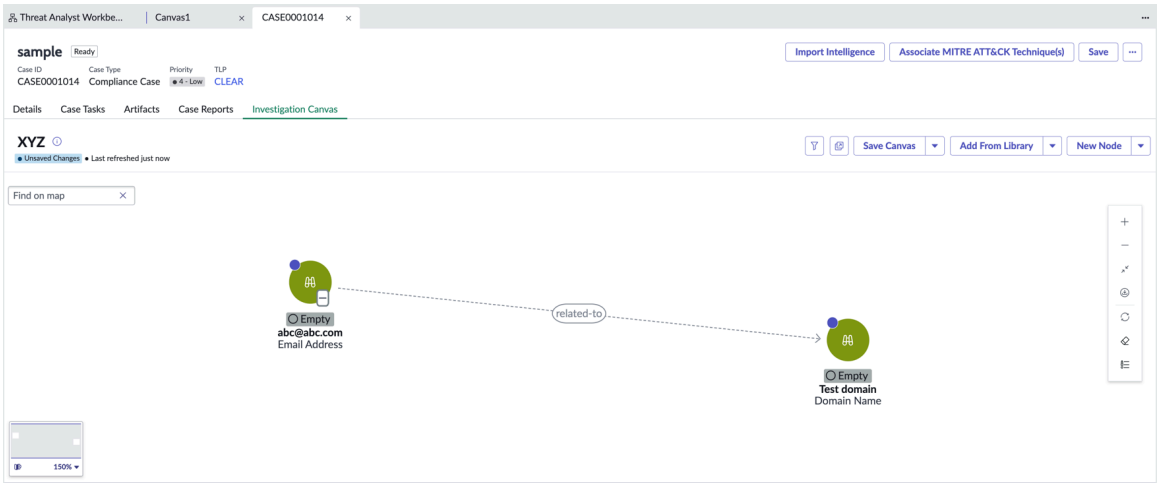
9. Clique com o botão direito do mouse no novo nó e selecione **Adicionar relacionamento** opção para criar relacionamentos entre os nós.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Ao criar novos relacionamentos, as bordas aparecem como linhas pontilhadas, indicando que são nós temporários e não foram salvos na Biblioteca de inteligência contra ameaças.
- As bordas recém-adicionadas são temporárias e não são salvas na biblioteca ou na tela de inteligência contra ameaças. Se você atualizar a tela antes de salvar, essas bordas serão perdidas. Certifique-se de salvar a tela depois de adicionar novas bordas para manter as mudanças.



10. Clique com o botão direito do mouse e selecione **Mostrar detalhes** para exibir os detalhes relacionados à entidade selecionada.

Nota: Para adicionar dados, você pode clicar no hiperlink no painel de detalhes ou selecionar **Registro em aberto** e adicione os dados relacionados ao nó necessário.

11. Selecione **Adicionar dados à biblioteca** opção para salvar todos os nós e bordas que foram adicionados temporariamente durante sua investigação.
Ao executar esta ação, os registros temporários são convertidos em registros agregados permanentes na Biblioteca de inteligência contra ameaças.

Tela de investigação e MITRE ATT&CK

Na Tela de investigação, você pode exibir as técnicas e subtécnicas DO MITRE ATT&CK associadas a todos os nós presentes no momento na tela.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

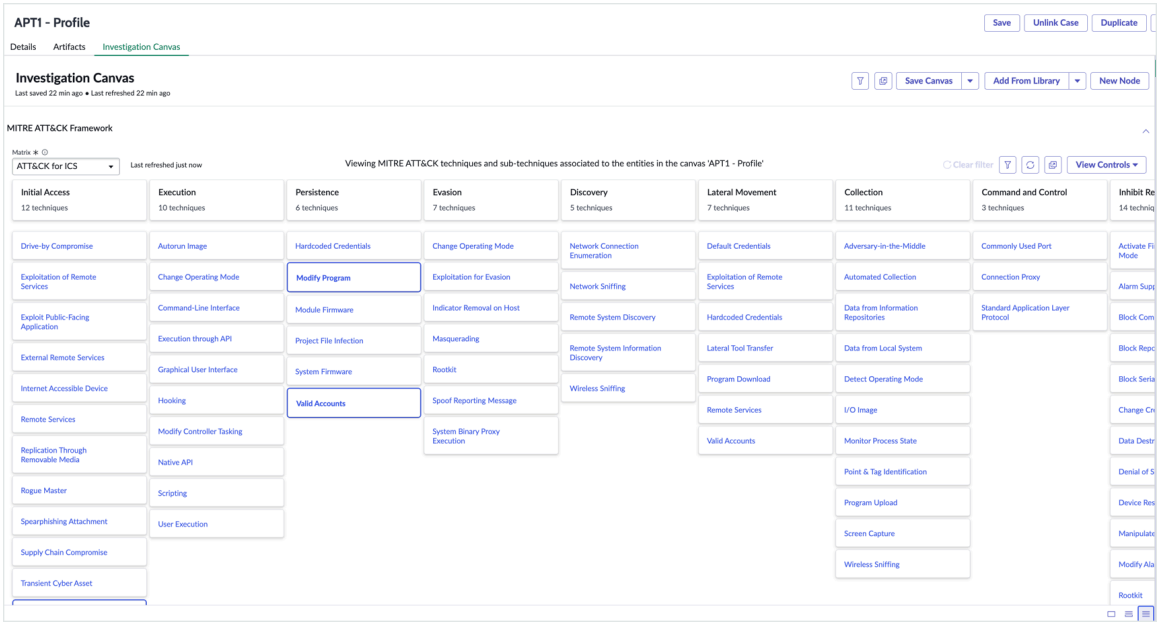
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Selecione **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
4. Abra qualquer caso.
5. Vá para **Tela de investigação** guia.
6. Na tela de investigação, use **Alças divisoras de painéis redimensionáveis** Para arrastar para exibir a estrutura MITRE ATT&CK.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione a matriz MITRE ATT&CK necessária em **Matriz** lista suspensa.



O MITRE ATT&CK Framework mostra diferentes níveis de associação de táticas e técnicas.

a. A linha superior exibe todas as táticas presentes na matriz MITRE ATT&CK selecionada.

b. Por padrão, cada tática mostra a contagem do total de técnicas e subtécnicas associadas a ela.

c. Use **Atualizar** Ícone para recarregar a estrutura MITRE ATT&CK e exibir as associações técnica-tática mais recentes.

d. Exiba as técnicas e as subtécnicas DO MITRE ATT&CK relacionadas a todos os nós (entidades) na tela.

e. Clique em um ou mais nós para exibir as técnicas e subtécnicas DO MITRE ATT&CK associadas relacionadas aos nós selecionados na tela.

Importante: Na estrutura, as técnicas e subtécnicas associadas aos nós na tela são realçadas.

8. Selecione **Filtros** Para permitir que você crie e salve filtros para TTPs associados a adversários específicos e outros atributos da técnica MITRE.
Para obter mais informações sobre as opções de filtragem DO MITRE, consulte Filtros MITRE da tela de investigação.

9. Usar **Controles de exibição** para opções de filtragem avançadas.
Depois de selecionar o filtro apropriado, ele exibirá somente as técnicas MITRE ATT&CK e as subtécnicas associadas aos nós selecionados. As opções em **Controles de exibição** as listas são:
   - **Mostrar ID** : Exibe o ID exclusivo da técnica (por exemplo `T1059` em cada cartão para referência fácil.
   - **Mostrar subtécnicas** : Exibe as subtécnicas. Esta opção expande automaticamente os cartões de técnica primários para exibir suas subtécnicas, sem exigir expansão manual.
   - Selecione **Mostrar somente técnicas associadas** : Exibe somente as técnicas que estão atualmente vinculadas a nós na tela de investigação, ocultando todas as

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

técnicas irrelevantes, mesmo que atendam aos critérios de filtro. Quando esta opção é selecionada, cada tática exibe a contagem total de técnicas e subtécnicas associadas atualmente vinculadas à tela.

10. Clique no ícone pop-out para exibir o MITRE ATT&CK Framework em um espaço maior.

Importante:

- Sempre que você adiciona ou remove um nó, a estrutura MITRE ATT&CK é atualizada automaticamente. Você também pode usar o ícone de atualização para executar uma atualização manual a qualquer momento.
- Sempre que você filtra tipos específicos de nós, a estrutura MITRE ATT&CK é atualizada automaticamente para refletir as mudanças.

Filtros MITRE da tela de investigação

Os filtros MITRE permitem criar e salvar filtros para Táticas, técnicas e procedimentos (TTPs) associados a adversários específicos e outros atributos da técnica MITRE.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os analistas podem usar os filtros disponíveis no cartão MITRE para filtrar TTPs de atores específicos que são relevantes para adversários envolvidos na investigação.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Selecione **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
4. Abra qualquer caso.
5. Vá para **Tela de investigação** guia.
6. Selecione **Filtros** Criar filtros para Táticas, técnicas e procedimentos (TTPs) associados a adversários específicos e outros atributos da técnica MITRE.
7. Preencha os valores necessários no painel de filtro para aplicar os filtros desejados.
   O painel de filtro MITRE permite filtrar e visualizar técnicas MITRE ATT&CK com base em critérios selecionados, como Grupos, Malware, Ferramentas, Marcadores e Prioridade.

Campo	Descrição
Filtros Salvos	Os analistas podem salvar critérios específicos como **Filtros salvos** para reutilização. Os filtros salvos por um analista são específicos do usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Por exemplo, se o analista X salvar uma configuração de filtro, ela ficará visível somente para o analista X. Quando outro analista fizer login e exibir o menu suspenso de filtro, ele não verá os filtros salvos por outras pessoas. Isso garante que cada usuário possa criar e gerenciar exibições personalizadas sem afetar ou ser afetado pelas preferências de filtro de outros usuários.
Nome do Filtro	Nome do filtro.
Grupo MITRE	Indica o Grupo MITRE. Selecione um ou mais grupos para filtrar técnicas associadas a eles.
Malware MITRE	Indica o malware MITRE. Selecione um ou mais itens de malware para filtrar técnicas associadas a eles.
Ferramentas MITRE	Indica as ferramentas MITRE. Selecione uma ou mais ferramentas para filtrar técnicas associadas a elas.
Marcadores de TISC	Indica TISC marcadores. Selecione um ou mais marcadores para filtrar técnicas com base em sua classificação.
Prioridade das técnicas	Indica o nível de prioridade das técnicas. Você pode selecionar uma ou mais opções para filtrar técnicas com base na prioridade atribuída.
Limpar Tudo	Permite limpar as entradas inseridas no painel de filtros.
Salvar como novo filtro	Salva os critérios inseridos no painel de filtros como um novo filtro salvo. **Nota:** O nome do filtro salvo deve ser exclusivo.
Salvar filtro atual	Salva as mudanças nos critérios no filtro salvo selecionado no momento. Você também pode renomear um filtro usando esta opção. **Nota:** O nome do filtro salvo deve ser exclusivo.
Aplicar	Esta opção permite que você aplique as mudanças aos filtros no cartão MITRE.
Excluir	Selecione esta opção para remover um filtro salvo selecionado.

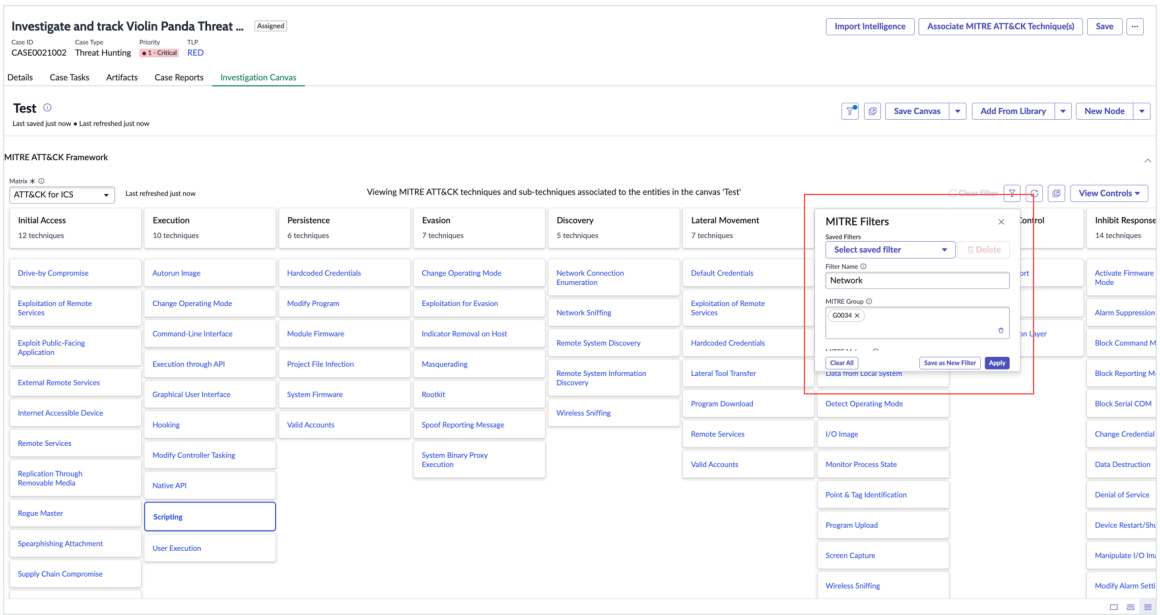
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Ao clicar em **Excluir** ao lado de um filtro salvo, uma mensagem de confirmação será exibida se você tiver certeza de que deseja excluir este filtro. Confirmar esta ação removerá permanentemente o filtro salvo. Para remover um valor de campo individual no painel de filtro, clique em **Excluir (lixeira)** ícone ao lado desse campo específico.

Ao aplicar filtros usando esses valores, a matriz MITRE é atualizada dinamicamente para exibir somente as técnicas associadas aos atributos selecionados. Essa exibição focada permite que os analistas se concentrem mais nas táticas, técnicas e procedimentos (TTPs) mais relevantes durante as investigações.

Além disso, os analistas podem restringir ainda mais os TTPs usando filtros para malware, ferramentas, marcadores e níveis de prioridade.



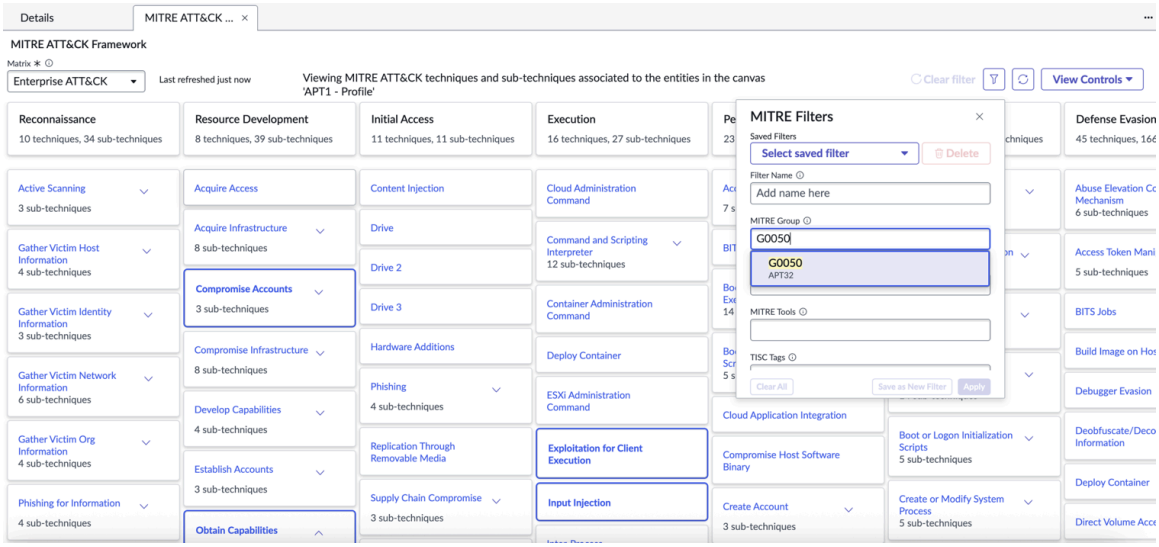
8. **Opcional:** Selecione **Salvar como Novo Filtro** para salvar seus critérios de filtro.
9. Selecione **Aplicar** para aplicar as mudanças.

Example: Filtrando por Grupo MITRE

Selecione um grupo MITRE como APT32 (G1001, consulte a captura de tela a seguir). Quando você aplica este filtro, a matriz MITRE é atualizada para exibir somente as técnicas que estão diretamente vinculadas ao grupo selecionado.

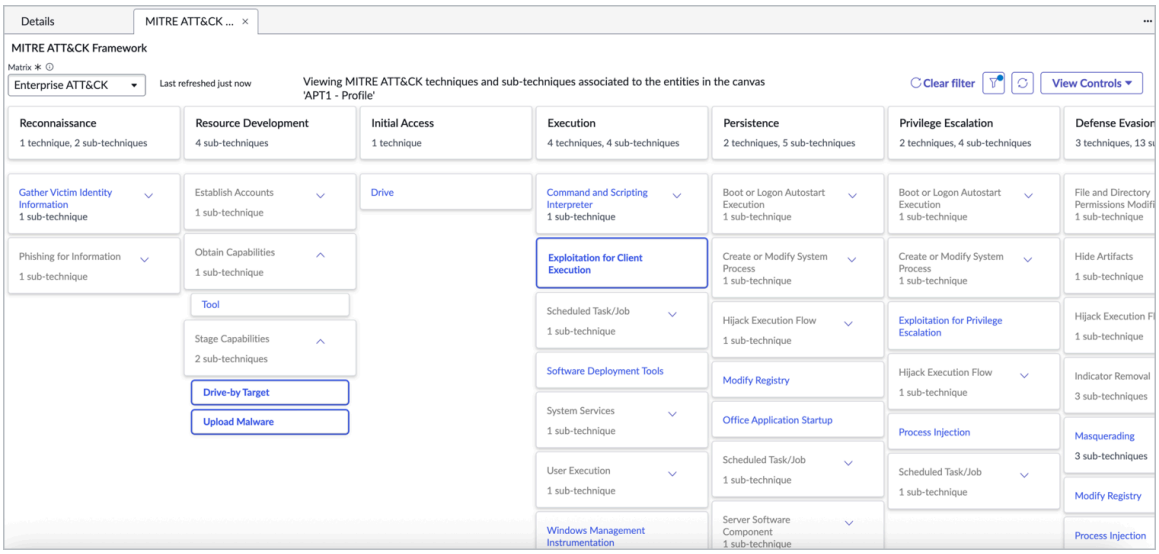
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Esta exibição focada ajuda os analistas a se concentrarem especificamente nas táticas, técnicas e procedimentos (TTPs) associados ao grupo de ameaças selecionado.

Quando você aplica o filtro, algumas técnicas na matriz são exibidas em texto azul, enquanto outras técnicas aparecem em cinza.



A representação visual no MITRE Framework indica como as técnicas e subtécnicas se relacionam com os filtros aplicados e o contexto de investigação.

- **Texto azul:** As técnicas ou subtécnicas mostradas em texto azul indicam aquelas que correspondem aos critérios de filtro.
- **Texto azul em negrito com borda azul:** As técnicas ou subtécnicas exibidas em texto azul em negrito com uma borda azul indicam aquelas que correspondem aos critérios de filtro e estão associadas a um ou mais nós na tela.
- **Cartão cinza:** As técnicas primárias são exibidas em cinza quando não correspondem diretamente aos critérios de filtro (o que significa que não estão vinculadas ao grupo selecionado), mas são mostradas para representar o relacionamento parental com subtécnicas vinculadas que correspondem aos critérios de filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar artefatos a caso(s) ou tarefa(s) de caso(s)

Depois de criar um caso, você pode exibir ou adicionar artefatos, como incidentes de segurança, ICs e indicadores de comprometimento, ao caso. Esses artefatos atuam como pistas na resolução do caso.

Antes de Iniciar

Função necessária: administrador

Nota: Os artefatos estão disponíveis somente para os casos existentes. Para observáveis e indicadores, os artefatos também podem ser adicionados ou associados a um caso do trabalho de importação usando o botão Inteligência de importação. Para obter mais informações sobre como importar, consulte, Importar Inteligência em TISC

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso ou tarefa de caso.
5. Vá para **Artefatos** guia.
   Os artefatos associados são exibidos como listas relacionadas para esse caso ou tarefa de caso específico.
6. Vincular ou desvincular os registros do caso ou da tarefa do caso.

Nota: Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.

A tabela a seguir lista as listas relacionadas a artefatos relacionadas aos casos ou tarefas de caso:

Registros relacionados

Lista relacionada	Descrição
Técnicas MITRE	Liste as técnicas MITRE relacionadas aos casos. As técnicas MITRE também exibem todas as técnicas associadas em um caso.
Observável	Lista de observáveis relacionados a estes casos ou tarefas de caso.
Indicadores	Lista de indicadores relacionados a estes casos ou tarefas de caso.
Padrões de ataque	Lista de padrões de ataque relacionados a estes casos ou tarefas de caso.
Campanhas	Liste as campanhas relacionadas a estes casos ou tarefas de caso.
Linhas de ação	Liste o curso das ações relacionadas a estes casos ou tarefas de caso.
Componentes de dados	Lista de componentes de dados relacionados a estes casos ou tarefas de caso.
Grupos de ameaças	Liste os agrupamentos de ameaças relacionados a estes casos ou tarefas de caso.
Identidades	Liste as identidades relacionadas a estes casos ou tarefas de caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Infraestrutura	Liste a infraestrutura, como sistemas, serviços de software e todos os recursos físicos ou virtuais associados relacionados a esses casos ou tarefas de caso.
Conjuntos de intrusão	Liste os conjuntos de invasão, como um conjunto de comportamentos e recursos adversários com propriedades comuns relacionadas a esses casos ou tarefas de caso.
Localizações	Liste os registros de locais relacionados a estes casos ou tarefas de caso.
Malware	Liste os registros de origem de malware relacionados a estes casos ou tarefas de caso.
Definições de marcação	Liste os registros de definições de marcação relacionados a estes casos ou tarefas de caso.
Anotações de ameaça	Liste os registros de definições de marcação relacionados a estes casos ou tarefas de caso.
Dados observados	Liste os dados observados relacionados a estes casos ou tarefas de caso.
Opiniões sobre ameaças	Liste as opiniões de ameaça relacionadas a esses casos ou tarefas de caso.
Relatórios de ameaças	Liste os relatórios de ameaças relacionados a esses casos ou tarefas de caso.
Detecções	Lista de vistas relacionadas a estes casos ou tarefas de caso.
Agentes da ameaça	Liste os agentes de ameaça relacionados a estes casos ou tarefas de caso.
Ferramentas	Liste as ferramentas relacionadas a estes casos ou tarefas de caso.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que têm um endereço IP correspondente que estão relacionados a esses casos ou tarefas de caso.
Casos Relacionados	Lista os casos relacionados.
Tarefas do caso relacionado	Lista as tarefas de caso relacionadas.
Incidentes de segurança	Liste os incidentes de segurança relacionados a estes casos ou tarefas de caso.
Itens de configuração afetados	Liste os itens de configuração afetados que estão relacionados a estes casos ou tarefas de caso.
Serviços afetados	Liste os serviços afetados relacionados a estes casos ou tarefas de caso.
Ativos afetados	Liste os ativos afetados relacionados a estes casos ou tarefas de caso.
Entradas de Vulnerabilidade	Liste as entradas de vulnerabilidade relacionadas a estes casos ou tarefas de caso.

Acúmulo de técnicas MITRE de artefatos para o caso

Quando registros de inteligência são adicionados a um caso, todas as técnicas MITRE associadas são automaticamente acumuladas para o nível do caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Vá para **Artefatos** guia.
   Os artefatos associados são exibidos como as listas relacionadas para esse caso específico.

Mostrar estrutura MITRE ATT&CK para um(s) caso(s)

Exibe todas as técnicas associadas de um caso na estrutura MITRE ATT&CK.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa
Selecione a matriz MITRE ATT&CK necessária em **Matriz** lista suspensa. O MITRE ATT&CK Framework mostra diferentes níveis de associação de táticas e técnicas.

1. A linha superior exibe todas as táticas que estão presentes no selecionado **Matriz** . Por padrão, todas as táticas exibem a contagem do total de técnicas e subtécnicas presentes para essas táticas correspondentes. Você pode usar **Atualizar** Ícone para recarregar a estrutura MITRE ATT&CK e exibir as associações mais recentes.
2. Em cada tática, a estrutura exibe todas as técnicas que estão presentes como um relacionamento com essa tática correspondente.
3. A estrutura exibe as subtécnicas que estão presentes em cada técnica. Expanda cada técnica para exibir as subtécnicas.

Importante: Na estrutura, as técnicas e subtécnicas associadas a um caso são realçadas.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Vá para **Artefatos** guia.
   Os artefatos associados são exibidos como as listas relacionadas para esse caso específico.
6. Selecione **Mostrar estrutura MITRE ATT&CK** botão
   Quando você seleciona este botão, a estrutura exibe todas as técnicas associadas de um caso e artefatos no MITRE ATT&CK.
7. Exibir técnicas MITRE ATT&CK e subtécnicas relacionadas ao caso a partir das técnicas MITRE que você selecionou para exibir.
8. Selecione qualquer registro para exibir as técnicas MITRE ATT&CK e as subtécnicas relacionadas ao caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Usar **Controles de exibição** Para exibir as técnicas e subtécnicas DO MITRE ATT&CK conforme desejado.
   Nas listas de controles:
   - Selecione **Mostrar ID** Para exibir as técnicas e subtécnicas IDs DO MITRE.
   - Selecione **Mostrar subtécnicas** para exibir todas as subtécnicas. Quando você seleciona esta opção, todas as técnicas são mostradas na exibição expandida. A exibição expandida da técnica mostra todas as subtécnicas que estão presentes para essa técnica correspondente.
   - Selecione **Mostrar somente técnicas associadas** Para exibir somente as técnicas MITRE associadas a um caso. Quando você seleciona esta opção, cada tática mostra o número total de técnicas e subtécnicas associadas.

Execute ações de aprimoramento em um caso

Use esta seção para entender como as ações de aprimoramento são realizadas nos casos.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

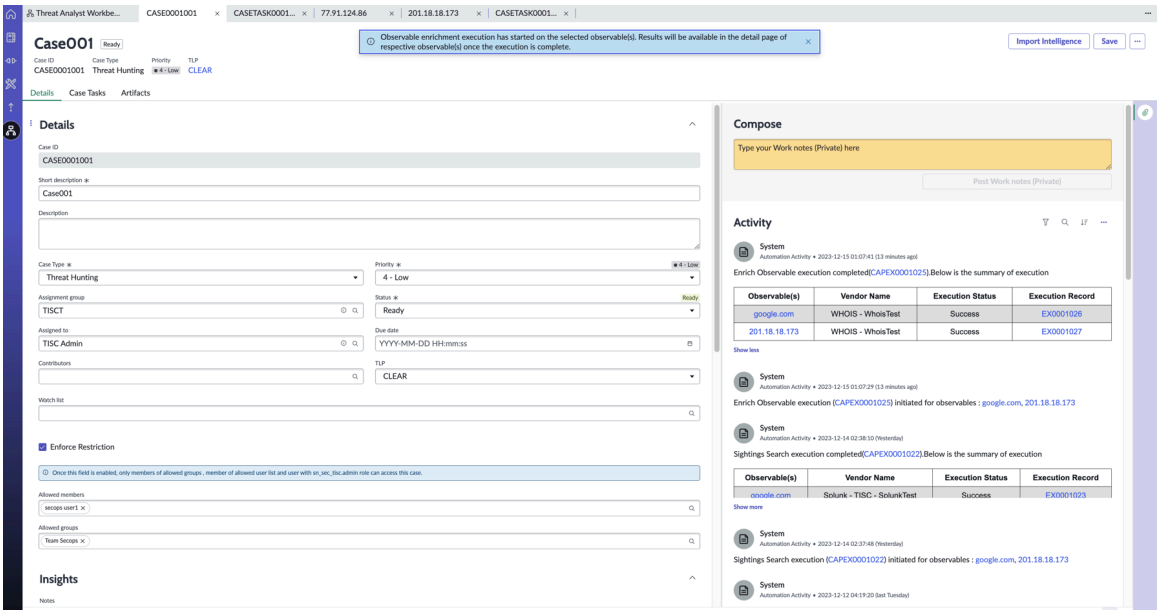
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso ou tarefa de caso.
5. Vá para **Artefatos** guia.
6. Selecione a lista relacionada Observáveis.
7. Selecione um ou mais observáveis.
8. Clique em qualquer ação de aprimoramento na lista suspensa.
9. Selecione as implementações disponíveis.
10. Clique em **Enviar**.
    Por exemplo, Executar pesquisa de ameaças. A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida A execução de aprimoramento do observável foi iniciada no observável(s) selecionado(s). Os resultados estarão disponíveis na página de detalhes dos respectivos observáveis quando a execução for concluída .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando a execução é iniciada ou concluída, as anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.



Exibir Relatórios de Caso

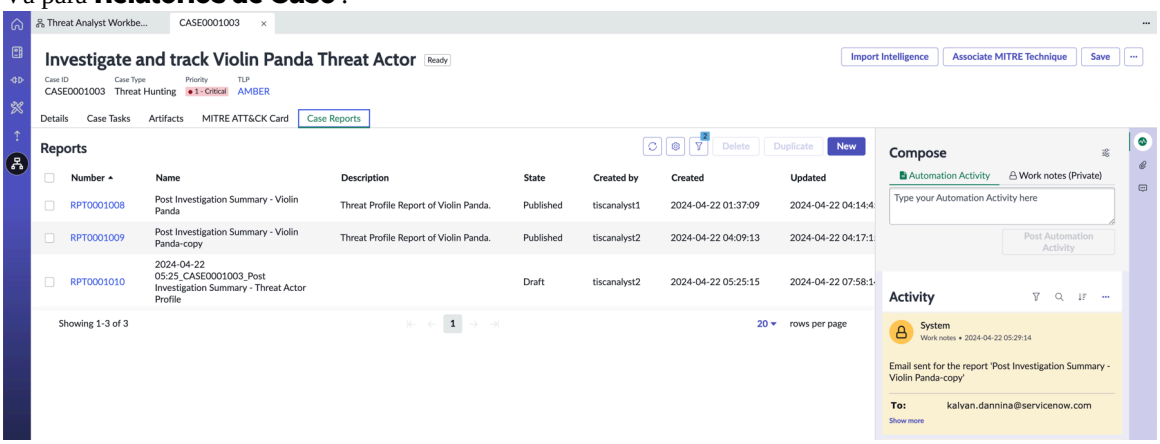
Use o recurso de relatórios de caso para gerar relatórios relacionados aos casos. Esses relatórios incluem um relatório pós-investigação ou um relatório de resumo executivo.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Vá para **Relatórios de Caso** .

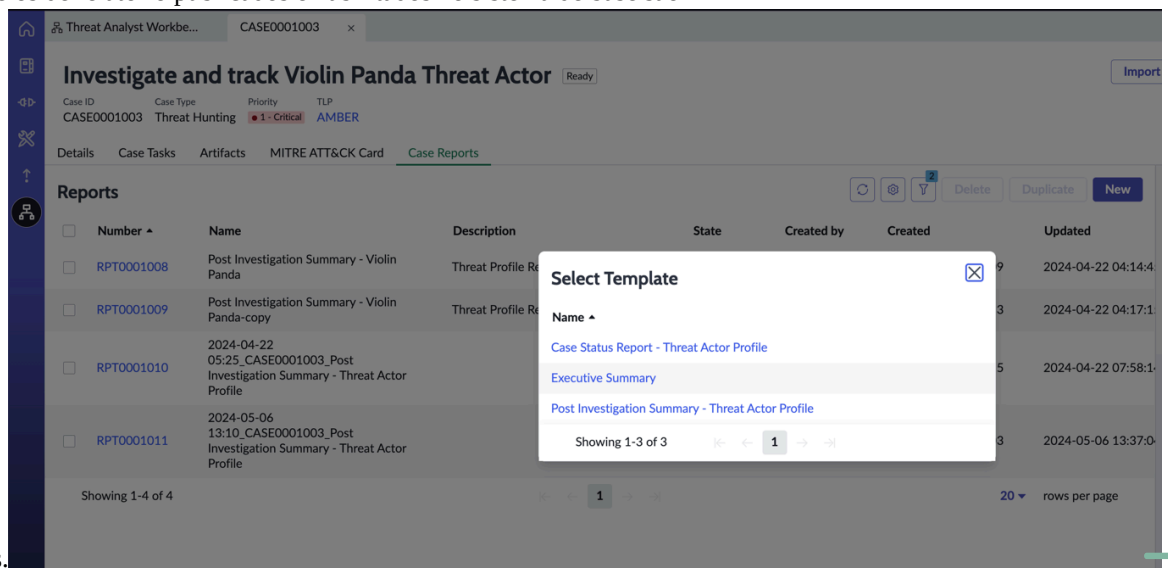


Nota: Você pode excluir os relatórios da lista, criar uma cópia duplicada dos relatórios existentes e personalizar seu próprio relatório.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Nova**.
   Os modelos de relatório publicados e habilitados no sistema de base são exibidos.



7. Selecione o Modelo de relatório desejado.
   O modelo de relatório selecionado para o tipo de relatório é gerado. Aqui, depois que o relatório é publicado, isso significa que um grupo maior de usuários pode exibi-lo, mas se o relatório estiver em um estado de rascunho, esse relatório ficará oculto para os usuários. Como analista, você só pode exibir os relatórios publicados, mas não os relatórios no estado de rascunho.

   Nota:

   - Se você quiser adicionar mais campos, selecione os campos e adicione-os diretamente no relatório de caso.
   - Se você quiser adicionar uma lista relacionada, por exemplo, uma lista de observáveis, selecione Observáveis. Todos os observáveis associados a esse caso específico serão listados. Selecione um ou mais observáveis e clique em **Adicionar** . Você também pode filtrar o observável necessário e adicioná-lo ao seu caso.

8. Clique em **Salvar conteúdo** para salvar o conteúdo do seu relatório.
9. Clique em **Visualização** para visualizar o relatório.

   Nota: Você pode fazer o seguinte:

   - **Maximizar** a janela de relatório.
   - **Download** o relatório usando **Download** ícone.
   - Destaque o relatório em uma nova guia, caso seja a altura ou o tamanho do relatório para ter uma melhor experiência de exibição.
   - **Editar** Nome do relatório e Descrição do relatório.
   - **Publicar** o relatório.

10. Clique em **Editar conteúdo** botão para republicar o relatório.

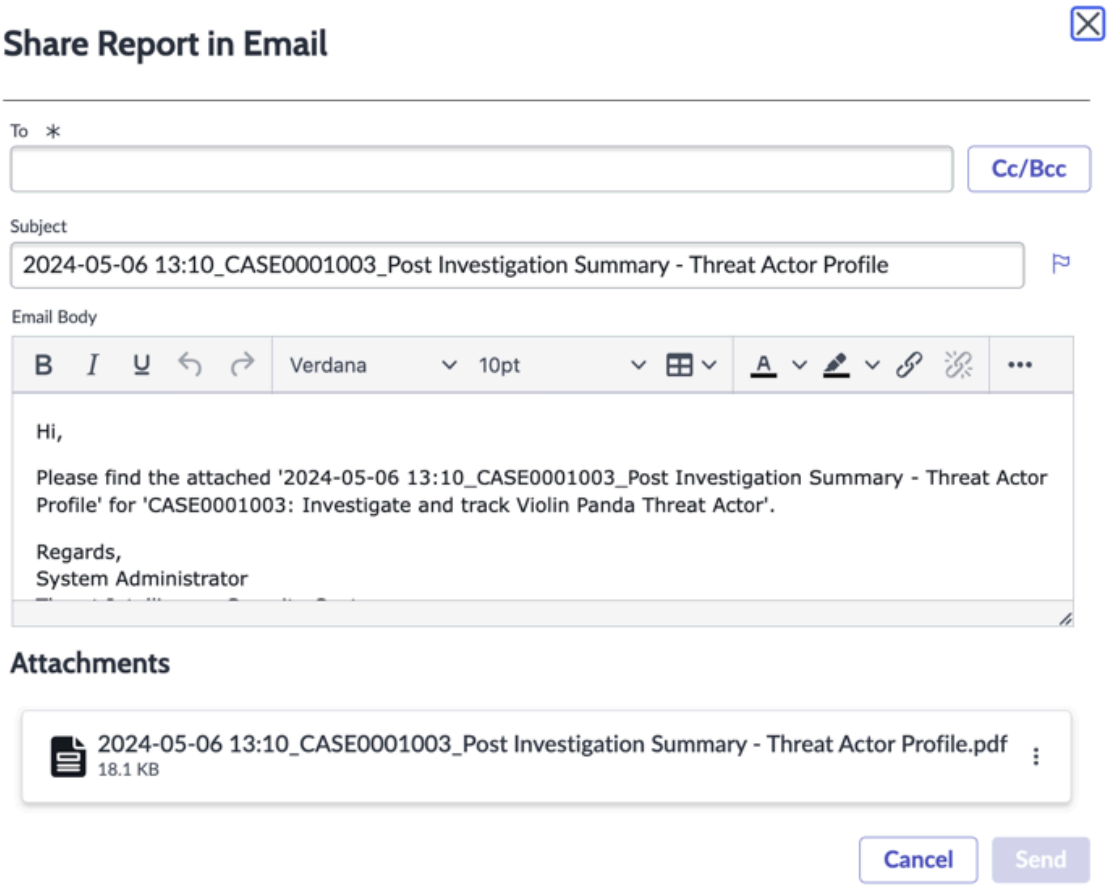
    Nota: Uma mensagem de aviso é exibida para você compartilhar o relatório:

    Republicar o relatório depois de fazer mudanças, para baixar ou compartilhar o relatório. Ainda deseja continuar editando?

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Clique em **Editar**.
    Se você quiser editar o relatório, poderá continuar editando o relatório conforme explicado ou publicar o relatório. Depois que for publicado, o relatório será somente leitura.
12. Clique em **Compartilhar relatório por e-mail** para compartilhar o relatório.
    Ao compartilhar o relatório, o relatório PDF gerado é anexado como um anexo ao e-



    mail.
13. Adicione os campos de e-mail obrigatórios, como Para (quem você deseja compartilhar o relatório), CC e Cco
14. Marque o e-mail como importante, se necessário.
15. Clique em **Enviar**.
    O relatório será compartilhado com o grupo maior de usuários.

Crie um incidente de segurança a partir de um TISC caso

Crie incidentes de segurança e associe observáveis aos incidentes de segurança de um TISC caso.

Antes de Iniciar

Função necessária: sn_si_basic

Procedimento

1. Navegar até **Tudo** > **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Abra qualquer caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Criar incidente de segurança** botão.

   Nota: Em **Workbench da Gestão de casos** . **Criar incidente de segurança** o botão está habilitado somente para os registros de casos em aberto e desabilitado para os registros de casos encerrados.

   A caixa de diálogo Criar incidente de segurança é exibida.

6. Preencha o formulário com os detalhes do incidente apropriados:

   Adicionar detalhes

Campo	Descrição
Descrição resumida	Insira uma descrição resumida do incidente de segurança.
Descrição	Insira uma descrição do incidente de segurança.
Categoria	Define a classificação do incidente de segurança.
Prioridade	Define a prioridade do incidente de segurança.
Subcategoria	Define a subclassificação do incidente de segurança com base em sua categoria.
Grupo de atribuição	Especifica o grupo de atribuição ao qual o incidente de segurança deve ser atribuído.
Primário	Indica o incidente de segurança primário, que é um TISC caso a partir do qual esta ação é acionada.

7. Clique em **Próximo** para continuar.

   Nota: Você deve inserir todos os campos obrigatórios, os **Próximo** o botão permanecerá desabilitado até que você insira todos os campos obrigatórios.

8. Selecione os observáveis associados ao TISC para vinculá-los a um incidente de segurança e clique em **Próximo** para prosseguir

9. Revise os detalhes do incidente de segurança e o observável que serão associados ao incidente de segurança recém-criado e clique em **Criar** para continuar e criar o incidente de segurança.

   Nota: Uma mensagem de confirmação é exibida indicando que o incidente de segurança foi criado, com um link para o incidente de segurança. Clicar no link direcionará você para o incidente de segurança no Espaço de resposta a incidentes de segurança.

   Depois que o incidente de segurança for criado, você será redirecionado para TISC **Artefatos** do caso.

10. Vá para **Incidentes de segurança** seção em TISC **Artefatos** para exibir os incidentes.

    Nota: Anotações de trabalho também são publicadas no TISC fluxo de atividades do caso que indica que o incidente de segurança (número do incidente de segurança) foi criado com o associado a. TISC observáveis. Estas anotações de trabalho incluem os detalhes, como o tipo de observável e o valor do observável.

    Em Espaço de resposta a incidentes de segurança formulário de incidente de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Anotações de trabalho são publicadas no fluxo de atividades indicando que o incidente de segurança foi criado com sucesso TISC caso. Estas anotações de trabalho também incluem um link para TISC caso confirmando que os observáveis selecionados foram associados ao incidente de segurança.
- Você também pode verificar isso acessando **Registros relacionados** . Espaço de resposta a incidentes de segurança e revisando as entradas de observáveis em **Inteligência sobre ameaça** > **Observáveis Associados**. A partir daí, você também pode exibir os observáveis associados em **Contexto do TISC** seção. Você pode notar que esses observáveis foram diretamente associados de TISC.

Carregar anexos de arquivo seguro

Use esta seção para entender como carregar os anexos de arquivo seguro para o(s) caso(s).

Antes de Iniciar

Função necessária: sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

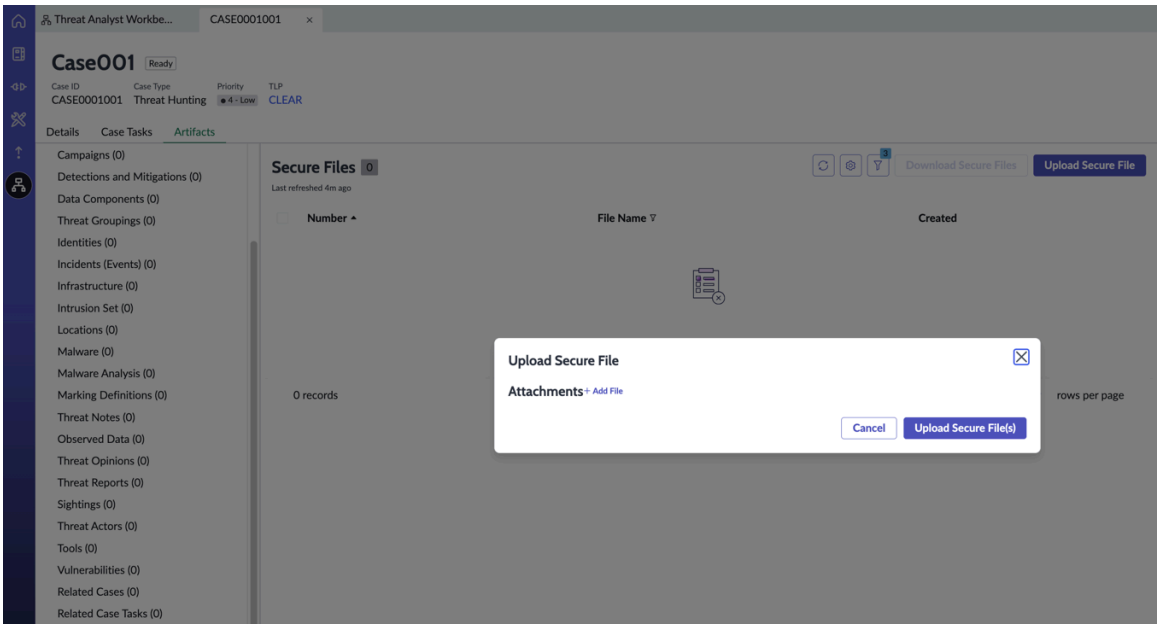
Nota: As listas relacionadas a Arquivos seguros são exibidas somente quando você tem a função de usuário, sn_sec_tisc.secure_file_access.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Ir para **Artefatos** > **Arquivos seguros** listas relacionadas.
6. Clique em **Carregar arquivo seguro** botão.
7. Clique em **Adicionar arquivo** para adicionar os anexos.
8. Selecione os arquivos e clique em **Carregar arquivo(s) seguro(s)** botão.
   Os anexos do arquivo são carregados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Baixar arquivos seguros** para baixar os anexos.
   Os anexos estão disponíveis no formato zip.
10. Como alternativa, você pode baixar o arquivo navegando até a página de detalhes do registro de arquivo seguro.

Nota:

- Todos os anexos seguros são criptografados e armazenados no sistema usando o Key Management Framework (KMF). Para obter mais informações, consulte Criptografia de anexo .
- Se os usuários tiverem assinatura para *ServiceNow IntegrationHub* **Instalador do Professional Pack** , os arquivos seguros são compactados em formato zip e também criptografados e armazenados

Central de segurança de inteligência contra ameaças Biblioteca

Uma biblioteca de ameaças é definida como um grupo de objetos e entidades organizados que atendem às organizações com informações de ameaças à segurança estruturadas e não estruturadas.

As informações de ameaça estão disponíveis na forma de feeds. Os feeds fornecem dados valiosos sobre ameaças de fontes como STIX, MISP e assim por diante, que listam entidades de inteligência contra ameaças.

A biblioteca da Central de segurança do Inteligência contra ameaças explica como navegar pelos dados, executando pesquisas básicas e avançadas e regras de filtragem, invocar assistente de importação, adicionar registros de inteligência contra ameaças manualmente, executar as ações necessárias, como adicionar à lista de permissões, lista de proibições e lista de observação.

A exibição detalhada fornece as informações para os registros de inteligência e, nas exibições de lista, você pode executar ações rápidas em um ou mais registros.

Noções básicas do Modelo de dados

O modelo de dados e a arquitetura do módulo do Centro de segurança de inteligência contra ameaças foram projetados para oferecer suporte aos recursos da plataforma de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

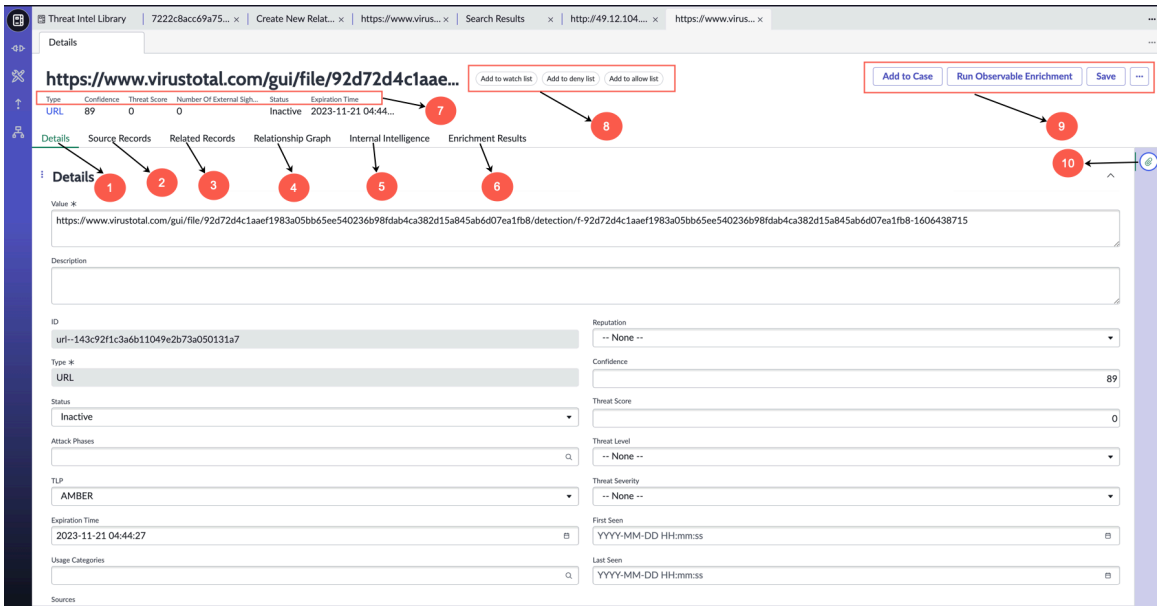
inteligência contra ameaças e a diferentes exibições de segurança que fornecem dados detalhados para os analistas de ameaças.

O modelo de dados tem as estruturas de dados que são representadas como objetos no repositório de inteligência contra ameaças.

TISC Exibição do formulário Objetos da biblioteca

. Central de segurança de inteligência contra ameaças a página inicial de objetos consiste nos seguintes recursos.

Use ou navegue até estas seções a seguir e saiba mais sobre cada SDOs em detalhes.



TISC exibição do formulário objetos da biblioteca

Ordem	Menu/guia	Descrição
1	Guia **Detalhes**	Use esta seção para exibir ou editar os SDOs na exibição de formulário.
2	**Registros de origem** guia	Registros de origem contribuem para um registro agregado conforme exibido na exibição do formulário. Esses registros de origem são criados automaticamente a partir de feeds ou criados manualmente pelo usuário.
3	Guia **Registros relacionados**	Lista todos os registros relacionados associados ao SDO.
4	**Gráfico de relacionamento** guia	Representação visual dos objetos relacionados.
5	**Inteligência interna** guia	Lista os registros de inteligência interna dos objetos associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição do formulário objetos da biblioteca

Ordem	Menu/guia	Descrição
6	**Resultados de aprimoramento** guia	Lista as integrações de aprimoramento associadas aos objetos.
7	**Faixa do formulário**	Esta é uma seção somente leitura, que contém os campos principais, como Tipo, Confiança, Pontuação de ameaça, Número de vistas, Status e Tempo de expiração.
8	**Ações de IU da faixa do formulário**	Estas são as listas de controle de segurança que estão disponíveis para você clicar se for necessário adicioná-las à lista de permissões, removê-las da lista de permissões (lista de proibições) ou adicioná-las à lista de observação com base nos observáveis. Clique para: • adicionar à lista de observação • adicionar à lista de proibições • adicionar à lista de permissões **Nota:** As ações de formulário são aplicáveis somente a observáveis.
9	**Ações de IU do formulário**	As ações de IU de formulário disponíveis são: 1. **Adicionar ao caso** : Adicione os objetos ao caso. 2. **Executar aprimoramento de observável** Executar os aprimoramentos nos objetos selecionados. 3. **Salvar** : Salve o registro. 4. **Excluir** Exclua o registro.
10	**Menu contextual direito**	Fornece acesso fácil aos controles rápidos, como anexos, anotações e assim por diante, com base nas tarefas associadas a esse objeto. Esta opção está disponível nas duas guias restantes para o analista de ameaças acessar sempre que necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição do formulário objetos da biblioteca

Ordem	Menu/guia	Descrição
		O menu contextual fornece navegação fácil para: 1. **Anexos** Anexe qualquer arquivo relacionado aos objetos. **Nota:** Sempre que você cria um novo observável, indicadores ou qualquer objeto ou exibe os objetos existentes, o. **Anexos** por padrão, o painel é exibido na respectiva exibição de formulário. Você pode clicar em **Anexos** no menu contextual direito ou acesse **Preferências** > **Espaços** e desabilite o. **Mostre a barra lateral** . Para obter mais informações, consulte Configure as preferências do Next Experience Workspace . 2. **Informações** : Adicione informações adicionais relacionadas aos observáveis ou indicadores associados a esse objeto.
N/D	**Pesquisar no Navegador**	Use esta função de pesquisa para pesquisar vários objetos na biblioteca Threat Intel (TI). Por exemplo, você pode pesquisar todos os registros de observáveis no módulo da biblioteca de TI.
N/D	**PESQUISE na Biblioteca Intel de ameaças**	Use esta função de pesquisa para pesquisar os registros de origem em várias origens com base em seus critérios de pesquisa. Os resultados serão exibidos em separado **Resultados da pesquisa** guia. Por exemplo, para um endereço IP 104.227.137.35, se você precisar pesquisar os registros, inserindo 104.* A pesquisa restringirá os registros e exibirá os registros que contêm o endereço IP que começa com

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição do formulário objetos da biblioteca

Ordem	Menu/guia	Descrição
		104 no separado **Resultados da pesquisa** guia. • Você também pode modificar as palavras-chave de pesquisa existentes nos Critérios de pesquisa na mesma página de resultados da pesquisa sem voltar para a página da Biblioteca de ameaças. • Da mesma forma, você também pode pesquisar com base no nome e na descrição de qualquer registro específico. • Depois que os registros forem filtrados e listados, você poderá clicar na exibição de lista, que o levará ao respectivo registro em uma nova guia.

Repositório da biblioteca TISC

O repositório IOC contém objetos STIX, cada um desses objetos contém uma informação específica.

Observáveis

Observáveis representam propriedades com estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes.

Estes são os tipos de observáveis disponíveis na aplicação:

- Artefato
- Número do AS
- Diretório
- Nome do domínio
- Endereço de E-mail
- Mensagem de E-mail
- Assunto do E-mail
- Arquivo
- Endereço IPv4
- CIDR de IPv4

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço de IPv6
- CIDR de IPv6
- Endereço MAC
- Hash MD5
- Nome de mutex
- Rede
- Outro observável
- Processo
- Hash SHA1
- Hash SHA256
- Hash SHA512
- Software
- URL
- Conta de usuário
- Chave de Registro do Windows
- Certificado X.509

Defina um observável

Observáveis podem ser recuperados da ingestão de feed programada ou do assistente de importação. No entanto, você pode criar observáveis, conforme necessário.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Clique em **Nova**.
3. Selecione **Tipo de observável** .
   O formulário Criar novo registro observável é exibido.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

4. No formulário, preencha os campos.

   Nota: Sempre que você cria um novo observável ou exibe os observáveis existentes, o **Anexos** por padrão, o painel é exibido na exibição do formulário. Você pode clicar no ícone Anexos no menu contextual direito ou ir para **Preferências** > **Espaços** e desabilite o. **Mostre a barra lateral** . Para obter mais informações, consulte Configure as preferências do Next Experience Workspace .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção de detalhes

Campo	Descrição
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável.
Descrição	Descrição do registro observável.
Autor	Insira o nome.
Tipo	O tipo de classificação observável, como endereço IP, nome de domínio, artefato, diretório, arquivo, ou hash. Por padrão, isso é exibido quando você seleciona o novo registro.
Status	O status ativo ou inativo do observável.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
TLP	Valor exclusivo que indica a configuração de confidencialidade de dados por TLP.
Reputação	Especifica a reputação mal-intencionada do observável.
Status	Insira o status do observável se ativo ou inativo.
Pontuação de ameaça	Indica a pontuação de ameaça desse observável.
Tempo de expiração	Especifica o tempo de expiração do registro observável.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Confiança	Insira a confiança deste registro observável. A propriedade Confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Impedir atualizações do sistema	Definir este sinalizador como verdadeiro impedirá que o sistema substitua valores de campos no registro.
É falso-positivo	Um sinalizador booliano que indica se o observável é identificado como falso positivo.

Atributos

Campo	Descrição
Resolve para	Especifica uma lista de referências a um ou mais endereços IP ou nomes de domínio para os quais o nome de domínio resolve.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
É FQDN	Um nome de domínio totalmente qualificado (FQDN) é o endereço completo de um host de internet ou computador. Ele fornece sua localização exata no sistema de nomes de domínio (DNS) especificando o nome de host, o nome de domínio e o domínio de nível superior (TLD).

Informações adicionais

Campo	Descrição
Nível de ameaça	Indica o nível de ameaça do registro observável.
Visto pela primeira vez	A hora em que este registro observável foi visto pela primeira vez realizando atividades mal-intencionadas.
Gravidade da ameaça	Indica a gravidade da ameaça do registro observável.
Visto pela última vez	A hora em que este registro observável foi visto pela última vez executando atividades mal-intencionadas.
Categorias de uso	Categorias nas quais o observável se enquadra, como botnet ou phishing.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
Contexto adicional	Adicione qualquer contexto adicional.
Origens	Especifica a origem da ameaça a partir da qual este registro é criado.

Importante: **Pontuação relatada de origem** : Este campo contém o valor agregado das pontuações de ameaça relatadas pelas origens das quais o observável é ingerido. Para ver este campo no formulário de registro observável, você deve adicioná-lo manualmente, pois ele não está disponível por padrão.

Atributos

Campo	Descrição
Resolve para	Especifica uma lista de referências a um ou mais endereços IP ou nomes de domínio para os quais o nome de domínio resolve.
É FQDN	Um nome de domínio totalmente qualificado (FQDN) é o endereço completo de um host de internet ou computador. Ele fornece sua localização exata no sistema de nomes de domínio (DNS) especificando o nome de host, o nome de domínio e o domínio de nível superior (TLD).

Nota: **Resolve para** e. **FQDN** os atributos são aplicáveis somente ao **Nome do domínio** tipo de observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributos do tipo de observável

Nome de Atributo	Tipos de Atributo
Artefato	○ Chave de descriptografia ○ Algoritmo de criptografia ○ Hash MD5 ○ Tipo de MIME ○ Hash SHA1 ○ Hash SHA256 ○ Hash SHA512 ○ URL
Número do AS	○ Nome ○ RIR
Diretório	○ Hora de criação do diretório ○ Hora do último acesso ao diretório ○ Hora da última modificação do diretório ○ Caminho codificado
Nome do domínio	○ É FQDN ○ Resolve para
Endereço de E-mail	○ Nome de exibição ○ Corpo do e-mail ○ Destinatários de e-mail Cco ○ Destinatários de e-mail Cc ○ Destinatários de e-mail Para ○ Remetente do e-mail ○ Assunto do E-mail ○ Data de envio
Arquivo	○ Informações adicionais ○ Nome do arquivo codificado ○ Hora de criação do arquivo ○ Hora do último acesso ao arquivo ○ Hora da última modificação do arquivo ○ Número mágico do nome do arquivo ○ Hash MD5 ○ Tipo de MIME

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	◦ Hash SHA1 ◦ Hash SHA256 ◦ Hash SHA512
Endereço IPv4	◦ Número do AS ◦ Endereço MAC
CIDR de IPv4	◦ Número do AS ◦ Endereço MAC
Endereço de IPv6	◦ Número do AS ◦ Endereço MAC
CIDR de IPv6	◦ Número do AS ◦ Endereço MAC
Rede	◦ Bytes de destino ◦ Contagem de pacotes de destino ◦ Porta de Destino ◦ Hora de término ◦ Tamanho do corpo da mensagem HTTP ◦ Cabeçalho da solicitação HTTP ◦ Método de solicitação HTTP ◦ Valor da solicitação HTTP ◦ Versão da solicitação HTTP ◦ Byte de código ICMP ◦ Byte de tipo ICMP ◦ Está ativo na rede ◦ É bloqueio de soquete ◦ É escuta de soquete ◦ Protocolos de rede ◦ Família de endereços de soquete ◦ Descritor de soquete ◦ Identificador de soquete ◦ Opções de soquete ◦ Contagem de bytes de origem do tipo de soquete ◦ Contagem de pacotes de origem ◦ Porta de origem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	○ Hora de início ○ Sinalizadores de destino de TCP ○ Sinalizadores de origem de TCP
Processo	○ ASLR habilitado ○ Linha de comando ○ Diretório de trabalho atual (CWD) ○ DEP habilitada ○ Variáveis do Ambiente ○ Está oculto ○ SID do proprietário ○ ID do Processo ○ Prioridade ○ Hora de criação do processo ○ Descrições dos serviços ○ Nome de exibição do serviço ○ Nome do Grupo de serviço ○ Nome do serviço ○ Tipo de início do serviço ○ Tipo de serviço Status do serviço ○ Informação de inicialização ○ Nível de integridade do Windows ○ Título da janela
Software	○ Enumeração de plataforma comum (CPE) ○ Idiomas compatíveis ○ Identificação de software (SWID) ○ Versão do fornecedor
Conta de usuário	○ Hora de criação da conta ○ Hora de vencimento da conta ○ Login da conta ○ Tipo de Conta ○ Informações adicionais ○ Pode escalar privilégios ○ Hora da última mudança de credenciais ○ Nome de exibição ○ Hora do primeiro login

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	○ É conta desabilitada ○ É privilegiado ○ É conta de serviço ○ Hora do último login ○ ID do usuário
Chave de Registro do Windows	○ Chave modificada ○ Valor do registro de tempo ○ Contagem de subchaves
Certificado X.509	○ Informações adicionais ○ Identificador de chave de autoridade ○ Restrições básicas ○ Políticas de certificação ○ Pontos de distribuição de CRL ○ Uso de chave estendido ○ Inibir qualquer política ○ Emissor ○ Nome alternativo do emissor ○ É autoassinado ○ Uso de chave ○ Restrições de nome ○ Restrições de política ○ Mapeamentos de políticas ○ Uso de chave privada válido a partir de ○ Uso de chave privada válido até ○ Algoritmo de assinatura ○ Assunto ○ Nome Alternativo do Assunto ○ Atributos do diretório de assunto ○ Identificador de chave do assunto ○ Algoritmo de chave pública do assunto ○ Expoente de chave pública do assunto ○ Módulo de chave pública do assunto ○ Válido de ○ Válido Até ○ Versão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um registro observável.

5. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
6. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione a taxonomia associada a um observável.
Adicionar valores de taxonomia	Adicione os valores de taxonomia associados a um observável.

Registros de Origem

Campo	Descrição
Os detalhes dos registros de origem de um observável são exibidos, se houver.	

Tradução automática

O que Fazer Depois

A tabela a seguir lista os registros relacionados aos observáveis:

Registros relacionados

Lista relacionada	Descrição
Observável	Lista de observáveis relacionados a este observável. **Nota:** Esta seção também contém os possíveis relacionamentos entre dois observáveis. Para obter mais informações, consulte Confirmar o relacionamento possível observável-observável e consulte Defina relacionamentos observável-observável para os relacionamentos confirmados entre os dois observáveis.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Lista relacionada	Descrição
Indicadores	Lista de indicadores relacionados a este observável.
Padrões de ataque	Lista de padrões de ataque relacionados a este observável.
Campanhas	Liste as campanhas relacionadas a este observável.
Infraestrutura	Liste a infraestrutura, como sistemas, serviços de software e todos os recursos físicos ou virtuais associados relacionados a este observável.
Conjuntos de intrusão	Liste os conjuntos de invasão, como um conjunto de comportamentos e recursos adversários com propriedades comuns relacionadas a este observável.
Malware	Liste os registros de origem de malware relacionados a este observável.
Agentes da ameaça	Liste os agentes de ameaça relacionados a este observável.
Eventos de ameaça	Liste os eventos de ameaça relacionados a este observável.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente que estejam relacionados a este observável.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Do **Registros relacionados** , você pode confirmar os relacionamentos entre dois observáveis usando **Possíveis relacionamentos** seção disponível no **Observáveis** exibição de formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
3. Você pode adicionar observáveis a casos. Para obter mais informações, consulte Adicionar ao caso.
4. Você também pode executar ações de aprimoramento para observáveis. Para obter mais informações, consulte Execute ações de aprimoramento em um caso.

Registros de origem de observáveis

Os registros de origem contribuem para um registro agregado conforme exibido na exibição do formulário. Esses registros de origem são criados automaticamente a partir de feeds ou criados manualmente pelo usuário.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

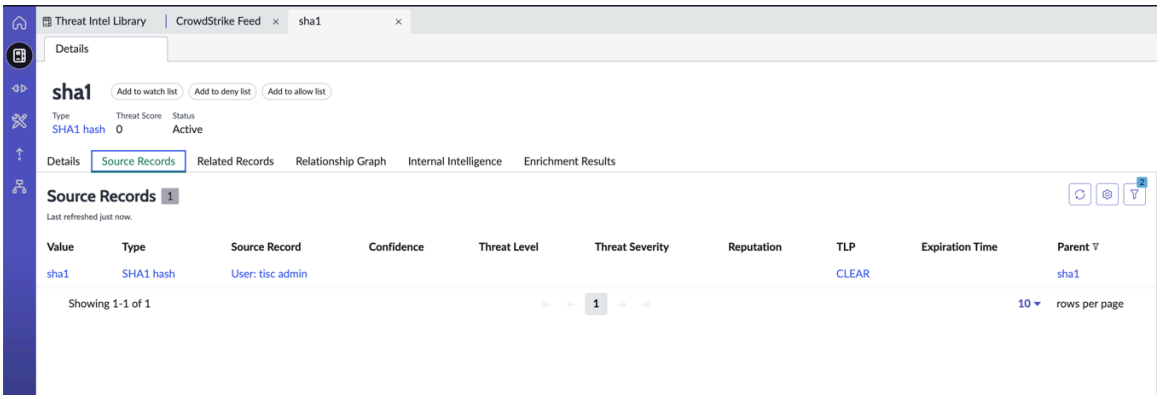
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione um ou mais observáveis.
5. Vá para **Registros de origem** .
   Os registros de origem para um registro agregado são exibidos.



6. Exiba os registros.

Vincular registros relacionados à Intel contra ameaças

Vincule os registros relacionados aos objetos de inteligência contra ameaças correspondentes.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro observável(s) como exemplo.
3. Vá para **Registros relacionados** seção.
4. Selecione qualquer registro relacionado.
5. Clique em **Vincular**.
   A caixa de diálogo Vincular objetos é exibida.
6. Selecione os objetos na lista e clique em **Link** botão.
   Os objetos associados a um registro observável serão vinculados e exibidos na exibição da lista Registros relacionados.
7. Clique em **Salvar**.
   Clique em **Desvincular** botão para desvincular os objetos

Buscar dados de observáveis

Busque os dados de registros relacionados aos observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

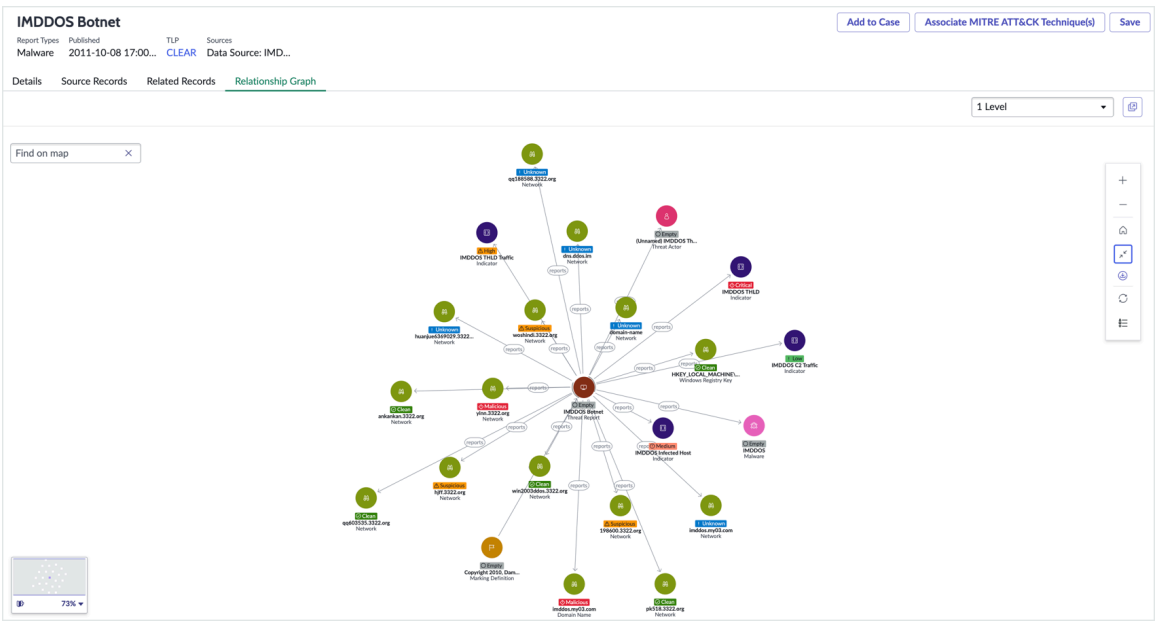
3. Vá para **Observáveis** .
   Os observáveis relacionados associados a esse objeto selecionado são exibidos.
4. Selecione qualquer registro observável.
   Se os observáveis fornecidos tiverem CVEs associados a ele, você poderá buscar seus dados relacionados vulneráveis automaticamente usando o botão fornecido, e esses registros associados serão exibidos na seção Contexto de negócios das Vulnerabilidades.
5. Ir para **Inteligência interna** > **Entradas vulneráveis**.
   Os registros CVEs associados para os observáveis são exibidos.
6. Selecione Qualquer CVE e clique em **Buscar dados relacionados a vulnerabilidades** botão.

Nota:

- Uma mensagem informativa é exibida informando que este objeto de vulnerabilidade específico não tem entradas vulneráveis associadas a ele. Você deve associar o(s) objeto(s) às entradas vulneráveis para buscar os dados. Para obter mais informações, consulte, Buscar dados de vulnerabilidade sobre como vincular os registros e executar o trabalho agendado para buscar os dados. E para obter mais informações sobre trabalhos agendados, consulte Trabalhos agendados .
- Este botão acionará um trabalho programado em segundo plano e os detalhes de início e execução do trabalho serão exibidos na seção Fluxo de atividades. Por exemplo, quando o trabalho é acionado, o fluxo de atividades exibe uma atividade que começou a buscar dados associados às entradas vulneráveis. O trabalho agendado em segundo plano verificará continuamente se há observáveis que tenham alguma entrada vulnerável associada ao observável e será executado automaticamente, e este trabalho agendado será executado a cada uma hora. se os registros não forem obtidos, você poderá vincular manualmente os registros e buscar os dados.

Exiba detalhes no Visualizador

Usando o Visualizador, você pode exibir os relacionamentos entre objetos, observáveis e indicadores, o que fornece contexto para você investigar mais. O Visualizador usa cores e ícones para ilustrar várias informações sobre os objetos.



Você pode fazer o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aplique zoom em qualquer objeto, ajuste-o na tela, arraste os nós ou fixe-os para se concentrar em um relacionamento específico.
- Clique em qualquer objeto para abrir o painel de detalhes. No painel de detalhes, você pode obter mais informações associadas ao objeto. Você pode exibir as propriedades do nó, como Objeto, Nome do objeto, Descrição e Origens. Por padrão, a seção de detalhes de cada nó do gráfico não é exibida e você precisa clicar em cada nó no gráfico para exibir os detalhes do nó selecionado.

  Nota: O Visualizador está disponível para todos os objetos de domínio (SDOs) do STIX, exceto os objetos de dados observados. Clique em **Atualizar** botão para atualizar o visualizador.

- Você também pode clicar no ícone pop-out para exibir o gráfico em uma janela muito maior.

Vincular ações de nó no Gráfico de relacionamento

Adicione novos registros relacionados para vincular os nós.

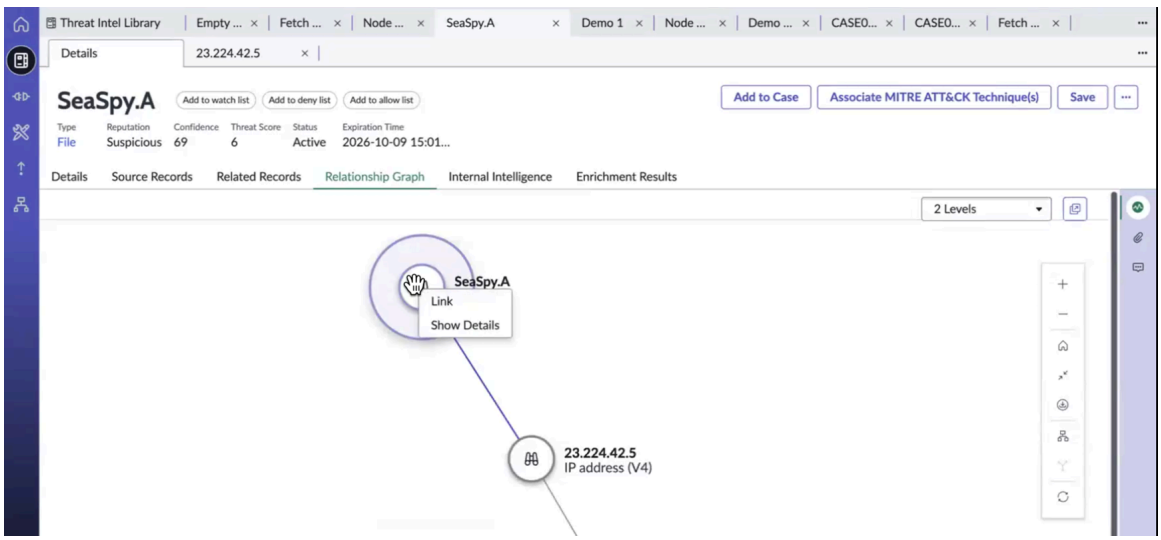
Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro observável(s) como exemplo.
3. Vá para **Gráficos de relacionamento** seção.
4. Clique no nó.
5. Clique em **Vincular**.

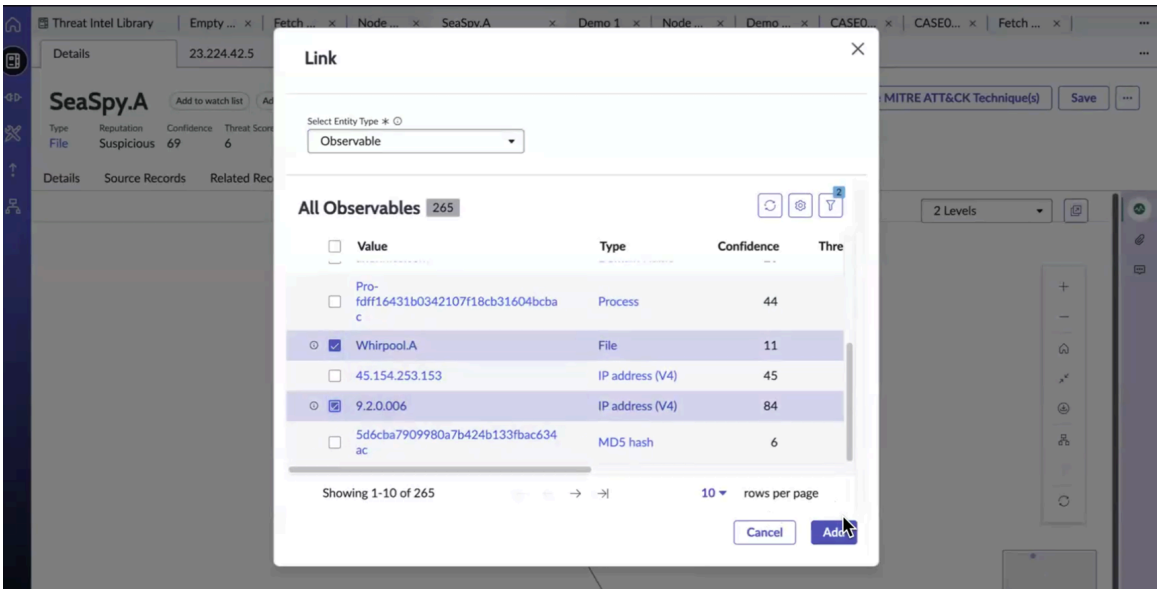
   Nota: Esta ação só está disponível no nível de nó inicial.



6. Selecione o tipo de entidade, como Observável.
7. Selecione um ou mais observáveis para o nó primário.
8. Clique em **Adicionar**.
   Os observáveis são adicionados ao nó primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Selecione **Desvincular** para desvincular os registros relacionados dos nós.

> **Nota:** Os dados de registros relacionados estão desvinculados, mas esses relacionamentos entre o nó inicial e o observável ainda estarão lá na biblioteca de inteligência contra ameaças.

10. Selecione **Mostrar detalhes** para ver os dados de observáveis associados.

Trabalhar com registros de inteligência interna

Use este recurso para trabalhar com os dados de inteligência interna coletados do Configuration Database Management System (CMDB) na Central de segurança do Inteligência contra ameaças.

Exibir registros de inteligência interna

Exiba os registros de inteligência interna coletados do CMDB, Resposta a incidentes de segurança (SIR), Resposta a vulnerabilidades (VR) nesses registros.

Antes de Iniciar

A seção Inteligência interna fornece o contexto de outras aplicações na plataforma, como SIR, VR e CMDB, para fornecer uma perspectiva mais ampla da ameaça para os analistas.

Função necessária: sn_sec_tisc.analyst

> **Nota:** A guia Inteligência interna só está visível para observáveis e objetos de vulnerabilidade.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro de observável(s).
3. Vá para **Inteligência interna** guia.
   A seção Inteligência interna é composta por três subseções, como Resposta a incidentes de segurança, Contexto de negócios e Resposta a vulnerabilidades.

> **Nota:** Você deve ter as respectivas aplicações instaladas em sua instância para que essas seções sejam listadas em **Inteligência interna** guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. **Resposta a incidentes de segurança** : Exibe todos os incidentes vinculados aos observáveis associados e aos itens de vulnerabilidade.

> **Nota:** O valor de observável(s) deve corresponder entre o incidente SIR e também no TISC, somente depois que os observáveis ou indicadores associados forem listados na seção Resposta a incidentes de segurança. Você também pode vincular e desvincular os registros pesquisando os registros nos sistemas de origem. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.

- Selecione qualquer registro para navegar e exibir os detalhes no sistema de origem. Por exemplo, observáveis associados na Resposta do incidente de segurança para buscar os registros de observáveis associados.
- Como parte da versão atual, a seguir estão os dados de inteligência que você pode buscar dos registros de origem (SIR):
  - Observáveis Associados
  - Itens de vulnerabilidade

b. **Contexto de negócios** : Exibe os usuários afetados e quaisquer outros itens de configuração. Como parte da versão atual, a seguir estão os dados de inteligência que você pode buscar dos registros de origem (contexto de negócios):
  - Itens de configuração
  - Serviços afetados
  - Ativos afetados

c. **Resposta a vulnerabilidades** : Exibe os dados de inteligência de vulnerabilidades.

Entradas de vulnerabilidade: Esta opção corresponde às vulnerabilidades e busca os registros relacionados.

Execute ações de aprimoramento do observável

Use esta seção para entender como as ações de aprimoramento são realizadas em observáveis e outros objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Clique em qualquer ação de aprimoramento no botão de divisão.
5. Selecione as implementações disponíveis.
6. Clique em **Enviar**.
   Por exemplo, Executar pesquisa de ameaças. A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida A execução de aprimoramento do observável foi iniciada no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

observável(s) selecionado(s). Os resultados estarão disponíveis na página de detalhes dos respectivos observáveis quando a execução for concluída .

Nota: Quando a execução é iniciada ou concluída, as anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.

Adicionar ao caso

Adicione observáveis, indicadores ou outros objetos ao caso.

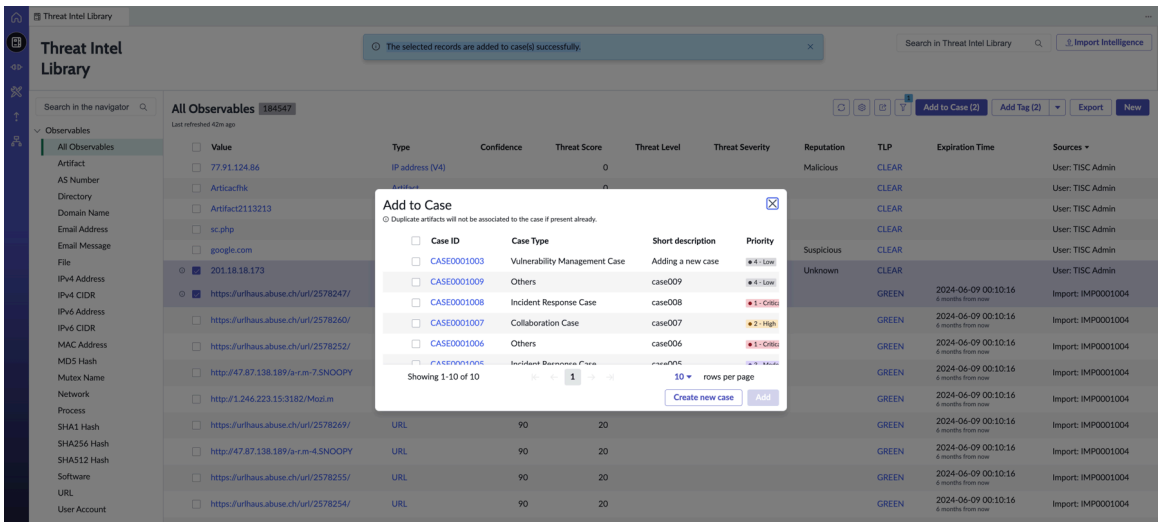
Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

A seguir está o procedimento que mostra como adicionar um caso a um registro observável.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione o(s) observável(s).
3. Clique em **Adicionar ao caso** botão.
   Exibe somente os casos em que o registro ainda não está associado.



4. Verifique se você deseja adicionar o registro aos casos existentes e, em caso afirmativo, selecione o caso existente. Caso contrário, clique em **Criar Novo Caso** .
   Insira as seguintes informações para criar um novo caso.

Criar novo caso

Campo	Descrição
ID do caso	Um identificador exclusivo do caso. Este é o ID gerado pelo sistema.
Descrição Resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de Caso	Selecione o tipo de caso que está sendo investigado. As opções possíveis para a investigação são: ○ Busca de ameaças ○ Solicitação de informações ○ Caso de gestão de vulnerabilidade ○ Caso de conformidade ○ Caso de resposta do incidente ○ Caso de colaboração ○ Outros
Prioridade	Uma avaliação da gravidade da solicitação ou problema.
Grupo de Atribuição	O grupo atribuído responsável por trabalhar no caso.
Atribuição a	O analista responsável por trabalhar em um caso.

5. Clique em **Criar** se você estiver criando um novo caso.

   Nota: O novo caso é adicionado à lista de casos existentes.

6. Selecione o(s) caso(s) recém-adicionado(s).
7. Clique em **Adicionar**.
   Uma mensagem informativa é exibida informando que os registros selecionados foram adicionados aos casos com sucesso.

Execute operações de aprimoramento no TISC

A tabela a seguir descreve as interações envolvidas na execução de diferentes operações de aprimoramento do TISC.

Telas modais do TISC

Capacidade	Interações de estruturas de UX	Integrações compatíveis
Executar pesquisa de ameaças	Na tela 1 - Selecione as implementações e envie. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Executar pesquisa de ameaças.	• Total de vírus • Crowd Strike Falcon Intelligence
Executar Pesquisa de detecções	As telas 1 - Selecionar Implementações e Tela 2 - Entradas comuns são aplicáveis.	• Pesquisa elástica • Splunk avistamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Interações de estruturas de UX	Integrações compatíveis
	A pesquisa de vistas usa a frequência de data e hora como entradas comuns em várias implementações do Splunk e outras integrações.	
Executar Aprimoramento do observável	Somente tela 1 - Selecione Implementações. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Executar aprimoramento do observável.	• WHOIS • Shodan

Executar Pesquisa de ameaças

Selecione uma ou mais implementações conforme aplicável para executar a pesquisa de ameaças em observáveis.

Antes de Iniciar

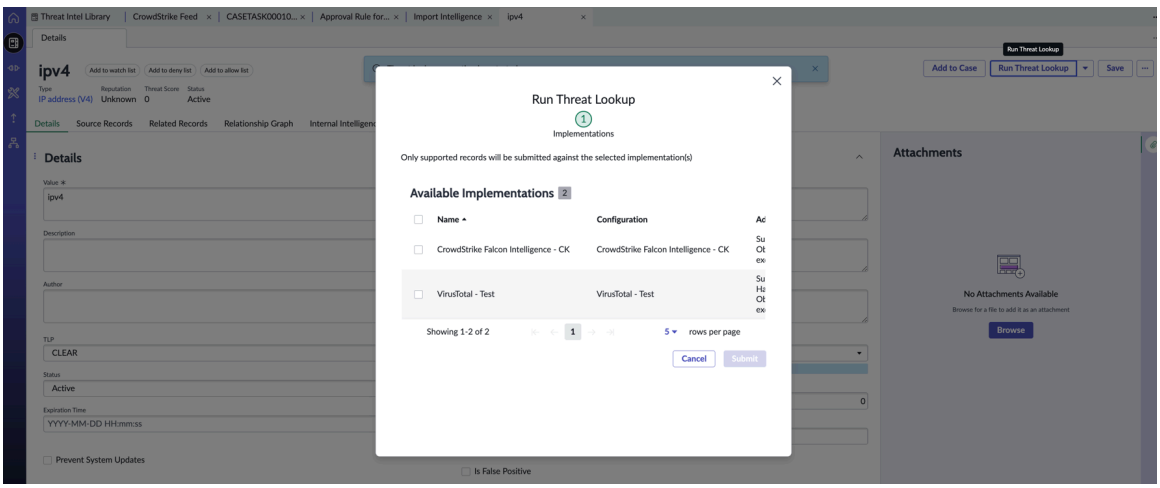
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique em **Executar Pesquisa de ameaças** .
   Executar pesquisa de ameaças **Selecione Implementações** a tela modal é exibida.

   Nota: Executar pesquisa de ameaças executa as pesquisas de inteligência contra ameaças para determinar se os observáveis estão associados a ameaças conhecidas.

6. Selecione as implementações necessárias na lista.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.
   A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida A execução da pesquisa de ameaças foi iniciada.

Nota:

- Quando a execução é iniciada ou concluída, as anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados em **Resultados de aprimoramento** Da página de detalhes dos observáveis correspondente no Espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando **Origem** campo da tabela de resultados de aprimoramento.

Executar Pesquisa de detecções

Executar integração relacionada à Pesquisa de detecção.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

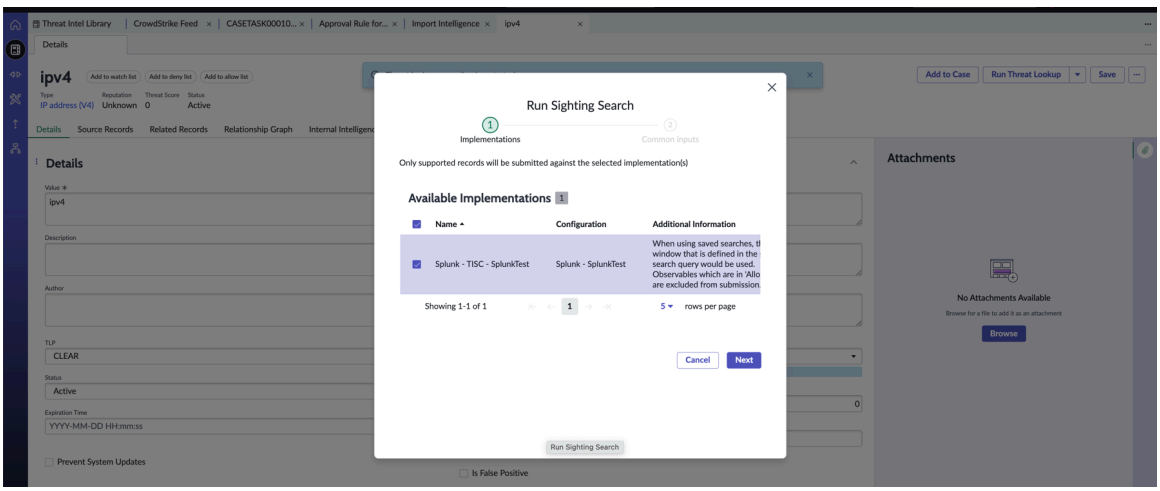
Para executar esta ação, selecione a implementação e adicione entradas de tempo de execução comuns que se aplicam a todas as implementações selecionadas, conforme aplicável.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique em **Executar Pesquisa de vistas** .
   Executar pesquisa de vistas **Selecione Implementações** a tela modal é exibida.

Nota: Executar pesquisa de detecção executa as pesquisas de inteligência contra ameaças para determinar se os observáveis estão associados a ameaças conhecidas.

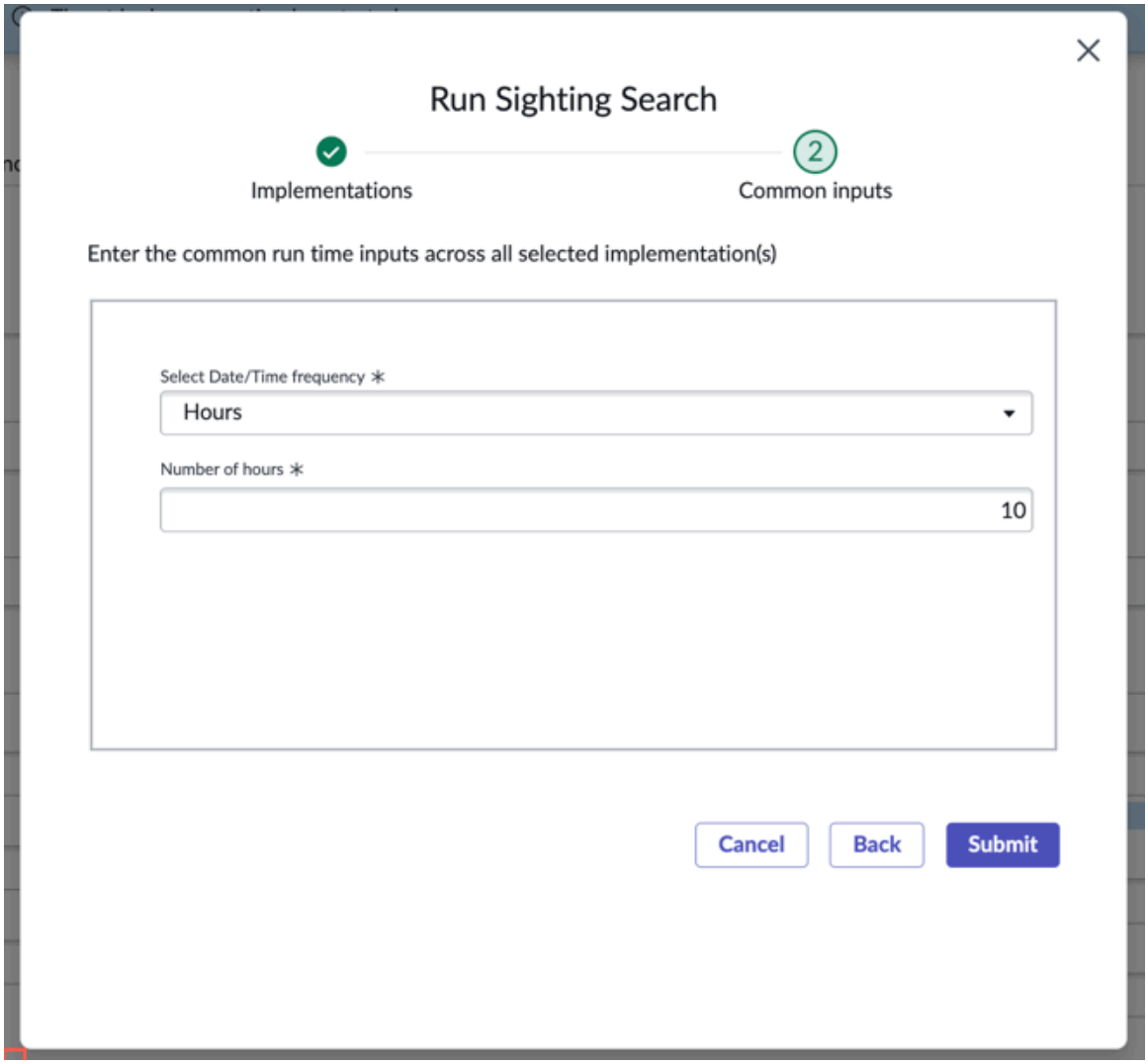
6. Selecione as implementações necessárias na lista.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Avançar**.
8. Selecione o valor de entrada de tempo de execução comum, como Selecionar frequência de data/hora e número de horas.



9. Clique em **Enviar**.
   A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida A execução da Pesquisa de vistas foi iniciada.

Nota:

- Quando a execução é iniciada ou concluída, as anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados em **Resultados de aprimoramento** Da página de detalhes dos observáveis correspondente no Espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando **Origem** campo da tabela de resultados de aprimoramento.

Executar Aprimoramento do observável

Selecione uma ou mais implementações conforme aplicável para executar a pesquisa de ameaças em observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

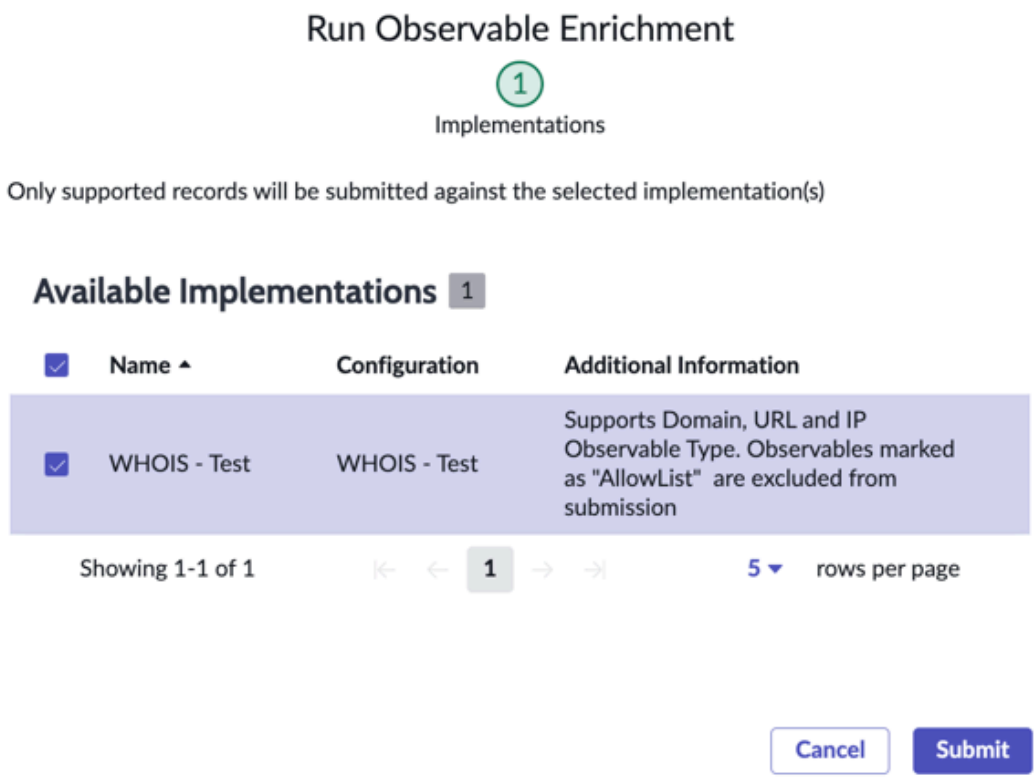
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Workbench do analista de ameaças** ícone.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique em **Executar aprimoramento de observável** .
   Executar aprimoramento do observável **Selecione Implementações** a tela modal é exibida.

   Nota: Somente registros compatíveis serão enviados em relação às implementações selecionadas

6. Selecione as implementações necessárias (por exemplo, WHOIS) na lista.



7. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida A execução da pesquisa de ameaças foi iniciada.

Nota:

- Quando a execução é iniciada ou concluída, as anotações de trabalho são publicadas no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados em **Resultados de aprimoramento** Da página de detalhes dos observáveis correspondente no Espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando **Origem** campo da tabela de resultados de aprimoramento.

Exibir resultados de enriquecimento

Exiba observáveis, indicadores e vários resultados de aprimoramento de objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro de observável(s).
3. Vá para **Resultados de aprimoramento** guia.
   Os resultados de aprimoramento exibem os resultados de aprimoramento das integrações do TISC.

Nome de aprimoramento	Descrição
Resultados da Pesquisa de ameaças	Lista todos os resultados de pesquisa de ameaças associados para um observável.
Detecções	Lista todas as vistas associadas a um observável.
Resultados de enriquecimento observável	Lista todos os resultados de aprimoramento de observável associados a um observável.

Indicadores

Os indicadores são artefatos observados em uma rede ou sistema operacional que provavelmente indicarão uma invasão. IOCs típicos são assinaturas de vírus e endereços IP, hashes MD5 de arquivos ou URLs de malware ou nomes de domínio.

Defina um Indicador

Defina um Indicador.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Indicadores**.
2. Selecione **Indicador** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

4. No formulário, preencha os campos.

Seção de detalhes

Campo	Descrição
ID	ID exclusivo do indicador.
Descrição	Descrição do indicador.
Nome	Nome do indicador.
Padrão	O padrão de detecção para este Indicador pode ser expresso como um padrão STIX.
Tipo de Padrão	O idioma padrão usado neste indicador.
Versão do padrão	A versão da linguagem padrão que é usada para os dados na propriedade padrão que deve corresponder ao tipo de dados padrão incluídos na propriedade padrão.
Válido de	O tempo a partir do qual este Indicador é considerado um indicador válido dos comportamentos relacionados ou que representa.
Válido Até	O tempo após o qual este Indicador não deve mais ser considerado um indicador válido dos comportamentos aos quais ele está relacionado ou representa.
Classificação IOC	A classificação IOC dos indicadores.
Tipos de Indicador	Indica as várias categorias do indicador.
Status	Indica o status dos indicadores.
Plataformas	Define as plataformas para as quais este indicador é aplicável.
TLP	Valor exclusivo que indica a configuração de confidencialidade de dados por TLP.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
Confiança	Insira a confiança deste registro de indicador. A propriedade Confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Nível de ameaça	Indica o nível de ameaça do registro do indicador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tempo de expiração	Especifica o tempo de expiração do registro do indicador.
Gravidade da ameaça	Indica a gravidade da ameaça do registro do indicador.
Categorias de uso	Categorias nas quais o observável se enquadra, como botnet ou phishing.
Visto pela primeira vez	A hora em que este registro de indicador foi visto pela primeira vez realizando atividades mal-intencionadas.
Visto pela última vez	A hora em que este registro de indicador foi visto pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um indicador.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este indicador.
Versão de especificação	A versão da especificação STIX usada para representar o indicador. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação em	Especifica a hora em que o indicador é criado no sistema.
Atualização em	Especifica a hora em que o indicador é atualizado no sistema.
Extensões	Indica as extensões do indicador.
Processando Status	Representa o status de processamento deste indicador.

5. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um indicador.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione a taxonomia associada a um indicador.
Adicionar valores de taxonomia	Adicione os valores de taxonomia associados a um indicador.

Registros de Origem

Campo	Descrição
Os detalhes dos registros de origem de um indicador são exibidos, se houver.	

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos indicadores.

Registros relacionados

Lista relacionada	Descrição
Técnicas MITRE	Lista as técnicas MITRE relacionadas a este indicador.
Padrões de ataque	Lista a origem de padrões de ataque que descreve os métodos que os adversários tentam comprometer destinos relacionados a este indicador.
Campanhas	Lista a Origem de campanhas que descreve um conjunto de atividades ou ataques mal-intencionados que ocorrem ao longo do tempo em relação a um conjunto específico de destinos relacionados a este indicador.
Linhas de ação	Lista os cursos de ação relacionados a este indicador.
Fontes de dados	Lista as fontes de dados relacionadas a este indicador.
Componentes de dados	Lista os componentes de dados relacionados a este indicador.
Identidades	Lista as identidades relacionadas a este indicador.
Indicadores	Lista os indicadores relacionados a este indicador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Lista relacionada	Descrição
	Nota: Esta seção também contém os possíveis relacionamentos entre dois indicadores. Para obter mais informações, consulte Confirmar possíveis relacionamentos indicador-indicador e consulte Defina relacionamentos indicador-indicador para os relacionamentos confirmados entre os dois observáveis.
Infraestrutura	Lista a origem da infraestrutura que descreve todos os sistemas, serviços de software e recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque relacionada a este indicador.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns relacionadas a este indicador.
Localizações	Lista as localizações geográficas associadas ao objeto.
Malware	Lista registros de origem de malware relacionados a este indicador.
Definições de marcação	Lista as definições de marcação associadas a este objeto.
Análise de malware	Lista os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância de malware associada a este indicador.
Observáveis	Lista os registros observáveis relacionados que estão relacionados a este indicador.
Dados observados	Lista os dados observados que são entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, e associados a este indicador.
Detecções	Lista os registros de origem de vistas associados a este objeto.
Agentes da ameaça	Lista as mudanças associadas ao observável.
Eventos de ameaça	Lista o evento ou a situação que pode causar consequências ou impacto indesejáveis associados ao indicador.
Grupos de ameaças	Lista os agrupamentos de ameaças como objetos que têm um contexto compartilhado.
Anotações de ameaça	Lista as anotações de ameaça que transmitem informações para fornecer contexto ou análise adicionais associadas ao indicador.
Opiniões sobre ameaças	Lista as opiniões de ameaça como uma avaliação da precisão das informações associadas ao indicador.
Relatórios de ameaças	Lista os relatórios de ameaças associados a este indicador.
Ferramentas	Lista a ferramenta associada a este objeto.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Casos Relacionados	Lista os casos relacionados associados a este indicador.
Tarefas do caso relacionado	Lista as tarefas de caso relacionadas associadas a este indicador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Lista relacionada	Descrição
Telas relacionadas	Lista as telas de pintura relacionadas associadas a este indicador.
Referências de indicadores	Lista de referências externas que descreve este indicador.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Do **Registros relacionados** , você pode confirmar os relacionamentos entre dois observáveis usando **Possíveis relacionamentos** seção disponível no **Indicadores** exibição de formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
3. Você pode adicionar indicadores a casos. Para obter mais informações, consulte Adicionar ao caso.

Padrões de ataque

Padrões de ataque são um tipo de táticas, técnicas e procedimentos (TTPs) que descrevem os métodos que os adversários tentam comprometer os alvos.

Os padrões de ataque são usados para ajudar a categorizar os ataques. Eles generalizam ataques específicos para os padrões que seguem e fornecem informações detalhadas sobre como os ataques são realizados.

Por exemplo, spear phishing é um tipo comum de ataque em que um invasor envia uma mensagem de e-mail cuidadosamente criada para uma parte com a intenção de fazer com que ela clique em um link ou abra um anexo para entregar malware. Os padrões de ataque são mais específicos, como spear phishing por um agente de ameaça específico (exemplo - que o alvo ganhou um concurso) também pode ser um padrão de ataque.

Defina um padrão de ataque

Defina um padrão de ataque para ajudar os analistas de ameaças a categorizar os ataques.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Padrão de ataque** .
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes do padrão de ataque

Campo	Descrição
ID	ID exclusivo para um padrão de ataque.
Nome	Insira um nome para este padrão de ataque.
Descrição	Insira uma descrição para um padrão de ataque.
Aliases	Nomes alternativos para identificar este padrão de ataque. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Fase de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
Permissões necessárias	Selecione as permissões necessárias para este padrão de ataque.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este modo de padrão de ataque. A propriedade Confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Impedir atualizações do sistema	Definir este sinalizador como verdadeiro impedirá que o sistema substitua valores de campos no registro.

Importante: Depois de criar um novo registro de objeto, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um padrão de ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto, padrão de ataque. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação em	Especifica a hora em que o registro é criado no sistema.
Atualização em	Especifica a hora em que o registro é modificado no sistema.
Extensões	Indica as extensões do padrão de ataque.
Processando Status	Representa o status de processamento deste objeto, padrão de ataque.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a um padrão de ataque.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a um padrão de ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao padrão de ataque.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campanha

Campanha é definida como o agrupamento de comportamentos adversários que descreve um conjunto de atividades ou ataques mal-intencionados, às vezes chamados de ondas que ocorrem durante um período de tempo em relação a um conjunto específico de metas.

Definir campanha

Defina uma campanha para agrupar comportamentos adversários.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Campanha** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição da campanha

Campo	Descrição
ID	ID exclusivo para um comportamento adversário.
Nome	Insira um nome para um comportamento adversário.
Descrição	Insira uma descrição para esta campanha.
Objetivo	O objetivo primário, o objetivo, o resultado desejado ou o efeito pretendido da campanha. O que o agente de ameaça ou o conjunto de intrusão espera realizar com esta campanha.
Aliases	Nomes alternativos a serem identificados para esta campanha. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
TLP	O protocolo de semáforo (TLP) indica as informações confidenciais compartilhadas com o público correto. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade para esse padrão de ataque.
Confiança	Insira a confiança para esta campanha.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para uma campanha.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta campanha.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando comportamento adversário.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando comportamento adversivo.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação em	Especifica a data e a hora em que o objeto foi criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Processando Status	Representa o status de processamento deste objeto, campanha.

Tradução automática

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a uma campanha.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a uma campanha.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados à campanha.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à campanha.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Linhas de ação

Cursos de ação são uma ação realizada para impedir um ataque ou para responder a um ataque que está em andamento.

Os cursos de ação descrevem respostas técnicas ou automatizadas, como aplicação de patches e reconfiguração de firewalls. Também pode descrever ações de nível superior, como treinamento de funcionários ou mudanças na política.

Por exemplo, os cursos de ação para mitigar uma vulnerabilidade podem descrever a aplicação do patch que a corrige.

Definir Cursos de Ação

Defina cursos de ação para evitar um ataque ou responder a um ataque em andamento.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Cursos de ação** objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes dos cursos de ação

Campo	Descrição
ID	ID exclusivo para cursos de ação para evitar um ataque.
Nome	Insira um nome descritivo para estes cursos de ação.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre os cursos de ação, potencialmente incluindo sua finalidade e suas principais características.
Ação	Para capturar cursos de ação estruturados ou automatizados.
TLP	O protocolo de semáforo (TLP) indica as informações confidenciais compartilhadas com o público correto. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade para esse padrão de ataque.
Confiança	Insira a confiança para estes cursos de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um curso de ação.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, cursos de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a um padrão de ataque.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a um padrão de ataque.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos cursos de ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Identidade

As identidades representam indivíduos, organizações ou grupos reais e classes de indivíduos, sistemas ou grupos. As identidades se aplicam ao STIX 2.x.

Um SDO de identidade pode capturar informações básicas de identificação, informações de contato e os setores aos quais a identidade pertence. A identidade representa alvos de ataques, fontes de informação, criadores de objetos e identidades de agentes de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina identidades

Defina identidades que representam indivíduos, organizações ou grupos reais.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Identidade** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes da identidade

Campo	Descrição
ID	ID exclusivo de uma identidade.
Nome	Insira um nome descritivo para esta identidade. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o curso da ação, potencialmente incluindo sua finalidade e suas principais características.
Funções	A lista de funções que esta identidade executa.
Classe da identidade	O tipo de entidade que esta identidade descreve. Por exemplo, indivíduo ou organização.
Setores	A lista de setores do setor aos quais esta identidade pertence.
Informações de Contato	As informações de contato, como e-mail e número de telefone desta identidade.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para esta identidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para a identidade.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional relacionado a esta identidade.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado.
   Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à identidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada à identidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados à identidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Infraestrutura

A infraestrutura SDO representa um tipo de táticas, técnicas e procedimentos (TTPs). Eles descrevem todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque. A infraestrutura se aplica ao STIX 2.x.

Os elementos de um ataque são representados por outros SDOs ou SCOs. No entanto, o SDO de infraestrutura representa um grupo nomeado de dados que constitui a infraestrutura.

Os exemplos de infraestrutura incluem servidores C2 usados em um ataque, um dispositivo ou um servidor que faz parte de uma defesa ou servidores de banco de dados visados por um ataque.

Definir infraestrutura

Defina uma infraestrutura que sejam todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Infraestrutura** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes da infraestrutura

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Nome	Insira um nome descritivo para este curso de ação. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a infraestrutura, incluindo potencialmente sua finalidade, como ela está sendo usada, como ela se relaciona com outras atividades de inteligência capturadas em objetos relacionados e suas principais características.
Tipos de infraestrutura	Descreve a categorização da infraestrutura.
Aliases	Nomes alternativos para identificar esta infraestrutura. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Visto pela primeira vez	A hora em que esta infraestrutura foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta infraestrutura foi vista pela última vez executando atividades mal-intencionadas.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta infraestrutura.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta infraestrutura.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a hora em que o registro é criado na origem.
Atualização em	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à infraestrutura.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta infraestrutura.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta infraestrutura.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Conjunto de intrusão

Um conjunto de invasão é um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns. Um conjunto de Intrusão geralmente envolve uma única organização. O conjunto de intrusão se aplica ao STIX 2.x.

Um conjunto de invasão pode capturar várias campanhas ou outras atividades. Essas atividades compartilham atributos que indicam um agente de ameaça comumente conhecido ou desconhecido.

Uma nova atividade pode ser atribuída a um conjunto de Intrusão, mesmo que os agentes de ameaça por trás do ataque não sejam conhecidos. Os agentes de ameaça podem passar do suporte a um conjunto de invasão para o suporte a outro, ou podem oferecer suporte a vários conjuntos de invasão.

Um Conjunto de Intrusão é o pacote de ataque inteiro e pode ser usado por um longo período em várias campanhas para alcançar possíveis finalidades múltiplas.

Defina o conjunto de invasão

Defina um conjunto de intrusão que seja um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Conjunto de intrusão** .
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do conjunto de invasão

Campo	Descrição
ID	ID exclusivo para um conjunto de invasão.
Nome	Insira um nome descritivo para este conjunto de invasão. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar este conjunto de intrusão. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Objetivos	Os objetivos de alto nível deste conjunto de Intrusão, ou seja, o que eles estão tentando fazer. Eles podem ser motivados por ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito. Para fazer isso, eles podem executar campanhas específicas que tenham objetivos detalhados, como comprometer sistemas de ponto de venda em um grande Varejista.
Visto pela primeira vez	A hora em que este conjunto de invasão foi visto pela primeira vez executando atividades mal-intencionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visto pela última vez	A hora em que este conjunto de invasão foi visto pela última vez executando atividades mal-intencionadas.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste conjunto de invasão. A motivação é a razão pela qual o Intrusion Set deseja alcançar o objetivo (o que eles estão tentando alcançar).
Motivações secundárias	As razões secundárias, motivações ou finalidades por trás deste conjunto de invasão. Essas motivações podem existir como uma causa igual ou quase igual à motivação primária. No entanto, não substitui ou necessariamente amplia a motivação primária, mas pode indicar contexto adicional. A posição na lista não tem significado.
Nível de recurso	Esta propriedade especifica o nível organizacional no qual este conjunto de invasão normalmente funciona, o que, por sua vez, determina os recursos disponíveis para este conjunto de invasão para uso em um ataque.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este conjunto de invasão.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este conjunto de invasão.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este conjunto de invasão.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o registro é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a hora em que o registro é criado na origem.
Atualização em	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao conjunto de invasão.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este conjunto de intrusão.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este conjunto de intrusão.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao conjunto de invasão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Local

Um local representa uma localização geográfica. Os locais são usados principalmente para dar contexto a outros SDOs. Os locais se aplicam ao STIX 2.x.

O local pode conter alguns ou todos os seguintes: Região (América do Norte), endereço cívico (Nova York, EUA), latitude e longitude.

O SDO do local pode estar relacionado a um conjunto de identidade ou invasão para indicar que o conjunto de identidade ou invasão está nesse local. Ele também pode estar relacionado a um malware ou padrão de ataque para indicar que a vítima de destino está em um local específico.

Por exemplo, um Local poderia ser usado em um relacionamento para descrever que o conjunto de intrusão Bourgeois Swallow tem origem na Europa Oriental.

Pelo menos uma das seguintes propriedades ou conjuntos de propriedades deve ser fornecida:

- região
- país
- latitude e longitude

Definir local

Defina uma localização geográfica para fornecer mais contexto a outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Local** objeto.
4. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos

Exibição Detalhes da identidade

Campo	Descrição
ID	ID exclusivo do local.
Nome	Insira um nome descritivo para identificar o local.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Latitude	A latitude do Local em graus decimais. Números positivos descrevem latitudes ao norte do equador, e números negativos descrevem latitudes ao sul do equador. O valor desta propriedade deve ser de -90,0 a 90,0, respectivamente.
Longitude	A longitude do local em graus decimais. Números positivos descrevem longitudines a leste do Meridiano Primário e números negativos descrevem longitudines a oeste do Meridiano Primário. O valor desta propriedade deve ser de -180,0 a 180,0, inclusive.
Precisão	Define a precisão das coordenadas especificadas pelas propriedades de latitude e longitude. É medido em metros. O local real pode estar em qualquer lugar até metros de precisão do ponto definido. Se esta propriedade não estiver presente, a precisão não será especificada. Se esta propriedade estiver presente, as propriedades de latitude e longitude deverão estar presentes.
Região	A região em que este local está.
País	O país em que este local está.
Área administrativa	O estado, província ou outra área administrativa subnacional em que este local está.
Cidade	A cidade em que este local está.
Endereço	O endereço descrito por este local. Esta propriedade inclui todos os aspectos ou partes do endereço.
CEP	O CEP em que este local está.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este local.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este local.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões para este local.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a hora em que o registro é criado na origem.
Atualização em	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao local.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este local.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este local.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao local.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Malware

Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido de forma secreta em um sistema. O malware se aplica ao STIX 2.x.

A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

O SDO de malware caracteriza, identifica e categoriza instâncias e famílias de malware a partir de dados derivados da análise. Este SDO captura informações detalhadas sobre como o malware funciona e o que ele faz.

Definir malware

Defina um malware que represente código mal-intencionado.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Malware** Objeto Intel de ameaça.
4. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do malware

Campo	Descrição
ID	ID exclusivo para identificar a instância de malware.
Nome	Insira um nome para identificar a instância ou a família de malware, conforme especificado pelo produtor da SDO. Para uma família de malware, o nome deve ser definido.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a instância ou família de malware, potencialmente incluindo sua finalidade e suas principais características.
Tipos de malware	Indica as várias categorias do malware.
É família	Marque esta caixa de seleção para especificar se o objeto representa uma família de malware ou uma instância de malware.
Aliases	Os nomes alternativos usados para identificar este malware ou família de malware. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas
Arquiteturas de processo	Indica as arquiteturas de processo para este malware.
Idiomas de implementação	Indica os idiomas de implementação deste malware.
Capacidades do malware	Os recursos que podem ser exibidos por uma instância ou família de malware.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Confiança	Insira a confiança deste malware.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para o registro de malware.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este registro de malware.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, malware.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao malware.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada ao malware.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados ao malware.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações relacionadas a este malware.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Análise de malware	Lista registros de análise de malware associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Malware	Lista registros de malware associados a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Análise de malware

A Análise de malware captura os metadados e os resultados de um malware. A análise de malware se aplica ao STIX 2.x.

A Análise de malware inclui análise estática ou dinâmica realizada em uma instância ou família de malware.

Definir Análise de malware

Defina a análise de malware que captura os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Análise de malware** objeto.
4. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes da análise de malware

Campo	Descrição
ID	ID exclusivo para identificar a análise de malware.
Produto	O nome do mecanismo de análise ou do produto usado. Os nomes dos produtos DEVEM ser todos minúsculos com palavras separadas por um hífen "-". Para casos em que o nome de um produto não pode ser especificado, um valor anonimizado deve ser usado.
Versão	A versão do produto de análise que foi usada para executar a análise.
VM da hospedagem	Uma descrição do ambiente de máquina virtual usado para hospedar o sistema operacional convidado, se aplicável, que foi usada para a análise dinâmica da instância ou família de malware. Se este valor não estiver incluído em conjunto com a propriedade operating_system_ref, isso significa que a análise dinâmica pode ter sido realizada em bare metal (ou seja, sem virtualização) ou que as informações foram editadas. O valor desta propriedade DEVE ser o identificador de um objeto de software SCO.
Sistema operacional	O sistema operacional usado para a análise dinâmica da instância ou família de malware. Isso se aplica a sistemas operacionais virtualizados, bem como aqueles em execução em bare metal. O valor desta propriedade DEVE ser o identificador de um objeto de software SCO.
Versão da configuração	Os nomes alternativos usados para identificar este malware ou família de malware.
Módulos	Os módulos de análise específicos que foram usados e configurados no produto durante esta execução de análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Versão do mecanismo de análise	A versão do mecanismo de análise ou produto (incluindo mecanismos AV) que foi usada para executar a análise.
Versão da definição de análise	A versão das definições de análise usadas pela ferramenta de análise, incluindo ferramentas de AV.
Análise iniciada	A data e a hora em que a análise de malware foi iniciada.
Análise finalizada	A data e a hora em que a análise de malware foi encerrada.
Resultado	O resultado da classificação conforme determinado pelo processo de análise do scanner ou da ferramenta.
Nome do resultado	O resultado da classificação ou o nome atribuído à instância de malware pela ferramenta de verificação.
Enviado	A data e a hora em que o malware foi enviado pela primeira vez para verificação ou análise. Este valor permanecerá constante enquanto a data de verificação pode mudar. Por exemplo, quando o malware foi enviado para uma ferramenta de análise de vírus.
Observável analisado	Selecione o observável que foi analisado.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para esta análise de malware.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para o registro da família de malware.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este registro de malware.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, malware.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao malware.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada ao malware.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados ao malware.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros Relatd

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Malware	Lista registros de malware associados a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Detecção de objeto

Avistamentos indicam que um objeto foi visto. Os objetos podem ser malware, ferramenta, agente de ameaça e assim por diante.

As vistas rastreiam quem e o que é o alvo, como os ataques são realizados e para rastrear tendências no comportamento de ataque.

O objeto de relacionamento de vistas contém propriedades extras que não estão presentes nos objetos de relacionamento genéricos. Essas propriedades extras representam dados específicos dos relacionamentos de avistamento.

Defina a detecção do objeto

Defina a detecção de objeto que descreve que um objeto (malware, ferramenta, agente de ameaça e assim por diante) foi visto.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Vá para **Vista de objeto** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Escolha Entidade e valor

Campo	Descrição
Entidade	Selecione o registro de detecção do objeto da entidade. **Nota:** Qualquer criação de novo registro de observação de objeto, um registro de relacionamento associado é necessário para agregação.
Detecção de	Indica que uma entidade ou indicador específico foi observado em um ambiente que pode ser uma indicação de uma possível ameaça. **Nota:** Selecione o registro relacionado à vista que está associado ao objeto selecionado no campo Entidade para que os registros relacionados possam ser criados e agregar os registros de vista.

Exibição Detalhes da vista do objeto

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o avistamento.
Visto pela primeira vez	O início da janela de tempo durante a qual o SDO fez referência à propriedade.
Visto pela última vez	O fim da janela de tempo durante a qual o SDO fez referência à propriedade.
Contagem	Se presente, deve ser um número inteiro entre 0 e 999,999,999, inclusive, e representa o número de vezes que o SDO fez referência à propriedade.
É resumo	Indica se o avistamento deve ser considerado os dados de resumo. Os dados resumidos são uma agregação de relatórios de vistas anteriores e não devem ser considerados dados de origem primária.
É interno	Indica se a mira é interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este conjunto de invasão.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.

7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à identidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta infraestrutura.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta infraestrutura.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vista do objeto.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Objetos	Lista os objetos associados às vistas.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Dados observados

Os dados observados transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os objetos de observação cibernética (SCOs) do STIX. Os dados observados se aplicam ao STIX 2.x.

Os dados observados capturam uma única observação de uma única entidade (arquivo, conexão de rede), bem como a agregação de várias observações de uma entidade.

Você pode usar Dados observados por conta própria (sem relacionamentos) para transmitir dados brutos coletados de qualquer fonte. As origens incluem relatórios de analistas, áreas restritas e ferramentas de detecção baseadas em rede e host.

Por exemplo, Dados observados podem capturar informações sobre um endereço IP, uma conexão de rede, um arquivo ou uma chave de registro. Os dados observados não são uma asserção de inteligência, são simplesmente a informação bruta sem qualquer contexto para o que significam.

Definir dados observados

Transmite informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os objetos de observação cibernética (SCOs) do STIX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Dados observados** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes dos dados observados

Campo	Descrição
ID	ID exclusivo para identificar os dados observados.
Observado pela primeira vez	A hora inicial em que os dados foram vistos.
Observado pela última vez	A última vez em que os dados foram vistos.
Contagem de observações	O número de vezes que cada objeto Cyber-observável foi visto. O valor deve ser um número inteiro de 1 a 999,999,999.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança dos dados observados
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esses dados observados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esses dados observados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados aos dados observados.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a estes dados observados.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a estes dados observados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos dados observados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Agente da ameaça

Os agentes de ameaça são indivíduos, grupos ou organizações que agem com intenção mal-intencionada. Os agentes de ameaça se aplicam ao STIX 2.x.

Um agente de ameaça não é um conjunto de invasão, mas pode oferecer suporte ou ser afiliado a vários conjuntos de invasão, grupos ou organizações ao longo do tempo.

Os agentes de ameaça usam seus recursos e os recursos de um conjunto de invasão para conduzir ataques e executar campanhas contra destinos.

Você pode identificar os agentes de ameaça por motivos, capacidades, objetivos, nível de sofisticação, atividades anteriores, recursos aos quais eles têm acesso e sua função na organização.

Definir agente de ameaça

Defina agentes de ameaça que são indivíduos, grupos ou organizações que agem com intenção mal-intencionada.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Agente de ameaça** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes do agente da ameaça

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Nome	Insira um nome descritivo para identificar o local.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Aliases	Uma lista de outros nomes para identificar este agente de ameaça. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Objetivos	Os objetivos de alto nível desse agente de ameaça, ou seja, o que ele está tentando fazer. Eles podem ser motivados por ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito.
Tipos de Agente da Ameaça	O(s) tipo(s) deste agente de ameaça.
Funções de agente da ameaça	As várias funções do agente de ameaça para este objeto.
Visto pela primeira vez	A hora em que este agente de ameaça foi visto pela primeira vez. Esta propriedade é uma propriedade resumida de dados de avistamentos e outros dados que podem ou não estar disponíveis no STIX. Se forem recebidas novas vistas anteriores ao carimbo de data/hora visto pela primeira vez, o objeto poderá ser atualizado para considerar os novos dados.
Visto pela última vez	A hora em que este agente de ameaça foi visto pela última vez.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste agente de ameaça. A motivação é o motivo pelo qual o agente de ameaça deseja atingir o objetivo (o que ele está tentando alcançar). Um Ator de Ameaça com o objetivo de perturbar o setor financeiro em um país pode ser motivado pelo ódio ideológico ao capitalismo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Sofisticação	A habilidade, o conhecimento específico, o treinamento especial ou a experiência que um agente de ameaça deve ter para executar o ataque.
Motivações secundárias	Esta propriedade especifica os motivos secundários, motivações ou finalidades por trás deste Agente de ameaça. Essas motivações podem existir como uma causa igual ou quase igual à motivação primária. No entanto, não substitui ou necessariamente amplia a motivação primária, mas pode indicar contexto adicional. A posição na lista não tem significado.
Nível de recurso	O nível organizacional no qual esse agente de ameaça normalmente trabalha, que, por sua vez, determina os recursos disponíveis para esse agente de ameaça para uso em um ataque. Este atributo está vinculado à propriedade Sofisticação. Um nível de recurso específico implica que o Agente da ameaça tem acesso a pelo menos um nível de sofisticação específico.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agente de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agente da ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agente de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agente de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agente de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista de locais associados a este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Evento de ameaça

Um evento ou situação que pode causar consequências ou impactos indesejáveis.

Um invasor que ataca um site é um evento de ameaça. Se os hackers conseguirem danificar qualquer site ou roubar informações, isso seria definido como um evento de ameaça.

Definir evento de ameaça

Defina um evento de ameaça quando for um evento que resulte em acesso não autorizado e aquisição de informações não públicas ou na interrupção ou uso indevido de qualquer sistema de informação.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Evento de ameaça** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do agente da ameaça

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um evento de ameaça.
Nome	Insira um nome descritivo para identificar o evento de ameaça.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o evento de ameaça, potencialmente incluindo sua finalidade e suas principais características.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agente de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao evento de ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este evento de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este evento de ameaça.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao evento de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Grupo de ameaça

Um objeto de agrupamentos de ameaças declara explicitamente que os objetos STIX referenciados têm um contexto compartilhado. Os agrupamentos de ameaças se aplicam ao STIX 2.x.

Um objeto de Agrupamentos de ameaças representa um conjunto de dados que, dada análise suficiente, amadurece para transmitir um incidente ou relatório de ameaça como um objeto de Relatório STIX. Por exemplo, um agrupamento pode ser usado para caracterizar uma investigação em andamento em um evento ou incidente de segurança.

Um objeto de agrupamentos de ameaças também pode ser usado para declarar que os objetos STIX referenciados estão relacionados a um processo de análise em andamento. Por exemplo, um analista de ameaças pode colaborar com outras pessoas em sua comunidade de confiança para examinar uma série de campanhas e indicadores.

O SDO de agrupamento de ameaças contém uma lista de referências a SDOs, SCOs e SROs, junto com uma declaração explícita do contexto compartilhado pelo conteúdo, uma descrição textual e o nome do agrupamento.

Defina o agrupamento de ameaças

Defina agrupamentos de ameaças como objetos que têm um contexto compartilhado.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Agrupamento de ameaças** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do agrupamento de ameaças

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir que um tipo de ataque de grupo de ameaças aconteça.
Nome	Insira um nome descritivo para identificar o grupo de ameaças.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o evento de ameaça, potencialmente incluindo sua finalidade e suas principais características.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agrupamento de ameaças.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agrupamento de ameaças.

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Anotação de ameaça

Uma anotação de ameaça transmite texto informativo para fornecer análise adicional não contida nos objetos STIX, objetos de definição de marcação ou objetos de conteúdo de idioma aos quais a anotação está relacionada. As anotações de ameaças se aplicam ao STIX 2.x.

Por exemplo, um analista pode adicionar uma anotação a um objeto de campanha criado por outra organização. A anotação pode indicar que eles viram publicações relacionadas a essa campanha em um fórum de hackers.

As anotações geralmente são criadas por analistas humanos e são compostas de texto orientado para o ser humano, elas contêm uma propriedade extra para capturar o autor que criou a anotação.

Definir anotação de ameaça

Defina anotações de ameaça que transmitem informações para fornecer contexto ou análise adicional que não está disponível em objetos existentes.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Anotação de ameaça** .
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes da anotação de ameaça

Campo	Descrição
ID	ID exclusivo para uma anotação de ameaça.
Resumo	Especifique um breve resumo do conteúdo da anotação.
Conteúdo	Especifica o conteúdo da anotação.
Autores	Especifica o nome do autor (exemplo, um analista).
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta anotação de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à anotação de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opinião sobre ameaças

Uma opinião é uma avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente. As opiniões sobre ameaças se aplicam ao STIX 2.x.

A propriedade de opinião captura o nível de acordo ou discordância usando uma escala fixa. A escala fixa também oferece suporte a um mapeamento numérico para permitir operações estatísticas consistentes em todas as opiniões.

Por exemplo, um analista de uma organização consumidora pode dizer que "discorda totalmente" de um objeto de campanha e fornecer uma explicação sobre o motivo.

As opiniões são subjetivas e a especificação não aborda a melhor forma de interpretá-las.

Os analistas humanos criam opiniões e são compostos de texto orientado para o ser humano, eles contêm uma propriedade extra para capturar o autor que criou a opinião.

Definir opinião de ameaça

Defina opiniões de ameaça como uma avaliação da precisão das informações em um objeto STIX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Opinião de ameaça** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes da opinião sobre ameaças

Campo	Descrição
ID	ID exclusivo para uma opinião de ameaça.
Opinião	A opinião do produtor sobre o objeto STIX.
Explicação	Especifica o conteúdo da opinião.
Autores	Especifica o nome do autor (exemplo, um analista).
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta opinião de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta opinião de ameaça.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a hora em que o registro é criado na origem.
Atualização em	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à opinião de ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta opinião de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta opinião de ameaça.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à opinião de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Relatório de ameaças

Relatórios de ameaças são coleções de inteligência contra ameaças com foco em um ou mais tópicos. Os relatórios de ameaças se aplicam ao STIX 2.x.

Os relatórios de ameaças incluem a descrição de um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças relacionada a ameaças para que ela possa ser publicada como uma história abrangente de ameaças cibernéticas.

O relatório de ameaças SDO contém uma lista de referências a objetos STIX junto com uma descrição textual e o nome do relatório.

Definir relatório de ameaças

Defina relatórios de ameaça que descrevem um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Relatório de ameaças** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do relatório de ameaças

Campo	Descrição
ID	Especifique um nome para identificar o relatório de ameaça.
Nome	Especifique um breve resumo do conteúdo da anotação.
Descrição	Uma descrição que fornece informações e contexto adicionais sobre o relatório.
Tipos de relatório	Especifica o nome do autor (exemplo, um analista).
Publicado	A data em que este relatório foi publicado oficialmente pelo autor do relatório.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta anotação de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos relatórios de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Grupos de ameaças	Lista os agrupamentos de ameaças associados a este objeto.
Relatórios de ameaças	Lista os relatórios de ameaças associados a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Ferramenta

Ferramentas são software legítimo que são usados por agentes de ameaça para executar ataques. As ferramentas se aplicam ao STIX 2.x.

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Por exemplo, as ferramentas de acesso remoto (RDP) e as ferramentas de verificação de rede (Nmap) são ferramentas que um agente de ameaça usa durante um ataque.

Definir ferramentas

Defina ferramentas como software legítimo que é usado para executar ataques.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Ferramenta** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes das ferramentas

Campo	Descrição
ID	ID exclusivo para identificar uma ferramenta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a ferramenta.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a ferramenta, potencialmente incluindo sua finalidade e suas principais características.
Tipos de Ferramentas	O(s) tipo(s) de ferramenta(s) que está(ão) sendo descrito(s).
Aliases	Nomes alternativos usados para identificar esta ferramenta. **Nota:** Para adicionar um novo alias que não existe na aplicação, clique em **Adicionar novos aliases** Ícone que está disponível no próprio campo Alias.
Versão da ferramenta	O identificador de versão associado à Ferramenta.
Fases de ataque	Representa a fase de ataque em uma cadeia de destruição, como LM, MITRE ATT&CK.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta ferramenta.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta ferramenta.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados às ferramentas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Vulnerabilidade

Uma vulnerabilidade é um ponto fraco ou defeito em um componente de software ou hardware que os invasores exploram. As vulnerabilidades se aplicam ao STIX 2.x.

O ponto fraco ou defeito está nos requisitos, designs ou implementações do código encontrado em um componente de software ou hardware. Essa fraqueza é diretamente explorada para afetar negativamente a confidencialidade, integridade ou disponibilidade desse sistema.

CVE é uma lista de vulnerabilidades e exposições de segurança da informação que fornece nomes comuns para problemas conhecidos publicamente [CVE].

Por exemplo, se um malware explorar CVE-2015-12345, um objeto de malware poderá ser vinculado a um objeto de vulnerabilidade que faça referência a CVE-2015-12345.

Definir Vulnerabilidade

Defina a vulnerabilidade como uma fraqueza ou defeito em um componente de software ou hardware que os invasores exploram.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Vulnerabilidade** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição Detalhes das vulnerabilidades

Campo	Descrição
ID	ID exclusivo para identificar uma vulnerabilidade.
Nome	Um nome usado para identificar a Vulnerabilidade.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, potencialmente incluindo sua finalidade e suas principais características.
Gravidade	Indica o grau normalizado de gravidade desta vulnerabilidade
CVSS3.0	Indica o CVSS v3 para esta vulnerabilidade.
CVSS 2.0	Indica o CVSS v2 para esta vulnerabilidade.
Status de exploração	Indica o status de exploração associado a esta vulnerabilidade
Publicado	Indica quando a vulnerabilidade é publicada.
Última modificação do registro	Indica quando o registro foi modificado pela última vez.
Software afetado	Lista o software afetado associado à vulnerabilidade.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta vulnerabilidade.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta vulnerabilidade.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Buscar dados de vulnerabilidade

Busque dados relacionados a vulnerabilidades, como itens de configuração, entradas vulneráveis e contexto de negócios.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Vulnerabilidade** objeto.
   As vulnerabilidades relacionadas associadas a este objeto são exibidas.
4. Selecione o respectivo registro de vulnerabilidade.
   Se houver CVEs associados a ele, você poderá buscar seus dados relacionados vulneráveis automaticamente usando o botão fornecido, e esses registros associados serão exibidos na seção Contexto de negócios das Vulnerabilidades.
5. Ir para **Inteligência interna** > **Entradas vulneráveis**.
   Os registros CVEs associados são exibidos.
6. Selecione Qualquer CVE e clique em **Buscar dados relacionados a vulnerabilidades** botão.

Nota:

- Este link associará automaticamente os registros e buscará esse contexto de negócios específico dos registros.
- Se não houver registros associados, uma mensagem informativa será exibida informando que este objeto de vulnerabilidade específico não tem entradas vulneráveis associadas a ele. Você deve associar manualmente o(s) objeto(s) às entradas vulneráveis para buscar os dados.
- Este botão acionará um trabalho programado em segundo plano e os detalhes de início e execução do trabalho serão exibidos no **Fluxo de atividades** seção. Por exemplo, quando o trabalho é acionado, o fluxo de atividades exibe uma atividade que começou a buscar dados associados às entradas vulneráveis. Para obter mais informações sobre como os trabalhos agendados são executados para buscar os dados, consulte Trabalhos agendados .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Link** vincular manualmente os objetos.
8. Selecione os registros a serem vinculados e busque os dados relacionados à vulnerabilidade usando **Buscar dados relacionados a vulnerabilidades** botão.
   Quando você clicar neste botão, o trabalho em segundo plano será acionado e os dados serão obtidos automaticamente para sua respectiva seção. Uma mensagem é exibida informando que o trabalho para buscar dados associados às entradas vulneráveis foi iniciado. Você pode rastrear o status no fluxo de atividades e atualizar a lista quando o trabalho estiver concluído para verificar os resultados. Por exemplo, se os dados estiverem relacionados aos itens de configuração, você verificará os resultados na seção Itens de configuração. Para obter mais informações sobre como adicionar CVEs, consulte Adicione CVEs a entradas de terceiros .

   Nota: Da mesma forma, você pode buscar os dados de registros de observáveis. Para obter mais informações, consulte Buscar dados de vulnerabilidade.

Definição de marcação

O objeto de definição de marcação representa uma marcação específica. As marcações de dados normalmente representam requisitos de manipulação ou compartilhamento de dados.

Definição de marcação

Defina definições de marcação para manipular e compartilhar os requisitos dos dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Definição de marcação** objeto.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes da origem da definição de marcação

Campo	Descrição
ID	ID exclusivo para identificar uma definição de marcação.
Nome	Um nome usado para identificar a Definição de marcação.
Tipo de definição	A propriedade de tipo identifica o tipo de objeto. A propriedade definition_type identifica o tipo de Definição de marcação.
Definição	A propriedade de definição contém o próprio objeto de marcação, por exemplo, TLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança deste objeto. A propriedade Confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta Definição de marcação.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta Definição de marcação.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.

7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vulnerabilidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Identidades	Lista as identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IOC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e todos os recursos físicos ou virtuais associados associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Conjuntos de intrusão	Lista um conjunto de comportamentos e recursos adversários com propriedades comuns associadas a este objeto.
Localizações	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código mal-intencionado associado a este objeto.
Análise de malware	Lista a análise mal-intencionada associada a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associados a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Grupos de ameaças	Lista os agrupamentos de ameaças associados a este objeto.
Anotações de ameaça	Lista as Anotações de ameaça associadas a este objeto.
Opiniões sobre ameaças	Lista as opiniões de ameaça associadas a este objeto.
Ferramentas	Lista as Ferramentas associadas a este objeto.
Vulnerabilidades	Lista as vulnerabilidades associadas a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Componente de dados

Os componentes de dados são usados para identificar propriedades ou valores específicos de uma fonte de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina o componente de dados

Defina um componente de dados para identificar as propriedades ou valores de uma fonte de dados

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Componente de dados** objeto.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes do componente de dados

Campo	Descrição
ID	ID exclusivo para identificar um componente de dados.
Nome	Um nome usado para identificar o componente de dados.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, potencialmente incluindo sua finalidade e suas principais características.
Fonte de dados	Indica o grau normalizado de gravidade desta vulnerabilidade
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Confiança	Indica a confiança deste objeto. A confiança deve estar entre 0 e 100.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este componente de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este componente de dados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do componente de dados.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao componente Dados.

Registros relacionados

Campo	Descrição
Padrões de ataque	Lista os padrões de ataque associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Fontes de dados

As fontes de dados representam os vários assuntos/tópicos de informações que podem ser coletados por sensores/logs. As fontes de dados também incluem componentes de dados, que identificam propriedades/valores específicos de uma fonte de dados.

Definir Fontes de Dados

Defina uma fonte de dados para representar os vários assuntos ou tópicos de informações.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Fontes de dados** objeto.
4. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e, em seguida, o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição Detalhes das vulnerabilidades

Campo	Descrição
ID	ID exclusivo para identificar a fonte de dados.
Nome	Um nome usado para identificar a fonte de dados.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a fonte de dados, potencialmente incluindo sua finalidade e suas principais características.
Camadas de coleção	Indica a descrição de onde a fonte de dados pode ser coletada fisicamente, como Host, Rede, Plano de controle de nuvem e assim por diante.
Plataformas	Indica que o sistema no qual um adversário está operando pode ser um sistema operacional ou aplicação.
Colaboradores	Indica os colaboradores desta fonte de dados.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta fonte de dados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta fonte de dados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2,1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação em	Especifica a data e a hora em que o objeto é criado na origem.
Atualização em	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando isso Um novo registro observável é criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro observável, **Impedir atualizações do sistema** a caixa de seleção é exibida.

Marque esta caixa de seleção para impedir atualizações do sistema após a criação dos registros observáveis, indicadores ou objetos STIX.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à fonte de dados.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta fonte de dados.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta fonte de dados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à fonte de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados à Intel contra ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, você usa **Possíveis relacionamentos** link do **Biblioteca Intel de ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirme possíveis relacionamentos objeto-objeto.
3. Além disso, use **Registros relacionados** Da exibição do formulário Objetos para confirmar os relacionamentos entre dois objetos usando **Possíveis relacionamentos** seção disponível na exibição do formulário. Para obter mais informações sobre consulte, Confirme possíveis relacionamentos de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Definir feeds RSS

Um feed de inteligência contra ameaças é um fluxo de dados contínuo em tempo real que coleta informações relacionadas a riscos ou ameaças cibernéticas. RSS Feeds fornece uma maneira fácil de se manter atualizado com seus sites favoritos, como blogs ou notícias mais recentes de segurança cibernética.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Feeds RSS** objeto.

   Nota: Os feeds ingeridos podem ser pesquisados usando esta seção, mas você não pode criar novos registros.

4. No formulário, os seguintes campos são preenchidos automaticamente.

Exibição de detalhes de feeds RSS

Campo	Descrição
Título	Título do Feed RSS.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre os feeds RSS, potencialmente incluindo sua finalidade e suas principais características.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Link	Indica o link adicionado aos feeds RSS.
Origem	Especifica a origem do feed RSS a partir da qual este registro de objeto é criado.
Datas de publicação	Indica quando o feed RSS é publicado.
Autor	Indica o autor do feed RSS.

5. Clique em **Salvar**.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este feed.

Informações adicionais

Campo	Descrição
URL da mídia	Indica o URL da mídia.
Comentários de feedback	Comentários de feedback adicionais sobre o feedback.

Tradução automática

Objetos de relacionamentos

Use os objetos Relacionamentos para vincular dois observáveis ou um observável e SDO para explicar como eles se relacionam entre si.

SROs (STIX Relationship Objects, objetos de relacionamento do STIX) representam tipos de relacionamentos entre vários objetos do STIX. Os seguintes objetos de relacionamento estão disponíveis:

- **Relacionamento observável-observável** : Este objeto define relacionamentos entre observáveis.
- **Relacionamento objeto-objeto** : Este objeto define relacionamentos entre SDOs, exceto o objeto indicador. Um exemplo de um relacionamento definido objeto-objeto é que um padrão de ataque entrega um malware.
- **Relacionamento objeto-observável** : Este objeto define relacionamentos entre SDOs e o objeto observável (SCO). Um exemplo de um relacionamento definido objeto observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.
- **Relacionamento objeto-indicador** : Este objeto define relacionamentos entre SDOs e o objeto indicador.
- **Relacionamentos Indicador-Indicador** : Este objeto define relacionamentos entre objetos indicadores.
- **Relacionamento indicador-observável** : Este objeto define relacionamentos entre o objeto indicador e outros SDOs. Um exemplo de um relacionamento definido por objeto-indicador é que um indicador detecta evidências de uma campanha.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto

Objeto de relacionamento	Origem de exemplo	Destino de exemplo	Descrição de exemplo
Relacionamentos observável-observável	Endereço IP, nome do domínio		Este relacionamento descreve entre os observáveis.
Relacionamentos objeto-objeto	Padrão de ataque	Malware	Este relacionamento descreve que este padrão de ataque é usado para entregar esta instância (ou família) de malware.
Relacionamentos objeto-observável			Este relacionamento descreve entre os objetos e os observáveis.
Relacionamentos objeto-indicador	Indicador	Ataque-padrão, Campanha, Infraestrutura, Conjunto de Intrusão, Malware, agente de ameaças, ferramenta	Este relacionamento descreve que o indicador pode detectar evidências do padrão de ataque relacionado, campanha, infraestrutura, conjunto de invasão, malware, agente ou ferramenta de ameaça. As evidências podem não ser diretas. Por exemplo, o indicador pode detectar evidências secundárias da campanha, como malware que é comumente usado por essa campanha específica.
Indicador - Relacionamentos do indicador	Infraestrutura	Dados observados	Este relacionamento descreve que o indicador é criado com base nas informações de um objeto de dados observado. Um exemplo de um relacionamento definido objeto observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto

Objeto de relacionamento	Origem de exemplo	Destino de exemplo	Descrição de exemplo
Indicador observável			Este relacionamento descreve entre os indicadores e os observáveis.

Defina relacionamentos observável-observável

Defina relacionamentos entre observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Observable-observable**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observável de origem	Selecione e defina o objeto de origem.
Observável de destino	Selecione e defina o objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. As opções disponíveis são: Defina a direção do relacionamento, seja direta ou inversa. ○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Base para correlação	Nome da regra de correlação com base na qual o sistema identificou como os registros relacionados desse observável. Esta regra é preenchida automaticamente.

6. Clique em **Enviar**.

Defina relacionamentos objeto-objeto

Defina relacionamentos entre SDOs, exceto o objeto indicador.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Object-Object**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto de origem	Selecione e defina o objeto de origem.
Tipo de objeto de origem	Define o tipo de objeto de origem.
Objeto de destino	Selecione e defina o objeto de destino.
Tipo de objeto de destino	Define o tipo de objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.
Descrição	Uma breve descrição sobre os relacionamentos de objetos.

6. Clique em **Enviar**.

Defina relacionamentos objeto-observável

Defina relacionamentos entre SDOs e o objeto observável (SCO).

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Objeto observável**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Observável	Selecione e defina o observável.
Objeto	Selecione e defina o objeto.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.
Descrição	Uma breve descrição sobre os relacionamentos de objetos.

6. Clique em **Enviar**.

Defina relacionamentos objeto-indicador

Defina relacionamentos entre o objeto indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Indicador de objeto**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Indicador	Selecione e defina o indicador.
Objeto	Selecione e defina o objeto.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.
Descrição	Uma breve descrição sobre os relacionamentos de objetos.

6. Clique em **Enviar**.

Defina relacionamentos indicador-indicador

Defina relacionamentos entre o objeto indicador e outros Use os objetos Relacionamentos para vincular dois observáveis ou um observável e SDO para explicar como eles se relacionam entre si.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Indicador-Indicador**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Descrição	Especifica a origem da ameaça a partir da qual este registro é criado.
Domínio	Define o escopo do registro do objeto. O valor neste campo é preenchido automaticamente.
Indicador de destino	Selecione e defina o objeto indicador de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Indicador de origem	Selecione e defina o indicador de objeto de origem.

6. Clique em **Enviar**.

Defina relacionamentos indicador-observável

Defina relacionamentos entre o objeto indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos** > **Indicador observável**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observável	Selecione e defina o observável.
Indicador	Selecione e defina o objeto indicador.

6. Clique em **Enviar**.

Relacionamentos potenciais

A aplicação usa correlação automatizada para estabelecer relacionamentos potencialmente possíveis entre dois SDOs, dois observáveis ou um observável e SDO.

1. Selecione um ou mais registros potencialmente relacionados e aplique esta ação na IU, o que mudará ainda mais os registros para a seção Relacionamentos confirmados e Visível nos registros relacionados.
2. Todas as correlações confirmadas ingeridas ou criadas manualmente por um analista substituirão os possíveis relacionamentos criados pela correlação automática.

Confirmar o relacionamento possível observável-observável

Use esta seção para confirmar os relacionamentos entre os observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos potenciais** > **Observable-observable**.
4. Selecione o registro Observável(s).
5. Clique em **Confirmar relação** .
   Um registro de relacionamento potencial é criado idealmente, que é identificado com base em suas regras de correlação. Depois de confirmar o relacionamento, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre os observáveis e observáveis foi confirmada. O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por exemplo, um possível relacionamento pode ser criado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

   Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia Registros relacionados de cada observável.

   a. Abra qualquer registro observável.
   b. Vá para **Registros relacionados** guia.
   c. Clique em **Link** botão.
   d. Selecione um ou mais observáveis.
   e. Clique em **Vincular**.
      Isso criará um novo relacionamento entre o registro observável selecionado e os observáveis recém-vinculados.
6. Clique em **Excluir** para excluir os relacionamentos.

Confirme possíveis relacionamentos objeto-objeto

Defina os possíveis relacionamentos entre os objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Ir para **Relacionamentos potenciais** > **Object-Object**.
4. Selecione o registro observável.
5. Clique em **Confirmar relação** .
   Um registro de relacionamento potencial é criado idealmente, que é identificado com base em suas regras de correlação. Depois de confirmar o relacionamento desta seção, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre os observáveis e observáveis foi confirmada. O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exemplo, um possível relacionamento pode ser criado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia Registros relacionados de cada observável.

a. Abra qualquer registro observável.

b. Vá para **Registros relacionados** guia.

c. Clique em **Link** botão.

d. Selecione um ou mais observáveis.

e. Clique em **Vincular**.
Isso criará um novo relacionamento entre o registro observável selecionado e os observáveis recém-vinculados.

6. Clique em **Excluir** para excluir os relacionamentos.

Confirmar possíveis relacionamentos indicador-indicador

Defina os possíveis relacionamentos entre os objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.

2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.

3. Ir para **Relacionamentos potenciais** > **indicador-indicador**.

4. Selecione o registro observável.

5. Clique em **Confirmar relação** .
Um registro de relacionamento potencial é confirmado idealmente com base em regras de correlação automatizadas. Depois de confirmar o relacionamento, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre os observáveis e observáveis foi confirmada.

O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por exemplo, um possível relacionamento é confirmado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia Registros relacionados de cada observável.

a. Abra qualquer registro observável.

b. Vá para **Registros relacionados** guia.

c. Clique em **Link** botão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Selecione um ou mais observáveis.

e. Clique em **Vincular**.
Isso criará um novo relacionamento entre o registro observável selecionado e os observáveis recém-vinculados.

6. Clique em **Excluir** para excluir os relacionamentos.

Exporte dados de inteligência

Use o recurso de exportação para exportar manualmente os dados de inteligência em vários formatos.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa
Atualmente, a funcionalidade de exportação está limitada a observáveis, indicadores e gestão de casos. O procedimento a seguir descreve como você pode exportar os dados dos observáveis e seguir o mesmo procedimento para exportar os dados dos indicadores.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.

2. Selecione qualquer observável(s).

3. Clique em **Exportação** botão.

Nota: . **Exportação** o botão é habilitado somente quando observáveis são selecionados para exportação. Se nenhum observável estiver selecionado, o botão permanecerá desabilitado.

4. Selecione o tipo de arquivo desejado para exportação.
Atualmente, os formatos de exportação compatíveis são Excel, CSV e STIX 2,1 JSON. Se o seu tipo de exportação for Excel, o número de registros que podem ser exportados por vez será limitado a 10 000, independentemente do tipo de formato selecionado.

Se a seleção exceder 10 000 registros, uma mensagem de erro será exibida indicando que o limite máximo do tipo de formato selecionado foi ultrapassado e somente os primeiros 10000 registros serão exportados.

Se o formato de exportação for CSV e o limite de registro for excedido, uma mensagem de alerta será exibida indicando que a exportação é **em andamento** , junto com um link para exibir o status da exportação. Você pode clicar no link para exibir o status, atualizar o registro e depois que ele for movido para **processado** depois de atualizar, você pode baixar o anexo.

5. Clique em **Exportar**.

Nota: Você também pode exibir dados de exportação do **Importações/exportações** módulo.

Uma mensagem de confirmação exibida indicando que a exportação foi bem-sucedida e que o download está concluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Confirme possíveis relacionamentos de registros relacionados

Confirme os relacionamentos entre os dois SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

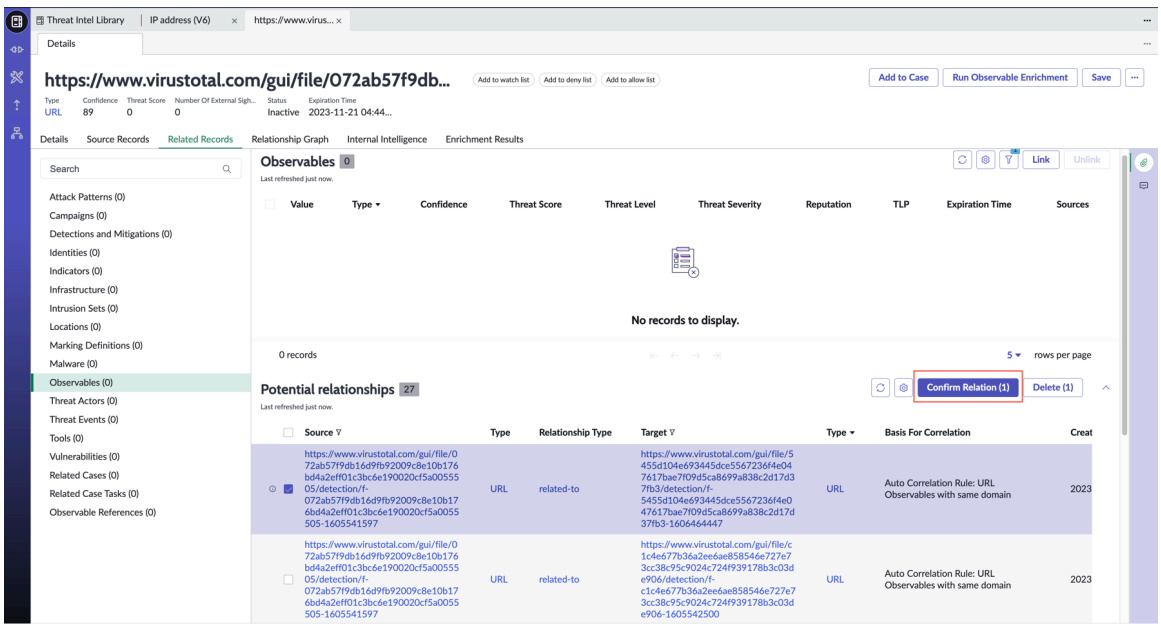
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Vá para **Registros relacionados** seção.
4. Expandir **Possíveis relacionamentos** .
5. Abra qualquer registro, como observáveis, indicadores ou quaisquer outros objetos que você deseja confirmar os relacionamentos entre dois SDOs.
6. Por exemplo, aqui selecione **Observáveis** na navegação à esquerda.
7. Selecione **Observável(s)** registros da lista.

   Nota: A seção de lista mostra todos os registros observáveis vinculados do observável associado.

8. Clique em **Confirmar relacionamentos** botão para confirmar os relacionamentos entre os objetos.

   Nota: Para obter mais informações, consulte Objetos de relacionamentos e. Relacionamentos potenciais.



9. Clique em **Excluir** para excluir os observáveis associados.
   Para obter informações sobre como os possíveis relacionamentos e relacionamentos são estabelecidos entre SDOs, consulte Relacionamentos potenciais e. Objetos de relacionamentos.

Correlação automatizada

A correlação automatizada ajuda a identificar os relacionamentos entre observáveis, indicadores e objetos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com o processo de correlação, a aplicação estabelece automaticamente a correlação entre os registros de inteligência contra ameaças com base nas regras predefinidas. Com base no tipo de regra que foi aplicada, o relacionamento pode ser um relacionamento confirmado ou um relacionamento potencial. Se os relacionamentos entre os objetos forem confirmados, esses objetos serão exibidos automaticamente na exibição de detalhes desse objeto em **Registros relacionados** seção.

A seguir descreve os relacionamentos e os possíveis relacionamentos:

- **Relacionamentos** : Use os objetos Relacionamentos para vincular dois observáveis ou um observável e SDO para explicar como eles se relacionam entre si.
- **Possíveis relacionamentos** : Use os relacionamentos potenciais para estabelecer relacionamentos potencialmente possíveis entre dois SDOs, dois observáveis ou um observável e SDO usando a correlação automatizada.

A seguir estão as regras de correlação predefinidas provisionadas no sistema de base:

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
Observáveis com o mesmo hash de arquivo	A regra compara os valores de hash dos observáveis (do mesmo tipo) e identifica se eles compartilham o mesmo hash.	A regra compara os valores de hash (do mesmo tipo) dos indicadores e identifica se eles compartilham o mesmo hash.	Cria um relacionamento
Observáveis de URL com o mesmo domínio	A regra examina os pontos comuns na estrutura dos URLs para identificar se eles compartilham o mesmo domínio de base.	A regra examina os pontos comuns na estrutura de URLs - identifica se eles compartilham o mesmo domínio de base e têm uma estrutura de subdiretório semelhante.	Cria um possível relacionamento
Observável encontrado como origens no objeto de rede	A regra corresponde ao valor do atributo de origem da rede com observáveis IPV4, IPV6 ou nome de domínio no sistema e links como a origem do tráfego.	A regra corresponde ao valor do atributo Origem com observáveis IPV4, IPV6 ou nome de domínio no sistema e links como Origem de tráfego.	Cria um relacionamento
Observável encontrado como destino no objeto de rede	A regra corresponde ao valor do atributo de destino de rede com OBSERVÁVEIS IPV4, IPV6 ou nome de domínio no sistema e links como o destino do tráfego.	A regra corresponde ao valor do atributo Origem com observáveis IPV4, IPV6 ou nome de domínio no sistema e links como destino do tráfego.	Cria um relacionamento
Relacionar observáveis com base na comunicação	Com base em objetos de rede, a regra identifica todos os observáveis (IPV4, IPV6 e nome	No baixo de objetos de rede, a regra identifica todos os indicadores que se comunicaram	Cria um relacionamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
	de domínio) que se comunicaram com o mesmo destino (IPV4, IPV6 ou nome de domínio) e estabelece um relacionamento entre esses observáveis. Observáveis relacionados (IPV4, IPV6 e nome de domínio) se estiverem relacionados ao mesmo objeto de rede que a origem se comunica com o destino.	com o mesmo destino (IPV4, IPV6, mac-addr ou domain-name) e estabelece um relacionamento entre esses indicadores como conectados à mesma infraestrutura C2.	
Observáveis de domínio raiz relacionados a subdomínios	A regra vincula um domínio raiz a subdomínios e vice-versa para o tipo de domínio de observáveis.	A regra vincula um domínio raiz a subdomínios.	Cria um relacionamento
Domínios relacionados a IPs com base em resoluções DNS	Usando atributos domain-ipv4 ou domain-ipv6 de observáveis de domínio, a regra estabelece relacionamentos entre os domínios e os IPs.	Use os atributos domain-ipv4 ou domain-ipv6, a regra identifica todos os domínios ou subdomínios que resolvem para o mesmo endereço IP e estabelece relacionamentos entre os indicadores, indicando sua conexão com a mesma infraestrutura C2.	Cria um relacionamento
Domínios correspondentes a certificados SSL	A regra analisa as informações do certificado SSL associadas aos observáveis de domínio e estabelece uma relação entre eles.	A regra analisa as informações do certificado SSL associadas aos indicadores e identifica que ambos os certificados são emitidos pela mesma autoridade de certificação e compartilham a mesma data de expiração e estabelece relacionamentos entre os indicadores, indicando sua conexão com a mesma infraestrutura C2 ou campanha de ameaça.	Cria um relacionamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
Relacionar entidades com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a duas entidades diferentes e as relaciona entre si.	A regra compara se o mesmo observável está relacionado a duas entidades diferentes e as identifica como relacionadas entre si.	Cria um possível relacionamento
Relacionar indicadores com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a dois indicadores diferentes e os relaciona entre si.	A regra compara se o mesmo observável está relacionado a dois indicadores diferentes e os identifica como relacionados entre si.	Cria um possível relacionamento
Relacionar indicadores a objetos com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a indicadores e objetos e os relaciona entre si.	A regra compara se o mesmo observável está relacionado a dois indicadores e objetos diferentes e os identifica como relacionados entre si.	Cria um possível relacionamento

Trabalhando com exportações de dados

Central de segurança de inteligência contra ameaças oferece suporte à exportação manual de observáveis, indicadores e casos nos formatos recomendados.

Esta funcionalidade permite extrair facilmente os dados para análise posterior. Os principais recursos são:

- Exporte observáveis, indicadores e casos individualmente ou em massa.
- Saída em formatos recomendados, como CSV, STIX 2,1 para integração perfeita.

Nota: Atualmente, a funcionalidade de exportações de dados é compatível somente com observáveis, indicadores e gestão de casos. Na Gestão de casos, as exportações são limitadas às listas Observável e Indicador em Artefatos de caso.

Exibir todas as exportações

Use esta seção para exibir todos os registros exportados manualmente.

Antes de Iniciar

Função necessária: sn_sec_tisc.export

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações/ Exportações**.
2. Selecionar **Exportações** > **Todas as exportações**
   Esta página exibe os registros de exportação.
3. Abra qualquer registro para exibir o status do processo de exportação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir minhas exportações

Exiba e baixe as exportações que você está autorizado a acessar.

Antes de Iniciar
Função necessária: sn_sec_tisc.export

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações/Exportações**.
2. Selecionar **Exportações** > **Minhas exportações**
   Esta página exibe os registros de exportação.
3. Abra qualquer registro para exibir o status do processo de exportação.

Exportar propriedades do sistema de inteligência

Esta seção descreve as limitações de registro e suas propriedades durante a exportação de dados.

Nota: TISC fornece o seguinte limite para exportações de dados. Para definir as propriedades a seguir, navegue até **Propriedades do sistema** > **Importação/Exportação**.

Função necessária: sn_sec_tisc.export

Formato	Propriedade	Descrição
STIX 2.1 JSON	sn_sec_tisc.stix_export_limit	Número máximo de linhas que podem ser exportadas para um arquivo STIX 2,1. O padrão e é 10000.
STIX 2.1 JSON	sn_sec_tisc.stix_export_payload_streaming_attachment_objects_size	Se a contagem de objetos na matriz "objetos" da carga de exportação do STIX for maior do que o número especificado nesta propriedade, JSONStreamingAPI será usada para criar anexo. O limite de exportação padrão é 4000.
STIX 2.1 JSON	sn_sec_tisc.stix_json_from_json_streaming_api_timeout_in_seconds	Tempo limite (em segundos) que será usado ao acionar a ação do Flow Designer para gerar anexo JSON STIX usando a API de fluxo JSON. O limite de exportação padrão é 900.

Nota: Para entender melhor o limite de exportação em outros tipos de formato, consulte Limites de exportação .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE-ATT&CK™ Repositório

. MITRE-ATT&CK O repositório está disponível na Biblioteca de inteligência, onde os dados das origens DO MITRE são ingeridos.

Os dados DO MITRE que estão chegando ao repositório são armazenados em um repositório MITRE separado dos dados da Biblioteca Intel de ameaças, em que os dados DO MITRE não são acumulados para fluxo de agregação ou desduplicação e são independentes.

As fontes de dados disponíveis na aplicação são:

1. MITRE - ENTERPRISE ATT&CK
2. MITRE - MOBILE ATT&CK
3. MITRE - ICS ATT&CK

Esses dados dessas fontes são armazenados em um repositório MITRE separado na biblioteca TI no sistema de base. Se você quiser criar uma nova origem DO MITRE, configure uma origem personalizada. Para obter mais informações, consulte Exibir Feed personalizado e na exibição do formulário, clique em **Avançado** e selecione **Processador de relatório** : **MITRECollectionDataProcessor** .

Gerenciar matrizes

Gerencie as matrizes importadas das coleções MITRE TAXII. Matrizes são uma coleção de táticas e técnicas. Você pode exibir as matrizes para revisar se suas coleções estão disponíveis no repositório MITRE-ATT&CK.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Depois de habilitar as fontes de dados do feed relacionadas AO MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** Para executar as integrações e buscar as informações relacionadas AO MITRE.
   Para obter mais informações sobre como habilitar as integrações
2. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK**.
   Os registros relacionados AO MITRE ATT&CK são exibidos. Por padrão, todos os registros estão no estado Habilitado.

   Nota: Você pode habilitar somente as matrizes que são relevantes para sua organização.

3. Selecione qualquer registro de matriz e clique em **Desabilitar** se você quiser desabilitar qualquer registro específico.
4. Como alternativa, você pode criar um novo registro de matrizes clicando em **Novo** Para criar manualmente as matrizes MITRE ATT&CK.
5. Preencha os campos adequadamente.

Criar nova mitigação DO MITRE - Detalhes

Campo	Descrição
Nome	Insira o nome da matriz.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Ativo	Marque esta caixa de seleção para ativar o registro de matriz.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este tipo de objeto.
Comentários	Adicione quaisquer comentários que você possa ter além disso.

Gerenciar técnicas

Gerencie as técnicas importadas das coleções MITRE TAXII. As técnicas contêm várias maneiras pelas quais os invasores desenvolveram para empregar uma determinada tática. Você pode revisar e desativar técnicas que não são relevantes para sua organização. No STIX, as técnicas são conhecidas como padrões de ataque.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

As técnicas representam como um adversário atinge um objetivo tático executando uma ação.

Procedimento

1. Depois de habilitar as fontes de dados do feed relacionadas AO MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** Para executar as integrações e buscar as informações relacionadas AO MITRE.
   Para obter mais informações sobre como habilitar as integrações
2. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Técnicas**.
   Os registros das técnicas MITRE ATT&CK são exibidos. Por padrão, todos os registros estão no estado Habilitado.
3. Selecione qualquer registro de técnica e clique em **Desabilitar** se você quiser desabilitar qualquer registro específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Como alternativa, você pode criar novos registros de técnicas clicando em **Novo** Para criar manualmente as técnicas MITRE ATT&CK.
5. Preencha os campos adequadamente.

Criar nova mitigação DO MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo para uma técnica.
Nome	Insira o nome da técnica.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Plataformas	Adicione as plataformas necessárias.
Permissões necessárias	Adicione as permissões necessárias.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Prioridade	Indica o nível de prioridade atribuído à técnica MITRE, como Baixo, Moderado, Alto ou Crítico. **Nota:** As prioridades podem ser atribuídas a técnicas para adicionar relevância à sua organização.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de invasão, potencialmente incluindo sua finalidade e suas principais características.
Detecção	A técnica de detecção é usada para identificar o acesso de adversários ou atividades não autorizadas em redes de computadores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este tipo de objeto.
Comentários	Adicione quaisquer comentários que você possa ter além disso.
Marcadores de TISC	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar marcadores da TISC	Selecione marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. **Nota:** Marcadores podem ser atribuídos a técnicas para adicionar relevância à sua organização.

Gerenciar mitigações

Gerencie as mitigações importadas das coleções MITRE TAXII. As mitigações permitem impedir que um adversário execute técnicas ou subtécnicas com sucesso em sua organização. No STIX, as mitigações são conhecidas como curso de ações.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Depois de habilitar as fontes de dados do feed relacionadas AO MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** Para executar as integrações e buscar as informações relacionadas AO MITRE.
   Para obter mais informações sobre como habilitar as integrações.
2. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Mitigações**.
   Clique em uma mitigação para exibir todas as informações associadas.
3. Clique em **Novo** Para criar manualmente as mitigações DO MITRE ATT&CK.
4. Preencha os campos adequadamente.

Criar novas ferramentas MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, potencialmente incluindo sua finalidade e suas principais características.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.

Gerenciar grupos

Gerencie os grupos importados das coleções MITRE TAXII. Grupos são conjuntos de atividades de invasão relacionadas que são rastreados por um nome comum na comunidade de segurança. Os analistas rastreiam clusters de atividades usando vários termos, como grupos de ameaças, grupos de atividades, agentes de ameaças, conjuntos de invasão e campanhas. No STIX, os grupos são conhecidos como conjuntos de intrusão.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Grupos**.
   Você pode exibir os grupos listados.
2. Clique em **Novo** Para criar manualmente os grupos MITRE ATT&CK.
3. Preencha os campos adequadamente.

Criar novos grupos DO MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, potencialmente incluindo sua finalidade e suas principais características.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

4. Clique em **Salvar**.
5. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos** .

Gerenciar malware

Gerencie as informações de malware que você importou das coleções MITRE TAXII. É um tipo de TTP que representa código mal-intencionado.

Antes de Iniciar

Refere-se a um programa que é inserido de forma secreta em um sistema. A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Grupos**.
   Você pode exibir o malware listado.
2. Clique em um malware para exibir todas as informações associadas.
3. Clique em **Novo** Para criar manualmente o malware MITRE ATT&CK.
4. Preencha os campos adequadamente.

Criar novo malware MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, potencialmente incluindo sua finalidade e suas principais características.
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos** .

Gerenciar ferramentas

Gerencie as informações de ferramentas que você importou das coleções MITRE TAXII. Ferramentas são software legítimo que são usados por agentes de ameaça para executar ataques.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa
As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Procedimento

1. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Ferramentas**.
   Você pode exibir as ferramentas listadas.
2. Clique em uma ferramenta para exibir todas as informações associadas.
3. Clique em **Novo** Para criar manualmente as ferramentas MITRE ATT&CK.
4. Preencha os campos adequadamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar novas ferramentas MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, potencialmente incluindo sua finalidade e suas principais características.
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos** .

Gerenciar relacionamentos DO MITRE

Gerencie as informações de relacionamentos DO MITRE que você importou das coleções DO MITRE TAXII.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Relacionamentos**.
   Você pode exibir os relacionamentos listados.
2. Clique em qualquer objeto de origem para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Novo** Para criar manualmente os relacionamentos MITRE ATT&CK.
4. Preencha os campos adequadamente.

Criar novas ferramentas MITRE - Detalhes

Campo	Descrição
Objeto MITRE de origem	Adicione o objeto MITRE de origem.
Objeto MITRE de destino	Adicione o objeto MITRE de destino.
Tipo de MITRE de origem	Insira o tipo MITRE de origem.
Tipo de MITRE do destino	Insira o tipo de MITRE de destino.
Tipo de relacionamento	Defina relacionamentos entre objetos. Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. As opções disponíveis são: Defina a direção do relacionamento, seja direta ou inversa. ○ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ○ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Origem	Selecione e defina o objeto de origem.
ID do relacionamento	Defina o ID do relacionamento.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos** .

Migração de dados em TISC

A migração de dados é um processo quando você move todos os dados de uma IU clássica para TISC.

A finalidade desta migração é permitir que os usuários migrem os dados de dados de inteligência contra ameaças existentes para TISC. Para executar este processo, uma nova estrutura é introduzida em TISC que é explicado na seção adicional.

Migração de dados do SIR TI para TISC

Configuração do trabalho de migração de dados em TISC Permite mover os dados do plug-in de inteligência contra ameaças existentes para TISC plug-in de dados diretamente.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

- **Migração de registro seletivo** : Somente registros da tabela selecionada que atendem às condições especificadas são migrados.
- **Incluir relacionamentos** : Os registros relacionados serão migrados somente se **Incluir relacionamentos** a caixa de seleção está marcada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Status de migração da entidade** : Depois que uma entidade (observável ou objeto) for migrada, ela não será incluída em migrações futuras, a menos que esteja sendo migrada como um registro relacionado.

  Nota: Critérios de exclusão de registros para utilitário de migração

  O utilitário de migração exclui determinados registros com base nos seguintes critérios:

  - **Observáveis** Observáveis do tipo **arquivo** que contenham anexos de arquivo seguros não serão migrados.
  - **Indicadores** Indicadores com valores em branco nos campos Padrão ou Tipo de padrão não serão migrados.
  - **Objetos** Objetos ingeridos do perfil MITRE TAXII nos dados de inteligência contra ameaças não serão migrados para a Central de segurança de inteligência contra ameaças.

- **Registros de Caso** : Somente registros ativos são migrados por padrão, a menos que **Incluir casos encerrados** a caixa de seleção está marcada.

Procedimento

1. Navegar até **Tudo** > **Central de segurança de inteligência contra ameaças** > **Configuração do trabalho de migração de dados**.
2. Clique em **Nova**.
3. No formulário, preencha os campos conforme apropriado.

Configuração do trabalho de migração de dados

Campo	Descrição
Nome	Nome da migração de dados.
Tabela	Selecione a tabela da qual os registros devem ser migrados TISC. . TISC as opções de tabela para migração são: ○ Observável(sn_ti_observable) ○ Indicador de compromisso (sn_ti_indicator) ○ Caso de segurança (sn_ti_case) ○ Objetos STIX V2 (sn_ti_stix2_object) (opções como padrões de ataque, campanhas, curso de ação)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Quando você seleciona a opção STIX V2, todos os objetos STIX são migrados, exceto o MITRE ATT&CK, pois o TISC tem uma estrutura diferente para migrar o MITRE ATT&CK. ◦ Quando você seleciona migrar o caso de segurança, os casos encerrados não serão migrados, mas somente os casos ativos serão migrados. Por exemplo, selecione **Observável** tabela de migração.
Ativo	Marque esta caixa de seleção se o processo de migração de dados estiver ativo.
Incluir relacionamentos	Marque a caixa de seleção para migrar os relacionamentos dos registros de inteligência contra ameaças para TISC registros. **Nota:** Quando você marca esta caixa de seleção, todas as entidades relacionadas são migradas junto com o observável e, se a caixa de seleção não estiver marcada, somente o observável único será migrado, sem entidades relacionadas.
Incluir casos encerrados	Marque esta caixa de seleção se quiser incluir os casos encerrados como parte da migração de registros de caso.
Migrar somente observáveis associados ao incidente de segurança	Marque a caixa de seleção para migrar os observáveis associados aos incidentes de segurança e, se a caixa de seleção não estiver marcada, todos os observáveis serão migrados, independentemente de sua associação a incidentes de segurança.
Condições	Opção para selecionar as condições que podem ser usadas para filtrar os dados que estão sendo migrados.
Configurações adicionais	
Confiança	Insira a confiança para as entidades do TISC migradas (observáveis, objetos ou indicadores). A confiança deve estar entre o intervalo de 0-100.
Período de expiração (dias)	O período de expiração dos migrados TISC entidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O sistema ignora ou ignora os registros que já foram migrados para TISC quando buscado novamente.

4. Clique em **Enviar**.
5. Clique em **Executar agora** para executar a migração de dados.
   Quando você executa a migração de dados, um trabalho em segundo plano é executado e o trabalho de migração é criado. Este trabalho cria um processo de migração e o tamanho do lote desses registros de migração é 5000.
6. Verifique o status do trabalho de migração em **Execuções de trabalho de migração** seção.
   O status do trabalho será enfileirado e o limite máximo do tamanho do lote não deve exceder 5000 registros. Clique no registro para exibir os objetos que são todos migrados para essa entidade específica.
7. Verifique o status do trabalho de migração em **Execuções de trabalho de migração** lista relacionada.
8. Clique no registro para exibir o status do processamento.
9. Verifique o status da migração em lote em **Fila de processamento de migração** seção da lista relacionada registros no registro de execução do trabalho de migração.
   O tamanho do lote para migração de registros é 5000.
10. Verifique as entidades TISC criadas como parte da migração em lote nas respectivas listas relacionadas em **Fila de processamento de migração** registro.

Fluxo funcional de processamento de dados do TISC

O Centro de segurança de inteligência contra ameaças (TISC) fornece uma solução que automatiza a coleta e o processamento de dados, o que ajuda a reduzir a carga sobre os analistas da Intel contra ameaças, evitando as etapas manuais envolvidas.

A Central de segurança de inteligência contra ameaças (TISC) coleta inteligência usando um dos seguintes métodos:

1. Ingestão de fontes de dados pré-configuradas e executadas em uma programação.
2. Analistas da Intel contra ameaças que importam dados usando o recurso Inteligência para importação.
3. Criação manual de registros individuais na aplicação.

Nota: Os dados coletados na aplicação serão processados para normalizar, desduplicar e agregar as informações antes de carregar na biblioteca Intel de ameaças.

Terminologia básica usada no processamento de dados

1. Tabelas de origem : As tabelas de origem contêm os dados relacionados às entidades que são obtidas de várias origens e, em seguida, os registros serão criados por cada origem.
2. Registros agregados : As tabelas de registros agregados contêm os dados relacionados a uma entidade específica, agregando os dados de todos os registros de origem de uma entidade específica.

Tradução automática

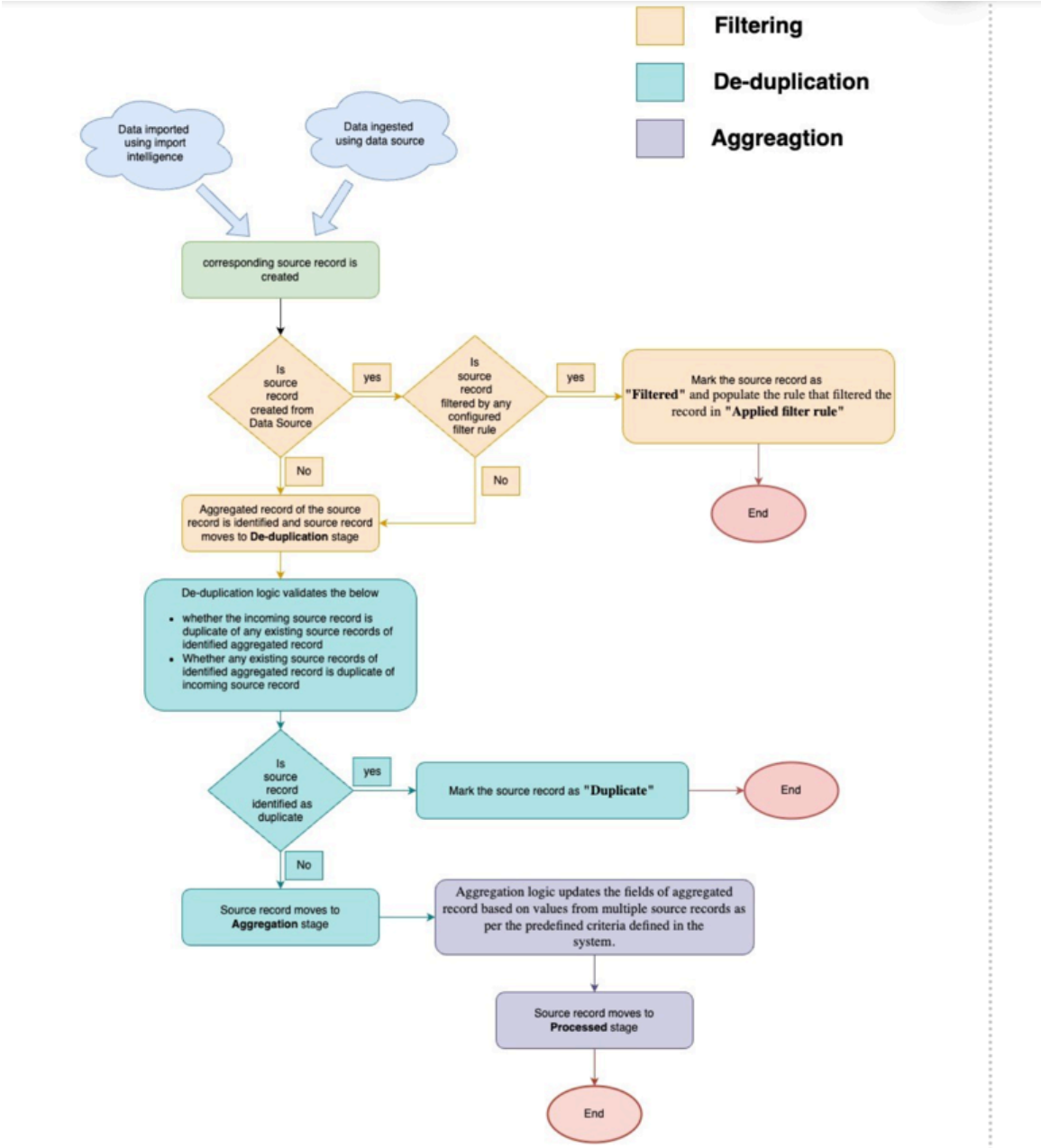
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de dados do TISC

1. Em uma execução bem-sucedida da inteligência de importação/fonte de dados, os registros seriam criados nas tabelas de origem correspondentes.
2. Quando os dados entram na tabela de origem, os dados passam pela lógica de filtragem para validar se o registro deve ser filtrado com base em configurado **Regras de filtragem de entrada** . (Vamos considerar SourceRecord1 como um registro de origem para nossa explicação).
3. Se o registro for filtrado por qualquer uma das regras de filtragem de entrada configuradas, o registro de origem correspondente (SourceRecord1) será marcado como **Filtrado** E a regra que filtrau o registro podem ser encontradas em Regra de filtro aplicada.
4. Vamos presumir que o registro de origem (SourceRecord1) seja agregado ao AggregateRecord1.
5. Se o registro não for filtrado, ele será marcado para desduplicação definindo o status de processamento como Pronto para desduplicação.
6. A lógica de desduplicação valida o seguinte:
   a. Se o registro de origem de entrada (SourceRecord1) é duplicado de qualquer registro de origem existente para AggregateRecord1.
   b. Qualquer um dos registros de origem existentes para AggregateRecord1 é uma duplicata do registro de origem de entrada (SourceRecord1).
7. Cada entidade tem campos e relacionamentos específicos com base nos quais o registro de origem é validado para duplicação.
8. Se o registro de origem de entrada (SourceRecord1) for uma duplicata de qualquer registro de origem existente do AggregateRecord1, o registro de origem de entrada (SourceRecord1) será marcado como duplicado.
9. Se algum registro de origem existente (Registro de origem existente 1) do AggregateRecord1 for identificado como duplicado do registro de origem de entrada (SourceRecord1), o registro de origem existente (Registro de origem existente 1) será marcado como duplicado e o registro de origem de entrada (SourceRecord1) será marcado para agregação definindo o status de processamento como Pronto para agregação.
10. Como parte da agregação, os campos do registro agregado AggregateRecord1 serão atualizados com base nos valores de vários registros de origem que serão agregados de acordo com os critérios predefinidos definidos no sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

TISC Arquivamento de dados

Os dados crescem rapidamente em tabelas com o aumento da adoção da plataforma. Algumas tabelas vêm no sistema de base com várias políticas de gestão de dados, mas outros usuários precisam ser implementados por eles mesmos.

Gestão de dados em TISC

Os dados são armazenados e gerenciados no TISC instância de acordo com TISC estrutura de objetos da biblioteca para que os administradores exibam e configurem de acordo com a necessidade da organização.

O arquivamento e restauração de dados é uma das principais funcionalidades para proteger os registros para uso futuro. A seção a seguir descreve o. TISC processo de arquivamento e retenção de registros como Inteligência contra ameaças contém grandes volumes de dados e registros.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Existem alguns métodos diferentes nos quais os usuários podem gerenciar seus dados em tabelas:

- Arquive os dados
- Exclua os dados

Nota: Se os usuários não adotarem nenhum dos métodos para gerenciar seus dados com eficácia, o uso aumentará com o tempo e os dados tenderão a ficar muito maiores, o que terá um grande impacto no desempenho da instância da aplicação e no armazenamento.

Arquivamento de dados do TISC

. Central de segurança de inteligência contra ameaçasé provisionado com regras de arquivamento no sistema de base para TISC tabela. Os registros relacionados também são adicionados no sistema de base ao TISC regra de arquivamento.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Arquivamento do Sistema** > **Regras de arquivamento**.
   A lista de regras de arquivamento aplicáveis a TISC são exibidos. Essas regras de arquivamento são diferentes para cada tipo de objeto e são aplicáveis independentemente.
2. Os nomes das tabelas começam com sn_sec_tisc.
3. Exiba TISC registros relacionados.

Registro de inteligência contra ameaças	Tabela de Referência
Padrão de ataque de arquivamento	sn_sec_tisc_attack_pattern
Arquivar campanha	sn_sec_tisc_campaign
Arquivar curso de ação	sn_sec_tisc_course_of_action
Componente de Dados de Arquivamento	sn_sec_tisc_agregado_data_component
Arquivar fonte de dados	sn_sec_tisc_agregado_data_source
Identidade do arquivamento	sn_sec_tisc_identity
Infraestrutura de arquivamento	sn_sec_tisc_infrastruction
Conjunto de Intrusão de Arquivamento	sn_sec_tisc_intrusão_set
Arquivar malware	sn_sec_tisc_malware
Arquivar análise de malware	sn_sec_tisc_malware_analysis
Definição de Marcação de Arquivamento	sn_sec_tisc_marking_definition
Arquivar detecção de objeto	sn_sec_tisc_object_sighting
Arquivar dados observados	sn_sec_tisc_observed_data
Agente de ameaça de arquivamento	sn_sec_tisc_threat_actor
Arquivar evento de ameaça	sn_sec_tisc_threat_event
Agrupar ameaças de arquivamento	sn_sec_tisc_threat_grouping
Arquivar anotação de ameaça	sn_sec_tisc_threat_note

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de inteligência contra ameaças	Tabela de Referência
Arquivar opinião de ameaça	sn_sec_tisc_threat_opinion
Arquivar relatório de ameaças	sn_sec_tisc_threat_report
Ferramenta de arquivamento	sn_sec_tisc_tool
Vulnerabilidade de arquivamento	sn_sec_tisc_vulnerability
Artefato	sn_sec_tisc_artifact
Número do AS	sn_sec_tisc_as_number
Diretório	sn_sec_tisc_directory
Endereço de E-mail	sn_sec_tisc_email_address
Mensagem de E-mail	sn_sec_tisc_email_message
Assunto do E-mail	sn_sec_tisc_email_subject
Arquivo	sn_sec_tisc_file
Regra de arquivamento do indicador	sn_sec_tisc_indicator
Endereço IPv4	sn_sec_tisc_ipv4_address
CIDR de IPv4	sn_sec_tisc_ipv4_cidr
Endereço de IPv6	sn_sec_tisc_ipv6_address
Local	sn_sec_tisc_location
Endereço MAC	sn_sec_tisc_mac_address
Hash MD5	sn_sec_tisc_md5_hash
Nome de mutex	sn_sec_tisc_mutex_name
Outro observável	sn_sec_tisc_other_observable
Processo	sn_sec_tisc_process
Hash SHA1	sn_sec_tisc_sha1_hash
Hash SHA256	sn_sec_tisc_sha256_hash
Hash SHA512	sn_sec_tisc_sha512_hash
URL	sn_sec_tisc_url
Conta de usuário	sn_sec_tisc_user_account
Chave de Registro do Windows	sn_sec_tisc_windows_registry_key
Certificado X.509	sn_sec_tisc_x_509_certificate
Regra de arquivamento de relacionamento objeto-objeto	sn_sec_tisc_m2m_object
Regra de arquivamento de relacionamento objeto-observável	sn_sec_tisc_m2m_object_observable
Regra de arquivamento do indicador relacionado	sn_sec_tisc_m2m_indicator
Regra de arquivamento do feed RSS	sn_sec_tisc_m2m_object_indicator
Regras de arquivamento de importações	sn_sec_tisc_m2m_indicator_observable

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Para obter informações sobre como as regras de arquivamento são criadas, consulte Crie uma regra de arquivamento .

4. Selecione uma regra de arquivamento.
   Por exemplo, selecione Registro Observável de diretório para ver a regra de arquivamento do sistema de base.
5. Atualize a regra, se necessário.

Arquivamento TISC registros relacionados

Use a lista relacionada Arquivar registros relacionados para TISC para adicionar os registros relacionados à regra de arquivamento.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
2. Os nomes das tabelas começam com sn_sec_tisc.
3. Vá para **Arquivar registros relacionados** seção de lista relacionada para exibir TISC registros relacionados.

Regras de destruição em TISC

Exiba as regras de destruição provisionadas no sistema de base.

Antes de Iniciar
Função necessária: administrador

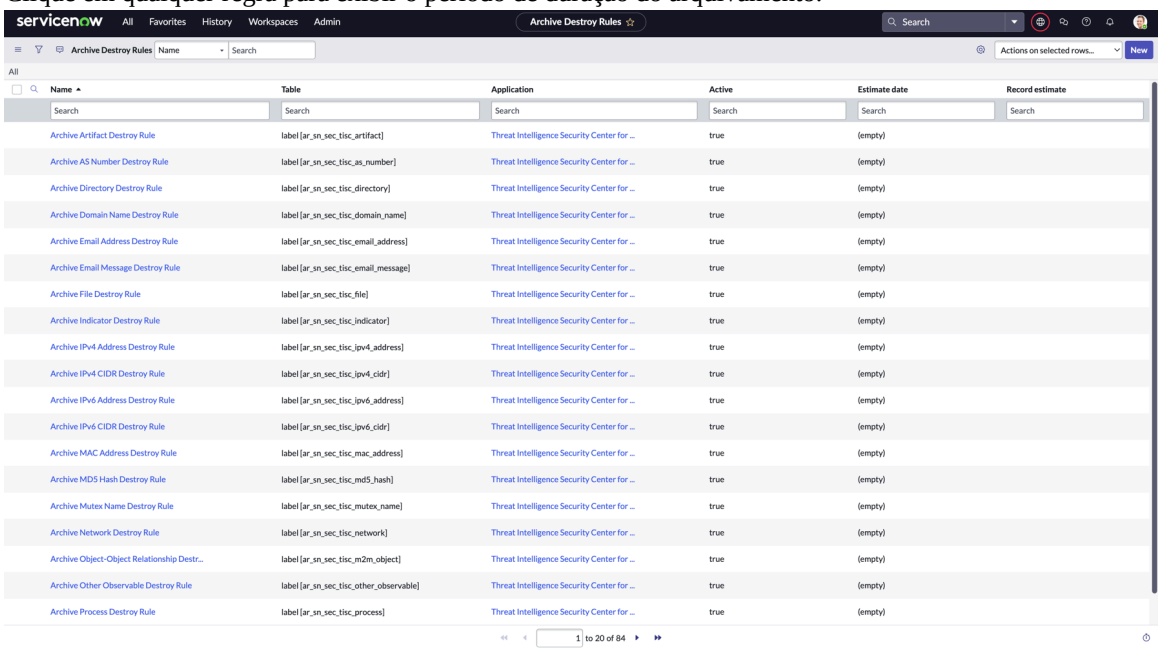
Procedimento

1. Navegar até **Tudo** > **Arquivamento do Sistema** > **Regras de Destruição de Arquivo**.
   A lista de regras de destruição aplicáveis a TISC são exibidos. Essas regras de destruição são diferentes para cada tipo de objeto e são aplicáveis independentemente.
2. Exiba as regras de destruição aplicáveis para TISC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em qualquer regra para exibir o período de duração do arquivamento.



Excluir registros de inteligência

Excluir registros de Inteligência contra ameaças biblioteca.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique em **Biblioteca Intel de ameaças** ícone no espaço.
3. Abra qualquer registro.
4. Vá para **Registros de origem** seção.
5. Selecione **Excluir** para excluir os registros de origem.
6. Exclua o registro da biblioteca.

Nota:

a. Se um registro de biblioteca com registros de origem associados for excluído, os registros de origem serão reprocessados e um novo registro de biblioteca será criado agregando os valores de campo dos registros de origem.

b. Para excluir permanentemente os dados da biblioteca de inteligência contra ameaças, use regras de arquivamento em vez de excluir os registros da biblioteca. Para obter mais informações, consulte, TISC Arquivamento de dados.

Data Loss Prevention Incident Response

. Data Loss Prevention Incident Response(DLP IR) permite revisar e gerenciar o fluxo de trabalho de correção de incidentes de DLP de várias origens, como endpoint, rede, e-mail e nuvem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Data Loss Prevention Incident Response

Explorar



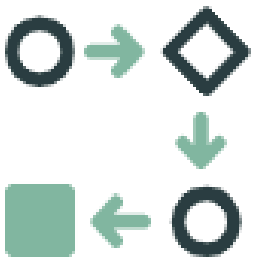
Saiba mais sobre como os analistas e administradores usam a Resposta a incidentes do DLP

Instalar e configurar



Instalação e configuração da aplicação Resposta de incidentes do DLP

Administrar



Tarefas de administração sobre como gerenciar os incidentes de DLP no ServiceNow AI Platform

Uso



Atualize e gerencie incidentes aproveitando o Portal do usuário final do DLP, o Portal de operações do DLP e o Painel do DLP.

Integrar



Estenda os recursos de DLP integrando com aplicações de terceiros

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solucionar problemas e obter ajuda

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

Explorando Data Loss Prevention Incident Response

Explorar Data Loss Prevention Incident Response aplicação para aprender a gerenciar informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social.

A perda de dados ocorre quando informações confidenciais ou confidenciais saem da rede corporativa como resultado de comunicação não autorizada. Com a aplicação DLP, você pode identificar, responder e proteger seus canais de perda de dados.

Usando o. Data Loss Prevention Incident Response sua organização tem os seguintes benefícios principais:

- Integre com várias soluções DLP de terceiros para obter uma exibição unificada dos incidentes no ServiceNow AI Platform.
- Monitore e atribua incidentes aos usuários finais para que você possa simplificar a gestão de incidentes do DLP.
- Treine seus funcionários por meio dos modelos de e-mail personalizados e das notificações que são enviadas para cada incidente, bem como na forma de um resumo.
- Escale os incidentes de DLP atrasados dos usuários finais para os gerentes.
- Exiba relatórios resumidos de incidentes em aberto por política, gravidade, principais infratores e assim por diante.
- Rastreie tendências de incidentes de DLP, tendências de falso-positivos e tendências de correção.

Use esta seção para saber mais sobre os principais recursos e as várias funções envolvidas no trabalho com incidentes de DLP.

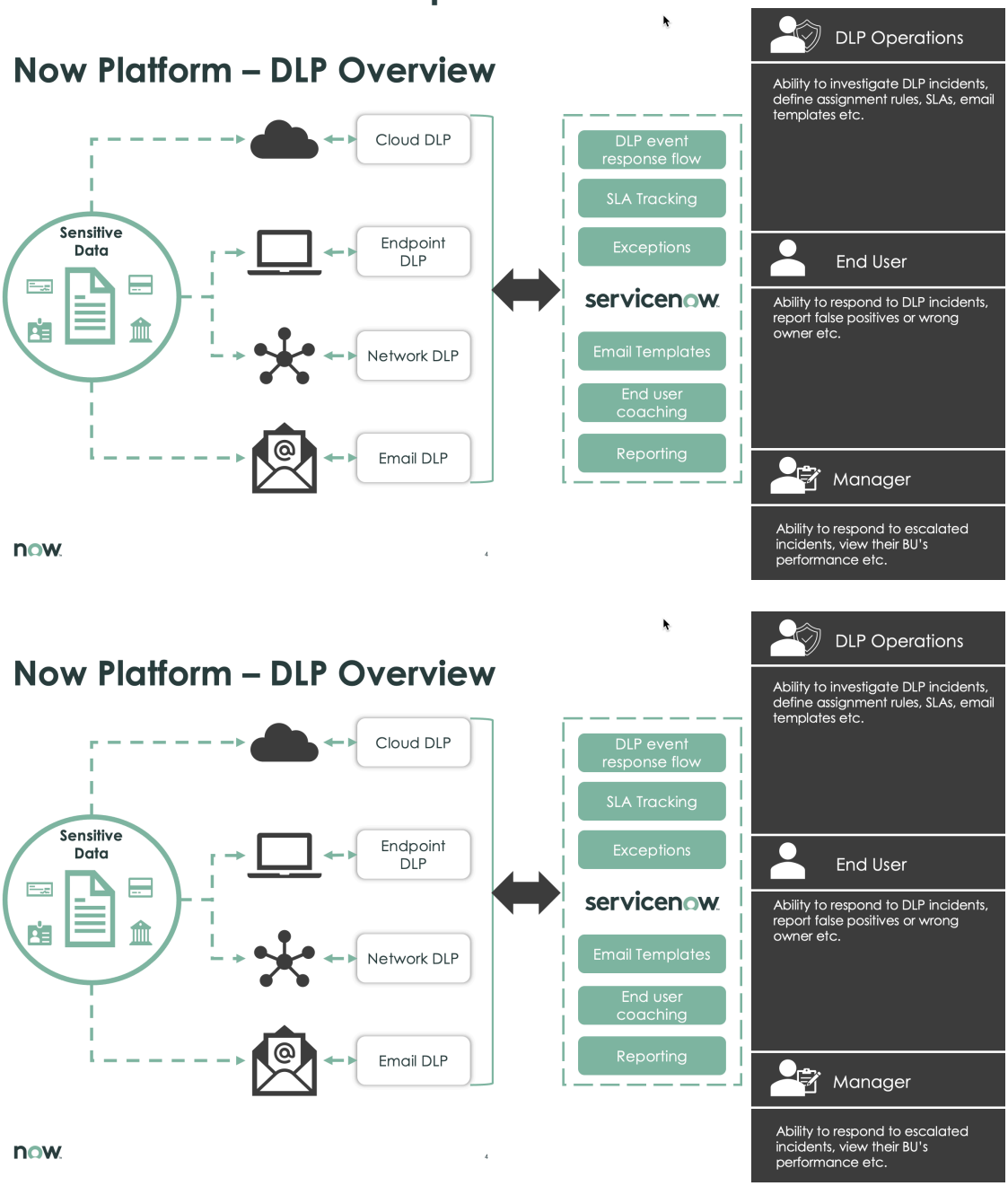
Visão geral da resposta a incidentes do DLP

Saiba como você pode usar o. ServiceNow AI Platform e o. Data Loss Prevention Incident Response(DLP IR). Gerencie informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social. Automatize os fluxos de trabalho de correção com a aplicação Resposta de incidentes do DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Data Loss Prevention Incident Response e o ServiceNow AI Platform



Tradução automática

1. Esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre o DLP
2. Tarefas de administrador do DLP - Esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre o DLP
3. Uso do portal do usuário final do DLP - Esta é uma imagem clicável, para que você possa tentar clicar nas diferentes seções para saber mais sobre o DLP
4. DLP Ops Portal - Esta é uma imagem clicável, para que você possa tentar clicar nas diferentes seções para saber mais sobre o DLP
5. Uso do painel do DLP: Esta é uma imagem clicável, para que você possa tentar clicar nas diferentes seções para saber mais sobre o DLP

. Data Loss Prevention Incident Response a aplicação inclui os seguintes recursos:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um espaço do usuário final em que os usuários finais ou funcionários podem revisar e responder aos incidentes de DLP atribuídos.
- Um espaço do gerente em que um gerente pode revisar os incidentes de DLP escalados e agir sobre eles adequadamente.
- Um espaço unificado em que sua equipe de operações de DLP pode rastrear as tendências nos incidentes em aberto, principais infratores, incidentes por origem de verificação e pode exibir, editar, atribuir e fechar os incidentes de DLP em várias origens (endpoints, redes e e-mail).
- Controles administrativos que definem os modelos de e-mail para coaching e comunicação do usuário final, regras de atribuição para atribuição automática de incidentes, regras de escalação automática e delegação para respostas de incidentes.

Comece a usar a Resposta a incidentes do DLP

Revise as informações a seguir antes de começar a configurar seu Data Loss Prevention Incident Response(DLP IR).

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform E funções do DLP.	A Resposta a incidentes do DLP oferece suporte às seguintes funções: • O administrador (admin) instala as aplicações do ServiceNow Store E atribui o administrador do DLP (sn_dLIR.admin). • sn_dlir.admin • sn_dlir.analyst
Verifique se o ServiceNow aplicações principais que são necessárias para oferecer suporte ao Data Loss Prevention Incident Response as aplicações estão instaladas e ativadas.	. Data Loss Prevention Incident Response o plug-in (com.snc.data_loss_incident) é necessário para oferecer suporte ao Data Loss Prevention Incident Response produto. Verifique o seguinte Operações de segurança as aplicações são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative um aplicativo de cada vez na seguinte ordem para garantir uma instalação tranquila: • Resposta a incidentes de prevenção contra perda de dados (com.snc.data_loss_incident) • Security Support Common Para obter mais informações sobre como configurar seu ServiceNow AI Platform instância da integração, consulte Obtenha direito para um produto ou aplicação de Operações de segurança ou Ativar uma aplicação da ServiceNow Store .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Domain Separation	Verifique Domain Separation e Resposta a incidentes do DLP se você pretende separar dados, processos e tarefas administrativas.

Instalação e configuração do DLP IR Resposta do incidente

Baixe o. Data Loss Prevention Incident Response(DLP IR) do ServiceNow Store e instale-o em sua instância.

Antes de invocar os fluxos de trabalho para a integração, instale e configure o. Data Loss Prevention Incident Response aplicação do ServiceNow Store em seu ServiceNow AI Platform instância.

Instale e configure a aplicação Resposta de incidentes do DLP

Gerencie informações confidenciais e automatize os fluxos de trabalho de correção usando Data Loss Prevention Incident Response(DLP IR) em seu ServiceNow AI Platform instância.

Antes de Iniciar

Antes de concluir as etapas de configuração, você deve baixar o aplicativo do ServiceNow Store e instale-o em sua instância.

Funções necessárias: administrador e sn_dLIR.admin

Procedimento

1. Siga as instruções para Download de uma aplicação da ServiceNow Store .
2. Depois de baixar o. **Resposta a incidentes do DLP** e todas as suas aplicações de dependência, navegue até **Tudo** > **Administração da DLP** > **Configuração padrão** para concluir o restante do configuração da aplicação .

Domain Separation e Resposta a incidentes do DLP

Você pode usar Domain Separation com o DLP Incident Response para separar os dados, os processos e as tarefas administrativas em agrupamentos lógicos chamados domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui todos os aspectos de **Básico** suporte de nível.
- As propriedades da aplicação reconhecem domínio conforme necessário.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona com a Resposta a incidentes do DLP

- Crie um usuário com as funções sn_dLIR.admin e sn_dLIR.analyst necessárias no respectivo domínio.
- Execute as configurações de Resposta a incidentes do DLP no domínio apropriado.

DLP Incident Response Administration

Você pode configurar e atribuir regras, configurar regras de prazo, usar modelos de e-mail, configurar ações de resposta do usuário final e muito mais para gerenciar o. Data Loss Prevention Incident Response(DLP IR) incidentes no ServiceNow AI Platform.

. Data Loss Prevention Incident Response a aplicação permite que você execute as seguintes configurações.

Definições de configuração padrão do DLP

Defina as definições de configuração padrão para Data Loss Prevention Incident Response(DLP IR) Incidentes para identificar e configurar as preferências de notificação de incidente e atribuição de incidente para seus usuários finais.

Antes de Iniciar
Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa
Você pode usar este módulo para definir as definições de configuração padrão quando as regras de atribuição principal e as regras de identificador estiverem esgotadas e não puderem corresponder a uma condição ou usuário. Você também pode definir e reaplicar regras de pesquisa do usuário final e regras de atribuição a incidentes de DLP ativos existentes.

A notificação de incidente do usuário final permite que você especifique a frequência com que as notificações por e-mail são enviadas aos usuários finais. Por exemplo, você pode configurar preferências de notificação para acumular incidentes e enviar um resumo de e-mail uma vez por semana. Ao atribuir um incidente, você pode especificar a qual grupo você atribui inicialmente os incidentes do DLP. Você também pode especificar como os usuários finais são identificados pela equipe de operações do DLP.

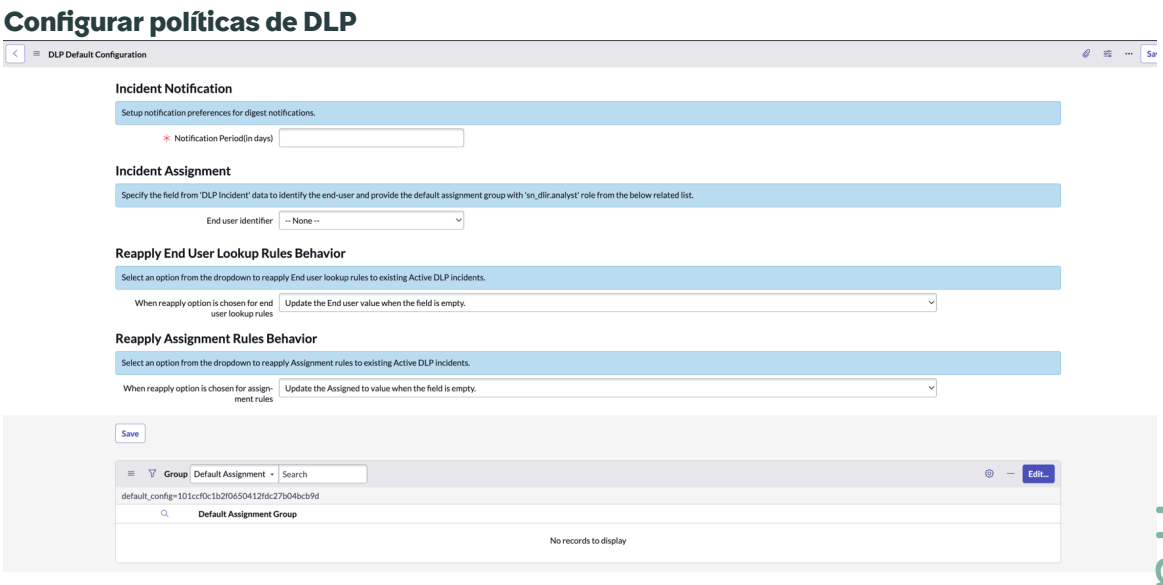
Por exemplo, digamos que um usuário tenha armazenado informações de cartão de crédito em um arquivo em uma rede. Quando o produto de integração DLP de terceiros cria um incidente para uma violação de política de dados confidenciais, os dados do incidente são ServiceNow AI Platform As ingestões do DLP conteriam informações sobre o usuário final. Você poderá atribuir o incidente ao usuário final certo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Configuração padrão**.



2. No formulário, preencha os campos.

Formulário Configuração padrão do DLP

Nome da configuração	Campo	Descrição
Notificação de incidente do usuário final	Período de notificação (dias)	Defina o número de dias após os quais uma notificação por e-mail deve ser enviada ao usuário final. O número de dias deve estar entre 1 e 60 dias.
	Atualiza automaticamente o estado primário com base em incidentes clonados/ secundários	Opção para atualizar automaticamente o incidente de estado primário com base nos incidentes clonados ou secundários.
Atribuição de incidente	Identificador do usuário final	Especifique o campo a ser usado a partir dos dados do incidente para identificar o usuário final. Os valores possíveis são os seguintes: ○ **E-mail do responsável pelos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Responsável pelo arquivo** ○ **Nome de usuário do FTP** ○ **Remetente**
Reaplicar comportamento das regras de pesquisa de usuário final	Quando a opção de reaplicação é escolhida para regras consulta de usuário final.	Opção para reaplicar regras de pesquisa do usuário final a incidentes de DLP ativos existentes. Você pode selecionar uma das seguintes opções para reaplicar:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da configuração	Campo	Descrição
		○ **Atualize o valor do usuário final quando o campo estiver vazio** Atualiza o valor de usuário final dos incidentes de DLP ativos existentes se esse campo estiver vazio. ○ **Atualize o valor do usuário final** Atualiza o valor do usuário final dos incidentes de DLP ativos existentes. ○ **Atualize o usuário final e Atribuído a valores quando ambos os campos estiverem vazios** : Atualiza o usuário final dos incidentes de DLP ativos existentes e os valores Atribuídos a se ambos os campos estiverem vazios. **Nota:** Se esta opção estiver selecionada, então **Atualize o valor Atribuído a quando o campo estiver vazio** A opção é desabilitada automaticamente na seção Comportamento Reaplicar regras de atribuição, pois é aplicável a ambos. ○ **Atualize o usuário final e Atribuído a valores para todos os incidentes de DLP ativos** Atualiza o usuário final e Atribuído a valores para todos os incidentes de DLP ativos. **Nota:** Se esta opção estiver selecionada, então **Atualize o valor Atribuído a para todos os incidentes de DLP ativos** A opção é desabilitada automaticamente na seção Comportamento Reaplicar regras de atribuição, pois é aplicável a ambos.
Reaplicar comportamento das regras de atribuição	Quando a opção de reaplicação é escolhida para regras de atribuição.	Opção para reaplicar regras de atribuição a incidentes de DLP ativos existentes. Você pode selecionar uma das seguintes opções para reaplicar: ○ **Atualize o valor de Atribuição a quando o campo estiver vazio.** ○ **Atualize o valor Atribuído a para todos os incidentes de DLP ativos.**

3. Selecione **Grupo de atribuição padrão** Na seção Lista relacionada à qual todos os incidentes do DLP são atribuídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique em **Editar** para adicionar o grupo de usuários. Ao clicar em **Editar** na seção lista relacionada e selecione um item no **Coleções** E, em seguida, adicione o designado selecionado às colunas Grupo em **Editar membros** e salve a lista.

Nota: Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dLIR.analyst na lista relacionada. Você só pode selecionar um grupo.

4. Clique em **Salvar**.

Criar regras de pesquisa do usuário final

Você pode criar e configurar regras de pesquisa do usuário final e atribuir os incidentes de DLP aos respectivos usuários finais com base nessas regras.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de pesquisa do usuário final para atribuir automaticamente os usuários finais a incidentes do DLP usando somente o campo Usuário final. A regra de pesquisa de usuário final do DLP permite que você atribua o usuário final em incidentes do DLP com base no identificador do usuário final, atributos personalizados ou script.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de pesquisa de usuário final da DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de pesquisa de usuário final do DLP

Campo	Descrição
Nome	Nome da regra de pesquisa do usuário final.
Ativo	Opção para indicar se a regra de pesquisa do usuário final está ativa.
Ordem de execução	A prioridade da regra de pesquisa do usuário final. Este campo indica a ordem na qual as regras de pesquisa do usuário final são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de pesquisa do usuário final com o menor número tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição exclusiva da regra de pesquisa do usuário final.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de pesquisa do usuário final, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . Por exemplo, você pode definir as condições para esta regra de pesquisa do usuário final selecionando a condição como **Origem de integração** , **contém** , **Symantec** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Pesquisar usuário final usando	Opção para pesquisar usuário final usando **Campo de incidente** ou **Script** .
Identificador do usuário final	O identificador do usuário final do incidente do DLP. Este campo aparece quando **Campo de incidente** selecionado em **Pesquisar usuário final usando** campo. Você pode selecionar um identificador de usuário final a partir do seguinte: ○ **E-mail do responsável pelos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Responsável pelo arquivo** ○ **Nome de usuário do FTP** ○ **Remetente**

Tradução automática

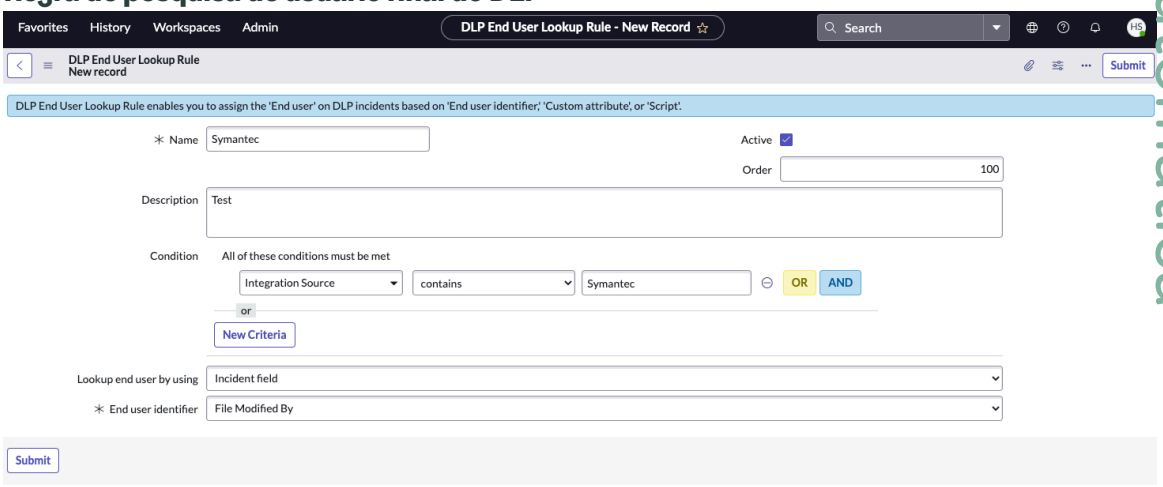
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os identificadores de usuário final listados acima são configuráveis usando a propriedade do sistema `sn_dlir.assignment.fields` . Para obter mais informações, consulte Definir configurações avançadas. ○ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo aparece somente quando **A** selecionado em **Identificador do usuário final** campo.
Script	Você pode usar o editor de scripts para personalizar e formatar os valores de campo durante a criação da regra de pesquisa do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

Example

O exemplo a seguir mostra uma regra de pesquisa do usuário final com o nome "Symantec". O Construtor de condições requer a "Origem de integração" como "Symantec". . **Pesquisar usuário final usando** A opção está definida como "Campo Incidente", e. **Identificador do usuário final** A opção está definida como "Arquivo modificado por".

Regra de pesquisa de usuário final do DLP



4. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de pesquisa do usuário final e reaplicá-las a todos os incidentes de DLP existentes.
5. Para reaplicar uma regra de pesquisa do usuário final em todos os incidentes de DLP existentes, clique em **Reaplicar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de atribuição

Use esta seção para criar regras de atribuição. Em seguida, atribua o. Data Loss Prevention Incident Response Incidentes (DLP IR) para grupos de usuários, usuários finais, gerentes ou usuários do incidente.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar regras de atribuição para atribuir incidentes DLP IR a grupos de usuários, usuários finais ou gerentes. A atribuição dos incidentes do DLP ocorre quando as condições na regra de atribuição são atendidas.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de atribuição**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de atribuição.
Ativo	Opção para indicar se a regra de atribuição está ativa.
Ordem de execução	A prioridade da regra de atribuição. Este campo indica a ordem na qual as regras de atribuição são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de atribuição com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva desta regra de atribuição.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de atribuição, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . Por exemplo, suponha que você crie uma regra de atribuição de DLP para um endpoint. Você pode especificar que a origem da verificação de condição é um sistema de arquivos de endpoint que deve ser atendido antes de atribuir um incidente. **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Atribuir a	Atribuição a um dos seguintes: ○ Grupo de usuários ○ Usuário final ○ Gerente ○ Usuário do incidente A atribuição ocorre quando as condições no construtor de condições são atendidas.
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários para atribuir os incidentes do DLP. Este campo aparece quando **Grupo de usuários** selecionado em **Atribuir a.** campo. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dLIR.analyst.
Usuário final	Opção para atribuir o incidente do DLP ao usuário final. A atribuição ocorre quando as condições no construtor de condições são atendidas.
Atribuir usando campos de gerente	Gerente do usuário final. Este campo aparece quando **Gerente** selecionado em **Atribuir a.** campo. Você pode atribuir os incidentes do DLP a um gerente específico selecionando um dos campos do gerente, como Sobrenome, E-mail, Cidade, Número do funcionário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Identificador de usuário	O identificador do usuário do incidente. Este campo aparece quando **Usuário do incidente** selecionado em **Atribuir a.** campo. Você pode selecionar um identificador de usuário a partir do seguinte: ○ **E-mail do responsável pelos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Responsável pelo arquivo** ○ **Nome de usuário do FTP** ○ **Remetente** ○ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo aparece somente quando **Usuário personalizado do incidente** selecionado em **Identificador do usuário** campo.
Anexar avaliação	Opção para indicar se você deseja anexar uma avaliação ao incidente.
Estado da resposta pré-avaliação	Opção para selecionar em qual estado o incidente deve estar antes que o usuário final responda. Também pode ser um estado personalizado. O valor padrão é Avaliação pendente.
Estado da resposta pós-avaliação	Opção para selecionar em qual estado o incidente do DLP deve estar depois que o usuário responder. O valor padrão é Avaliação concluída.
Avançado	Opção avançada para identificar o usuário final. Este campo aparece somente quando **Usuário personalizado do incidente** selecionado em **Identificador do usuário** campo. Você pode usar o editor de scripts para personalizar e formatar os valores de campo durante a criação da regra de atribuição para identificar o usuário final. Em seguida, você escolhe a quem deseja atribuir o incidente do DLP, que pode ser um usuário final ou o gerente do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

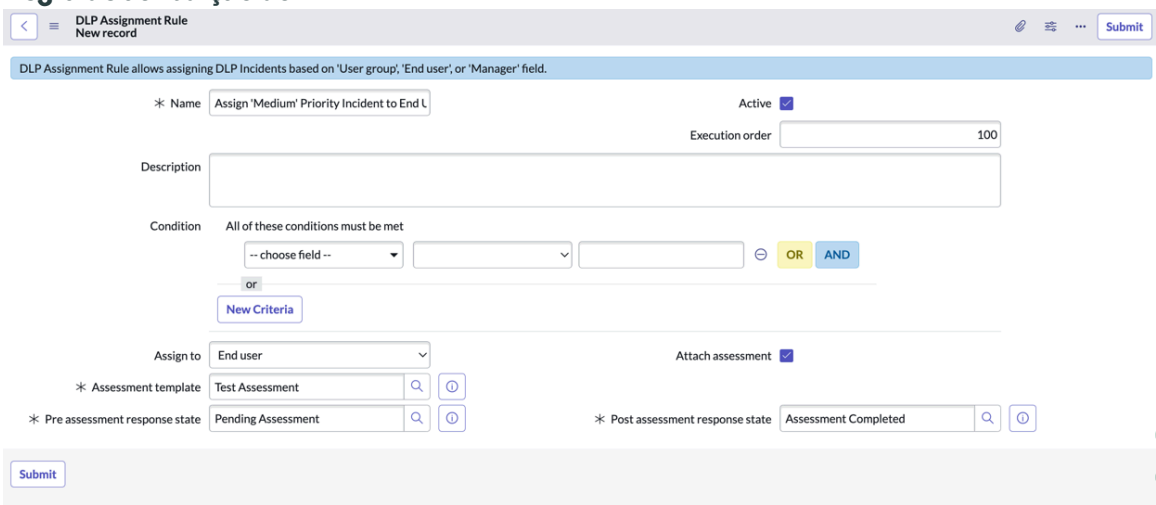
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example

O exemplo a seguir mostra uma regra de atribuição com o nome Atribuir incidente de prioridade "Média" ao usuário final . O Construtor de condições requer que a Origem de verificação seja Atribuir incidente de prioridade "Média" ao usuário final e Atribuir a. o campo está definido como Usuário final . Em seguida, você pode pesquisar o "E-mail" do usuário final.

Regra de atribuição do DLP



4. Selecione **Atribuir a.** Campo da seção da lista relacionada à qual todos os incidentes do DLP são atribuídos. Clique em **Editar** para adicionar o grupo de usuários. Ao clicar em **Editar** na seção lista relacionada e selecione um item no **Coleções** E, em seguida, adicione o designado selecionado às colunas Grupo em **Editar membros** e salve a lista.

   Nota: Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dLIR.analyst na lista relacionada. Você só pode selecionar um grupo.

5. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de atribuição e reaplicá-las a todos os incidentes de DLP existentes.

6. Para reaplicar uma regra de atribuição em todos os incidentes de DLP existentes, clique em **Reaplicar** .

Criar regras de consolidação de incidentes

Crie regra de consolidação de incidentes para consolidar vários incidentes de natureza semelhante em um incidente primário.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de consolidação de incidentes para consolidar automaticamente os incidentes do DLP da mesma natureza em um incidente primário.
A regra de consolidação de incidentes do DLP permite consolidar os incidentes do DLP com base na configuração fornecida para Duração da consolidação e Identificação da consolidação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Quando um incidente consolidado é criado, ele se torna secundário do incidente DLP primário. Se a gravidade do incidente consolidado for maior do que a do primário, a gravidade do incidente primário será atualizada para corresponder ao incidente secundário.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de consolidação de incidentes da DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de consolidação do incidente.
Ativo	Opção para indicar se a regra de consolidação do incidente está ativa.
Ordem de execução	A prioridade da regra de consolidação do incidente. Este campo indica a ordem na qual as regras de consolidação de incidentes são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de consolidação de incidentes com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de consolidação do incidente.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de consolidação de incidente, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para definir uma segunda condição de filtro, clique em **Novos critérios** . Por exemplo, você pode definir as condições para esta regra de consolidação de incidente selecionando a condição como **Origem de integração** , **contém** , **Symantec** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Duração da consolidação	Opção para definir a duração da consolidação do incidente. Os incidentes neste período com os mesmos valores para os campos selecionados serão consolidados no primeiro incidente. O primeiro incidente correspondente a esta regra será o incidente primário e o restante dos incidentes serão incidentes secundários.
Consolidar incidentes por	Selecione o campo Incidente do DLP para consolidar os incidentes quando tiver o mesmo valor no campo selecionado para incidentes diferentes. Selecione pelo menos um campo. Selecione pelo menos um campo.

O exemplo a seguir mostra uma regra de consolidação de incidentes com o nome Consolidar incidentes para integração da Symantec. O Construtor de condições requer a Origem de integração como Symantec. . **Duração da condição** A opção está definida como 1 hora e a opção Nome da política está selecionada para **Consolidar incidente por** .

No momento da ingestão de incidentes do Symantec DLP, esta regra será executada e, quando vários incidentes tiverem o mesmo nome de política, o incidente será consolidado no primeiro incidente ingerido correspondente a esta regra.

4. Clique em **Enviar**.
   Os incidentes consolidados com base na regra de consolidação estarão disponíveis na lista Incidentes secundários no Espaço do analista do DLP.

Criar regras de prazo de resposta

Configure as regras de prazo da resposta para determinar o tempo que você deseja dar aos usuários finais para responder ao atribuído Data Loss Prevention Incident Response(DLP IR) incidentes.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este módulo para definir as regras de prazo de resposta para os diferentes tipos de incidentes de DLP e as regras para começar a contar a data de vencimento. Após a expiração da data de vencimento, os usuários serão notificados sobre o incidente atrasado. Você também tem uma opção para escalar o incidente atrasado para um dos seguintes:

- Gerente
- Usuário personalizado do incidente
- Grupo de usuários

Por exemplo, quando você escala o incidente atrasado para um gerente e especificou um máximo de três níveis de escalação. O primeiro nível do gerente é notificado primeiro. Se o incidente estiver atrasado novamente, o segundo nível de gerente será notificado, seguido pelo terceiro nível se o incidente ainda estiver atrasado. Se o gerente tiver um delegado, o gerente terá a opção de atribuir a escalação ou o incidente atrasado ao delegado.

Você também pode criar várias regras de prazo de resposta.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de vencimento da resposta**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de prazo da resposta

Campo	Descrição
Nome	Nome da regra de prazo da resposta.
Ativo	Opção para indicar se a regra de prazo da resposta está ativa.
Vencimento em (dias)	Número de dias de vencimento.
Data de vencimento contada a partir de	Data de início que é usada para calcular a data de vencimento. A data de vencimento pode ser calculada a partir da primeira vez em que o usuário foi notificado sobre o incidente ou a partir da data de atribuição do incidente.
Notificar antes da data de vencimento	Opção para notificar o usuário final sobre o incidente do DLP antes da data de vencimento.
Notificar em (dias antes da data de vencimento)	Número de dias antes da data de vencimento em que a regra aciona uma notificação para o usuário final.
Descrição	Descrição exclusiva desta regra de data de vencimento da resposta.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de prazo da resposta, selecione qualquer um dos campos de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Escalar	Opção para escalar o incidente do DLP para alguém se a data de vencimento da resposta tiver sido violada. Para obter mais informações, consulte Adicione vários usuários para acessar incidentes do DLP.
Escalar incidente atrasado para	Opção para especificar se o incidente deve ser escalado para um gerente, um usuário personalizado ou um grupo de usuários. Este campo aparece somente quando **Escalar** a opção está habilitada.
Atribuir usando	Especifique como um gerente deve ser identificado. Este campo aparece somente quando **Gerente** selecionado em **Escale o incidente atrasado para** campo.
Níveis máximos de escalação	Opção para definir o número máximo de níveis de escalação para um gerente e um usuário personalizado. Como gerente ou usuário personalizado, você pode definir qualquer número de níveis de escalação. Três níveis de escalação são fornecidos por padrão. ○ Como gerente, você pode definir qualquer número de níveis de escalação atualizando o valor neste campo. ○ Como um usuário personalizado, você pode usar o ícone de adição para definir qualquer número de níveis de escalação.

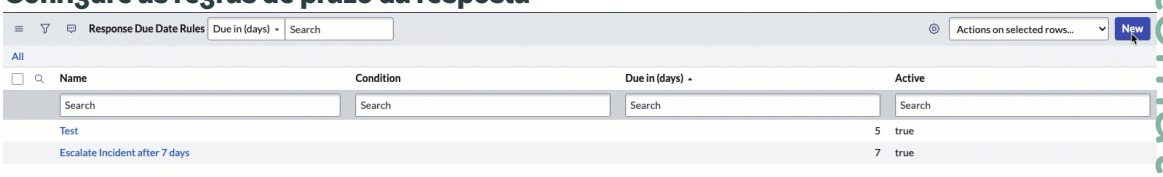
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo aparece somente quando **Usuário personalizado do incidente** selecionado em **Escale o incidente atrasado para** campo.
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários para o qual escalar incidentes de DLP. Este campo aparece somente quando **Grupo de usuários** selecionado em **Escale o incidente atrasado para** campo. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dLIR.analyst.

Example
O exemplo a seguir mostra a regra de prazo da resposta para determinar quanto tempo você deseja conceder aos usuários finais para responder ao atribuído Data Loss Prevention Incident Response Incidentes (DLP). Depois que o usuário final é notificado pela primeira vez, o prazo da resposta é de dois dias. O construtor de condições mostra que a origem da verificação deve corresponder ao sistema de arquivos de endpoint para prosseguir com a criação da data de vencimento da resposta. A opção de escalação está selecionada. O incidente será escalado para o gerente se a data de vencimento da resposta for violada.

Configure as regras de prazo da resposta



4. Clique em **Enviar**.

Adicione vários usuários para acessar incidentes do DLP

Use o recurso de cadeia de escalação para permitir que todos os respectivos usuários envolvidos no incidente acessem os incidentes do DLP na exibição de lista, embora o incidente seja atribuído a um usuário diferente.

Antes de Iniciar
Função necessária:

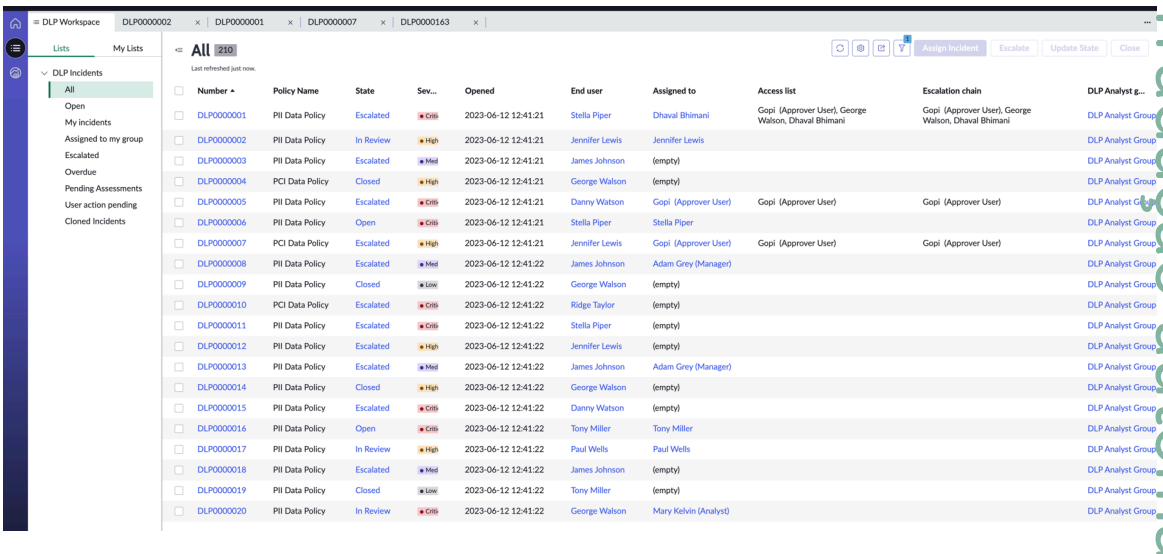
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.read, sn_dLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Procedimento

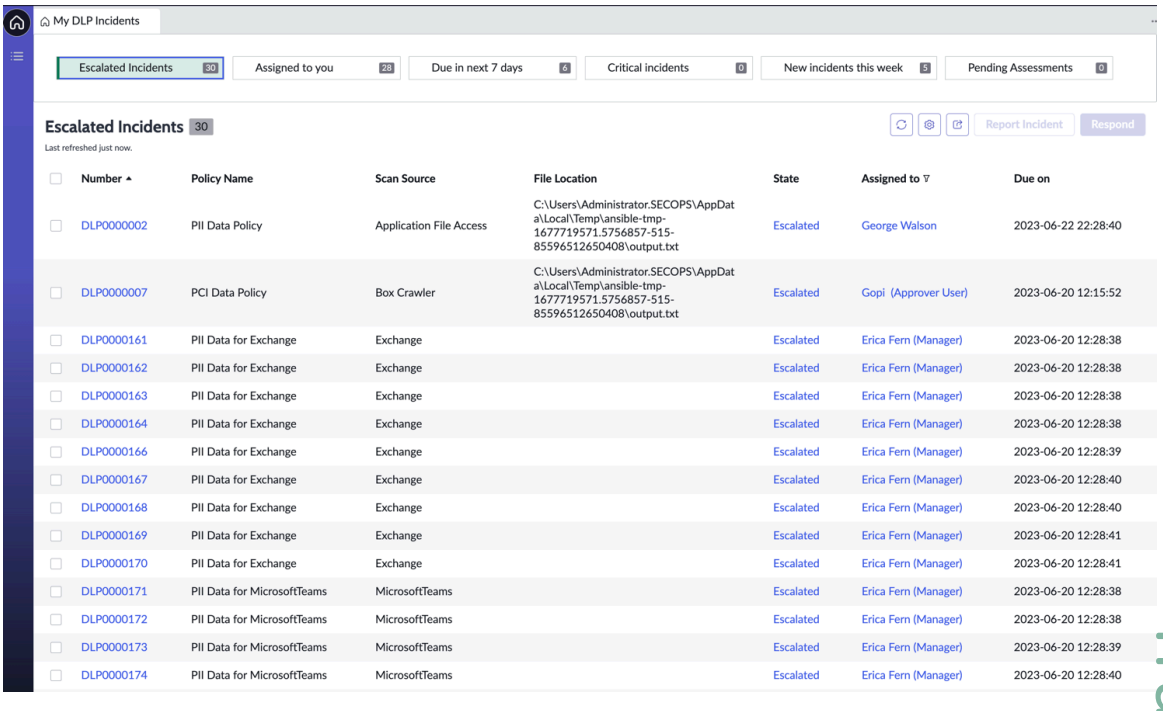
1. Navegar até **DLP** > **DLP Analyst Workspace**.
   Na exibição de lista, os usuários e seus delegados devem ser capazes de exibir o incidente do DLP em **Escalado** guia incidentes no portal do usuário final.
2. Abra qualquer incidente.
3. Clique em **Escalar** botão para escalar um incidente.
4. Selecione o usuário ou o grupo de usuários na lista suspensa.
   Você pode adicionar vários usuários à cadeia de escalação. Todos os usuários que têm acesso são listados na seção Detalhes da exibição do formulário e também em **Todos** guia incidentes. A cadeia de escalação é exibida com base nas definições de configuração. Para obter mais informações, consulte Definir configurações avançadas.



5. Clique em **Enviar**.
   Depois de enviar, o incidente será atribuído a um gerente, no entanto, o usuário final ainda poderá exibir o incidente.
6. Para verificar isso, navegue até **Espaço do usuário do DLP** como um usuário final.
   Todos os incidentes atribuídos ao usuário final são exibidos.
7. Exiba a lista de incidentes escalados em **Incidentes escalados** seção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Number	Policy Name	Scan Source	File Location	State	Assigned to	Due on
DLP0000002	PII Data Policy	Application File Access	C:\Users\Administrator.SECOPS\AppData\Local\Temp\ansible-tmp-1677719571.5756857-515-85596512650408\output.txt	Escalated	George Walson	2023-06-22 22:28:40
DLP0000007	PCI Data Policy	Box Crawler	C:\Users\Administrator.SECOPS\AppData\Local\Temp\ansible-tmp-1677719571.5756857-515-85596512650408\output.txt	Escalated	Gopi (Approver User)	2023-06-20 12:15:52
DLP0000161	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000162	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000163	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000164	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000166	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:39
DLP0000167	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40
DLP0000168	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40
DLP0000169	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:41
DLP0000170	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:41
DLP0000171	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000172	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000173	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:39
DLP0000174	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40

Você também pode exibir a lista de acesso de usuários em **Cadeia de escalação** na exibição de lista.

8. Abra qualquer incidente.
9. Clique em **Responder** botão para enviar a resposta do incidente.
10. Selecione a resposta na lista suspensa.
11. Clique em **Enviar**.

Criar regras de aprovação

Crie regras de aprovação para obter aprovação de vários níveis de usuários aprovadores sempre que uma opção de tipo avançado de resposta for selecionada.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de aprovação para conceder consentimento em solicitações geradas por usuários finais para a aprovação do tipo avançado de opção de resposta. O administrador do DLP também pode definir vários níveis de aprovação a partir daqui.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de aprovação do DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de aprovação.
Ativo	Opção para indicar se a regra de aprovação está ativa.
Ordem de execução	A prioridade da regra de aprovação. Este campo indica a ordem na qual as regras de aprovação são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de aprovação com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de aprovação.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de aprovação, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . Por exemplo, você pode definir as condições para esta regra de consolidação de incidente selecionando a condição como **Origem de integração** , **contém** , **Microsoft** .
Aplicável para opções de resposta	Opção para selecionar a opção de resposta do tipo avançado. Você pode selecionar as várias opções de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aprovador	Selecione o tipo de usuário aprovador que você deseja definir. ○ **Tabela do usuário** : Selecione esta opção se quiser selecionar o usuário aprovador na tabela Usuários (sys_user). ○ **Lista de aprovações personalizada** : Selecione esta opção se quiser configurar vários níveis de aprovador personalizado para uma única solicitação
Identificador do aprovador	Este campo aparecerá quando **Tabela do usuário** selecionado para **Aprovador** opção. Selecione o campo para identificar o aprovador na tabela Usuários (sys_user).
Número de níveis	Este campo aparecerá quando **Tabela do usuário** selecionado para **Aprovador** opção. Número final neste campo para definir os níveis de aprovação. Por exemplo, se 3 for adicionado ao campo Número de níveis e Gerente for selecionado no campo Identificador do aprovador, a solicitação de aprovação passará para três níveis de aprovação.

O exemplo a seguir mostra a regra de aprovação criada para uma das opções de resposta antecipada. A condição requer que o nome de origem da integração contenha a palavra-chave Microsoft que aciona esta configuração.

4. Para **Aprovador** opção, selecione **Lista de aprovações personalizada** .
5. Clique em **Enviar**.
6. **Níveis de aprovação** a lista relacionada será preenchida na exibição do formulário.
7. Em **Níveis de aprovação** clique em **Novo** .
8. No formulário, preencha os campos.

Formulário de nível de aprovação

Campo	Descrição
Nome	Nome do nível de aprovação.
Ativo	Opção para indicar se o nível de aprovação está ativo.
nível	O nível da regra de aprovação. Este campo indica a ordem na qual os níveis de aprovação são executados quando dois ou mais níveis são configurados. O nível de aprovação com o número mais baixo tem a prioridade mais alta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para definir o nível de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Regra de aprovação	Regra de aprovação para a qual você deseja definir esta configuração. Este será um campo somente leitura.
Descrição	Descrição exclusiva da regra de aprovação.
Aprovações obrigatórias	Selecione a opção para definir se a aprovação de todos os usuários/grupos configurados é necessária ou somente necessária de qualquer usuário.
Aprovadores	Opção para selecionar os aprovadores. **a.** Usuários e grupos: **i. Usuários** : Clique em ícone para adicionar um usuário específico da lista. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa dele. Para adicionar a si mesmo como o usuário a quem as condições do DLP são aplicáveis, clique em . **ii. Grupos** : Clique no ícone do <add_icon> para adicionar um grupo específico da lista. Você também pode adicionar um grupo usando a opção de pesquisa. **b. Localizar usando script** : Você pode usar o editor de scripts para personalizar e formatar os valores de campo durante a criação do nível de aprovação. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário aprovador.

9. Clique em **Enviar**.

Criar modelos de instruções do usuário

Crie e gerencie o modelo de instruções do usuário para incidentes de DLP para ajudar os usuários a entender as instruções envolvidas na resolução de incidentes e as próximas etapas envolvidas no processo de resolução.

Antes de Iniciar

O modelo de cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário.

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Quando um incidente é atribuído ao usuário final, o usuário pode ser solicitado a saber as instruções adicionais sobre como responder aos incidentes, apresentar aos usuários a terminologia e fornecer informações adicionais sobre o incidente. Esses modelos podem orientar os usuários a fornecer a resposta precisa aos incidentes do DLP.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Modelos de instruções do usuário**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

DLP Incident Assessment

Campo	Descrição
Nome	Nome do modelo de instrução do usuário.
Descrição Resumida	Descrição exclusiva deste modelo de instrução do usuário.
Ativo	Opção para indicar se o modelo de instrução do usuário está ativo.
Ordem de Execução	Prioridade do modelo de instrução do usuário do incidente. Este campo indica a ordem na qual a ordem é executada para avaliar o modelo de instrução do usuário quando um incidente é criado. A opção com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Condição de correspondência de incidentes	Os incidentes que correspondem às condições definidas no construtor de condições serão exibidos. Essas condições são baseadas nos dados do incidente do DLP. Para criar uma condição para uma instrução do usuário, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em E ou OU: Se E for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer condição poderá ser correspondida. Para definir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	uma segunda condição de filtro, clique em **Novos critérios** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Aplica-se a	Selecione o usuário ou os grupos de usuários aos quais o modelo é aplicável. As outras opções disponíveis são: ○ **Todos os usuários finais** : Marque esta caixa de seleção se o modelo de instruções se aplicar a todos os usuários. ○ **Todos os revisores de incidentes escalados** : Marque esta caixa de seleção se o modelo se aplicar a todos os revisores dos incidentes escalados. ○ **Usuários específicos** : Clique no ícone para adicionar um usuário específico da lista a quem as condições de incidente DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa dele. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário a quem as condições do DLP são aplicáveis, clique em **Adicionar-me** ícone. ○ **Grupos de usuários específicos** : Clique no ícone para adicionar um grupo específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.
Modelo de instruções: Instruções	Adicione instruções no editor de rich text com variáveis disponíveis em um nível de incidente.

4. Detalhar até **Modelo de instruções** insira a instrução do modelo e adicione informações de nível de incidente nesta seção, se necessário.
5. Arraste e solte as variáveis necessárias para exibir dinamicamente determinados campos.
6. Clique em **Enviar**.
   Os modelos de instruções do usuário agora foram criados e você pode clicar em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais de um incidente de DLP.

Para obter mais informações, consulte Data Loss Prevention Incident Response Espaço do usuário.

Configurar instruções do usuário da IU do DLP

Configure as mensagens de IU do sistema para adicionar cabeçalhos detalhados de instruções do usuário conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **IU do Sistema** > **Mensagens**.
2. Pesquisar **user_instruction_card_heading** .

   Por padrão, user_instruction_card_heading e. user_instruction_modal_window_heading As duas configurações de mensagem de IU são provisionadas para os usuários.
3. Clique em qualquer uma das instruções do usuário para atualizar ou modificar.

Criar modelos de e-mail

Crie e gerencie os modelos de e-mail pré-configurados para enviar notificações para seus usuários finais, grupos de usuários ou gerentes. Com esses modelos, você pode treinar e se comunicar com os usuários finais sobre o. Data Loss Prevention Incident Response(DLP IR) incidentes.

Antes de Iniciar
Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

> **Importante:** Para que os analistas exibam comunicações por e-mail de um incidente do DLP no fluxo de atividades, adicione ou anexe a função "n_dLIR.analyst" na propriedade do sistema global glide.ui.activity.email_roles .

Por Que e Quando Desempenhar Esta Tarefa
As notificações por e-mail são categorizadas pelas notificações de incidente que são enviadas aos usuários finais, pelas notificações de escalação que são enviadas aos gerentes ou pelas notificações de data de vencimento. Você pode enviar notificações por e-mail sobre as datas de vencimento dos incidentes de DLP ou até mesmo orientar os usuários finais sobre o que fazer quando determinadas condições são atendidas no filtro de condições de e-mail.
Os modelos de e-mail do DLP permitem que você envie a notificação por e-mail para usuários finais, gerentes e analistas. Você pode configurar os modelos a serem enviados por incidente ou como um resumo. O assunto e o corpo do e-mail podem conter variáveis para que você possa reutilizar o conteúdo existente.

O DLP fornece os seguintes modelos de e-mail pré-configurados com base nas categorias:

- **Modelo de e-mail do DLP - Notificação de aprovação por incidente:** Notifique os usuários sobre a aprovação de suas solicitações.
- **Modelo de e-mail do DLP - Notificação de escalação:** Envie notificações de escalação para gerentes na forma de resumos.
- **Modelo de e-mail do DLP - Notificação de aprovação pendente:** Notificar aprovadores sobre itens pendentes.
- **Modelo de e-mail do DLP - Notificação de cancelamento de solicitação de aprovação por incidente:** Notifique os usuários sobre uma solicitação de aprovação que foi cancelada pela equipe de analista do DLP.
- **Modelo de e-mail do DLP - Notificação de conclusão da resposta do usuário:** Notifique a equipe de analista do DLP sobre a resposta enviada pelos usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Modelo de e-mail do DLP - Notificação de incidente do usuário:** Este é um modelo padrão para notificação de resumo do usuário. Envie notificações de incidentes para os usuários finais na forma de resumos a cada poucos dias, mesmo se não houver novos incidentes, para informar os usuários sobre o número total de incidentes no nome do usuário específico. Você também pode enviar notificações resumidas para notificar os usuários sobre as próximas datas de vencimento de incidentes de DLP com gravidade crítica, alta, média ou baixa.
- **Modelo de e-mail do DLP - Notificação de aprovação pendente por incidente** Notificar aprovadores sobre aprovações pendentes.
- **Modelo de e-mail do DLP - Notificação de rejeição:** Enviar notificação de rejeição ao solicitante.
- **Modelo de e-mail do DLP - Notificação de data de vencimento:** Enviar notificação de data de vencimento do incidente. Se um incidente do DLP for atribuído ao usuário final e o usuário final não tiver realizado nenhuma ação antes da data de vencimento, uma notificação por e-mail será enviada ao usuário final. Você também tem a opção de escalar o incidente do DLP para um gerente, um usuário personalizado ou um grupo de usuários se a data de vencimento da resposta tiver sido violada.

  Nota: As notificações de data de vencimento devem estar na forma de resumos.

- **Modelo de e-mail do DLP - Notificação de resposta do usuário por incidente:** Notifique os analistas sobre a resposta enviada aos usuários por incidente.
- **Modelo de e-mail do DLP - Notificação de escalação por incidente:** Notificar gerentes sobre escalações por incidente.
- **Modelo de e-mail do DLP - Notificação do usuário por incidente:** Notificar usuários sobre atribuição por incidente.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Modelos de E-mail**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Modelo de e-mail do DLP

Campo	Descrição
Nome	Nome do modelo de e-mail.
Ativo	Opção para indicar se o modelo de e-mail do DLP está ativo. Se esta opção não estiver habilitada, as notificações não serão enviadas para este modelo de e-mail.
Categoria	Categoria de notificação por e-mail. O DLP oferece suporte às seguintes opções: ○ **Notificação de incidente para usuários finais** : Enviado quando os incidentes são atribuídos aos usuários finais. ○ **Notificação de escalação para gerentes** Enviado quando a data de vencimento da resposta é violada ou atribuída manualmente ao gerente por meio do portal DLP Ops.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Notificação de data de vencimento** Enviado quando a data de vencimento da resposta é violada. ○ **Notificação de resposta do usuário para analistas** Enviado quando o usuário final executa qualquer ação no incidente do DLP. ○ **Notificação de aprovações pendentes** Notificar aprovadores sobre itens pendentes. ○ **Notificação de aprovação para o solicitante** Notifique os usuários sobre a aprovação de suas solicitações. ○ **Rejeitar notificação para o solicitante** Notifique os usuários sobre a rejeição de suas solicitações. ○ **Notificação de cancelamento para o solicitante** Notifique os usuários sobre o cancelamento de suas solicitações.
Tipo	Opção para indicar se o e-mail é enviado por incidente ou como um resumo. **Nota:** Se você selecionou **Notificação de data de vencimento** em **Categoria** , em seguida, você pode usar apenas resumos. Selecione esta opção.
Descrição	Descrição exclusiva deste modelo de e-mail.
Ordem de Execução	Prioridade do modelo de e-mail. Este campo indica a ordem na qual os modelos de e-mail são executados quando dois ou mais modelos de e-mail compartilham as condições de acionamento. O modelo de e-mail com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Condição do modelo	Opções nas condições do modelo que são baseadas na tabela de incidentes do DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho do modelo de e-mail. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU** . ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Usuários de Destino	Usuários de destino para o modelo quando as condições forem atendidas. Os usuários de destino podem ser um dos seguintes: ○ **Todos os destinatários** : Envie o e-mail para os usuários de destino. ○ **Destinatários no grupo:** Envie o e-mail somente para destinatários em um grupo específico usando a opção de filtro. ○ **Destinatários que correspondem aos critérios** : Envie o e-mail para usuários de destino que correspondam aos critérios. Você pode usar o filtro para detalhar os usuários de destino com base nas condições. Por exemplo, cidade.

Modelo de e-mail	Modelo de e-mail que você pode selecionar. Você pode definir as variáveis para reutilizar o conteúdo existente para adicionar à notificação por e-mail.
	. **Categoria** e. **Tipo** os campos determinam as variáveis que estão disponíveis para seleção. Por exemplo, digamos que a categoria de e-mail esteja definida como notificação de incidente e que o tipo de e-mail seja um resumo, as variáveis para seleção sejam campos de resumo para acomodar o acúmulo de vários incidentes de DLP.
	Exemplo de HTML do corpo do e-mail de cada modelo de e-mail:
	○ **Modelo padrão para notificação de aprovação por incidente** :
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	`- Date protection team`
	○ **Notificação de cancelamento de solicitação de aprovação por incidente**
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	`No action is required from you at this point. Data protection team will contact you for any further information required.`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	- Data protection team ○ **Modelo padrão para notificação de data de vencimento** : Dear ${target_user.name}, Following incidents require your response. ${due_days_table} - Data protection team ○ **Modelo padrão para notificação do usuário por incidente** : Dear ${assigned_to.name}, DLP Incident ${number} is assigned to you. Please review and submit your response. - Data protection team ○ **Modelo padrão para notificação de incidente do usuário** : Hello ${target_user.name}, You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ○ **Modelo padrão para escalação - Resumo** : Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table}

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	- Data protection team ○ **Modelo padrão para escalação - Por incidente** : Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team ○ **Modelo padrão para notificação de Aprovação pendente** : Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team ○ **Modelo padrão para notificação de aprovação pendente por incidente** : Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ○ **Modelo padrão para notificação de rejeição por incidente** : Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team

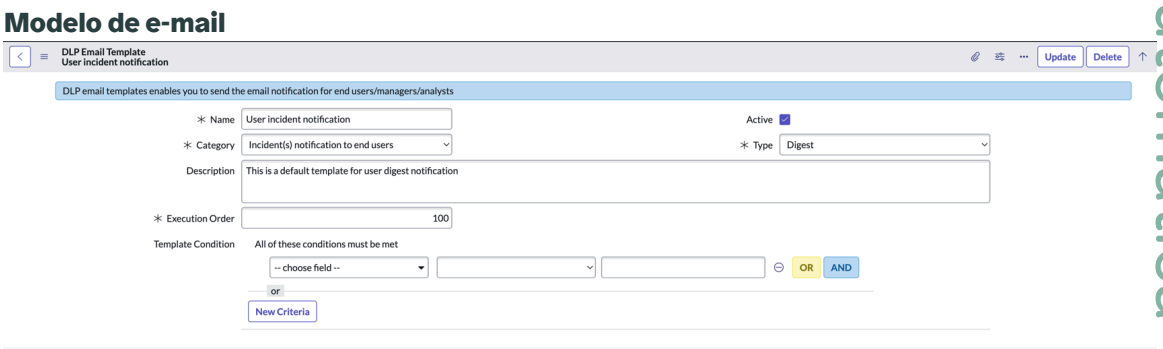
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Modelo padrão para notificação de resposta do usuário por incidente** : Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ **Modelo padrão para notificação de conclusão de resposta do usuário** : Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

Example

O exemplo a seguir mostra o modelo de e-mail do DLP com os usuários de destino definidos como todos os destinatários.

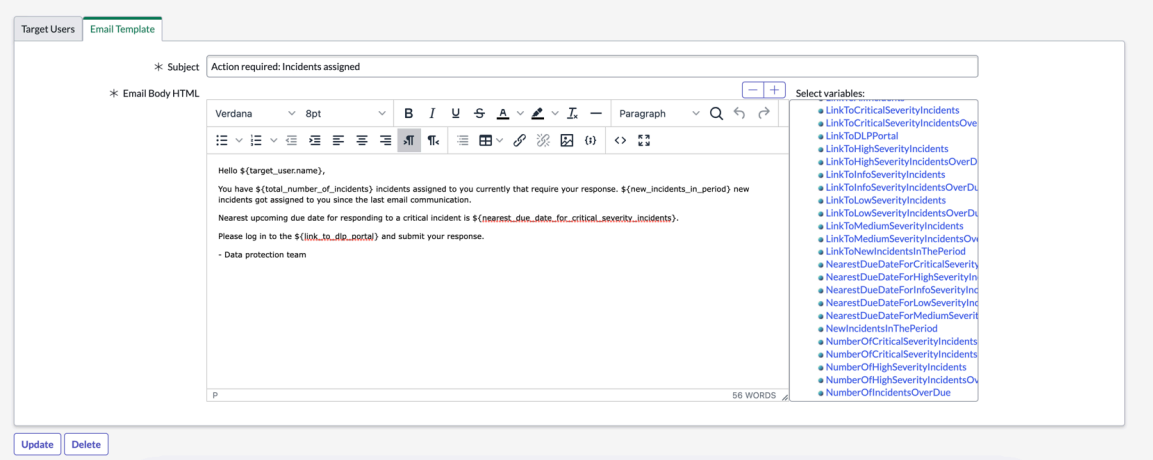


O exemplo a seguir mostra um modelo de e-mail com o assunto "Notificação de incidente do usuário" e uma variável *new_incidents_in_period* . O corpo do e-mail contém várias variáveis que são adicionadas da coluna Selecionar variáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de modelo de e-mail



4. Clique em **Enviar**.

Resultado

O usuário final recebe um e-mail de notificação resumida com todos os campos de variáveis selecionados no modelo.

Crie um Data Loss Prevention Incident Response Gatilho de ANS

Crie um Data Loss Prevention Incident Response Condição do gatilho de ANS que permite uma resposta rápida e eficiente a um incidente quando acionado.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, atualizar e excluir gatilhos de ANS do DLP
- sn_dLIR.analyst.read - Ler tabela do gatilho.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Gatilhos de ANS**.
2. Selecione **Novo** Para criar o gatilho de ANS.

Campo	Descrição
Nome	Nome do gatilho
Ordem	Ordem na qual o gatilho é considerado.
Ativo	Opção para avaliar o gatilho de ANS.
Acionar quando um incidente do DLP for atualizado	Opção para avaliar a condição do gatilho em cada atualização do incidente do DLP.

3. Configure uma condição selecionando o registro de regra e definindo condições no **Condição do gatilho** campo.
   Por exemplo, a condição do gatilho para definir ANS em incidentes de DLP de uma origem de verificação de e-mail seria **[Origem da verificação][IS][E-mail SMTP]** .
4. Selecione **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

Um ANS de tarefa é registrado para um Data Loss Prevention Incident Response O incidente é criado, a guia Registros de ANS se torna visível para esse incidente específico no espaço. Esta guia permite que você use um sistema de ANS para a tarefa da sua organização.

Crie um Data Loss Prevention Incident Response Definição de ANS

Crie um Data Loss Prevention Incident Response Definição de ANS que descreve as condições e a duração para responder a violações de dados. Estabelecer expectativas e protocolos claros ajuda a garantir uma resposta rápida a incidentes, minimizando possíveis danos e aprimorando as estratégias gerais de proteção de dados.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, atualizar e excluir definições de ANS do DLP.
- sn_dLIR.analyst.read - Leia as definições de ANS do DLP.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Definições do ANS**.
2. Crie uma definição do ANS.
   Para obter uma descrição dos valores dos campos, consulte Formulário Definição de ANS do DLP.
3. Selecione **Enviar**.

> **Nota:** Regras de prazo, escalações e definições de ANS são mutuamente exclusivas. Uma definição de ANS determina principalmente quando um ANS específico começará a entrar em vigor, parar, pausar ou ser acionado.

Criar avaliações

Crie e gerencie avaliações para permitir que os usuários finais respondam a incidentes de DLP. Você pode usar as avaliações para coletar informações sobre os dados confidenciais expostos ou vazados dos incidentes do DLP.

Criar e gerenciar avaliações para incidentes de DLP

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As avaliações de incidentes do DLP ajudam a identificar possíveis ameaças e vulnerabilidades aos seus dados com base na resposta do usuário final. Você pode usar essas informações para determinar as lacunas, preocupações e expectativas existentes dos usuários finais.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Avaliações**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

DLP Incident Assessment

Campo	Descrição
Nome	Nome da avaliação de incidente do DLP.
Ativo	Opção para indicar se a avaliação de incidente do DLP está ativa.
Descrição	Descrição exclusiva desta avaliação de incidente do DLP.
Introdução da avaliação	Forneça uma introdução ou contexto para sua avaliação. Você também pode usar variáveis da seção Selecionar variáveis para exibir dinamicamente determinados campos.

4. Clique em **Enviar**.
5. Depois de criar uma avaliação, abra a avaliação e clique em **Designer de avaliação** .
6. Na seção Nova avaliação, selecione um tipo de pergunta de avaliação na seção Controles.
7. Arraste e solte o tipo de pergunta de avaliação necessário na seção Nova avaliação.
   Por exemplo, você pode arrastar e soltar **Opção** Controle na seção Nova avaliação ou Nova categoria.
8. Para adicionar mais categorias à avaliação, clique em  ícone.
9. Para modificar uma categoria existente, clique em  ícone.
10. Depois de criar as diferentes perguntas de avaliação pela primeira vez, clique em **Salvar** e, em seguida **Publicar** .

Criar regras de opção de resposta a incidentes

Crie as regras de opção de resposta do incidente que o usuário final ou analista pode usar ao responder a um incidente.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode configurar o tipo de resposta que um usuário final deve executar com base no tipo de incidente DLP. A aplicação Resposta de incidentes DLP do sistema de base fornece as seguintes opções de resposta para os usuários:

- Avaliação concluída
- Conteúdo excluído
- Arquivo excluído
- Arquivo criptografado
- Conteúdo mascarado
- Relatar falso positivo
- Relatar responsável incorreto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Necessário para o processo de negócios
- Direitos revisados

Por exemplo, digamos que um usuário final relate um incidente de DLP como falso positivo. O estado desse incidente é marcado automaticamente como Encerrado porque o estado de destino configurado por você é Encerrado.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Regras de opção de resposta do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regras de opção de resposta do incidente

Campo	Descrição
Nome	Nome da opção de resposta do incidente.
Ativo	Opção para indicar se a opção de resposta do incidente está ativa.
Ordem de execução	Prioridade da opção de resposta do incidente. Este campo indica a ordem na qual as opções de resposta do incidente são executadas quando duas ou mais opções de resposta a incidentes compartilham as condições de acionamento. A opção de resposta do incidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Descrição	Descrição exclusiva desta opção de resposta a incidentes.
Estado de destino padrão	O estado de destino padrão que você configurou.
Condição	Condições no Construtor de condições. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para as opções de resposta do incidente, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU**:

Tradução automática

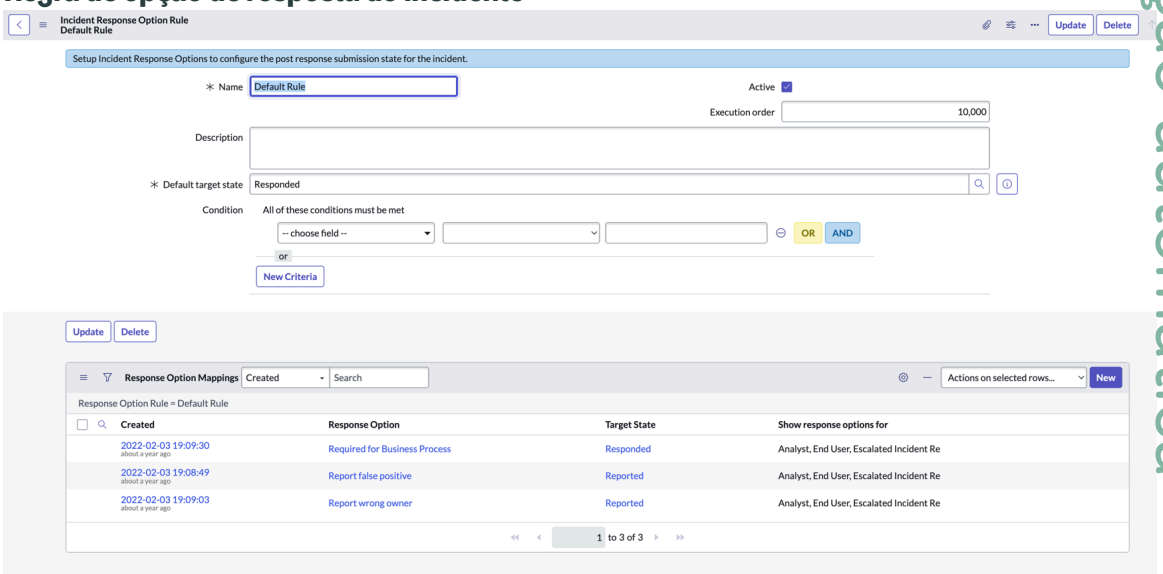
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.

Example

O exemplo a seguir mostra a configuração da ação do usuário final para um endpoint. A condição requer que a origem da verificação seja um sistema de arquivos de endpoint que aciona esta configuração de ação do usuário final. O mapeamento mostra que o responsável incorreto do relatório, o falso positivo do relatório e o arquivo excluído são as opções de resposta disponíveis para usuário final .

Regra de opção de resposta do incidente



4. Em **Mapeamentos de opção de resposta** clique em **Novo** .
5. No formulário, preencha os campos.

Formulário Mapeamento de opção de resposta

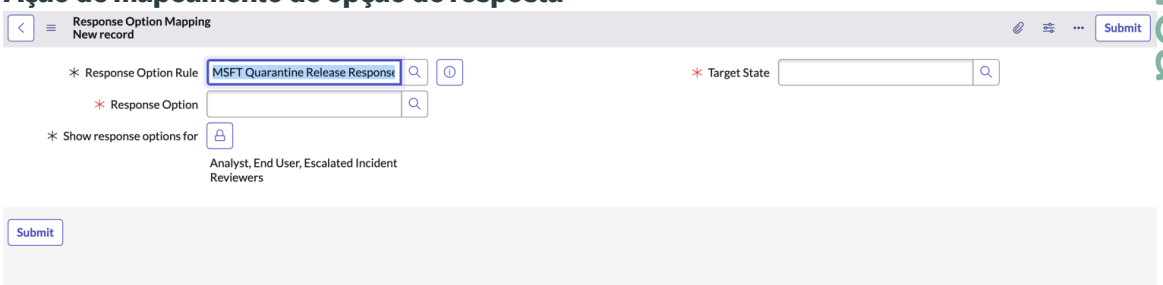
Regra de opção de resposta	Nome da regra de opção de resposta do incidente. Por exemplo, SharePoint Implica que a origem da verificação é o SharePoint. Você pode inserir o nome da resposta do incidente ou pesquisar usando a pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção de resposta	Opção para selecionar a opção de resposta. Você pode inserir a opção de resposta ou pesquisar usando a pesquisa.
Estado de destino	O estado de destino do incidente do DLP depois que o usuário final seleciona a ação apropriada. **Nota:** a. . **Estado de destino** o campo aparecerá somente quando você selecionar **Opção de resposta** que é de **Tipo: Básico** . Para obter mais informações sobre como os tipos de estado de destino são configurados, consulte Configure a opção de resposta para seus incidentes de DLP. b. Quando uma opção de resposta que é de **Tipo: Avançado** Selecionado, você não poderá definir o Estado de destino e ficará oculto. O Estado de destino será atribuído com base no estado personalizado configurado no subfluxo do Flow Designer.
Mostrar opções de resposta para	Opção para determinar as funções do usuário para mostrar as opções de resposta. Você pode escolher **Analista** , **Usuário final** e **Analistas escalados** usando a opção de desbloqueio. Você tem permissão para escolher uma ou todas as funções.

Ação de mapeamento de opção de resposta



6. Clique em **Enviar**.

Configure a opção de resposta para seus incidentes de DLP

Use este recurso para configurar o tipo de resposta que um usuário final ou analista deve executar.

Antes de Iniciar

A aplicação Resposta de incidentes DLP do sistema de base fornece as seguintes opções de resposta:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Avaliação concluída
2. Conteúdo excluído
3. Arquivo excluído
4. Arquivo criptografado
5. Conteúdo mascarado
6. Relatar falso positivo
7. Relatar responsável incorreto
8. Solicitar liberação de e-mail da quarentena

   Nota: Esta opção está disponível para os registros do Microsoft Exchange do DLP.

9. Necessário para o processo de negócios
10. Direitos revisados

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Opções de resposta**.

   Por padrão, o sistema de base fornece dois tipos de opção de resposta:

   a. **Básico** Uma opção de resposta manual enviada pelo usuário.

   b. **Avançado** : Uma opção de resposta automatizada aciona um subfluxo do Flow Designer quando o usuário envia a opção de resposta.

2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de opção de resposta do tipo: Básico

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar o tipo de opção de resposta.

Formulário de opção de resposta do tipo: Avançado

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar a opção de resposta. Por padrão, este campo exibe os dois tipos de opções a seguir:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Básico** : Quando você seleciona esta opção ao criar uma nova opção de resposta, pode ser necessário adicionar um nome de opção de resposta e o tipo. ○ **Avançado** : Quando você seleciona esta opção, os seguintes campos estarão disponíveis para seleção: ▪ **Fluxo** : Selecione o subfluxo do Flow Designer. ▪ **MID Server** : Marque esta caixa de seleção se o fluxo selecionado usar o MID Server.
Fluxo	Selecione o fluxo do Flow Designer necessário para ativar a aplicação MID e a capacidade DO MID. Ao criar um subfluxo para a opção de resposta, adicione as seguintes entradas de subfluxo: **a. Nome** : ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Type** (Tipo): ▪ Referência (para tabela de incidentes do DLP) ▪ SYS ID para a aplicação do MID Server e a capacidade do MID Server
Requer MID Server	Opção para determinar essa configuração do MID Server. Habilitando o. **MID Server** caixa de seleção **Aplicação do MID Server** e. **Capacidade do MID Server** Campos Você pode configurar a aplicação MID e a capacidade DO MID. **Nota:** Com base na aplicação MID Server e na configuração da capacidade DO MID Server e se algum MID estiver em execução, somente a opção Resposta ficará visível no espaço.
Aplicação do MID Server	Selecione a aplicação DO MID Server necessária na lista suspensa.
Capacidade do MID Server	Selecione a capacidade DO MID Server necessária na lista suspensa.

Tradução automática

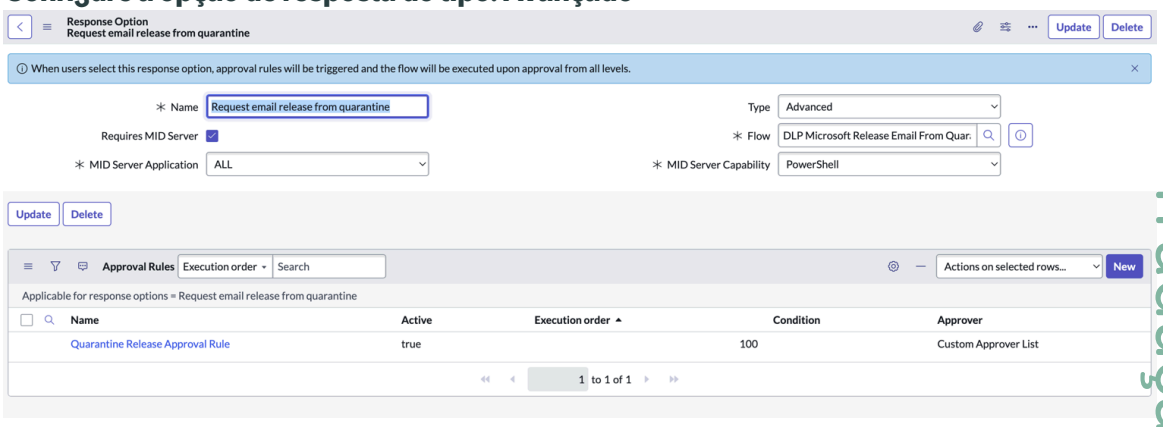
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se não houver nenhum MID Server disponível para o recurso DO MID Server selecionado, a opção de resposta não ficará visível. Se você quiser um MID Server específico da lista, será necessário configurar o aplicativo MID e torná-lo visível na lista e, em seguida, pelo menos um MID Server configurado deve estar em execução nas aplicações MID selecionadas e deve ter a capacidade do MID Server selecionado.

4. Clique em **Enviar**.

Nota: Se você estiver criando um **Avançado** tipo de opção de resposta e, em seguida, o. **Regras de aprovação** a lista relacionada será preenchida para que você configure a regra de aprovação para essa nova opção de resposta. Para obter mais informações, consulte Criar regras de aprovação.

Configure a opção de resposta do tipo: Avançado



Criar configurações de gráfico de idade

Configure o gráfico de idade que aparece em Data Loss Prevention Incident Response(DLP IR) Portal de operações. Este gráfico mostra a contagem de incidentes em aberto pelo número de dias.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Configuração de gráfico de idade**.
2. Revise as entradas do gráfico de idade na tabela a seguir e personalize as entradas para o seu ambiente.

Formulário Configurações do gráfico de idade do DLP

Nome	Condição
0 a 30 dias	Idade do incidente em aberto entre 0 e 30 dias.
31 a 60 dias	Idade do incidente em aberto entre 31 e 60 dias.
61 a 90 dias	Idade do incidente em aberto entre 61 e 90 dias.
Mais de 90 dias	Idade do incidente em aberto que é superior a 90 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicione uma nova configuração de gráfico de idade clicando em **Novo** .
4. No campo Nome, insira um **Nome** Para a configuração do gráfico de idade do DLP.
5. Defina as condições para a configuração do gráfico de idade do DLP.

   a. Para adicionar condições, clique em **E.** ou **OU** .
      - Se **E.** selecionado, todas as condições devem ser correspondidas.
      - Se **OU** está selecionado, qualquer condição pode ser correspondida.

      Nota: As condições no Construtor de condições diferenciam maiúsculas de minúsculas.

   b. Para definir uma segunda condição de filtro, clique em **Novos critérios** .
6. Clique em **Enviar**.

Criar configurações de delegação de usuário

Impeça que determinados executivos da organização recebam notificações sobre os incidentes atribuídos ou escalados a eles.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Considere um cenário em que o executivo é um usuário que pertence a uma liderança ou grupo executivo. O executivo não deve receber e-mails sobre atribuição de incidente ou escalação. Um usuário delegado pode executar a ação necessária em nome do executivo.

Depois que um usuário atribui uma pessoa específica, Henry, como delegado, outro usuário não pode atribuir Henry como delegado novamente. Da mesma forma, um delegado não pode atribuir outro usuário como delegado.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Delegar configuração**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Delegar formulário de configuração

Campo	Descrição
Usuário	Nome do usuário que precisa de um delegado para incidentes de DLP.
Delegado	Nome do usuário que pode responder ao incidente do DLP em nome do usuário final original.

4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de identificação de infrator recorrente

Crie regras de identificação de infrator recorrente para identificar usuários que repetem o mesmo problema várias vezes.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar infratores reincidentes usando determinadas regras ou critérios. Data Loss Prevention Incident Response fornece campos que você pode usar para identificar infratores reincidentes.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Repetir regras de identificação do infrator**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regras de identificação de infrator de repetição

Campo	Descrição
Nome	Nome da regra de identificação do infrator reincidente.
Ordem de execução	Prioridade das regras de identificação do infrator reincidente. Este campo indica a ordem na qual as regras de identificação de infrator reincidente são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de identificação de infrator recorrente com o menor número tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva desta regra de identificação de infrator recorrente.
Condição	Condições no construtor de condições que são baseadas na tabela de incidentes do DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho para a regra de identificação de infrator recorrente. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha.

Tradução automática

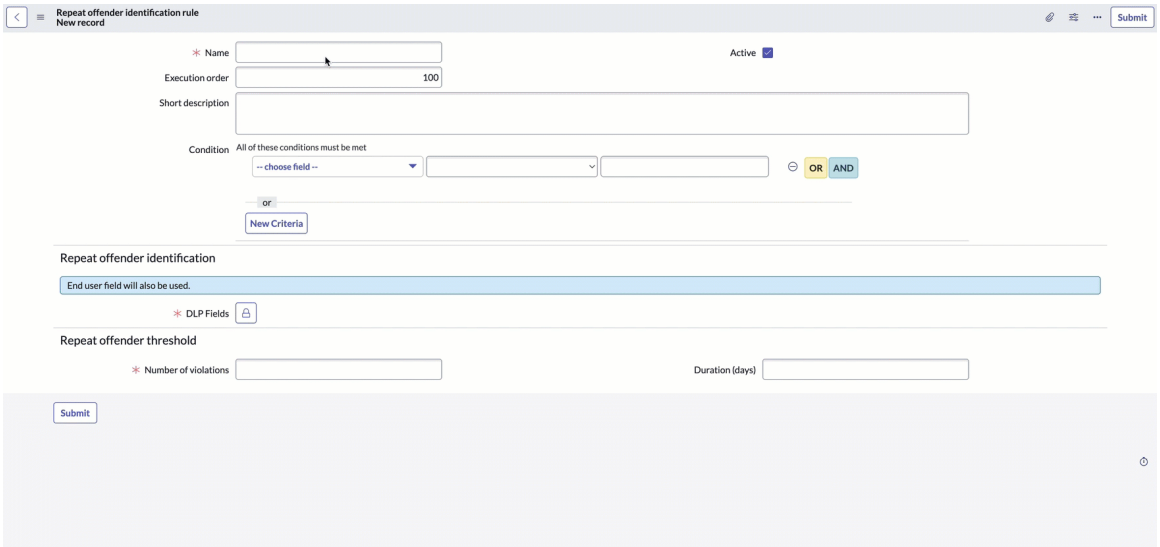
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar mais condições, clique em **E.** ou **OU** : ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios** . **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Campos do DLP	Identificar infratores reincidentes com base nos campos de DLP obrigatórios. Clique em Ícone ao lado dos Campos do DLP para exibir a lista de campos do DLP disponíveis. Selecione os campos DLP que você deseja usar na coluna Disponível e mova-os para a coluna Selecionado. Por exemplo, você pode selecionar **Nome do arquivo** e. **Proprietário do arquivo** Campos da coluna Disponível e mova-os para a coluna Selecionado. Em seguida, você pode identificar os infratores reincidentes com base em **Nome do arquivo** e. **Proprietário do arquivo** campos. Portanto, se um usuário violar o limite de infrator reincidente (número de violações e duração) e se o mesmo usuário corresponder aos campos DLP, esse usuário específico será identificado como infrator reincidente.
Número de violações	Defina o valor do limite de infrator recorrente. Depois que o usuário repete as mesmas ações e viola o número especificado de violações, o usuário é identificado como um infrator reincidente.
Duração (em dias)	Defina o limite de infrator recorrente na forma de dias. Depois que o usuário repete as mesmas ações e viola a duração do limite, o usuário é identificado como um infrator reincidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificar infratores reincidentes



4. Clique em **Enviar**.

Criar campos de dados de incidente adicionais

Crie seus campos de dados de incidente adicionais para os incidentes do DLP. Você pode criar diferentes tipos de campos de dados de incidentes adicionais, como cadeia de caracteres, número, caixa de seleção, opção, data e hora, e usá-los nos formulários de incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Importante: Campos de dados de incidentes adicionais para incidentes de DLP são compatíveis somente com a versão San Diego ou posterior.

Por Que e Quando Desempenhar Esta Tarefa

Campos de dados de incidentes adicionais estão associados a restrições de nível de campo, portanto, se houver restrições de nível de campo, isso se aplicará aos campos de dados de incidentes adicionais no portal de operações de DLP e no portal do usuário final.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Campos de Dados de Incidentes Adicionais**.
2. Clique em para criar campos de dados de incidente adicionais **Novo** .
3. No formulário, preencha os campos.

Formulário Campos de dados de incidentes adicionais do DLP

Campo	Descrição
Nome	Nome dos campos de dados adicionais do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

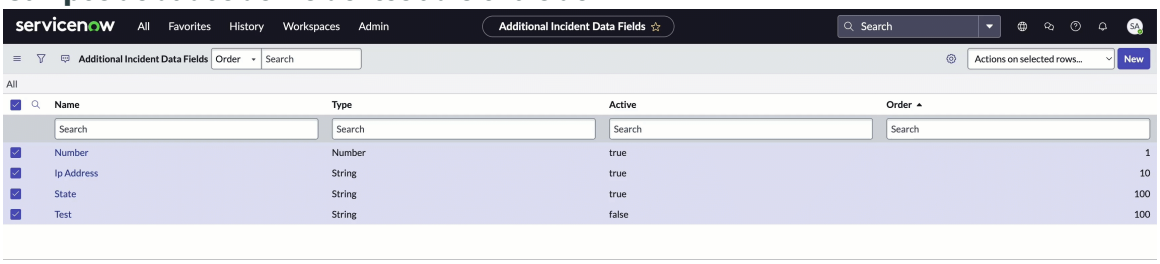
Campo	Descrição
Tipo	Opção para selecionar o tipo de Campos de dados de incidente adicionais. Você pode escolher um dos seguintes tipos: ○ **Cadeia de caracteres** ○ **"Number" (Número)** ○ **Caixa de seleção** ○ **Escolha** Se você selecionar o tipo Campos de dados de incidente adicionais como **Opção** Depois de criar os Campos de dados adicionais do incidente, você pode definir as opções de opção Campos de dados adicionais do incidente. Para criar uma opção de opção Campos de dados de incidente adicionais: **a.** Abra os Campos de dados de incidentes adicionais necessários. **b.** Na seção Opções de campo de escolha personalizada, clique em **Novo** . **c.** No campo Nome da opção, defina o nome da opção necessário. **d.** Clique em **Enviar**. ○ **Data** ○ **Data/hora** **Nota:** Depois de selecionar um tipo para seus novos Campos de dados de incidente adicionais, você não terá permissão para modificá-lo. Se você quiser modificar o tipo, será necessário criar novos Campos de dados de incidente adicionais novamente com o tipo necessário.
Ordem	Opção para escolher a ordem na qual os Campos de dados adicionais do incidente devem ser exibidos. Você pode definir o valor do pedido para cada Campos de dados de incidente adicionais. Os Campos de dados de incidentes adicionais são classificados com base nos valores de pedido que você define. Por padrão, os Campos de dados adicionais do incidente são classificados em ordem crescente. Você pode classificar os Campos de dados de incidentes adicionais em ordem decrescente clicando em **Pedido** coluna.
Ativo	Opção para indicar se os Campos de dados adicionais do incidente estão ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição dos Campos de dados de incidente adicionais que você criou.

Campos de dados de incidentes adicionais de DLP



4. Clique em **Enviar**.

Formulário Definição de ANS do DLP

Descrições de campo para o formulário Definição de ANS do DLP usado para criar um registro de ANS.

Campo	Descrição
Nome	Nome da definição.
Tipo	Tipo de acordo, que, neste caso, é ANS.
Meta	Destino usado para filtragem, pesquisa e emissão de relatórios sobre o acordo que está sendo definido. As opções disponíveis são: • Nenhum(a) • Resposta • Resolução
Tabela	Tabela que determina os registros rastreados pelo ANS, que deve ser Tarefa de ANS do DLP [sn_dLIR_incident_sla_task].
Fluxo	Fluxo a ser executado quando a definição de ANS é anexada a um registro de tarefa, que deve ser o fluxo de ANS padrão.
Tipo de Duração	Método para calcular a duração do ANS. As opções disponíveis são: • Duração especificada pelo usuário • 2 dias úteis até 16h • 3 dias úteis até 16h • Violação na data de vencimento • Fim do próximo dia útil • Próximo dia útil às 16h

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Duração	Tempo em que o ANS é executado antes de ser marcado como violado. Este campo está disponível somente quando Duração especificada pelo usuário é selecionada em **Tipo de duração** .
Origem da programação	Programe para usar ao criar os SLAs de tarefa.
Agendamento	Horas durante as quais o temporizador de ANS é executado. Este conjunto de cronogramas é definido na configuração principal.
Hora Origem da zona	Hora Origem da zona a ser usada ao criar SLAs de tarefa. As opções disponíveis são: • Fuso horário do solicitante • O fuso horário da definição do ANS • O fuso horário do local do IC • O fuso horário do local da tarefa • O fuso horário do local do solicitante
Ativo	Opção para tornar o gatilho efetivo quando a condição de início for atendida.
Guias	
Condição de início	Condição que inicia o temporizador de ANS e ativa o ANS.
Condição de pausa	Condições sob as quais o ANS é suspenso, o que aumenta o tempo total decorrido.
Condição de cancelamento	Condições sob as quais o ANS é cancelado.
Condição de redefinição	Condições sob as quais o ANS ativo é concluído e um novo ANS é estabelecido quando o valor de qualquer campo no registro de tarefa muda, muda ou muda de um valor específico no registro. Por exemplo, diga o valor de **Local** O campo no registro da tarefa é 101 Broadway East, Seattle, WA. Se você definir a condição de redefinição do ANS como **[Localização] [Mudanças de][101 Broadway East, Seattle, WA]** qualquer mudança no valor de **Local** O campo redefine o ANS do registro da tarefa.

Tópicos relacionados

Crie um Data Loss Prevention Incident Response Definição de ANS

Definir configurações avançadas

Defina as configurações avançadas para que você possa determinar os campos no Incidente para identificar os usuários finais, entre outros recursos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Definir configurações avançadas no Data Loss Prevention Incident Responseé opcional. Algumas configurações avançadas incluem o seguinte:

- Defina o número máximo de incidentes que podem ser enviados em um e-mail de resumo.
- Habilite o modo rápido para enviar e-mails mais rapidamente.
- Determine o detalhamento do log da aplicação.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Configurações avançadas**.
2. No formulário, preencha os campos.

Formulário Configurações avançadas

Campo	Descrição
Os dados confidenciais que causaram a violação devem ser exibidos no incidente?	Opção para escolher se você deseja exibir os dados confidenciais que causaram a violação no incidente do DLP. Por padrão, esta opção está habilitada.
Os dados confidenciais que causaram a violação também devem ser exibidos nos incidentes secundários?	Opção para escolher se você deseja exibir os dados confidenciais que causaram a violação no incidente secundário do DLP também. Por padrão, esta opção está desativada.
Lista de campos no incidente que são usados para identificar o usuário final	A lista de campos no incidente do módulo Regra de atribuição que são usados para identificar o usuário final. Você também pode especificar seus próprios atributos personalizados para identificar o usuário final.
Número máximo de incidentes em um e-mail de resumo	O número máximo de incidentes que podem ser enviados em um e-mail de resumo. Por padrão, o valor é 100.
Duração máxima da ofensa repetida (em dias)	A duração máxima para identificar um infrator reincidente. Por padrão, o valor é 90 dias.
Modo rápido para enviar e-mails	Opção para validar e-mails e identificar problemas. Você pode executar a validação habilitando o. **Sim** opção. Por padrão, esta opção está habilitada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Esta propriedade é usada para definir o detalhamento do log da aplicação	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** Por padrão, o valor é **informações**.
Excluir incidentes secundários e clonados de relatórios	Opção para excluir os incidentes clonados e secundários dos relatórios. Por padrão, esta opção é **Sim**.
Dia(s) para aguardar a exclusão do conteúdo correspondente no armazenamento em nuvem após o encerramento do incidente	Opção para escolher o número de dias de espera para limpar o conteúdo de correspondência dos incidentes que estão inativos por um período de tempo específico. Por padrão, o valor é 90. Se o incidente do DLP estiver inativo, o conteúdo correspondente será limpo do armazenamento em nuvem 90.
Atribuir incidente ao grupo de analistas de DLP após o último nível de escalação	Marque esta caixa de seleção para atribuir o incidente ao analista após o último nível de escalação.
Permitir que os usuários acessem os incidentes após a escalação	Marque esta caixa de seleção para permitir que os usuários atribuídos acessem o(s) incidente(s) após a escalação. Quando você seleciona esta opção, todos os usuários que foram adicionados à lista de cadeia de escalação poderão acessar o(s) incidente(s).
Permitir que o analista edite a avaliação concluída	Marque esta caixa de seleção para permitir que o analista edite a avaliação concluída. Quando você seleciona esta opção, os analistas podem editar as avaliações. Quando desmarcada, você pode exibir as avaliações no modo somente leitura.
Propriedades de visualização dos arquivos de evidências	
A habilitação desta propriedade do sistema ativa o recurso de visualização do arquivo de evidências no espaço do analista de DLP. sn_dlir.enable_evidence_file_preview	Opção para escolher se você deseja visualizar os arquivos de evidência diretamente no espaço. Por padrão, esta opção é **Sim**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Isso permitirá que os usuários do DLP baixem os arquivos de evidência visualizados. Quando esta propriedade estiver habilitada, os usuários verão um botão de download no visualizador de documentos para baixar o arquivo de evidência. sn_dlir.enable_download in_preview	Opção para escolher se você deseja exibir o botão de download no visualizador de documentos, o que permitirá que você baixe os arquivos de evidência visualizados. Por padrão, esta opção é **Sim** .
Esta propriedade determina a duração pela qual os arquivos serão retidos temporariamente para fins de visualização do arquivo de evidência. (em minutos) sn_dlir.preview_temp_files_cleanup_interval	A duração máxima durante a qual os arquivos são armazenados temporariamente para visualização do arquivo de evidência. Por padrão, o valor é 10. Se o incidente do DLP estiver inativo, o arquivo de evidência será limpo do espaço do analista 10.
Habilitar esta propriedade estenderá o intervalo de limpeza se os arquivos de evidência estiverem em uso. Isso permitirá que o sistema estenda o tempo de expiração dos arquivos de evidência com base no valor definido na propriedade do sistema "sn_dLIR.preview_temp_files_cleanup_interval". sn_dlir.extend_cleanup_interval_on_usage	Opção para estender o tempo antes que os arquivos de evidência sejam excluídos se estiverem sendo usados. Por padrão, esta opção é **Sim** .
Duração máxima para estender o intervalo de limpeza de arquivos de evidências (em minutos). sn_dlir.max_extension_duration_for_cleanup	Opção para selecionar por quanto tempo, em minutos, o sistema manterá seus arquivos de evidência antes de limpá-los. Por padrão, o valor é 60.

3. Clique em **Salvar**.

Monitorar o processo de execução de integração do DLP

Rastreie e monitore a ingestão contínua ou o processo de execução da integração. Os processos de execução de integração contêm as estatísticas sobre quanto os dados foram processados e o status da integração.

Função necessária: sn_dLIR.admin.

O processo de execução de integração lista os detalhes sobre quantos registros são ingeridos. Por exemplo:

1. Na integração Symantec, o processo contém execuções de integração secundária e primária. O registro primário indica os dados de ingestão e o registro secundário indica as chamadas de aprimoramento e os registros de atributo personalizados.
2. Na integração da Microsoft, há somente um processo de ingestão de registro primário a ser executado.

Processos de execução de integração do DLP Exibe as entradas da fila, o status das entradas da fila e os registros obtidos.

A execução de integração contém a Origem para a qual o perfil de integração e o registro de execução de integração são criados, intervalos de pesquisa de perfil, estados de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ingestão e subestados, contagem de incidentes que indica o número de registros que são ingeridos.

1. Navegar até **Administração da DLP** > **Execuções de integração**.
2. Selecione a execução de integração na lista.
3. Navegue até **Processo de execução de integração do DLP** .
4. Exiba o status de entrada da fila do registro.

Restrições de acesso a incidentes do DLP

Gerencie a visibilidade de um incidente de DLP específico que contém informações confidenciais. Você pode usar restrições de acesso a incidentes para definir quem pode acessar um incidente de DLP específico e restringir que usuários ou grupos específicos acessem esse incidente.

Criar restrições no nível de campo

Defina restrições de nível de campo em incidentes de DLP para proteger informações confidenciais contra a exposição. Você pode usar restrições no nível de campo para controlar os usuários ou grupos que podem acessar campos específicos nos incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições no nível de campo permitem exibir somente determinados campos para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os dados que um usuário pode acessar. Você pode criar uma Restrição de nível de campo definindo as condições de correspondência de incidente do DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e, em seguida, escolhendo os campos do DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de campo**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Restrição de nível de campo do DLP

Campo	Descrição
Nome	Nome da restrição de nível de campo.
Ativo	Opção para indicar se a restrição de nível de campo está ativa.
Ordem de execução	Prioridade das restrições de nível de campo. Este campo indica a ordem na qual as restrições de nível de campo são executadas quando duas ou mais restrições de nível de campo compartilham as condições de acionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	A restrição de nível de campo com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva desta restrição de nível de campo.
Condição de correspondência de incidente	Opções no incidente que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições no nível do campo. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU**: ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode selecionar o campo como Nome da política e defina a condição como em e Nome da política. **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas.
Aplica-se a	Opção para aplicar as condições de correspondência de incidente a usuários ou grupos específicos. Você pode aplicar as condições ao seguinte: ○ **Todos os usuários finais** Opção para selecionar todos os usuários finais aos quais as condições de incidente do DLP são aplicáveis. ○ **Todos os revisores de incidentes escalados** Opção para selecionar todos os revisores de incidentes escalados aos quais as condições de incidente do DLP são aplicáveis. Refere-se a todos os incidentes de DLP escalados para o gerente. ○ **Usuários**: Clique em Ícone para adicionar um usuário específico da lista a quem as condições de incidente do DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa dele. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário a quem as condições do DLP são aplicáveis, clique em

Tradução automática

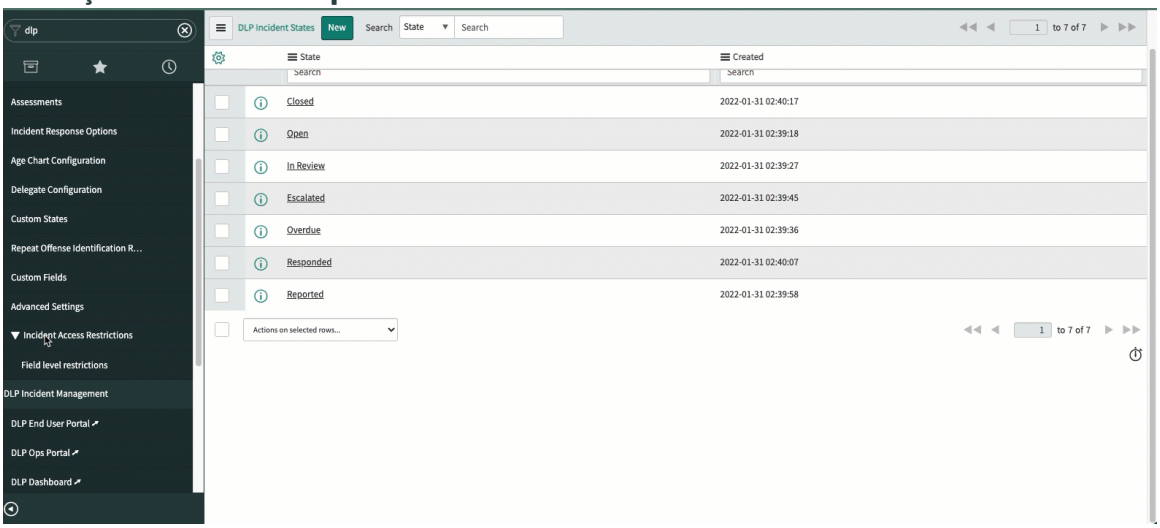
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Grupos** : Clique em  Ícone para adicionar um grupo específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.
Permitir acesso somente aos seguintes campos	○ **Campos do DLP** Opção para definir os campos do DLP que você deseja permitir acesso aos usuários ou grupos selecionados. Selecione os campos do DLP aos quais você deseja permitir acesso na coluna Disponível e mova-os para a coluna Selecionado. **Nota:** Os usuários ou grupos selecionados poderão acessar somente os campos DLP selecionados. Por exemplo, você pode selecionar **Atribuído a.** e. **Aberto** Campos da coluna Disponível e mova-os para a coluna Selecionado. Em seguida, os usuários ou grupos selecionados terão acesso somente aos campos Atribuído a e Aberto. ○ **Carregar anexos** Opção para indicar se você deseja permitir que os usuários ou grupos selecionados carreguem anexos. ○ **Campos personalizados** Opção para definir os campos personalizados que você deseja permitir acesso aos usuários ou grupos selecionados. Você pode exibir os campos personalizados que criou na coluna Disponível. Selecione os campos personalizados aos quais você deseja permitir acesso na coluna Disponível e mova-os para a coluna Selecionado. **Importante:** ▪ Campos personalizados para incidentes de DLP são compatíveis somente com a versão San Diego ou posterior. ▪ Os usuários ou grupos selecionados poderão acessar somente os campos personalizados selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrição de nível de campo da DLP



4. Clique em **Enviar**.

Criar restrições de nível de registro

Defina restrições de nível de registro em incidentes de DLP para proteger registros confidenciais contra a exposição. Você pode usar restrições de nível de registro para controlar os usuários ou grupos que podem acessar registros específicos nos incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dLIR.admin - Criar, editar e excluir.
- sn_DLIR.analyst e sn_dLIR.analyst_read - Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições de nível de registro permitem que você forneça acesso a registros somente para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os registros que um usuário pode acessar. Você pode criar uma restrição de nível de registro definindo as condições de correspondência de incidente do DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e, em seguida, escolhendo os registros do DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Tudo** > **Administração da DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de registro**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Restrição de nível de registro do DLP

Campo	Descrição
Nome	Nome da restrição de nível de registro.
Descrição resumida	Descrição exclusiva desta restrição de nível de registro.

Tradução automática

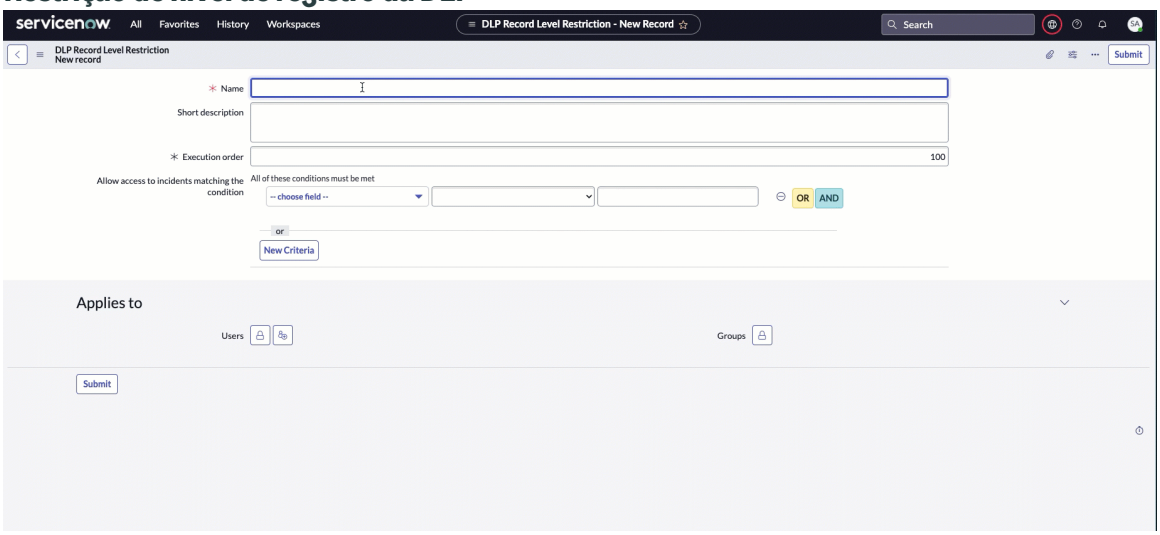
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem de execução	Prioridade das restrições de nível de registro. Este campo indica a ordem na qual as restrições de nível de registro são executadas quando duas ou mais restrições de nível de registro compartilham as condições de acionamento. A restrição de nível de registro com o número mais baixo tem a prioridade mais alta. Para definir a ordem da operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Permita acesso a incidentes que correspondam à condição	As opções permitem o acesso aos incidentes que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições de nível de registro. Use as listas e os campos do construtor de condições para definir os filtros para a primeira linha. Para adicionar mais condições, clique em **E.** ou **OU**: ○ Se **E.** selecionado, todas as condições devem ser correspondidas. ○ Se **OU** está selecionado, qualquer condição pode ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições diferenciam maiúsculas de minúsculas. Por exemplo, você pode selecionar o campo como Ativo e defina a condição como . e verdadeiro .
Aplica-se a	Opção para aplicar restrições de nível de registro a usuários ou grupos específicos. Você pode aplicar as condições da seguinte forma: ○ **Usuários**: Clique em ícone para adicionar um usuário específico da lista a quem o registro selecionado é aplicável. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa dele. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual o registro é aplicável, clique em . Por exemplo, administrador do sistema. ○ **Grupos**: Clique em ícone para adicionar um grupo específico da lista ao qual o registro selecionado é aplicável. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrição de nível de registro da DLP



4. Clique em **Enviar**.

Arquivamento de incidentes do DLP

. Data Loss Prevention Incident ResponseÉ provisionado com uma regra de arquivamento no sistema de base para a tabela de incidentes do DLP. Os registros relacionados também são adicionados no sistema de base à regra de arquivamento de incidentes do DLP.

Antes de Iniciar

Função necessária: administrador

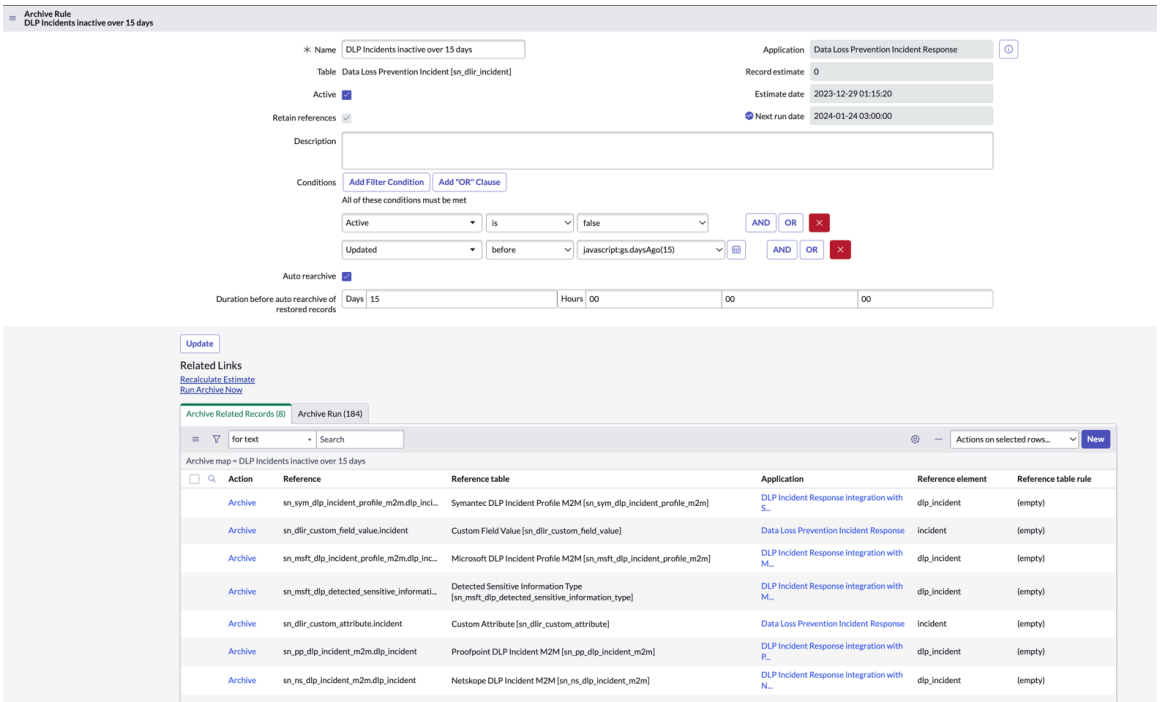
Procedimento

1. Navegar até **Tudo** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
   As regras de arquivamento do sistema que estão no sistema de base são exibidas.
2. Exiba a regra de arquivamento do DLP.

> **Nota:** **Incidentes do DLP inativos por mais de 15 dias** É a regra de arquivamento do sistema de base padrão para incidentes de DLP. Você pode modificar a regra de arquivamento, se necessário. Esta regra significa que os incidentes inativos acima de 15 dias serão arquivados automaticamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Para obter informações sobre como as regras de arquivamento são criadas, consulte Crie uma regra de arquivamento .

3. **Atualização** a regra, se necessário.

Arquive registros relacionados ao DLP

Use a lista relacionada Arquivar registros relacionados para incidentes de DLP para adicionar os registros relacionados à regra de arquivamento.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
2. Selecione **Incidentes do DLP inativos por mais de 15 dias** regra de arquivamento.
3. Vá para **Arquivar registros relacionados** lista relacionada.
4. Exiba os registros relacionados ao DLP.

Aplicação	Tabela de Referência
Integração de Resposta a incidentes do PPD com Symantec	Symantec DLP Incident Profile M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Valor do campo personalizado [sn_dLIR_custom_field_value]
Integração de Resposta a incidentes do PPD com Microsoft	Microsoft DLP Incident Profile M2M [sn_msft_dlp_incident_profile_m2m]
Integração de Resposta a incidentes do PPD com Microsoft	Tipo de informações confidenciais detectadas [sn_msft_dlp_detected_sensitive_information_type]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Tabela de Referência
Data Loss Prevention Incident Response	Atributo personalizado [sn_dLIR_custom_attribute]
Integração de Resposta a incidentes do PPD com Proofpoint	Incidente do Proofpoint DLP M2M [sn_pp_dlp_incident_m2m]
DLP Incident Response integration with Netskope	Netskope DLP Incidente M2M [sn_ns_dlp_incident_m2m]
Integração de Resposta a incidentes do PPD com Symantec	Tipo de informações confidenciais detectadas [sn_sym_dlp_detected_sensitive_information_type]

Nota: Todas as tabelas do sistema, como e-mails, avaliações e anexos, serão direcionadas automaticamente para o registro do DLP arquivado.

5. Selecione a regra de registro relacionada ao arquivamento que você deseja arquivar.

Nota: Para obter mais informações sobre como adicionar mais registros relacionados, consulte Arquive registros relacionados ao DLP ativado ServiceNow AI Platform.

Data Loss Prevention Incident Response Gestão de incidentes

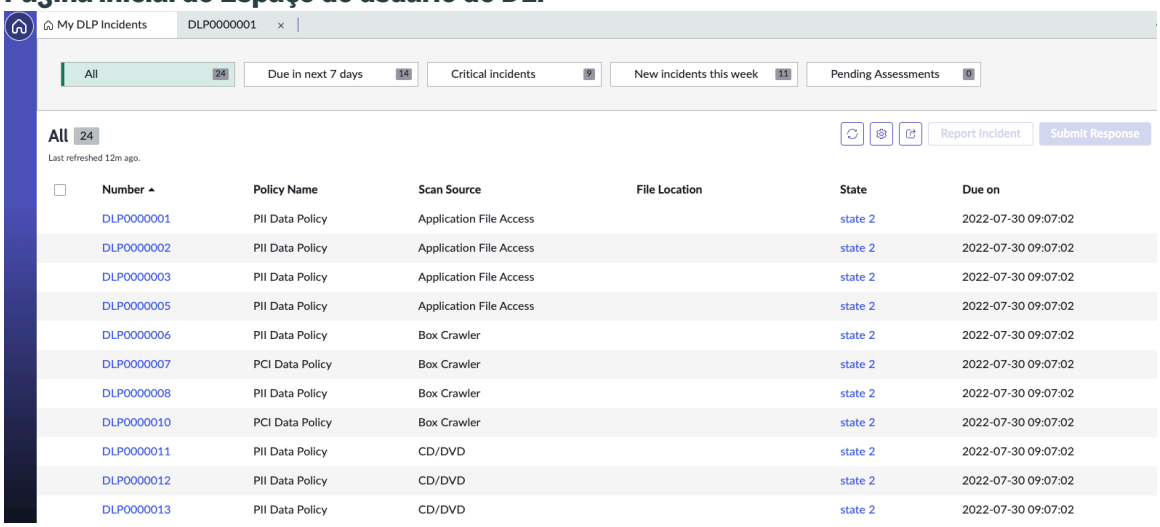
Use Data Loss Prevention Incident Response Gestão de incidentes para atualizar e gerenciar incidentes aproveitando o Espaço do usuário do DLP, o Espaço do analista do DLP e o Painel do DLP.

Data Loss Prevention Incident Response Espaço do usuário

. Data Loss Prevention Incident Response(IR do DLP) O Espaço do usuário é um espaço em que usuários finais, gerentes e aprovadores podem responder aos incidentes de DLP atribuídos. Os usuários finais, gerentes e aprovadores podem responder aos incidentes especificando as ações corretas.

Você também pode criar e gerenciar avaliações para permitir que os usuários finais respondam a incidentes de DLP. O espaço consiste em uma página principal e exibições de lista que permitem que você veja os incidentes de DLP atribuídos.

Página inicial do Espaço do usuário do DLP



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatar ou responder a incidentes de DLP

Acesse Data Loss Prevention Incident Response(DLP) Espaço do usuário, revise os incidentes de DLP atribuídos e relate ou responda aos incidentes.

Antes de Iniciar

Função necessária:

- Qualquer usuário/funcionário válido

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **Espaço do usuário do DLP**.
   A página Meus incidentes do DLP é aberta em uma nova guia.
2. Clique em uma exibição de lista para revisar os incidentes atribuídos a você.

Exibição em lista	Descrição
Tudo	Exibir todos os incidentes atribuídos.
Vencimento nos próximos 7 dias	Exiba todos os incidentes que vencem nos próximos 7 dias.
Incidentes críticos	Exiba todos os incidentes com o rótulo de gravidade crítico.
Novos incidentes esta semana	Exiba todos os incidentes atribuídos esta semana.
Avaliações pendentes	Exiba todas as avaliações que ainda estão pendentes.

3. Você pode revisar os incidentes do DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes de DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Página inicial do Portal do usuário final do DLP

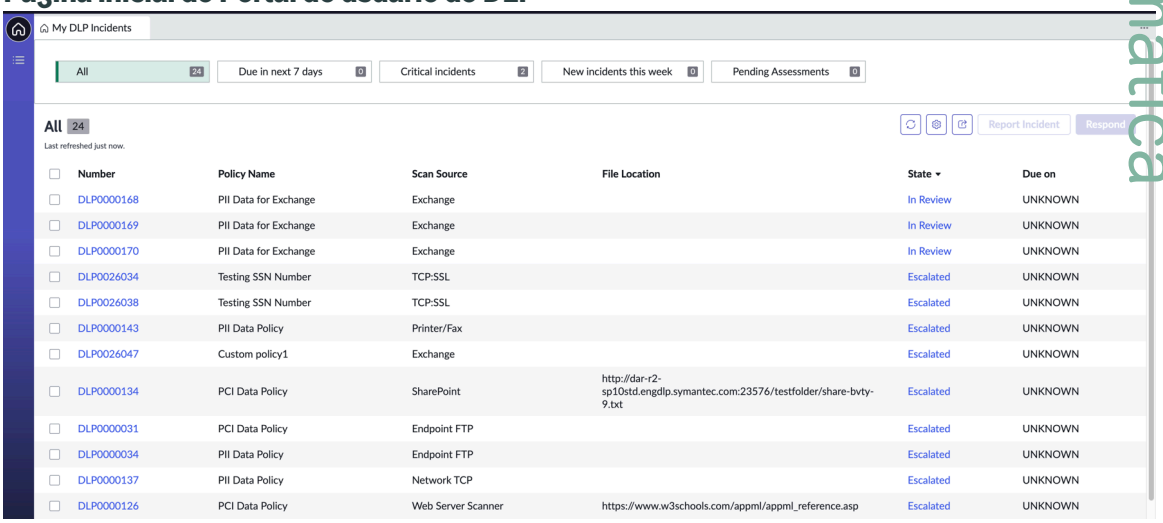
Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes de DLP se você fez uma atualização.
Ações de Lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Quando você tem sua própria lista personalizada que é criada em **Minhas listas** configurada para o seu espaço, você também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para todos	Opção para copiar os URLs de todos os incidentes do DLP.
Relatar incidente	Ação para relatar o incidente como falso positivo ou proprietário errado. Por exemplo, você pode relatar um proprietário errado e sugerir outro proprietário ou relatar o incidente como um falso positivo.
Responder	Responda a um incidente selecionando uma opção de resposta a incidente. Por exemplo, o usuário exclui um arquivo que viola uma política de DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena** .

Página inicial do Portal do usuário do DLP



c. A segunda maneira é clicar em um incidente DLP específico para abri-lo.
. **Detalhes** exibe as seguintes seções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Detalhes : Você pode exibir os detalhes do incidente do DLP, como número do incidente, gravidade e nome do arquivo.
- Compor : Para adicionar comentários sobre o incidente do DLP visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privadas).
- Atividade : Você pode exibir os detalhes das diferentes atividades no incidente do DLP.
- Anexos : Se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo da sua unidade local.

. **Detalhes adicionais** Exibe todas as informações adicionais sobre o incidente do DLP, incluindo campos personalizados.

Importante:

- Campos personalizados para incidentes de DLP são compatíveis somente com a versão San Diego ou posterior.
- Se houver dados de campos personalizados disponíveis para um incidente de DLP específico, você poderá exibi-los em **Detalhes adicionais** guia. Se não houver campos personalizados para o incidente do DLP, você verá uma página em branco.

- **Tipo de informação confidencial detectado** : Exibe as informações confidenciais detectadas pelo incidente.

Nota: Esta lista relacionada está visível somente para os incidentes de DLP criados para integrações da Microsoft ou Symantec. No registro de incidente da Microsoft ou Symantec, sempre que o usuário acessa o registro do tipo de informação confidencial detectada, o conteúdo de correspondência realçado em relação a essa integração é exibido.

d. Escolha a opção apropriada para você.

Opção	Descrição
Relatar falso-positivo	Ação para relatar que o incidente do DLP foi acionado ou criado incorretamente. Você pode mencionar os detalhes do motivo pelo qual marcou o incidente como falso positivo no campo Comentários.
Relatar responsável incorreto	Ação para relatar que o incidente do DLP foi atribuído ao usuário incorreto. Se você souber o responsável correto do incidente, poderá selecionar o nome do responsável no campo Sugerir responsável. Para adicionar detalhes adicionais, use o campo Comentários.
Responder	Responda a um incidente selecionando uma opção de resposta a incidente. Por exemplo, o usuário exclui um arquivo que viola uma política de DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar confirmação manual de que o arquivo foi excluído e fornecer comentários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

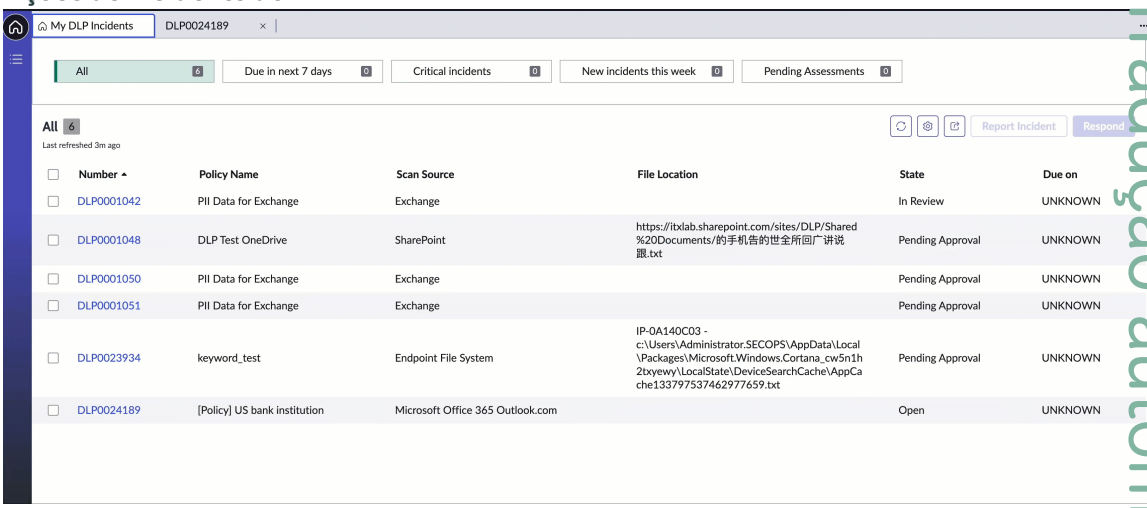
Opção	Descrição
	Aqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena** .

e. Selecione **Responder** botão após responder à consulta do analista.
Um pop-up para enviar uma resposta de incidente é exibido. Selecione a resposta no menu suspenso e adicione comentários.

f. Selecione **Enviar**.
Uma faixa é exibida confirmando que sua resposta foi enviada com sucesso.

Nota: O incidente é atribuído ao aprovador ou analista correspondente e o usuário final perderá o acesso ao incidente.

Ações de incidente do DLP



4. Para fazer avaliações, selecione **Avaliações pendentes** exibição de lista.

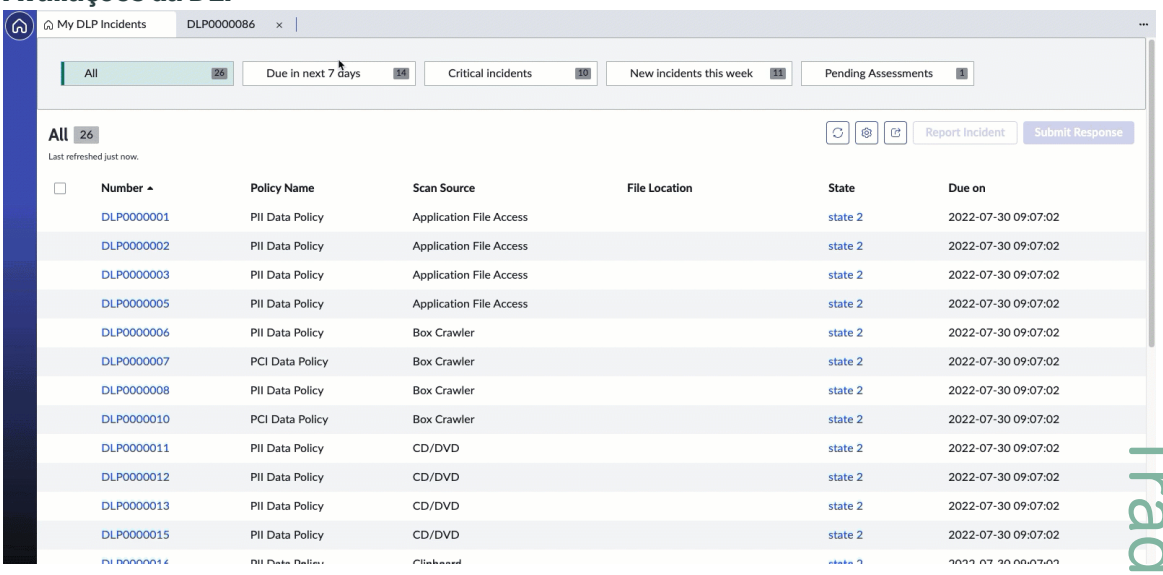
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em um número de avaliação específico para abri-lo.

b. Responda às perguntas de avaliação e clique em **Salvar** ou **Enviar** com base em suas necessidades.

Avaliações da DLP



5. Clique em **Instruções** Seção do cartão que é exibida na parte superior de todos os campos na exibição do formulário de incidente do DLP para exibir as informações adicionais sobre um incidente específico.

Nota: Esta seção no espaço orienta os usuários sobre as informações do incidente, o que ajuda a entender as próximas etapas da resolução do incidente.

O cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário. Clique em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais.

Para obter mais informações, consulte Criar modelos de instruções do usuário e Configurar instruções do usuário da IU do DLP.

Módulo Trabalhando com minhas aprovações

O módulo Minhas aprovações estará disponível no Espaço de usuários do DLP para os usuários conectados. Os usuários podem aprovar ou rejeitar as solicitações de aprovação de atribuição a partir daqui.

Antes de Iniciar

Função necessária:

- Usuário final
- Gerente
- Aprovador

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **Espaço do usuário do DLP**.
   . **Meus incidentes de DLP** a página será exibida em uma nova guia.
2. Clique em **Minhas aprovações** módulo presente em **Meus incidentes de DLP** módulo.
   A exibição da lista Minhas aprovações será exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O aprovador pode aprovar ou rejeitar as solicitações na exibição de lista de **Minhas aprovações** página. É possível aprovar ou rejeitar as várias solicitações da exibição de lista.

O aprovador pode exibir os detalhes da solicitação atribuída na exibição do formulário. Clicando em **Aprovar** ou **Rejeitar** Na exibição do formulário, é possível aprovar ou rejeitar a solicitação individual.

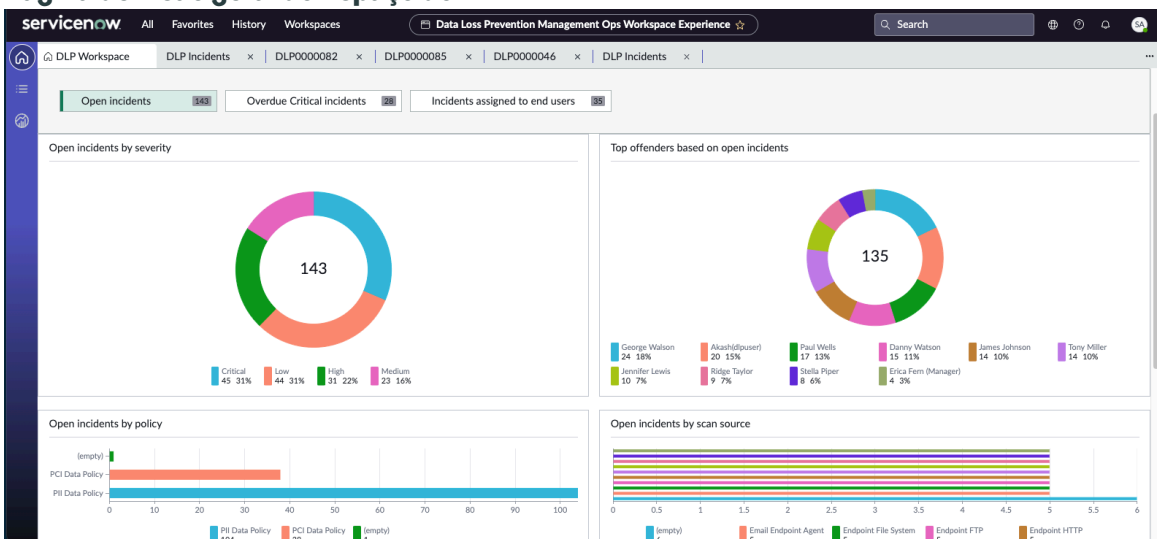
Nota: Para exibir os detalhes do incidente do DLP, clique em ícone de informações disponível no **Aprovar** campo.

Data Loss Prevention Incident Response Espaço do analista

Use Data Loss Prevention Incident Response(IR do DLP) Espaço do analista para exibir os incidentes do DLP. Atribua os incidentes aos usuários finais para resolução e muito mais.

O espaço do DLP consiste em uma página inicial com painéis, exibições de lista e exibições de formulário que permitem monitorar incidentes do DLP.

Página de visão geral do Espaço do DLP



Revise e atribua seus incidentes de DLP

Acesse Data Loss Prevention Incident Response(IR do DLP) Espaço do analista para que você possa revisar os incidentes do DLP e atribuí-los ou resolvê-los. Você pode rastrear tendências em incidentes por gravidade, principais infratores, incidentes por origem de verificação e incidentes por política.

Página inicial do Espaço do DLP

Visão geral do Espaço do DLP

Antes de Iniciar

Função necessária:

- sn_dLIR.analyst - Editar e exibir incidentes do DLP.
- sn_DLIR.analyst_read e sn_dLIR.read - Exibir incidentes do DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
   A página da lista de operações Meus incidentes do Espaço do DLP é aberta em uma nova guia.
2. Clique em **DLP Workspace** ícone página inicial para exibir a exibição da página inicial do espaço.
3. Revise os widgets do painel para identificar tendências por incidentes por gravidade, principais infratores, incidentes por origem de verificação e incidentes por política.
4. Clique nos filtros apropriados na página inicial para exibir os widgets por suas várias categorias.

Filtros	Descrição
Incidentes em aberto	Exibir todos os incidentes em aberto.
Incidentes críticos atrasados	Exiba os incidentes que têm o rótulo de gravidade crítica e que estão atrasados.
Incidentes atribuídos a usuários finais	Exiba os incidentes atribuídos aos usuários finais.

5. Você pode revisar e atribuir os incidentes do DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes de DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes de DLP ao fazer uma atualização.
Ações de Lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras** **Nota:** Quando você tem sua própria lista personalizada que é criada em **Minhas listas** configurada para o seu espaço, você também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para todos	Opção para copiar os URLs de todos os incidentes do DLP.
Mostrar painel do filtro	Opção para detalhar os incidentes necessários usando a opção de filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	i. Clique no filtro no canto superior esquerdo da página e selecione **Exibição avançada** . **ii.** Use um filtro existente ou crie o seu próprio adicionando condições que contenham um campo, um operador e valores. **iii.** Para adicionar mais condições, clique em **E.** ou **OU** : ▪ Se **E.** selecionado, todas as condições devem ser correspondidas. ▪ Se **OU** está selecionado, qualquer condição pode ser correspondida. **iv.** Clique em **Atualizar**.
Atribuir Incidente	Ação para determinar a quem atribuir o incidente do DLP. Estas são as opções: ▪ **Atribuir incidente a.** Opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário** Opção para determinar a qual usuário o incidente deve ser atribuído. ▪ **Resposta pré-usuário do estado do incidente** Opção para determinar em qual estado o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação** Opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitado, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação** Opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário** Opção para selecionar em qual estado o incidente do DLP deve estar depois que o usuário responder.
Responder	Responda a um incidente selecionando uma opção de resposta a incidente. Por exemplo, o usuário exclui um arquivo que viola uma política de DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar opções de resposta avançadas. Por

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	exemplo, **Solicitar liberação de e-mail da quarentena** .
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escalá-lo. Você também pode obter informações adicionais no campo Comentários.
Atualizar Estado	Ação para atualizar o estado do incidente. Você pode atualizar o estado do incidente selecionando um dos estados nas opções suspensas. Também pode ser um estado personalizado.
Fechar	Ação para fechar os incidentes. Selecione o correspondente **Código de fechamento** na lista suspensa e adicione comentários de fechamento. . **Fechar** recurso em Data Loss Prevention Incident Responseé feito de forma assíncrona e síncrona na exibição de lista. **i.** Fechamento síncrono: Ao fechar incidentes de forma síncrona, isso significa que a ação de fechamento é realizada imediatamente. Quando você seleciona vários incidentes para fechamento e se a contagem de incidentes for menor ou igual a 100, os incidentes serão encerrados em primeiro plano na exibição da lista Incidentes do DLP. 100 é o valor padrão. **ii.** Fechamento assíncrono: Isso implica que a solicitação de fechamento é enviada e a aplicação executa a solicitação em segundo plano se a contagem de incidentes selecionados for maior que 100. Você precisa atualizar a exibição da lista de incidentes do DLP para ver o status atualizado dos incidentes. **Nota:** ▪ A contagem de incidentes selecionados para fechamento assíncrono ou síncrono é configurada usando a propriedade do sistema *`sn_dlir.closure_sync_count_limit`* . ▪ Por padrão, a contagem de incidentes é definida como 100.

c. A segunda maneira é clicar em um incidente DLP específico para abri-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Detalhes** Guia: Exibe as seguintes seções:
  - **Detalhes** : Você pode exibir os detalhes do incidente do DLP, como Número do incidente, Severidade, Nome do arquivo e assim por diante. Você também pode modificar os campos Severidade, Estado, Usuário final e Grupo de Analistas DLP, respectivamente, e salvá-los.
  - **Compor** : Para adicionar comentários sobre o incidente do DLP visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privadas).
  - **Atividade** : Você pode exibir os detalhes das diferentes atividades no incidente do DLP.
  - **Anexos** : Se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo da sua unidade local.
- **Detalhes adicionais** Guia: Exibe todas as informações adicionais sobre o incidente do DLP, incluindo campos personalizados.

  Importante:
  - Campos personalizados para incidentes de DLP são compatíveis somente com a versão San Diego ou posterior.
  - Você pode usar **Detalhes adicionais** Para ver se algum campo personalizado foi criado para um incidente de DLP específico ou não.

- **Atributos personalizados** Guia: Exibe a lista de atributos personalizados relacionados ao incidente do DLP.
- **Outros incidentes do usuário final** : Exibe o incidente do mesmo usuário final. É possível consolidar incidentes executando o. **Adicionar como incidente secundário** ação desta lista relacionada.
- **Tipo de informações confidenciais detectadas** : Exibe as informações confidenciais detectadas pelo incidente.

  Nota: Esta lista relacionada está visível somente para os incidentes de DLP criados para integrações da Microsoft ou Symantec. No registro de incidente da Microsoft ou Symantec, sempre que o usuário acessa o registro do tipo de informação confidencial detectada, o conteúdo de correspondência realçado em relação a essa integração é exibido.

- **Incidentes secundários** : Exibe os incidentes secundários criados manualmente (executando a ação "Adicionar como incidente secundário") ou a partir das regras de consolidação do DLP. É possível desvincular o incidente secundário executando "Desvincular incidente secundário" desta lista relacionada.
- **Incidentes clonados** : Exibe os incidentes clonados do incidente primário. Clicando em **Incidente de clone** ação da exibição do formulário, você pode criar um novo incidente clonado.
- **Avaliações** Guia: Exibe a lista de avaliações atribuídas ao incidente do DLP.

d. Escolha a opção apropriada para você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Atribuir Incidente	Ação para determinar a quem atribuir o incidente do DLP. Estas são as opções: ▪ **Atribuir incidente a.** Opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário** Opção para selecionar a qual usuário o incidente deve ser atribuído. ▪ **Resposta pré-usuário do estado do incidente** Opção para selecionar em qual estado o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação** Opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitado, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação** Opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário** Opção para selecionar em qual estado o incidente do DLP deve estar depois que o usuário responder.
Cancelar aprovação	Ação para cancelar a solicitação de aprovação. Esta ação ficará visível para os analistas na exibição do formulário somente quando o Incidente do DLP estiver em **Aprovação pendente** estado. As opções disponíveis são: ▪ **Atribuir incidente a.** Opção para atribuir o incidente a ninguém, a um analista ou a outra pessoa. ▪ **Usuário** Opção para selecionar a qual usuário o incidente deve ser atribuído. ▪ **Estado do incidente pós-cancelamento** Opção para selecionar em qual estado o incidente deve estar depois de cancelar a solicitação. ▪ **Comentários** : Para fornecer detalhes adicionais para cancelamento.
Designar Avaliação	Ação para anexar uma avaliação ao atribuir o incidente. As opções são as seguintes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ **Modelo de avaliação** Opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário** Opção para selecionar em qual estado o incidente do DLP deve estar depois que o usuário responder.
Baixar arquivo	Ação para baixar o arquivo ou e-mail que tem o conteúdo violando. Esta ação pode ser executada para incidentes criados para o Microsoft OneDrive, SharePoint Online ou Exchange Online.
Salvar	Ação para salvar todas as mudanças feitas. Você tem a opção de modificar os campos Severidade, Estado e Usuário final do incidente do DLP e salvá-los.
Responder	Responda a um incidente selecionando uma opção de resposta a incidente. Por exemplo, o usuário exclui um arquivo que viola uma política de DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar as opções de resposta avançadas. **Por exemplo: Solicitar liberação de e-mail da quarentena** .
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escalá-lo. Você também pode obter informações adicionais no campo Comentários.
Clonar incidente	Ação para criar um incidente de clone se o registro de incidente afetar vários usuários. Você pode atribuir os incidentes clonados a várias partes interessadas, como jurídico/TI. Depois de criar um registro de incidente de clone, um novo **Incidentes clonados** A guia é criada no incidente primário do DLP e todos os incidentes clonados são listados nesta exibição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

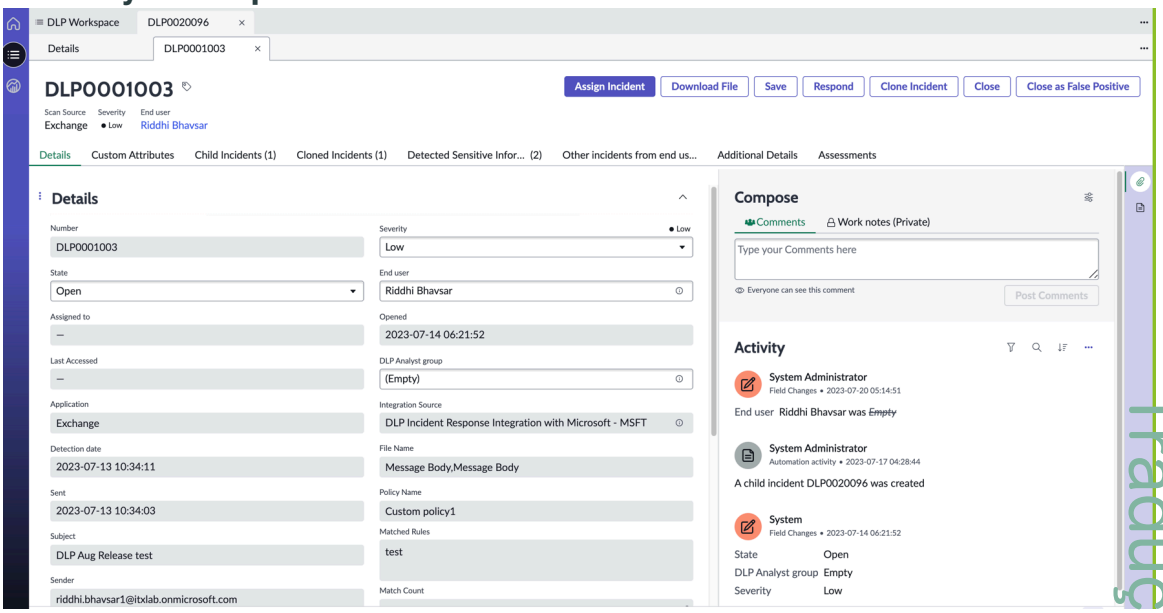
Opção	Descrição
	Nota: ▪ Se o registro de incidente do DLP primário estiver encerrado, todos os registros de incidente clonados serão encerrados automaticamente. ▪ Se um registro de incidente do DLP contiver um incidente clonado, ele não poderá ser atribuído aos usuários finais. Os registros de incidentes do DLP primário podem ser gerenciados somente por usuários com a função de analista. ▪ Você também tem uma opção para atualizar automaticamente o estado primário com base no estado dos incidentes clonados no módulo Configuração padrão. Por exemplo, se todos os incidentes clonados forem movidos para o estado escalado, o incidente primário também será movido para o estado escalado.
Fechar	Ação para fechar o incidente. Você deve selecionar o correspondente **Código de fechamento** na lista suspensa e adicione comentários de fechamento, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Fechar como falso positivo	Ação para fechar o incidente como falso positivo. Você também pode adicionar comentários adicionais antes de fechar o incidente.

DLP Analyst Workspace



6. Você pode ver a exibição de lista na página inicial indo para o canto superior esquerdo da página e clicando em **Listas** guia.
   A categoria Listas consiste nas páginas de lista padrão e personalizadas para incidentes do DLP.
   - **Listas** guia Listas padrão para incidentes de DLP. Estas são as listas padrão:
     - Tudo
     - Aberto
     - Meus incidentes
     - Atribuído ao meu grupo
     - Escalado
     - Atrasados(as)
     - Avaliações pendentes
     - Ação do usuário pendente
     - Incidentes clonados
     - Incidentes arquivados
   - **Minhas listas** guia : Exibe todas as listas renomeadas e todas as listas que você criou.

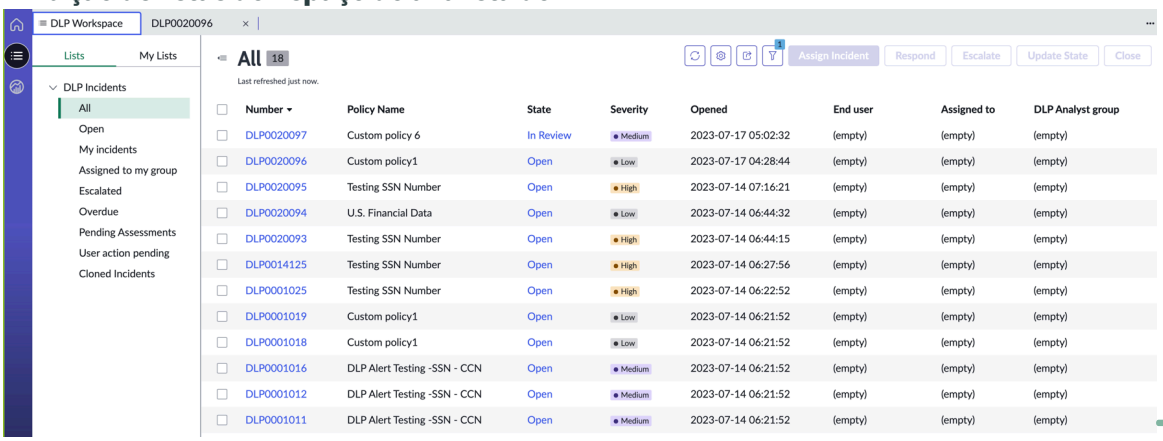
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example

O exemplo a seguir mostra o espaço do DLP com as categorias de exibição de lista. . **Todos** a opção de exibição de lista está selecionada.

Exibição de listas do Espaço do analista do DLP



Visualizar arquivos de evidência

Visualização Data Loss Prevention Incident Response Arquivos de evidência no espaço Analista de IR do DLP.

Antes de Iniciar

Importante: Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado. Se você não quiser armazenar os arquivos de evidência, desabilite o recurso de visualização de arquivos de evidência. Para obter mais informações, consulte Definir configurações avançadas.

Função necessária: sn_dLIR.analyst

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Na barra lateral contextual, selecione o ícone Arquivos de evidência ( ).
4. Em **Arquivos de evidência** , selecione **Arquivo de evidência** cartão para visualizar os arquivos de evidência no visualizador de documentos.

   O recurso de visualização é diferente para cada tipo de arquivo, conforme listado na tabela a seguir.

Formato do arquivo	Extensão de arquivo
Imagem	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg e .webp. Arquivos de imagem são abertos no modo de visualizador de documentos.
Microsoft Arquivos do Office	.doc, .docx, .ppt, .pptx, .xls, e .xlsx

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formato do arquivo	Extensão de arquivo
	Os arquivos do Office são abertos no modo de visualizador de documentos.
Arquivos de texto	.txt Arquivos de texto são abertos no modo de editor de texto.
Arquivos de e-mail	.eml **Nota:** O tamanho do arquivo deve ser inferior a 5 MB. Primeiro, você deve baixar o arquivo para visualizar seu conteúdo.
Arquivos PDF	.pdf ○ Insira uma palavra-chave para pesquisar o documento. ○ Recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade. ○ Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.

Nota:

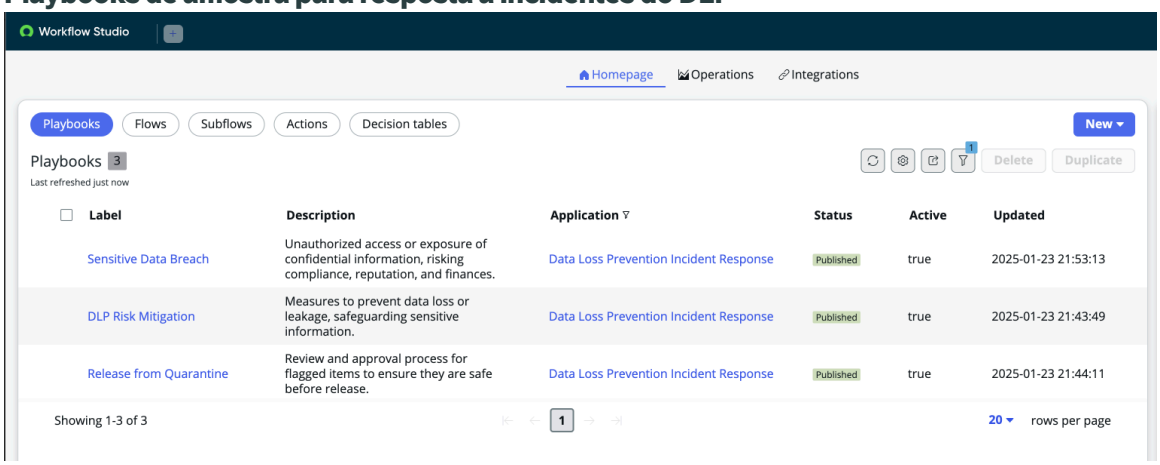
Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Playbook para Data Loss Prevention Incident Response

. Data Loss Prevention Incident Response O Playbook é um guia passo a passo para lidar com e mitigar incidentes de perda de dados, que podem incluir exposições não autorizadas, vazamentos ou violações de informações confidenciais que podem comprometer a segurança da sua organização.

A imagem a seguir mostra os playbooks de amostra disponíveis para DLP IR.

Playbooks de amostra para resposta a incidentes do DLP



Tradução automática

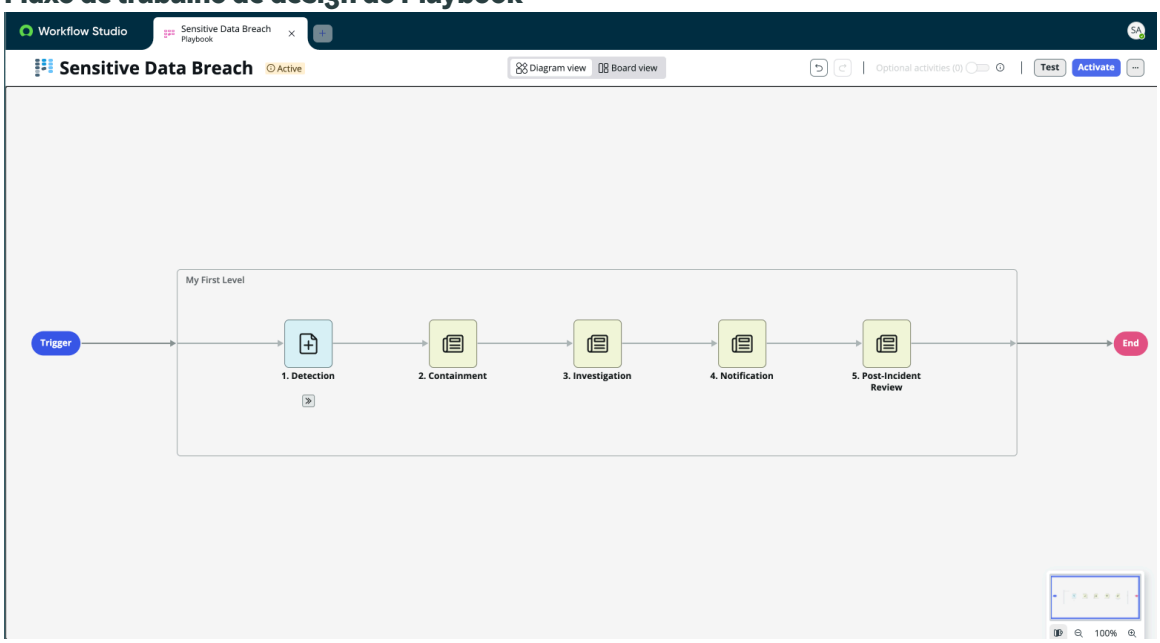
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir lista as atividades e fases disponíveis para criar um Playbook do DLP. Para obter mais informações, consulte Adicione um Playbook do DLP:

Atividade	Descrição
Detecção	Identificar e confirmar o acesso não autorizado ou a exposição de dados confidenciais.
Contenção	Isole sistemas ou usuários afetados para evitar mais vazamento de dados ou acesso não autorizado.
Investigação	Investigue a violação para entender como ela ocorreu, quais dados foram afetados e o possível impacto.
Notificação	Notifique equipes internas, partes interessadas externas e órgãos reguladores conforme exigido por lei ou política.
Correção	Aplique medidas corretivas para lidar com vulnerabilidades, atualizar políticas e evitar violações futuras.
Recuperação	Restaure sistemas a partir de backups seguros e valide a integridade dos dados pós-incidente.
Revisão pós-incidente	Analise o incidente para identificar as causas raiz, melhorar os controles de segurança e fortalecer as políticas.

A figura a seguir mostra o fluxo de trabalho de atividades e fases envolvidas na criação do Playbook de violação de dados confidenciais. As etapas do Playbook variam dependendo do fluxo de trabalho.

Fluxo de trabalho de design do Playbook



Tópicos relacionados

Adicione um Playbook do DLP

Cancelar um Playbook do DLP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicione um Playbook do DLP

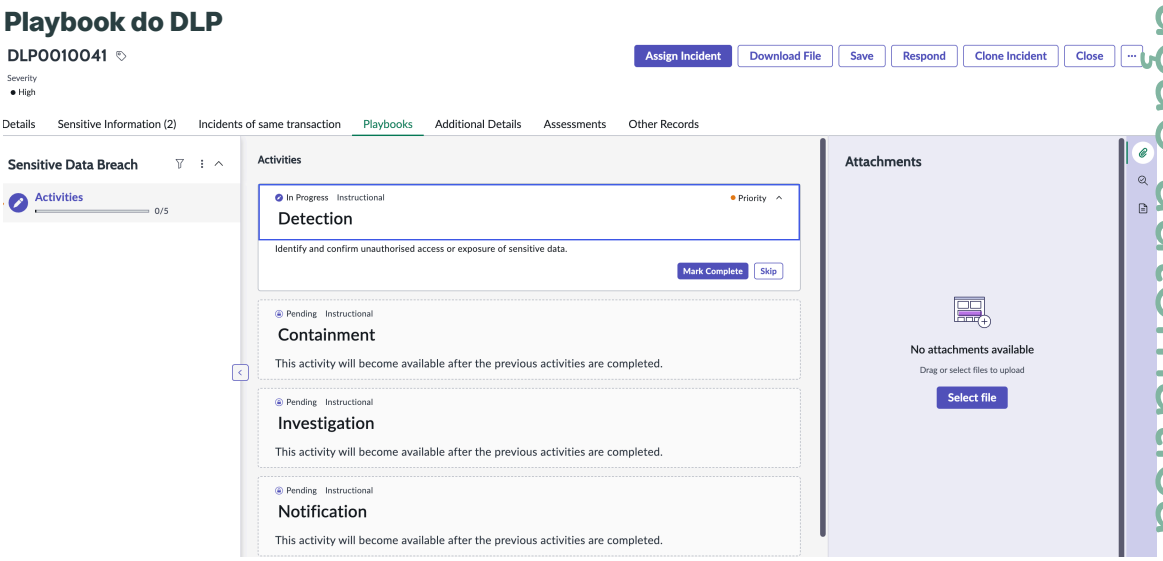
Adicione um Playbook no Data Loss Prevention Incident Response Espaço do analista que pode atuar como um guia para lidar e mitigar incidentes de perda de dados que podem comprometer a segurança da sua organização.

Antes de Iniciar

Função necessária: sn_dLIR.analyst - Adicione ou exiba playbooks no espaço do DLP.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Na página Espaço do analista do DLP - Meus incidentes, abra qualquer incidente do DLP.
3. Adicione o Playbook.
   a. Navegue até **Playbooks** guia.
   b. No menu Ações de IU, selecione o ícone Mais ações ( ) e selecione **Adicionar Playbooks** .
   c. Na caixa de diálogo, selecione um Playbook no menu suspenso.
   d. Selecione **Adicionar Playbooks** .
4. Selecione cada raia para explorar as tarefas que este Playbook executa.



Cancelar um Playbook do DLP

Cancelar um Data Loss Prevention Incident Response Playbook para interromper um fluxo de negócios quando ele não for mais válido.

Antes de Iniciar

Nota: Os playbooks são cancelados automaticamente quando o incidente de DLP associado é encerrado.

Função necessária: sn_dLIR.admin.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra qualquer incidente do DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegue até **Playbooks** guia.
4. No cabeçalho do Playbook que você deseja cancelar, selecione o ícone Ações do Playbook (⋮) e selecione **Cancelar Playbook** .
5. Forneça um motivo para cancelar o Playbook.
6. Selecione **Cancelar Playbook** .

Resultado

Uma faixa aparece abaixo do cabeçalho do Playbook confirmando que o Playbook foi cancelado.

Exibir incidentes de DLP arquivados

Use o espaço do analista de DLP para exibir os incidentes de DLP arquivados

Antes de Iniciar

Função necessária:

- sn_dLIR.analyst - Editar e exibir incidentes do DLP.
- sn_DLIR.analyst_read e sn_dLIR.read - Exibir incidentes do DLP.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
   Por padrão, a seção Meus incidentes é exibida.
2. Clique em **Incidentes arquivados** .
   A lista de incidentes de DLP arquivados é exibida.
3. Clique em **Mostrar Contagem de Incidentes** botão para exibir a contagem de incidentes arquivados.

   Nota:

   - Por padrão, a contagem de incidentes arquivados fica oculta para melhorar o tempo de carregamento da lista. Você deve clicar em **Mostrar Contagem de Incidentes** botão para exibir a contagem de incidentes. Uma mensagem informativa é exibida mostrando a contagem de incidentes.
   - A propriedade do sistema glide.ui.list.seismic.omit.count está habilitada no sistema de base para que os incidentes arquivados ocultem a contagem da lista de incidentes.

4. Selecione um ou mais incidentes de DLP que você deseja exibir.
   O incidente do DLP exibe a seção de detalhes do incidente.

   Nota:

   - . **Outros incidentes de usuários finais** também incluirá os incidentes arquivados.
   - **Corresponder conteúdo** é compatível com todos os incidentes arquivados (que também serão compatíveis com todas as integrações), mas **Arquivo de download** É compatível somente com integrações da Microsoft.

Painel da Data Loss Prevention Incident Response

. Data Loss Prevention Incident Response(IR do DLP) fornece uma visão geral de alto nível dos incidentes do DLP e das tendências diárias de incidentes em sua instância na forma de

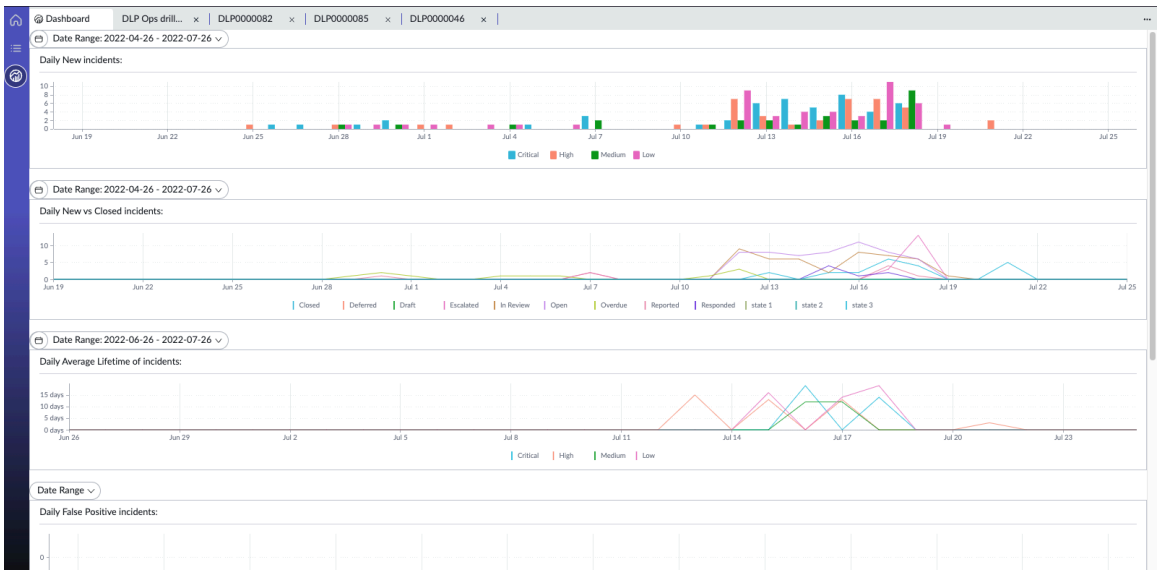
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

gráficos. Esses gráficos ajudam você a exibir, gerenciar e corrigir com eficácia os incidentes de DLP.

. Data Loss Prevention Incident Response O painel fornece informações importantes sobre seus incidentes de DLP diariamente. Você pode configurar indicadores e coletar regularmente snapshots de dados dos incidentes que correspondem às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel. Para analisar os incidentes do DLP em diferentes intervalos de tempo, você pode aplicar diferentes intervalos de datas.

Painel da DLP



Analise as tendências diárias de incidentes em seus incidentes de DLP

Acesse Data Loss Prevention Incident Response(IR do DLP) para analisar as tendências diárias em seus incidentes de DLP e corrigi-los com eficácia.

Antes de Iniciar

Função necessária:

- sn_dLIR.analyst - Editar e exibir incidentes do DLP.
- sn_DLIR.analyst_read e sn_dLIR.read - Exibir incidentes do DLP.

Por Que e Quando Desempenhar Esta Tarefa

Você pode visualizar as tendências diárias usando widgets no painel do DLP. Os dados ou estatísticas das tendências diárias de seus incidentes de DLP são coletados das propriedades do indicador de incidentes diários que são definidas pela sua organização. Você pode obter informações importantes aplicando diferentes intervalos de dados para analisar os incidentes do DLP em diferentes intervalos de tempo para os seguintes gráficos:

- **Novos incidentes diários** : Dados dos incidentes gerais do DLP criados diariamente, independentemente do estado dos incidentes. Os incidentes do DLP são categorizados com base nas gravidades, incluindo Média, Crítica, Alta e Baixa. Cada gravidade de incidente do DLP é representada por uma cor específica no gráfico.
- **Incidentes novos versus encerrados diários** : Os diferentes estados dos incidentes do DLP e uma comparação entre os novos incidentes diários e os incidentes encerrados diariamente. A categoria Novo diário inclui todos os incidentes do DLP em Aberto, Rascunho, Escalado, Em revisão, Atrasado, estados relatado, respondido ou personalizado (se houver). A categoria de incidente encerrado inclui os incidentes de DLP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

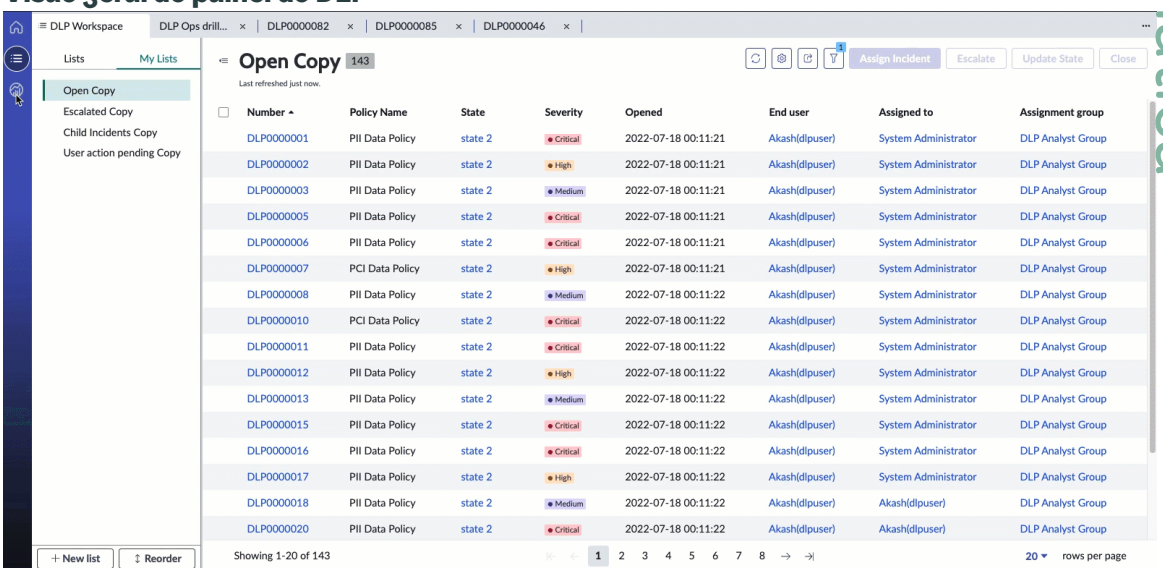
encerrados. Cada estado de incidente do DLP é representado por uma cor específica no gráfico.

- **Vida útil média diária dos incidentes** : A vida útil de um incidente é o período de tempo entre a abertura e o fechamento de um incidente DLP específico. A vida útil média diária é calculada somente para os incidentes de DLP encerrados.
- **Incidentes Falso-positivos diários** : Dados de todos os incidentes de DLP relatados como falsos positivos diários. Os incidentes falso-positivos diários são categorizados com base nas gravidades, incluindo Médio, Crítico, Alto e Baixo. Cada gravidade diária de incidente falso-positivo é representada por uma cor específica no gráfico.
- **Idade versus gravidade dos incidentes** Comparação de dados de todos os incidentes do DLP, categorizados pela idade e configurados com a gravidade dos incidentes do DLP. A categoria Idade inclui todos os incidentes de DLP abaixo da idade que sua organização define. Para obter mais informações sobre gráficos de idade, consulte Criar configurações de gráfico de idade. A gravidade dos incidentes inclui todos os incidentes do DLP na categoria Alta ou Baixa. Cada severidade é representada por uma cor específica no gráfico.
- **Incidentes escalados diários** : Dados de todos os incidentes de DLP escalados diariamente. Os incidentes escalados diários são categorizados com base nas gravidades, incluindo Média, Crítica, Alta e Baixa. Cada gravidade de incidente escalonada diária é representada por uma cor específica no gráfico.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **Painel da DLP**.
   A página Meu painel do DLP é exibida em uma nova guia do navegador.
2. Selecione um widget de painel para o qual você deseja executar uma análise de tendências diária.
   Por exemplo, o gráfico Novos incidentes diários.
3. Revise os widgets do painel para identificar tendências.
4. Clique em **Intervalo de datas** .

Visão geral do painel do DLP



5. Selecione um intervalo de datas no calendário e clique em **Aplicar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example
Por exemplo, o gráfico Novos incidentes diários é atualizado para o intervalo de dados selecionado.

6. Use os filtros abaixo do gráfico para detalhar e executar uma análise mais detalhada.

Integração de entrada para Data Loss Prevention Incident Response

Crie um ou vários incidentes de DLP usando a REST API de entrada.

Crie um único incidente do DLP

Função necessária: sn_dLIR.api_integration_user.

Para criar um único incidente do DLP, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
Cabeçalho de solicitação	**Aceitar:** `application/json` **Content-Type:** `application/json`
Carga de amostra	{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "",

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	"recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

Resposta de amostra	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Criar vários incidentes de DLP

Função necessária: sn_dLIR.api_integration_user.

Para criar vários incidentes de DLP a partir da mesma solicitação, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
Cabeçalho de solicitação	**Aceitar:** `application/json` **Content-Type:** `application/json`
Carga de amostra	{ "records": [

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

	{
	"file_name": "<value>",
	"file_modified_by": "<value>",
	"work_notes": "<value>",
	"url": "<value>",
	"scan_source": "<value>",
	"data_owner_email": "<value>",
	"file_created_by": "<value>",
	"file_owner": "<value>",
	"policy_name": "<value>"
	},
	{
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "<value>",
	"file_created": "<value>",
	"file_created_by": "<value>",
	"file_location": "<value>",
	"file_modified_by": "<value>",
	"file_name": "<value>",
	"file_owner": "<value>",
	}
	]
	}

Resposta de amostra	{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}

Nota: Por padrão, a transformação é assíncrona. Para definir a transformação síncrona, crie um novo registro na tabela REST Insert Multiple [sys_rest_insert_multiple], selecione a tabela de origem como **sn_dlir_incident_import** e defina a transformação como **síncrono** .

Integrações do DLP

. Data Loss Prevention Incident Response o sistema de base inclui integrações com pacotes de software de prevenção contra perda de dados de terceiros.

Esta seção fornece instruções para ativar os plug-ins e configurar ambos ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema de base inclui uma série de cartões para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências em Operações de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.

Data Loss Prevention Incident Response o oferece suporte aos seguintes pacotes de software de prevenção contra perda de dados de terceiros:

Symantec Integração para Data Loss Prevention Incident Response

. Symantec A integração do DLP oferece suporte à ingestão de Data Loss Prevention Incident Response incidentes criados no Symantec Data Loss Prevention Incident Response implantação. Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes do DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

. Symantec A integração do DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Esta integração inclui os seguintes recursos principais:

- Capacidade de criar vários perfis de integração para diferentes Symantec Endpoints de API.
- Ingestão programada de incidentes de DLP de Symantec em seu ServiceNow instância.
- Capacidade de aplicar filtros de API para recuperar os incidentes que correspondem aos critérios de filtro e também especificar o filtro para Symantec Incidentes do DLP que precisam ser importados.
- Mapeando os estados do incidente do DLP em seu ServiceNow A instância para o incidente do DLP estados em Symantec.
- Atualizar automaticamente o status do incidente em Symantec quando o estado muda em seu ServiceNow instância.
- Capacidade de personalizar e definir o mapeamento de gravidade entre incidentes do Symantec DLP com incidentes da ServiceNow.

Para saber mais sobre a integração, consulte Documentação do produto Symantec .

Introdução ao Symantec Integração do DLP para prevenção contra perda de dados

Antes de usar a integração, você deve baixá-la do ServiceNow® Store.

Check-list

Revise as informações a seguir antes de começar a configurar seu Symantec Integração do DLP para prevenção contra perda de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform Aplicação de prevenção de perda de dados, funções de aplicação MID.	As seguintes funções são usadas em Symantec Integração do DLP no ServiceNow AI Platform: • O administrador (admin) instala as aplicações do ServiceNow® Store E atribui o administrador de prevenção contra perda de dados (sn_dLIR.admin). • O usuário com a função sn_dLIR.admin pode configurar a integração e configurar os perfis de incidente. • Os usuários com a função sn_dLIR.analyst terão funções de leitura na integração.
Atribua o necessário Symantec Funções de usuário do DLP.	Revise Symantec Funções e permissões de integração do DLP.
Verifique se você está usando Symantec DLP 15,8	. Symantec A integração do DLP para prevenção contra perda de dados é testada com a versão 15,8 do Symantec Prevenção contra perda de dados. **Nota:** Certifique-se de que você está usando Symantec DLP 15,8
Verifique isso ServiceNow®aplicação principal necessária para oferecer suporte ao Symantec A integração do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative no aplicativo . • Security Support Common • Data Loss Prevention Incident Response

Instale e configure o. Symantec Integração do DLP para prevenção contra perda de dados

Instale e configure o. Symantec Integração do DLP do ServiceNow® Store em seu ServiceNow AI Platform instância. Comece a investigar incidentes de DLP usando Symantec Dados de incidentes do DLP.

Antes de Iniciar

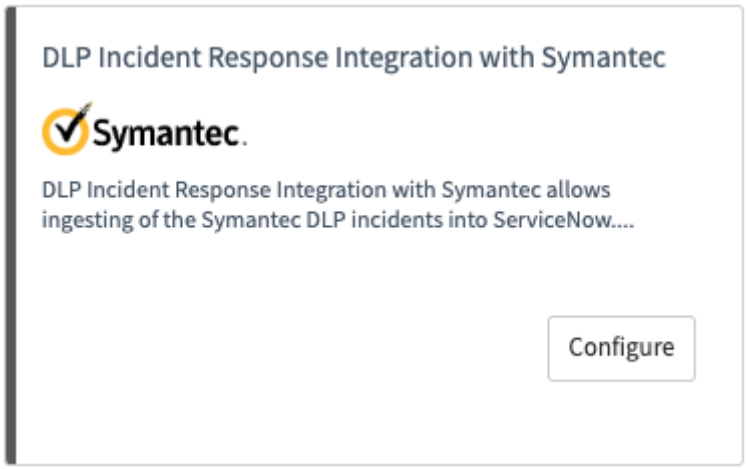
Função necessária: sn_dLIR.admin

Procedimento

1. Baixe o. Symantec Integração do DLP do ServiceNow® Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE a#Integração de resposta a incidentes do DLP comSymantec lado a lado e clique **Configurar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



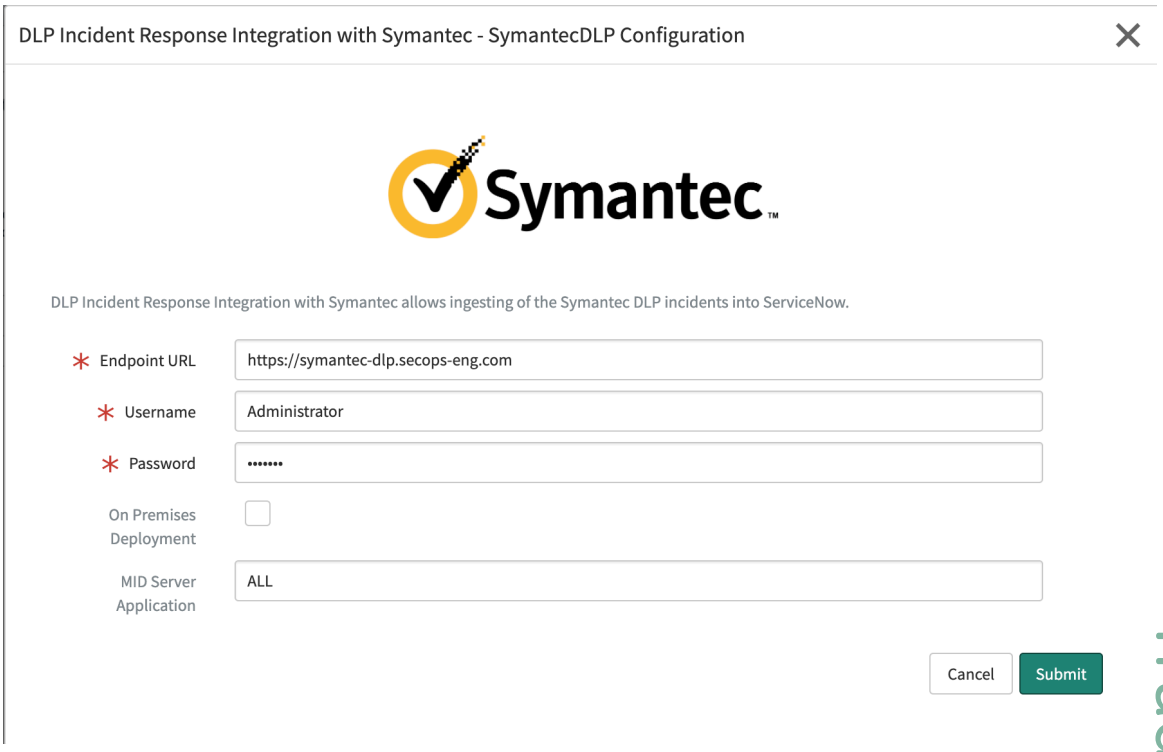
4. No formulário, preencha os campos.

Formulário Configuração de integração do Symantec DLP

Campo	Descrição
Nome	Nome do Symantec Configuração de integração do DLP.
URL de endpoint	Symantec Endpoint da REST API.
Nome do usuário	Symantec nome da conta. Para obter informações sobre as funções e permissões necessárias, consulte Funções e permissões .
Senha	Symantec senha da conta.
Implantação no local	Opção que você pode selecionar se for sua Symantecé implantado em uma instância no local. Ao selecionar esta opção, você deve usar o MID Server para se conectar à Symantec.
Aplicação do MID Server	O nome da aplicação MID que é usado para se comunicar com Symantec. Este campo é necessário quando você seleciona **Implantação no local** opção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.

Resultado

Nota: Conecte o subproduto symantec ao subproduto ServiceNow. Mantenha todos os nomes de usuário e senhas em sincronia nas instâncias para evitar que as contas sejam desconectadas.

Depois de validar e enviar a configuração com êxito, o Symantec A integração do DLP é salva na página Integrações de segurança como um bloco.

Crie um perfil para Symantec Integração do DLP

Crie um perfil de incidente em seu ServiceNow AI Platform instância. Determine Symantec Incidentes de DLP adequados para criar incidentes de DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Configure o. ServiceNow AI Platform®Para buscar os incidentes do DLP do Symantec endpoint. Armazene esses incidentes em seu ServiceNow® Instância como incidentes do DLP.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Perfil do incidente**.

2. Clique em **Nova**.

3. No formulário, preencha os campos na seção Nome.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

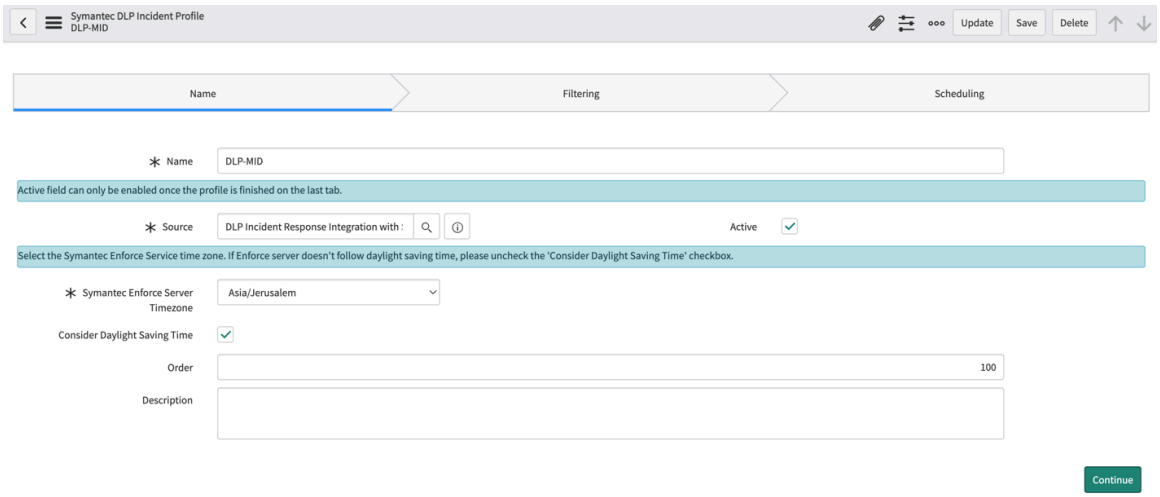
Crie um perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	Symantec Instância do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidente que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois que você clicar em **Concluir** Na seção Programação. Quando o perfil está ativo, isso implica que ServiceNow AI Platform está pesquisando ativamente Symantec Incidentes do DLP. Os incidentes do DLP correspondentes são criados no#DLP#quando as condições de filtragem são correspondidas com base nos parâmetros de programação fornecidos por você.
Fuso horário do servidor do Symantec Enforce	Selecione o fuso horário do servidor symantec Enforce no perfil para que os incidentes não sejam perdidos devido a problemas de fuso horário.
Considerar o horário de verão	Marque esta caixa de seleção se o servidor de imposição seguir o horário de verão.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição exclusiva deste perfil.



O que Fazer Depois

Para ir para a seção Filtragem,#clique em **Continuar** .

Defina filtros a serem aplicados à criação do incidente

Defina e defina condições de filtro para detalhar a entrada Symantec#Incidentes do DLP. Determine os incidentes que devem ser criados como incidentes do DLP em ServiceNow®.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

A filtragem ajuda a isolar incidentes de DLP e limitar o número de incidentes de DLP criados. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Selecione **Filtro baseado em API para ingestão de incidentes** Caixa de seleção para aplicar os filtros de API e recuperar os incidentes que correspondem aos critérios de filtro.
2. Adicione os filtros de API.
   A seguir está um exemplo que mostra os filtros de API.

```
{
        "operandOne": {
          "name": "incidentStatusName"
        },
        "filterType": "string",
        "operator": "EQ",
        "operandTwoValues": [
          "incident.status.New"
        ]
      }
```

Nota: Para obter mais informações sobre os filtros de API na integração da Symantec, consulte Listas de incidentes: Parâmetros - Detalhes do objeto da solicitação .

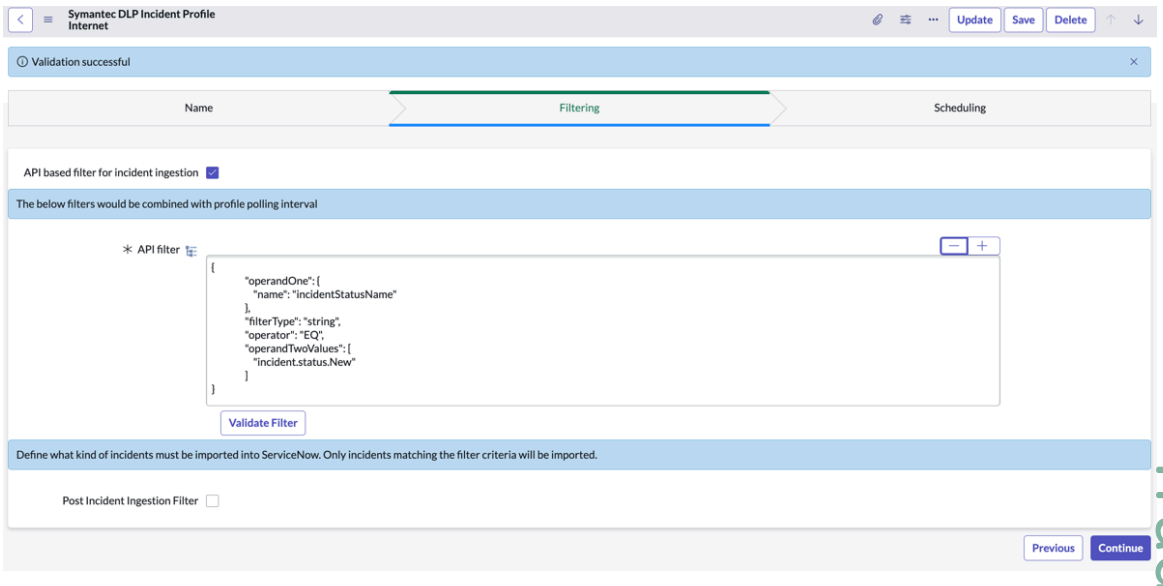
3. Clique em **Validar filtro** Depois de aplicar os filtros de API.

Tradução automática

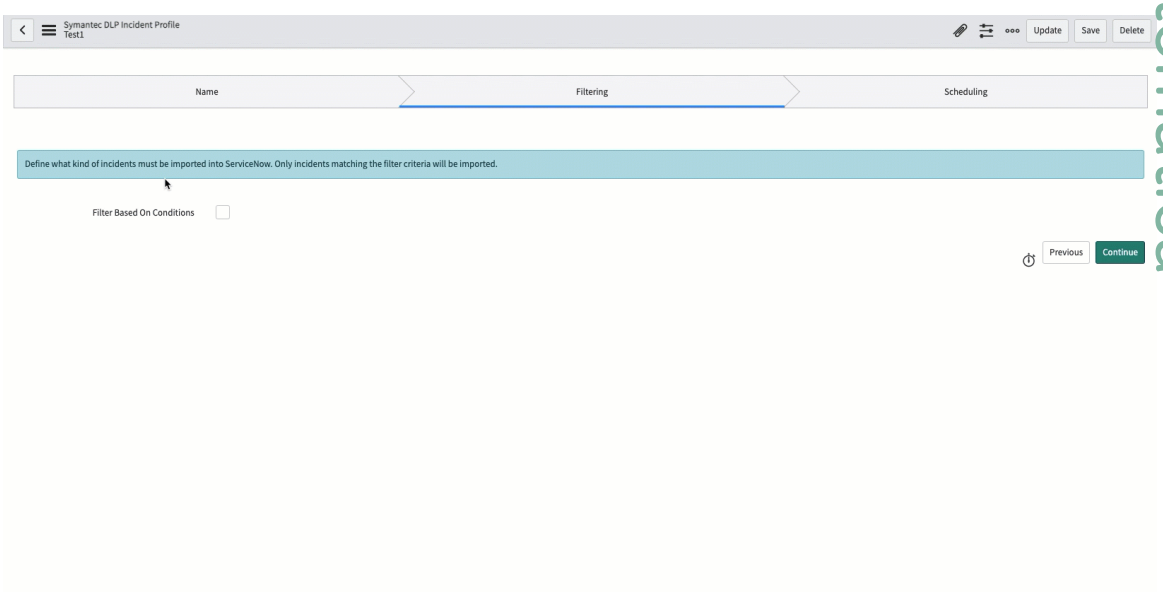
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se a validação não for bem-sucedida, uma mensagem de erro será exibida informando que a validação falhou e isso acontece quando os filtros não são inseridos corretamente de acordo com as APIs da Symantec.

Adicionando Filtros de API



4. Selecione **Filtro de ingestão pós-incidente** Caixa de seleção para definir os critérios que um incidente de entrada do Symantec DLP deve atender para que um incidente de DLP seja criado.
   As opções no primeiro campo em Condições de filtro correspondem aos campos que estão disponíveis no incidente do DLP. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
5. No Construtor de condições, defina os filtros no **Condições de filtro** campo.



6. Para adicionar mais condições, clique em **E.** #ou**OU** .
   - Se **E.** #selecionado, todas as condições devem ser correspondidas.
   - Se **OU** #está selecionado, qualquer condição pode ser correspondida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
Para configurar a programação, clique em **Continuar** .

Configurar o armazenamento de arquivos de evidências

Configure o armazenamento de arquivos de evidências para armazenar com segurança o arquivo de evidências dos incidentes do DLP.

Antes de Iniciar
Função necessária: sn_dLIR.admin

Verifique se o usuário Symantec que você está configurando para a integração do ServiceNow Symantec DLP deve ter as opções Corpo, Anexos e Mensagem original habilitadas na página de configuração Funções no portal Symantec DLP. Para obter mais informações, consulte a seção Atributos de exibição disponível em Configurar funções documento para obter mais informações.



Por Que e Quando Desempenhar Esta Tarefa
Você pode configurar o armazenamento de arquivos de evidências para armazenar arquivos com segurança. Isso fornece uma opção para armazenamento interno na instância da ServiceNow, garantindo que os arquivos sejam armazenados e criptografados usando a ServiceNow Criptografia de campo. Para obter mais informações, consulte Criptografia de campo Na documentação do NowPlatform.

Quando o analista de DLP executa a ação Baixar arquivos de evidência para incidentes de DLP no espaço do analista, o arquivo será baixado do armazenamento selecionado se a opção de armazenamento de arquivo de evidência estiver habilitada. Caso contrário, o arquivo será baixado diretamente da origem da Symantec e não persistirá na instância da ServiceNow.

Nota: Quando um analista de DLP executa a ação Baixar arquivos de evidência para incidentes de DLP no espaço do analista, o arquivo será baixado do armazenamento selecionado se a opção de armazenamento de arquivo de evidência estiver habilitada. Caso contrário, o arquivo será baixado diretamente da origem da Symantec e não persistirá na instância da ServiceNow.

Procedimento

1. Navegar até **Tudo** > **Integração da DLP da Symantec** > **Perfil do incidente**.
2. Clique em **Armazenamento de evidências** Formulário Perfil do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Armazenamento de arquivo de evidências** caixa de seleção para habilitar o armazenamento de arquivos.
4. Selecione o tipo de armazenamento preferencial.

Tipo	Descrição
Armazenamento de arquivos de evidências	Opção para habilitar o armazenamento do arquivo de evidências.
Tipo de armazenamento	Opção para selecionar o tipo de armazenamento preferencial. **Nota: Armazenamento da Service Now** : Isso armazenará os arquivos de evidência na instância da ServiceNow em um formato criptografado.

5. Clique em **Continuar** e mover para **Programação** seção.

Resultado
Os arquivos de evidência são armazenados de acordo com a configuração, após a conclusão da ingestão do incidente.

Baixar arquivos de evidência

Baixe arquivos de evidência de incidente DLP que violam a política de DLP na Symantec.

Antes de Iniciar
Baixe este arquivo em sua máquina local do espaço Analista do DLP IR e do espaço do usuário final do DLP IR. A ação Baixar arquivos estará disponível somente para os aprovadores no espaço Usuário final do DLP IR.

Função necessária:

- sn_dlir.analyst
- sn_dlir.secure_file_download (qualquer aprovador com esta função)

Procedimento

1. Navegar até **Tudo** > **Integração da DLP da Symantec** > **Configuração**.
2. Habilitar **O download do arquivo de violação do incidente relatado deve ser permitido** propriedade.
   Depois de habilitar esta propriedade, agora você poderá ver **Download do arquivo** Ação no Espaço do analista do DLP para qualquer incidente do Symantec DLP.
3. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
4. Abra um registro de incidente do DLP que é ingerido da origem da Symantec.
5. Clique em **Download do arquivo** .

   Nota: O arquivo que violou a política de DLP na Symantec será baixado para a máquina local do usuário.

   Para que o aprovador exiba a ação Baixar arquivo, siga as etapas mencionadas abaixo:

6. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **Espaço do usuário do DLP**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A página Meus incidentes do DLP será exibida em uma nova guia.

7. Selecione **Minhas aprovações** Módulo disponível no módulo Meus incidentes do DLP.
   A exibição da lista Minhas aprovações será exibida.
8. Abra um registro de solicitação de aprovação que é gerado para o incidente do Symantec DLP.
9. Clique no ícone de informações (i) disponível no campo Incidente do DLP na exibição do formulário.
10. Clique em **Download do arquivo** .

Resultado

Depois de executar esta ação, o arquivo de evidência no formato ZIP (se o incidente tiver violações em vários componentes e/ou os dados da mensagem original também estiverem disponíveis) ou um único arquivo (se o incidente tiver violações em um único componente ou somente os dados da mensagem original estiverem disponíveis) será baixado para a máquina local do usuário.

Nota: Como administrador do DLP, você pode controlar o acesso de **Download do arquivo** desabilitando o. **O download do arquivo de violação do incidente relatado deve ser permitido** . **Configurações avançadas** página. Para obter mais informações, consulte Defina configurações avançadas para Resposta a incidentes de prevenção contra perda de dados .

Visualizar arquivos de evidência

Visualização Data Loss Prevention Incident Response Arquivos de evidência no espaço Analista de IR do DLP.

Antes de Iniciar

Importante: Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado. Se você não quiser armazenar os arquivos de evidência, desabilite o recurso de visualização de arquivos de evidência. Para obter mais informações, consulte Definir configurações avançadas.

Função necessária: sn_dLIR.analyst

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Na barra lateral contextual, selecione o ícone Arquivos de evidência ( ).
4. Em **Arquivos de evidência** , selecione **Arquivo de evidência** cartão para visualizar os arquivos de evidência no visualizador de documentos.

   O recurso de visualização é diferente para cada tipo de arquivo, conforme listado na tabela a seguir.

Formato do arquivo	Extensão de arquivo
Imagem	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg e .webp. Arquivos de imagem são abertos no modo de visualizador de documentos.
Microsoft Arquivos do Office	.doc, .docx, .ppt, .pptx, .xls, e .xlsx

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formato do arquivo	Extensão de arquivo
	Os arquivos do Office são abertos no modo de visualizador de documentos.
Arquivos de texto	.txt Arquivos de texto são abertos no modo de editor de texto.
Arquivos de e-mail	.eml **Nota:** O tamanho do arquivo deve ser inferior a 5 MB. Primeiro, você deve baixar o arquivo para visualizar seu conteúdo.
Arquivos PDF	.pdf ○ Insira uma palavra-chave para pesquisar o documento. ○ Recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade. ○ Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.

Nota:

Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Programe o. Symantec Recuperação de incidentes do DLP

Defina uma programação para recuperar os dados do incidente e ingerir Symantec Incidentes do DLP que correspondem aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Symantec.

Antes de Iniciar
Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer recuperação única usando **Recuperação única** caixa de seleção. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho do Symantec Integração de incidentes do DLP. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

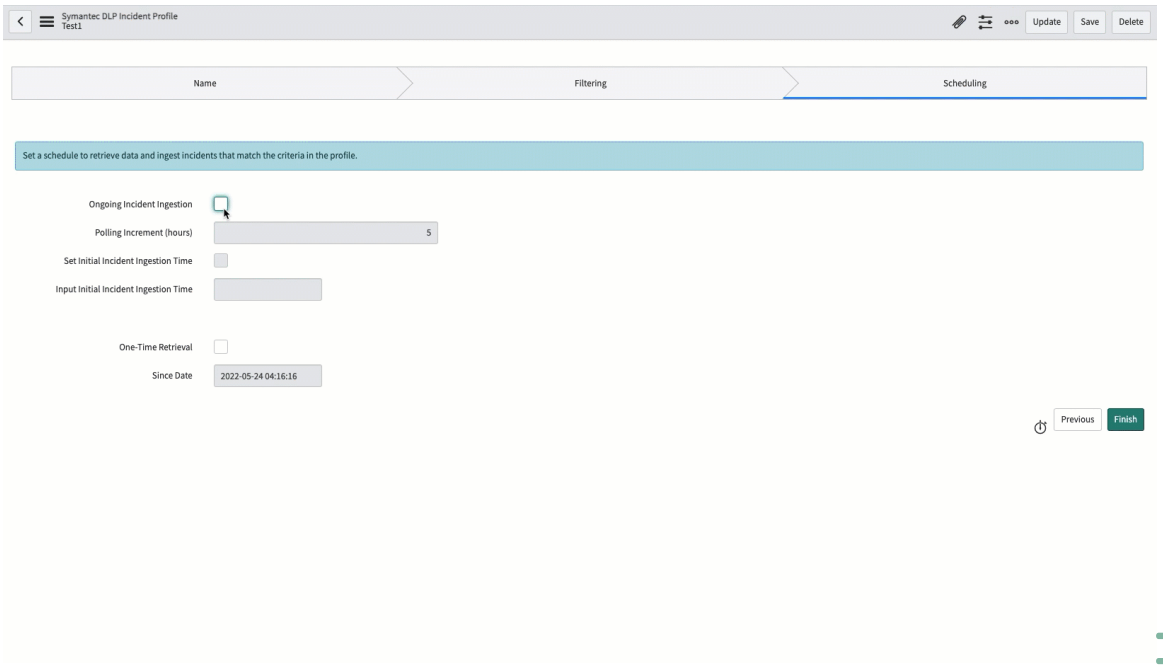
1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

Programar o incidente do DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidente em andamento que o ServiceNow AI Platform A instância extrai#novos incidentes da Symantec. Os incidentes de DLP serão criados se incidentes acionados forem encontrados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa definida em minutos. Este campo é definido automaticamente como 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora especificadas para a ingestão do incidente.
Horário de adição do incidente inicial	Primeira vez quando os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	Próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar extração única de dados históricos. Se este campo for selecionado, os dados históricos serão extraídos do Symantec DLP de acordo com a data adicionada em **A partir da data** campo.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Symantec. Este campo pode ser definido como no máximo três meses.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para salvar a configuração de perfil criada, clique em **Concluir** na janela pop-up.
4. Para ativar o perfil, abra o perfil criado.
5. Habilitar **Ativo** opção.
6. Clique em **Atualizar**.

Resultado
Após a criação e ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela Incidentes do DLP.

Mapeamento Symantec Status de incidentes do DLP com ServiceNow Status do incidente

Sincronize o status dos incidentes DLP ingeridos no ServiceNow Com os incidentes de DLP do Symantec. Mapeie o. **Status do incidente da ServiceNow** campo com **Status do incidente da Symantec** campo.

Antes de Iniciar
Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa
O status do incidente é recuperado dinamicamente do Symantec Origem do endpoint que é adicionada ao mapeamento. Você precisa executar um mapeamento de status de incidente individual.

Procedimento
1. Navegar até **Integração do Symantec DLP** > **Mapeamento de status do incidente**.
2. Forneça um **Nome** para identificar o mapeamento.
3. Selecione **Origem** integração de onde você deseja buscar o status.
4. Mapeie o. **Status do incidente do DLP** com **Status do incidente da Symantec** .

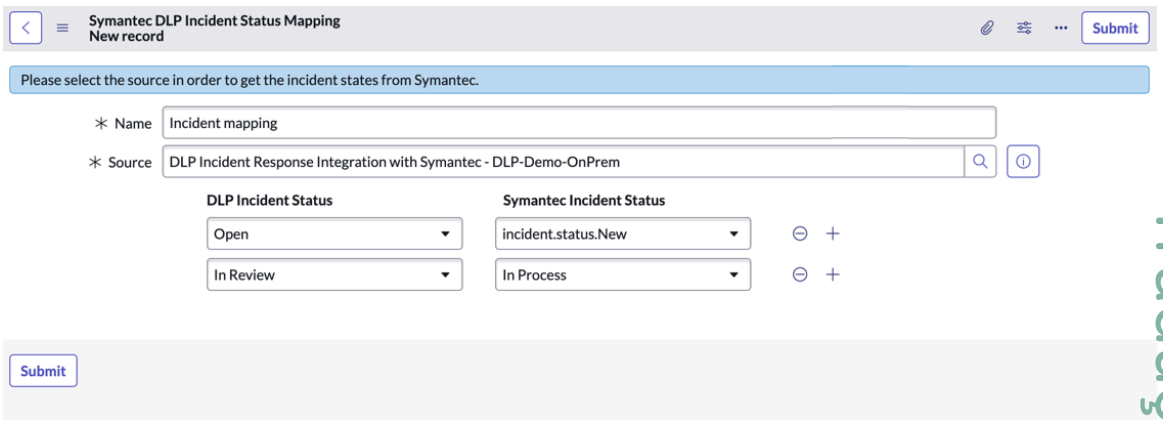
Nota: Não é necessário mapear todos os estados, você pode mapear somente os estados necessários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de status de incidentes do Symantec DLP

Campo	Descrição
Nome	Nome do registro de mapeamento.
Origem	A origem do Symantec Endpoint configurada de onde você deseja obter o status do incidente.
Status do incidente da DLP	Lista de status de incidentes do DLP.
Status do incidente da Symantec DLP	Lista de status obtido da origem (Endpoint Symantec).



5. Clique em **Enviar**.

Resultado

Depois de criar com sucesso o registro para status de mapeamento do ServiceNow incidentes, o. ServiceNow o status dos incidentes será sincronizado com Symantec Status de incidentes do DLP.

Se você mudar o status de qualquer incidente de DLP em seu ServiceNow e, em seguida, o status de associado Symantec Os incidentes do DLP serão alterados na origem Symantec plataforma baseada no mapeamento definido no registro.

Mapeamento de gravidade entre incidentes do Symantec DLP com incidentes da ServiceNow

Use o recurso de mapeamento de severidade para configurar e sincronizar o mapeamento entre Symantec incidentes e. ServiceNow AI Platform®incidentes.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

O mapeamento de gravidade do DLP permite mapear a gravidade de origem com a gravidade do incidente do DLP. Você pode personalizar e definir o valor de gravidade de origem e mapeá-lo para o valor de gravidade do incidente DLP desejado.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Mapeamento do incidente de gravidade**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

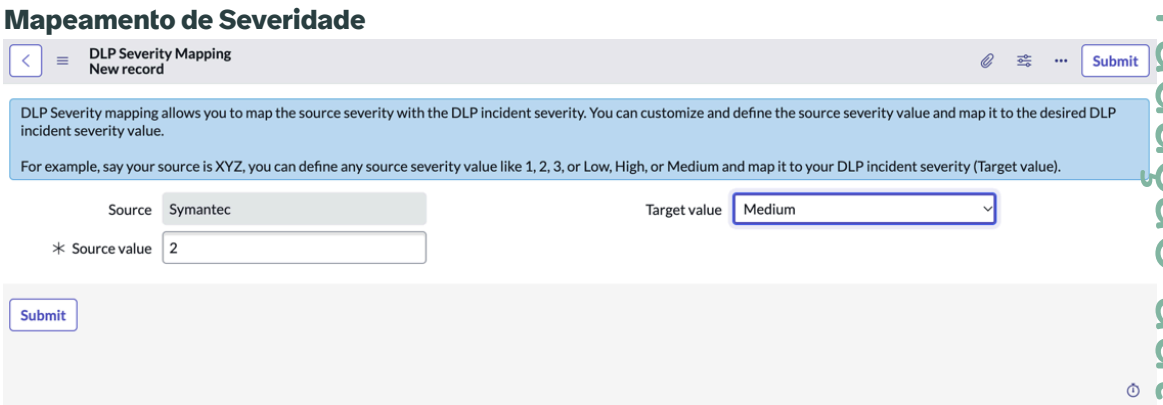
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de gravidade da DLP

Campo	Descrição
Origem	A origem do Symantec Endpoint configurada de onde você deseja buscar o incidente.
Valor de meta	O valor de destino é o ID de gravidade do incidente do DLP. Os valores disponíveis são Crítico, Alto, Médio, Baixo e Informações (usado como a gravidade das informações no Symantec).
Valor de Origem	O valor de origem é a gravidade do incidente da Symantec.

Nota: No sistema de base, há quatro mapeamentos de gravidade que são enviados para os usuários do DLP.

4. Clique em **Enviar**.



Configurar regras de resposta inteligente

Configure as regras de resposta inteligente da Symantec para executar ações de resposta nos incidentes do Symantec DLP ingeridos.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Verifique se o usuário da Symantec que você está configurando para a integração do ServiceNow Symantec DLP deve ter essas regras de resposta inteligente selecionadas em **Configuração de funções** página. Para obter mais informações, consulte **Ações** seção disponível em Configurar funções documento.

Para as regras de resposta inteligente buscadas, o administrador do DLP pode criar as regras de opção de resposta do incidente e os mapeamentos de opção de resposta para configurar as ações de resposta a serem realizadas nos incidentes do Symantec DLP ingeridos.

Procedimento

1. Navegar até **Tudo** > **Integração da DLP da Symantec** > **Regras de resposta inteligente**.
   Você pode ver todas as opções de resposta inteligente disponíveis para cada configuração de integração configurada. Para obter mais informações, consulte, Instale e configure o. Symantec Integração do DLP para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

prevenção contra perda de dados E siga o procedimento explicado para configurar a origem de configuração de integração da Symantec se não estiver configurada)

2. Clique em qualquer uma das Regras de resposta inteligente para abrir a exibição do formulário.

   Seguir Criar regras de opção de resposta a incidentes Para criar regras de opção de resposta do incidente e mapeamentos de opção de resposta para exibir esta regra de resposta inteligente no modal de resposta do espaço do DLP.

3. Crie as regras de aprovação para a regra de resposta inteligente usando **Regras de aprovação** Na lista relacionada ou seguindo o procedimento explicado na seção Configurar regras de aprovação.
   As regras de aprovação para cada regra de resposta inteligente estarão visíveis na lista relacionada Regras de aprovação.
4. Depois de criar as regras de opção de resposta do incidente, você pode ver o registro na lista relacionada do registro de regra de resposta inteligente.
5. Use **Atualizar regra de resposta inteligente** botão na exibição de lista para atualizar manualmente a origem.
   As regras de resposta inteligente adicionarão, atualizarão ou excluirão automaticamente todos os dias para cada origem.

Execute regras de resposta inteligente

Use este recurso para executar regras de resposta inteligente para os incidentes do Symantec DLP.

Antes de Iniciar

Você precisa configurar as regras de resposta inteligente seguindo o procedimento explicado aqui nesta seção, Configurar regras de resposta inteligente.

Função necessária: sn_dLIR.admin

Nota:

As opções de resposta no espaço estarão disponíveis para o usuário final, analista ou gerente com base na configuração mencionada na seção Configure a opção de resposta para seus incidentes de DLP.

Procedimento

1. Navegar até **Tudo** > **DLP** > **Espaço do usuário do DLP**.
2. Abra qualquer incidente do Symantec DLP.
3. Clique em **Responder** .
4. Selecione a opção de resposta na lista suspensa Resposta.
   As opções de resposta estarão visíveis com base na configuração do **Regra de opção de resposta do incidente** e. **Mapeamentos de opção de resposta** .
5. Clique em **Enviar**.

Nota: Você também pode configurar as regras de aprovação para as Opções de resposta seguindo o procedimento explicado em Criar regras de aprovação seção. Quando uma regra de aprovação é configurada para a regra de resposta inteligente, o fluxo de aprovação será acionado primeiro e, depois de receber todas as aprovações, o fluxo de opção de resposta inteligente será acionado. O estado do incidente do DLP será atualizado de acordo com o estado de destino do mapeamento de opção de resposta após a execução bem-sucedida da opção de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o. Symantec#Configurações de integração do DLP

Modifique o. Symantec#Propriedades do sistema padrão de integração do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

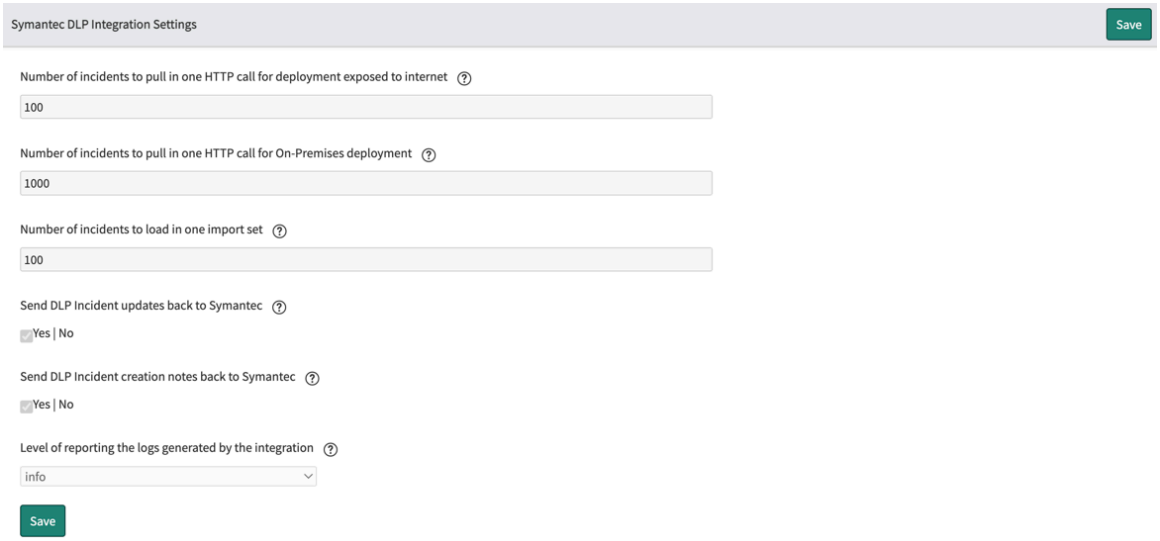
1. Navegar até **Integração da DLP da Symantec** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Configurações

Campo	Descrição
Impor um limite no número de incidentes para extrair uma chamada HTTP para implantação no local sn_sym_dlp.page_size_on_rem	Número máximo de incidentes a serem obtidos em uma chamada HTTP para implantação no local de Symantec. ○ Tipo: inteiro ○ Valor padrão: 1000
Impor um limite no número de incidentes para extrair uma chamada HTTP para implantação exposta à internet sn_sym_dlp.page_size_on_internet	Número máximo de incidentes a serem obtidos em uma chamada HTTP para Symantec implantação exposta à internet. ○ Tipo: inteiro ○ Valor padrão: 100
Número de incidentes a serem carregados em um conjunto de importação sn_sym_dlp.incidents_per_attachment	Número de registros a serem armazenados em um arquivo de anexo para processamento. ○ Tipo: inteiro ○ Valor padrão: 100
Envie atualizações de incidentes DLP de volta para o Symantec sn_sym_dlp.incident_update	Esta propriedade permite restringir qualquer sincronização de estado entre ServiceNow e. Symantec Incidentes do DLP. ○ Tipo: booleano ○ Valor padrão: **verdadeiro**
Envie as anotações de criação de incidente DLP de volta para o Symantec sn_sym_dlp.incident_creation_notes	Esta propriedade permite que você envie uma anotação de volta para a Symantec assim que um incidente é criado em ServiceNow. ○ Tipo: booleano ○ Valor padrão: **verdadeiro**
Nível de emissão de relatórios dos logs gerados pela integração sn_sym_dlp.logging.verbosity	Propriedade que define a emissão de relatórios dos logs gerados pela integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Salvar**.

Separação de domínios no Symantec Integração do DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com Symantec Integração do DLP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute Symantec Procedimentos de integração do DLP no domínio apropriado.

Integração de resposta a incidentes de prevenção contra perda de dados com Proofpoint

. Proofpoint A integração do DLP oferece suporte à ingestão de incidentes de prevenção contra perda de dados criados no Proofpoint Implantação da prevenção contra perda de dados. Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes do DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

. Proofpoint A integração do DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta integração inclui os seguintes recursos principais:

- Criação de vários perfis para diferente Proofpoint endpoints.
- Automatizar a criação de incidentes de DLP.
- Mapeamento do Proofpoint Campo de estado de incidente do DLP para o campo de estado de incidente do DLP.
- Filtragem de Proofpoint Incidentes do DLP.
- Ingestão de incidentes em seu ServiceNow instância assim que os incidentes são criados em Proofpoint Locatário do DLP.
- Proofpoint A integração do DLP é compatível com endpoints e tipos de e-mail de incidentes.
- Atualizações automáticas do Proofpoint Status e comentários do incidente do DLP para criação de incidente do DLP e para mudança de estado e fechamento em ServiceNow lado.

Conheça esta integração

Identificador do documento	Título do documento
Proofpoint site de documentação do produto	Documentação do produto Proofpoint
ServiceNow® site de documentação do produto	Site de documentação do produto da ServiceNow

Introdução ao Proofpoint Integração para prevenção contra perda de dados

. Proofpoint A integração do DLP oferece suporte à ingestão de incidentes de prevenção contra perda de dados criados no Proofpoint Locatário de prevenção contra perda de dados. Após a ingestão, as funcionalidades de gestão de incidentes que corrigem os incidentes do DLP serão usadas.

Check-list

Revise as informações a seguir antes de começar a configurar seu Proofpoint Integração do DLP para prevenção contra perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform e. Data Loss Prevention Incident Response funções da aplicação.	As funções a seguir são usadas em Proofpoint Integração do DLP no ServiceNow AI Platform: • O administrador (admin) instala as aplicações do ServiceNow® Store E atribui o administrador de prevenção contra perda de dados (sn_dLIR.admin). • O usuário com a função sn_dLIR.admin pode configurar a integração e definir os perfis de incidente. • Os usuários com a função sn_dLIR.analyst têm funções de leitura na integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
Atribua o necessário Proofpoint Funções de usuário do DLP.	Revise Proofpoint Funções e permissões de integração do DLP.
Verifique se você está usando Proofpoint DLP 1.0.1 ou posterior.	. Proofpoint A integração do DLP para prevenção contra perda de dados é testada com Proofpoint Prevenção contra perda de dados, versão 1.0.1 ou posterior.
Verifique se a aplicação principal do usuário final é necessária para oferecer suporte ao Proofpoint A integração do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas a partir de ServiceNow Store. Se não estiver instalado, instale e ative no aplicativo . • Security Support Common • Data Loss Prevention Incident Response

Instale e configure o. Proofpoint Integração para prevenção contra perda de dados

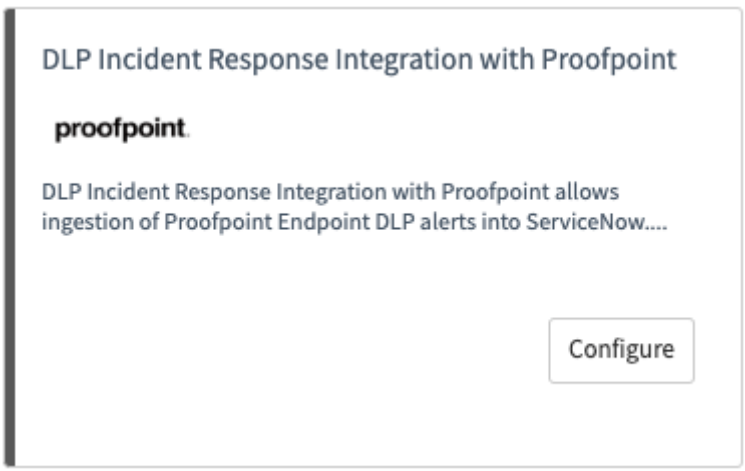
Instale e configure o. Proofpoint Integração do DLP do ServiceNow® Store em seu ServiceNow AI Platform instância. Comece a investigar incidentes de DLP usando Proofpoint Dados de incidentes do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Baixe o. Proofpoint Integração do DLP do ServiceNow® Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. PESQUISE Integração de resposta a incidentes do DLP com o Proofpoint lado a lado e clique **Configurar** .



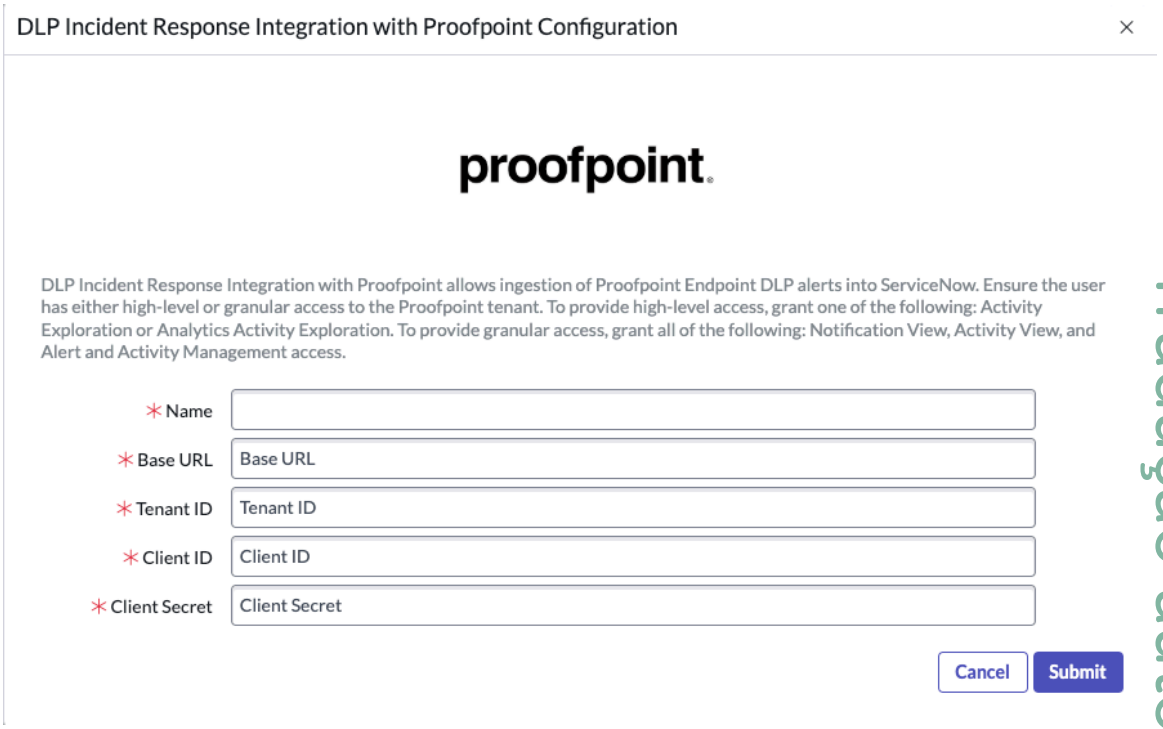
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proofpoint Formulário Configuração de integração do DLP

Campo	Descrição
Nome	Nome do Proofpoint Configuração de integração do DLP.
URL base	URL do Proofpoint Que serve como endpoint REST.
ID de cliente	O ID de Proofpoint cliente a ser usado.
Segredo do cliente	O segredo configurado para sua conta de usuário em Proofpoint.



Nota: Para os clientes existentes, continuamos a oferecer suporte à Autenticação básica para garantir que os blocos secundários existentes que têm autenticação básica funcionem conforme o esperado. No entanto, se um cliente quiser adicionar OAuth a um bloco secundário, ele não deverá remover as credenciais de Autenticação básica existentes (nome de usuário e senha). Embora eles possam substituir esses valores por entradas fictícias, deixar os campos vazios impedirá que o bloco seja enviado com sucesso.

5. Clique em **Enviar**.

Resultado

Depois de validar e enviar a configuração com êxito, o Proofpoint A integração do DLP é salva na página Integrações de segurança como um bloco.

Configure o webhook no Proofpoint Locatário do DLP para notificações de alerta para ServiceNow

Configurar um webhook em Proofpoint Usando o endpoint da REST API para começar a receber os alertas do Proofpoint Locatário do DLP. . ServiceNow A instância cria incidentes de DLP a partir desses alertas. . Proofpoint A integração do DLP fornece um endpoint da REST API para que os usuários finais configurem o webhook.

Antes de Iniciar

Função necessária: sn_pp_dlp.api_integration_user

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login em **Proofpoint** .
2. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Integração** > **Políticas de notificação**.
3. Crie uma política de notificação com um nome apropriado.
4. Clique em **Política de notificação** e gerenciam os webhooks configurados na política de notificação.
5. Clique em para criar uma nova configuração de webhook **Adicionar webhooks** .
6. Selecione o tipo de webhook como **Genérico** .
7. Em Entrada de URL, insira uma URL usando o formato: `https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts` .
8. Mantenha o método como **PUBLICAR** .
9. Adicione os seguintes cabeçalhos ao webhook:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. Não mude os outros valores.
11. Clique em **Salvar**.
12. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Políticas** > **Regras**.
13. Na seção Ações, selecione as regras para as quais a notificação do webhook deve ser gerada.
14. Adicione as políticas de notificação recém-criadas que tenham um webhook configurado.
15. Clique em **Salvar**.

Crie uma aplicação em Proofpoint E obter Credenciais do cliente

Crie uma aplicação em Proofpoint e definem as configurações necessárias para obter credenciais do cliente. Essas credenciais permitem o acesso seguro à API do Proofpoint para integração e automação perfeitas.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login no Proofpoint Console.
   Acesse Proofpoint Console usando suas credenciais.
2. Criar uma nova aplicação.
   a. Em **Desenvolvedor** , selecione Autorização.
   b. Selecione **Criar**.
   c. Insira um nome de aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Em Escopos permitidos, adicione escopos à sua aplicação conforme necessário.

e. Em Concessões permitidas, selecione **Credenciais do cliente** .

f. Selecione **Save** (Salvar).
O ID do cliente e o segredo do cliente são gerados.

3. Configurar detalhes da aplicação.

a. Selecione a aplicação recém-criada.

b. Em Políticas de acesso, selecione **Editar** .

Selecione Políticas de acesso de alto nível ou granular.

c. Clique em **Done** (Concluído).

Resultado

Use o ID do cliente e o segredo do cliente gerados para configurar a integração no DLP Proofpoint(PPT) e começar a usá-lo.

Criar um perfil para Proofpoint Integração do DLP

Crie um perfil de incidente em seu ServiceNow AI Platforminstância. Determine Proofpoint Incidentes de DLP adequados para criar incidentes de DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Configure o. ServiceNow AI PlatformPara preencher alertas do DLP de Proofpoint. Armazene os alertas como incidentes de DLP em seu ServiceNow instância.

Procedimento

1. Navegar até **Integração do Proofpoint DLP** > **Perfil do incidente**.

2. Clique em **Nova**.

3. No formulário, preencha os campos em **Nome** seção.

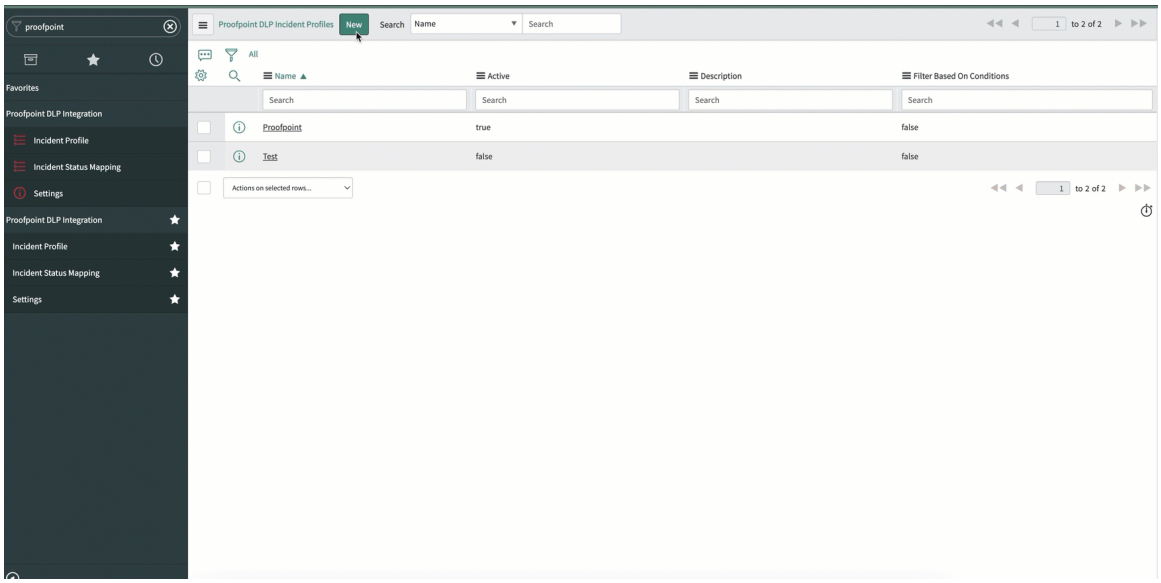
Crie um perfil para Proofpoint Formulário de integração do DLP

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda você a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	. Proofpoint Instância do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	apropriada para os tipos de incidente que você planeja ingerir para o perfil.
Ativo	Opção para ativar o perfil. Quando o perfil está ativo, seu ServiceNow AI Platform a instância está pronta para receber os incidentes de Proofpoint.
Descrição	Descrição para ajudar a distinguir este perfil de outros perfis.



4. Clique em **Continuar** E mover para a seção Filtragem.

Defina filtros a serem aplicados à criação do incidente

Defina e defina condições de filtro para filtrar a entrada Proofpoint#Incidentes do DLP. Controle em quais incidentes de DLP devem ser criados ServiceNow®.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Esse tipo de filtragem ajuda a isolar incidentes de DLP e limitar o número de incidentes de DLP criados. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

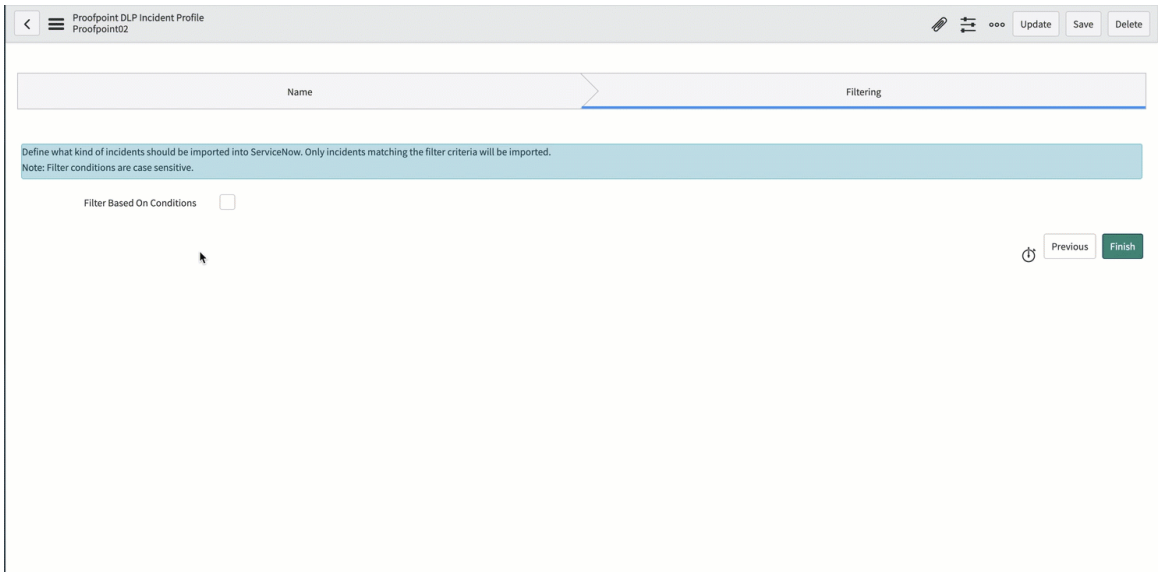
Procedimento

1. Selecione **Filtro com base em condições** e defina os critérios que um de entrada Proofpoint O incidente de DLP deve atender para que um incidente de segurança seja criado.
2. Usando as listas e os campos do construtor de condições, defina os filtros no **Condições de filtro** campo.

   As opções no primeiro campo em **Condições de filtro** Corresponde aos campos que estão disponíveis no incidente do DLP. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em para adicionar mais condições **E.** #ou**OU** .
   - Se **E.** #selecionado, todas as condições devem ser correspondidas.
   - Se **OU** #está selecionado, qualquer condição pode ser correspondida.
4. Clique em **Concluir**.

Visualizar arquivos de evidência

Visualização Data Loss Prevention Incident Response Arquivos de evidência no espaço Analista de IR do DLP.

Antes de Iniciar

Importante: Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado. Se você não quiser armazenar os arquivos de evidência, desabilite o recurso de visualização de arquivos de evidência. Para obter mais informações, consulte Definir configurações avançadas.

Função necessária: sn_dLIR.analyst

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Na barra lateral contextual, selecione o ícone Arquivos de evidência ( ).
4. Em **Arquivos de evidência** , selecione **Arquivo de evidência** cartão para visualizar os arquivos de evidência no visualizador de documentos.

   O recurso de visualização é diferente para cada tipo de arquivo, conforme listado na tabela a seguir.

Formato do arquivo	Extensão de arquivo
Imagem	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg e .webp. Arquivos de imagem são abertos no modo de visualizador de documentos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formato do arquivo	Extensão de arquivo
Microsoft Arquivos do Office	.doc, .docx, .ppt, .pptx, .xls, e .xlsx Os arquivos do Office são abertos no modo de visualizador de documentos.
Arquivos de texto	.txt Arquivos de texto são abertos no modo de editor de texto.
Arquivos de e-mail	.eml **Nota:** O tamanho do arquivo deve ser inferior a 5 MB. Primeiro, você deve baixar o arquivo para visualizar seu conteúdo.
Arquivos PDF	.pdf ○ Insira uma palavra-chave para pesquisar o documento. ○ Recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade. ○ Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.

Nota:

Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Mapa Proofpoint Status de incidentes do DLP com ServiceNow status do incidente

Sincronize o status dos incidentes DLP ingeridos em seu ServiceNow Incidentes de DLP e instância do Proofpoint. Mapeie o. ServiceNow Status do incidente com Proofpoint Status do incidente.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

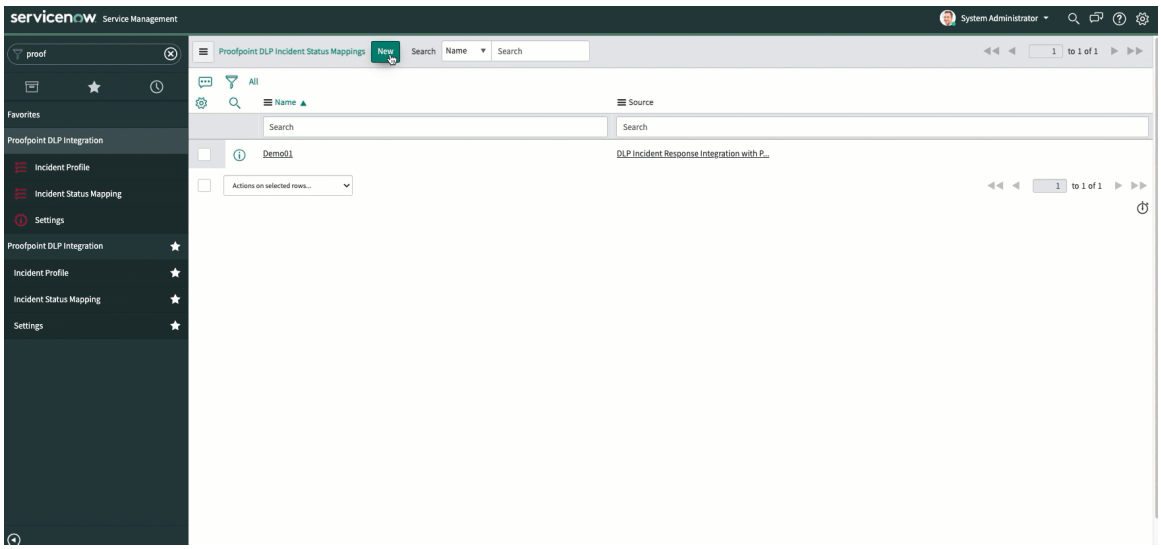
1. Navegar até **Integração do Proofpoint DLP** > **incidente** > **Mapeamento do status do incidente**.
2. Forneça um **Nome** para identificar o mapeamento.
3. Selecione **Origem** Bloco (configuração de integração) ao qual o Mapeamento de status deve ser aplicado.
4. Mapeie o. **Status do incidente do DLP da ServiceNow** com **Status do incidente do Proofpoint** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeie o status de incidentes do Proofpoint DLP com o formulário de status de incidente da ServiceNow

Campo	Descrição
Nome	Espaço reservado para o registro de mapeamento.
Origem	Configurado Proofpoint Origem do endpoint de onde você deseja buscar o status do incidente.
Status do incidente da ServiceNow	Lista de status de incidentes do DLP.
Status do incidente do Proofpoint	Valores mapeados padrão para estados padrão disponíveis em incidentes do DLP. Para estados personalizados, o padrão Proofpoint o status é **Novo** . Você pode modificar e adicionar o necessário Proofpoint status no campo de entrada.



5. Clique em **Enviar**.

Resultado

Um registro para mapeamento foi criado com sucesso. Os status do ServiceNow os incidentes serão sincronizados com Proofpoint Incidentes do DLP.

Quando você altera o status de qualquer incidente de DLP em seu ServiceNow e, em seguida, o status do associado Proofpoint O incidente do DLP será alterado na origem Proofpoint plataforma de acordo com o conjunto de mapeamento no registro.

Configurar Proofpoint Configurações de integração do DLP

Modifique o. Proofpoint#Propriedades do sistema padrão de integração do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Navegar até **Integração com o Proofpoint da DLP** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tempo limite máximo para chamadas HTTP sn_pp_dlp.maximum_http_time_out	Tempo limite máximo para chamadas HTTP (em segundos). ○ Tipo: inteiro ○ Valor padrão: 30
Envie atualizações de incidentes do DLP de volta para o Proofpoint sn_pp_dlp.incident_update	Esta propriedade permite restringir qualquer sincronização do seu ServiceNow instância para Proofpoint Incidentes do DLP. ○ Tipo: booleano ○ Valor padrão: verdadeiro
Nível de emissão de relatórios dos logs gerados pela integração sn_pp_dlp.logging.verbosity	O nível de logs de emissão de relatórios gerados pela integração.

3. Clique em **Salvar**.

Resultado

Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation em Proofpoint Integração do DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com Proofpoint Integração do DLP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute Proofpoint Procedimentos de integração do DLP no domínio apropriado.

Integração de resposta a incidentes de prevenção contra perda de dados com Netskope

. Netskope A integração do DLP oferece suporte à ingestão de incidentes de prevenção contra perda de dados criados no Netskope Implantação da prevenção contra perda de dados. Netskope O DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes do DLP.

Principais recursos

Esta integração inclui os seguintes recursos principais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Criação de vários perfis para diferente Netskope locatários.
- Automatizar a criação de incidentes do ServiceNow DLP de Netskope Incidentes do DLP.
- Filtragem de Netskope Incidentes do DLP.
- Ingestão programada de Netskope Incidentes de DLP que criam incidentes de DLP na ServiceNow.
- Atualizar automaticamente o status do objeto em Netskope Quando o estado do DLP muda em sua instância da ServiceNow.
- Exiba os detalhes forenses (conteúdo violando) do Incidente do DLP no espaço Analista de IR do DLP e no espaço do usuário final do DLP.

  Nota: O conteúdo que viola não persiste na ServiceNow. O conteúdo é extraído quando o incidente está aberto no espaço.

- Baixando arquivo de evidência diretamente do Netskope sob demanda.

  Nota: O arquivo de evidência não persiste na ServiceNow. O arquivo de evidência é extraído quando o analista clica em **Download do arquivo** no espaço .

- Notificação por e-mail para usuários administradores do DLP em Netskope expiração do token.
- A notificação por e-mail será enviada aos usuários administradores do DLP se exceder o limite de novas tentativas definido para falhas de chamada de API de incidente.
- Netskope também oferece suporte ao processo de execução de integração. Para obter mais informações, consulte Monitorar o processo de execução de integração do DLP.

Introdução ao Netskope Integração do DLP para prevenção contra perda de dados

Revise as informações a seguir antes de começar a configurar seu Netskope Integração do DLP para prevenção contra perda de dados.

Tarefa de configuração	Descrição
Verifique se você atribuiu a plataforma Now necessária, a aplicação Prevenção de perda de dados.	As funções a seguir são usadas em Netskope Integração do DLP no ServiceNow AI Platform: • O administrador (administrador) instala as aplicações do ServiceNow Store E atribui o administrador de prevenção contra perda de dados (sn_dLIR.admin). • O usuário com a função sn_dLIR.admin pode configurar a integração e definir os perfis de incidente. • Os usuários com a função sn_dLIR.analyst terão funções de leitura na integração.
Atribua os privilégios necessários para Netskope Token da API v2.	Os seguintes privilégios de endpoint são usados em Netskope API v2 tokenização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de configuração	Descrição
	• Leitura: /api/v2/incidents/dlpincidents • Leitura: /api/v2/events/dataexport/events/incident • Leitura e gravação: /api/v2/incidents/update
Verifique se a aplicação principal do usuário final é necessária para oferecer suporte ao Netskope A integração do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas a partir de ServiceNow Store. Se não estiver instalado, instale e ative no aplicativo . • Security Support Common • Data Loss Prevention Incident Response

Instale e configure o. Netskope Integração do DLP para prevenção contra perda de dados

Instale e configure o. Netskope Integração do DLP de ServiceNow StoreServiceNow AI Platform instância. Você pode começar a investigar incidentes de DLP usando Netskope Dados de incidentes do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

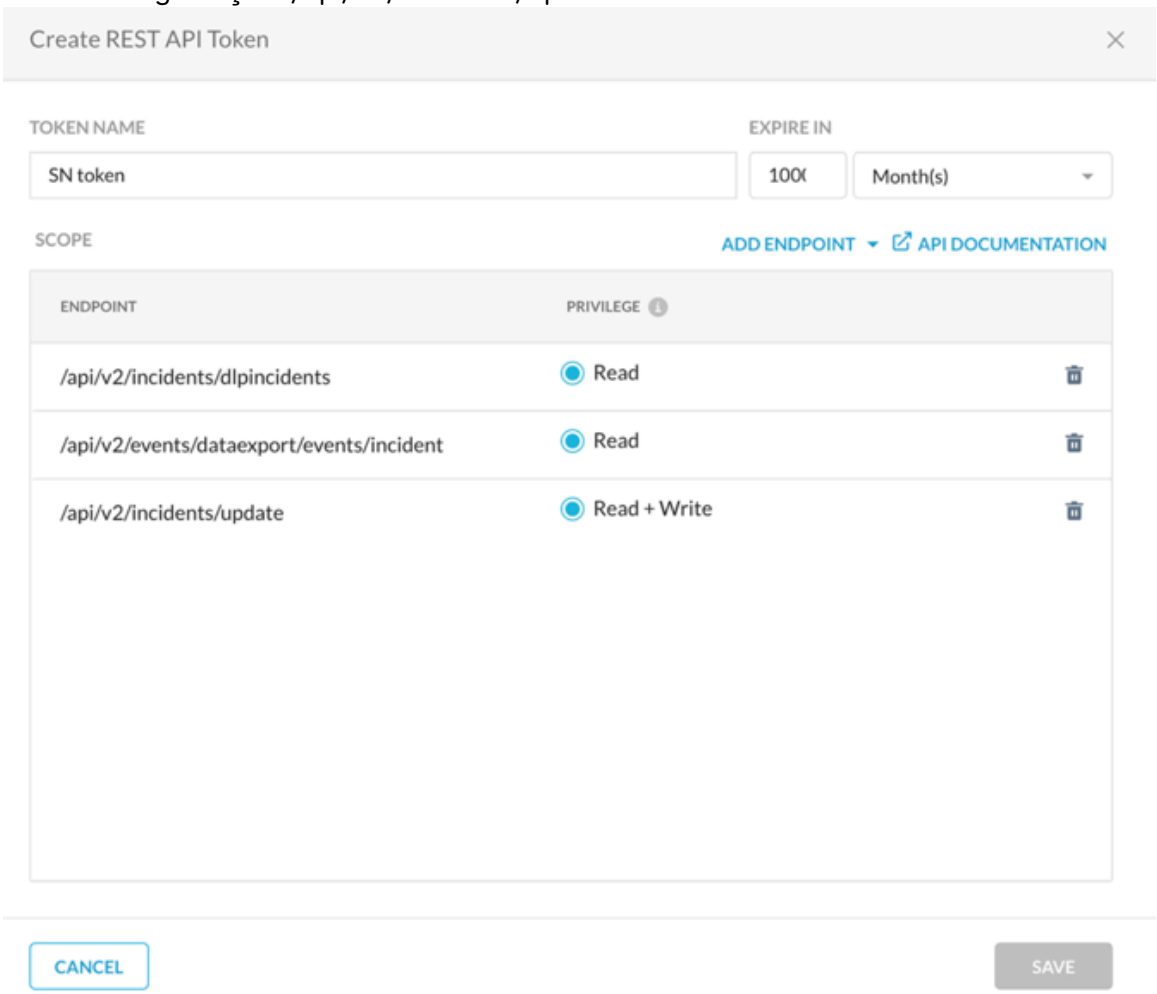
1. Baixe o. Netskope Integração do DLP do ServiceNow Store e instale-o.
2. Navegue até #**Operações de segurança** > **Integrações** > **Configurações de Integração**
3. Pesquisar Integração de resposta a incidentes do DLP com Netskope lado a lado e clique **Configurar** .
4. No formulário, preencha os campos.

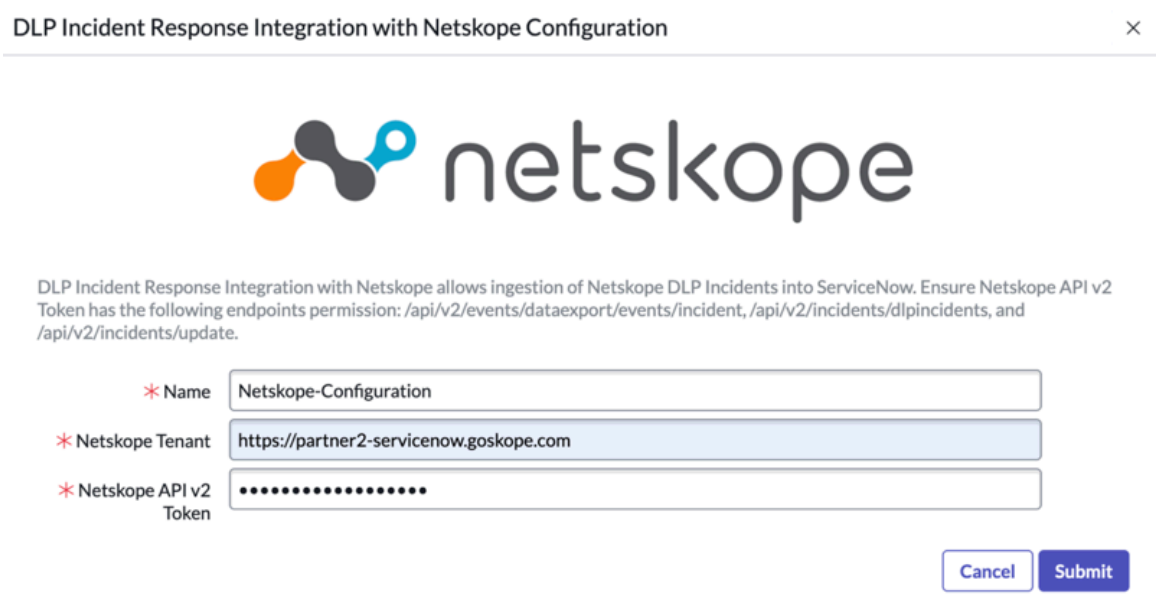
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Certifique-se de Netskope O token de API v2 tem os privilégios de endpoint abaixo:

- Leitura: /api/v2/incidents/dlpincidents
- Leitura: /api/v2/events/dataexport/events/incident
- Leitura e gravação: /api/v2/incidents/update





Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome do Netskope Configuração de integração do DLP.
Locatário do Netskope	. Netskope URL base para Netskope locatário.
Token da API da Netskope v2	Token configurado para REST API v2 em sua conta de usuário em Netskope.

5. Clique em **Enviar**.

Resultado

Nota: Conecte o subproduto netskope ao subproduto da ServiceNow. Mantenha todos os nomes de usuário e senhas em sincronia nas instâncias para evitar que as contas sejam desconectadas.

Depois de validar e enviar a configuração com êxito, o Netskope A integração do DLP é salva na página Integrações de segurança como um bloco.

Criar um perfil para Netskope Integração do DLP

Crie um perfil de incidente em seu ServiceNow AI Platform instância.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Configurar ServiceNow AI Platform Para recuperar os incidentes do DLP do Netskope endpoint. Armazene os incidentes em seu ServiceNow Instância como incidentes do DLP.

Procedimento

1. Navegar até **Integração do Netskope DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Criar um perfil

Campo	Descrição
Nome	Nome do perfil. O nome deve ser exclusivo para cada perfil. Este nome ajuda você a identificar o perfil.
Origem	Netskope Instância do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidente que você planeja ingerir para o perfil. **Nota:** Somente um perfil ativo é permitido por origem.
Ativo	Indicador de que o perfil está ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo fica disponível somente depois que você clica em **Concluir** Na última seção Programação. Quando o perfil está ativo, seu ServiceNow AI Platform a instância está pesquisando ativamente Netskope Incidentes do DLP. Os incidentes de DLP correspondentes são criados como incidentes de DLP da ServiceNow quando as condições de filtragem são correspondidas com base nos parâmetros de programação que você forneceu.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição para ajudá-lo a distinguir este perfil de outros perfis.

4. Clique em **Continuar** E mover para a seção Filtragem.

Defina Filtros a serem aplicados à criação do incidente

Defina e defina condições de filtro para filtrar a entrada Netskope#Incidentes do DLP. Controle quais desses incidentes devem ser criados como incidentes de DLP em seu ServiceNow instância.

Antes de Iniciar
Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa
Esse tipo de filtragem ajuda a isolar incidentes de DLP e limitar o número de incidentes de DLP criados. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Selecione **Filtro com base em condições** E defina os critérios que um incidente de entrada do Netskope DLP deve atender para que um incidente de DLP seja criado.
2. Usando as listas e os campos do construtor de condições, defina os filtros no **Condições de filtro** campo.

   As opções no primeiro campo em **Condições de filtro** corresponda os campos que estão disponíveis em **Importação de incidentes do Netskope DLP** tabela. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.

3. Clique em para adicionar mais condições **E.** #ou**OU** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **E.** #selecionado, todas as condições devem ser correspondidas.
- Se **OU** #está selecionado, qualquer condição pode ser correspondida.

4. Clique em **Continuar** E mover para a seção Programação.

Programe o. Netskope Recuperação de incidentes do DLP

Defina uma programação a ser recuperada Netskope Incidentes do DLP que correspondem aos critérios no perfil.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que você pesquisará novos líquidos Netskope incidentes que correspondem à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer recuperação única usando **Recuperação única** caixa de seleção. A data histórica pode ser de até um mês a partir do passado.

Procedimento

1. Configure a programação para definir como e quando você extrai incidentes de Netskope.
2. No formulário, preencha os campos.

Programe o. Netskope Incidentes do DLP

Campo	Descrição
Adição de incidentes em andamento	Ingestão de incidentes em andamento que você ServiceNow AI Platform extrações da instância de Netskope para novos incidentes. Se forem encontrados incidentes acionados que correspondam aos critérios de filtragem de incidentes, os incidentes do DLP serão criados.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos. Este valor padrão é definido como **5** .
Definir horário de adição do incidente inicial	Opção para definir a ingestão de incidente inicial com base na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora especificadas para a ingestão do incidente.
Horário de adição do incidente inicial	A primeira vez em que os dados são ingeridos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O valor ficará visível somente se **Defina o tempo de ingestão do incidente inicial** a opção está selecionada.
Horário de adição do próximo incidente (estimado)	O próximo tempo estimado de ingestão de incidente.
Recuperação Única	Opção para habilitar extração única de dados históricos. **Nota:** Se selecionado, os dados históricos serão extraídos de Netskope DLP de acordo com a data adicionada **A partir da data** .
Desde a Data	Data a partir da qual os dados são obtidos Netskope. **Nota:** No máximo, os últimos 30 dias de dados podem ser obtidos de Netskope.

3. Clique em **Concluir**.
4. No pop-up, salve a configuração de perfil criada clicando em **Concluir** .
5. Ative o perfil.
   a. Abra o perfil criado.
   b. Definido **Ativo** . **verdadeiro** .
   c. Clique em **Atualizar**.

Resultado
Após a ativação bem-sucedida da criação do perfil, os incidentes serão obtidos periodicamente de acordo com a configuração definida no perfil. Os incidentes serão adicionados à tabela Incidentes do DLP.

Mapeamento do status do incidente do DLP com Netskope

A seção Mapeamento de status do incidente permite que os usuários forneçam os mapeamentos entre o status do incidente do DLP na ServiceNow e. Netskope Status do objeto.

Antes de Iniciar
O mapeamento será usado ao ingerir qualquer incidente do DLP de Netskope Para a ServiceNow, bem como sincronizar qualquer mudança de estado do incidente DLP na ServiceNow de volta para Netskope.

Sincronize o status dos incidentes de DLP ingeridos na ServiceNow com o incidente de DLP da Netskope. Mapeie o campo Status do incidente da ServiceNow com Netskope Campo Status do objeto.

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa
Você precisa criar um mapeamento de status de incidente individual de Netskope E status da ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Integração do Netskope DLP** > **Mapeamento de status do incidente**.
2. Forneça um Nome para identificar o mapeamento.
3. Selecione a Integração de origem.
4. Mapeie o status do incidente do DLP com Netskope Status do objeto (duplicado Netskope também pode ser mapeado).
   A sincronização de status da ServiceNow para Netskope será desabilitado se você não criar um registro de mapeamento.

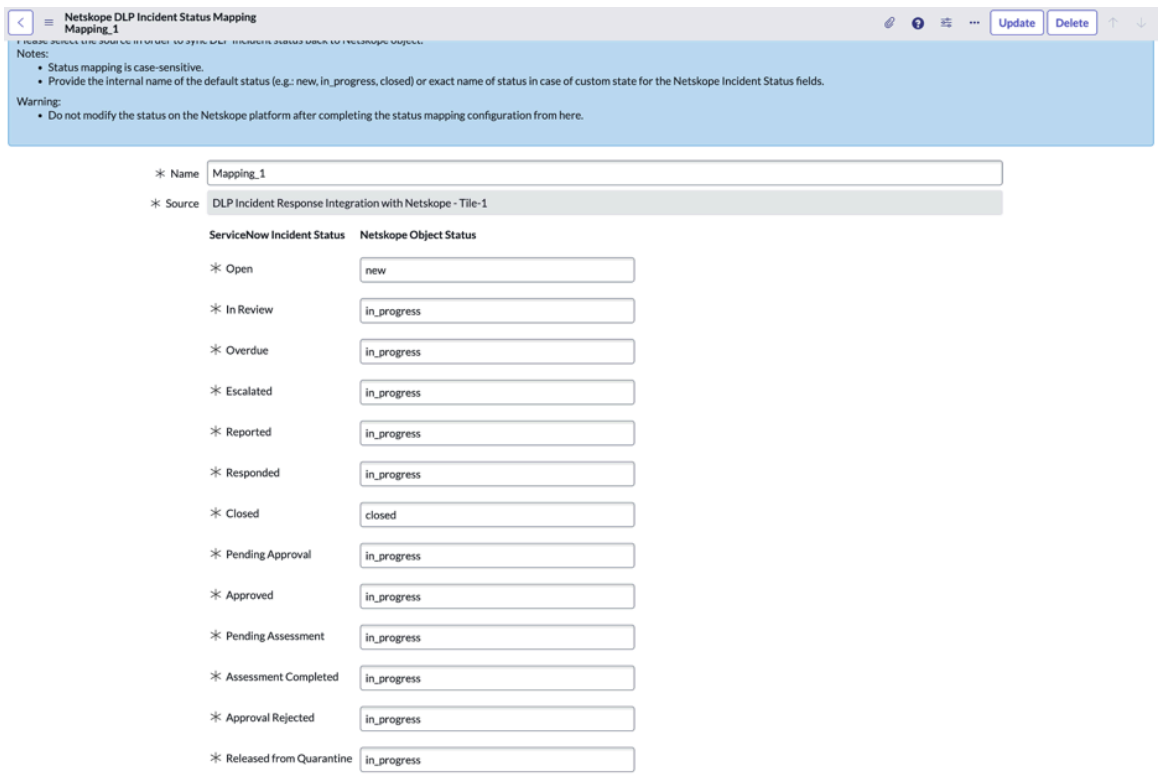
Importante: Você precisa mapear todos os Netskope Status do objeto para todos os status da ServiceNow. Selecione a origem para sincronizar o status do incidente do DLP de volta para Netskope objeto.

As seguintes informações e mensagens de alerta são exibidas quando você mapeia o status do incidente, revisa as mensagens e prossegue.

Nota:

- O mapeamento de status faz distinção entre maiúsculas e minúsculas.
- Forneça o nome interno do status padrão (por exemplo: Novo, in_progress, Encerrado) ou o nome exato do status em caso de estado personalizado para Netskope Campos Status do objeto.

Aviso: Não modifique o status no Netskope após concluir a configuração de mapeamento de status a partir daqui.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Netskope Mapeamento de status de incidente do DLP

Campo	Descrição
Nome	Nome do registro de mapeamento.
Origem	Configurado Netskope Origem do endpoint de onde você deseja sincronizar o status do incidente.
Status do incidente da DLP	Indica a lista de status de incidentes do DLP.
Netskope Status do objeto	Indica a lista de Netskope status do objeto.

5. Clique em **Enviar**.

Resultado

Depois de criar com sucesso o registro para mapeamento de status, sempre que houver uma atualização no estado do incidente do DLP da ServiceNow, ele o refletirá automaticamente Netskope lado de acordo com o mapeamento.

Nota: Se você mudar o status de qualquer incidente do DLP em Netskope Locatário diretamente e, em seguida, o status é sincronizado do SN para Netskope Não funcionará, considerando as limitações da API. Mapeie todos os status do incidente do DLP com Netskope status do objeto com cuidado.

Configurar Netskope Configurações de integração do DLP

Modifique o. Netskope#Propriedades do sistema padrão de integração do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Navegar até **Integração do Netskope DLP** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Configurar Netskope Configurações de integração do DLP

Campo	Descrição
O download do arquivo de violação do incidente relatado deve ser permitido sn_ns_dlp.enable_file_download.	Opção para escolher se você deseja habilitar o download do arquivo. Por padrão, esta opção está habilitada.
Tempo limite máximo para chamadas HTTP, em segundos sn_ns_dlp.maximum_http_time_out.	Tempo limite máximo para chamadas HTTP, em segundos. Este campo é definido automaticamente como 30.
Número máximo de novas tentativas a serem realizadas para falhas de API. sn_ns_dlp.maximum_retry.	Número máximo de novas tentativas a serem realizadas para falhas de API. O valor padrão é definido como 3.
Nível de emissão de relatórios dos logs gerados pela integração sn_ns_dlp.logging.verbosity.	Defina o nível de logs de emissão de relatórios gerados pela integração. Este campo é definido automaticamente como **informações** .

3. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Baixar arquivos de evidência

Baixe arquivos que violam a política de DLP em Netskope. Baixe este arquivo em sua máquina local do espaço Analista do DLP IR e do espaço do usuário final do DLP IR para aprovadores.

Antes de Iniciar

Função necessária:

- sn_dlir.analyst
- sn_dlir.secure_file_download (qualquer aprovador com esta função)

Por Que e Quando Desempenhar Esta Tarefa

Você precisa habilitar o download de arquivo para Netskope antes de avançar.

Procedimento

1. Navegar até **Tudo** > **Integração do Netskope DLP** > **Configurações**.
2. Habilite a propriedade **O download do arquivo de violação do incidente relatado deve ser permitido** .
   Você poderá ver **Download do arquivo** No Espaço do analista do DLP IR e no espaço do usuário final do DLP IR.
3. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
4. Abra um registro de incidente do DLP que é ingerido de Netskope origem.
5. Clique em **Download do arquivo** .
   O arquivo que viola a política de DLP no Netskope será baixado para a máquina local do usuário.

> **Nota:** O administrador do DLP pode controlar o acesso de **Download do arquivo** ação para todas as integrações desabilitando o. **O download do arquivo de violação do incidente relatado deve ser permitido** . **Configurações avançadas** Página de Administração do DLP. Para obter mais informações, consulte Definir configurações avançadas.

Visualizar arquivos de evidência

Visualize arquivos de evidência de incidente do DLP no espaço Analista de IR do DLP.

Antes de Iniciar

- Navegar até **Tudo** > **Administração da DLP** > **Configurações avançadas**.
- Certifique-se de **sn_ns_dlp.enable_evidence_file_preview** a propriedade já está habilitada.

> **Importante:** Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado pela duração que você selecionou usando **sn_dlir.preview_temp_files_cleanup_interval** propriedade do **Configurações avançadas** página. Você pode desabilitar **Arquivos de evidência** Visualize o recurso se você não quiser armazenar dados no banco de dados da ServiceNow. Para obter mais informações, consulte Definir configurações avançadas.

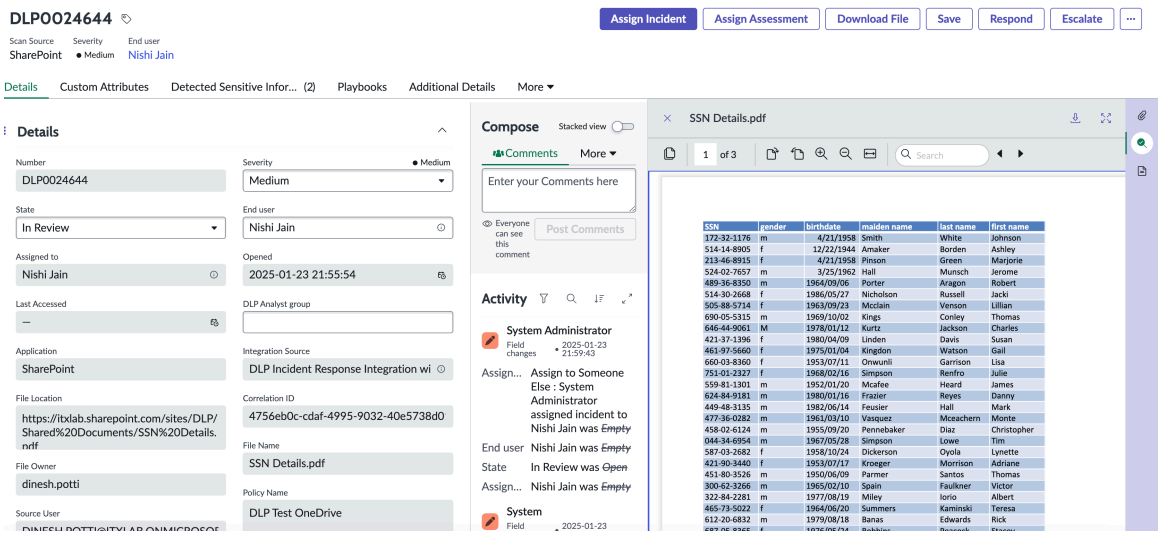
Função necessária: sn_dLIR.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Selecione **Arquivos de evidência** ícone, que está disponível no menu contextual.
   É aberta uma guia que busca todos os arquivos de evidência. Quando o download estiver concluído, você poderá exibir todos os arquivos de evidência no **Arquivos de evidência** guia.
4. Selecione **Arquivo de evidência** cartão que você deseja visualizar.
   O recurso de visualização é diferente para cada tipo de arquivo.
5. Visualize PDF e documentos do Office no visualizador de documentos selecionando **Expandir** ícone no canto superior direito do arquivo de evidência para abrir o pdf em tela cheia.
   Extensões do Office para as quais o visualizador de documentos abre os arquivos de evidência: Doc, docx, ppt, pptx, xls, xlsx.
   a. Localize a barra de pesquisa e insira a palavra-chave que você está procurando.
   b. Use os recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade.
   c. Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.
   Essas opções de controle aprimoram sua capacidade de entender o arquivo de evidências de forma abrangente. Somente o pdf tem opções de controle no cabeçalho.

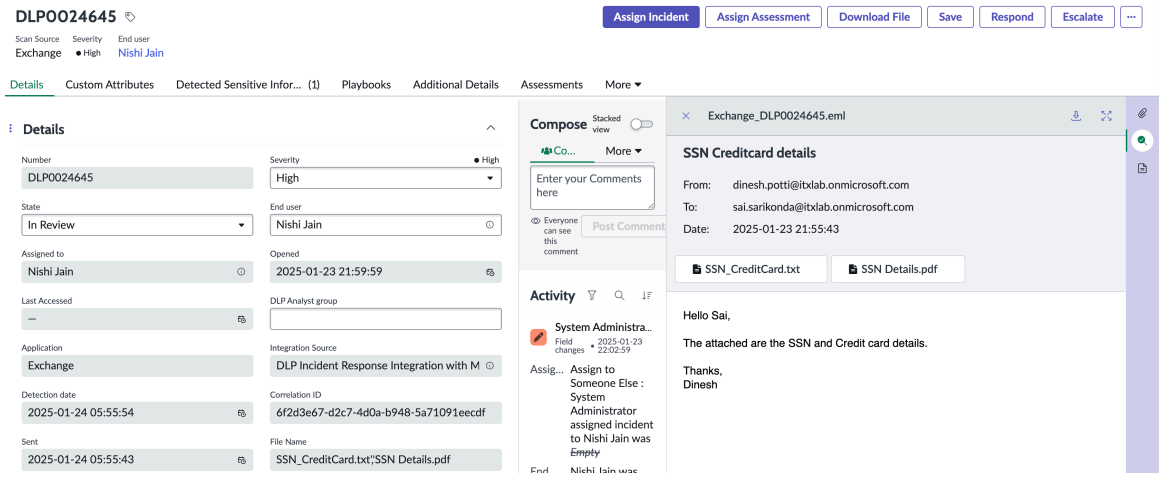


6. Visualizar arquivos eml.
   Selecione os anexos no e-mail e visualize-os.

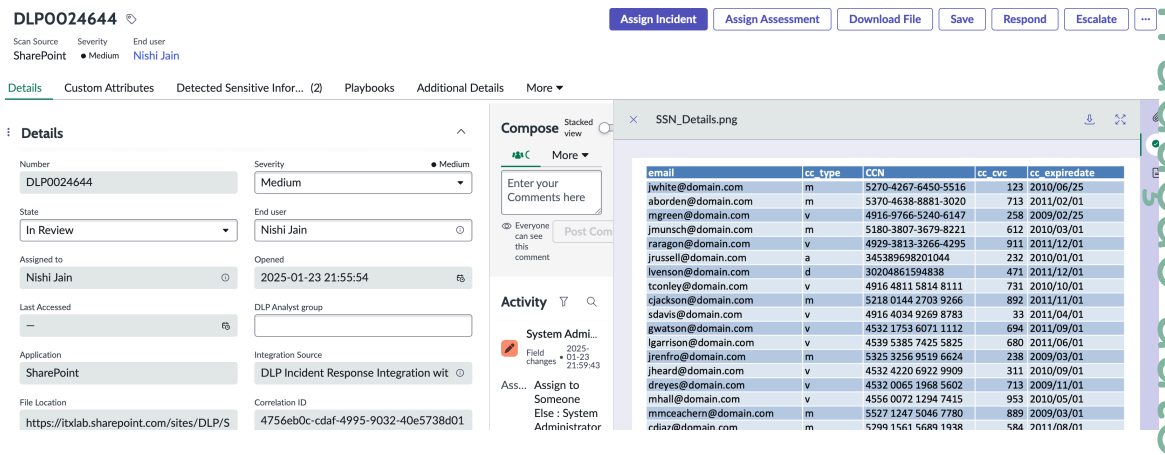
> **Nota:** Se o arquivo de evidência selecionado exceder o limite de 5 MB, ele não poderá ser visualizado no espaço do analista. Você precisa baixar o arquivo para visualizar seu conteúdo. Este limite é somente para arquivos .eml.

Tradução automática

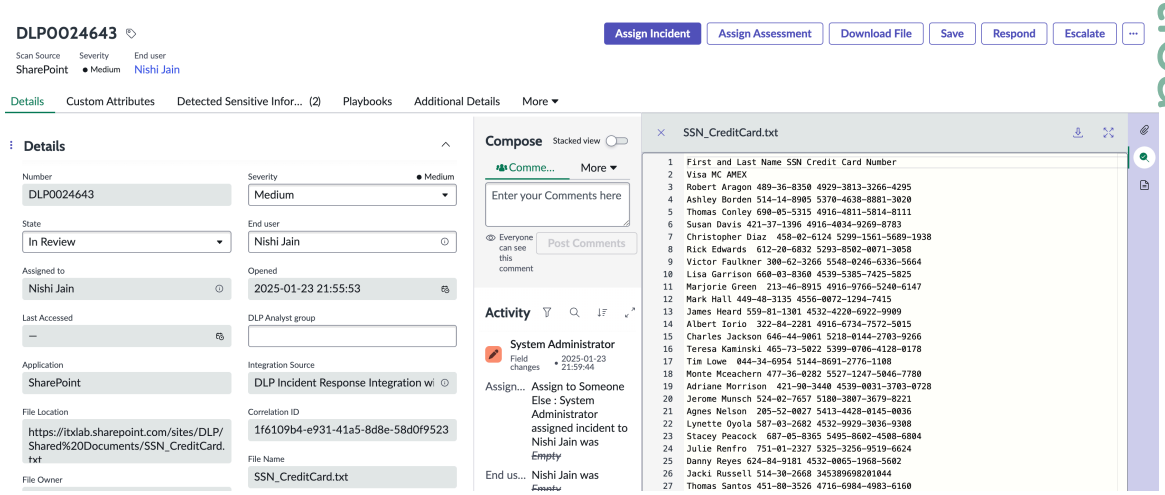
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Visualize imagens no espaço do analista do DLP.
Imagens somente com .bmp, .gif, .ico, .jpeg, .jpg, as extensões .png, .svg e .webp são compatíveis.



8. Visualize arquivos de texto no editor de texto selecionando **Expandir** ícone no canto superior direito do arquivo de evidência.



Nota: Arquivos de evidência, além dos documentos do Office, arquivos eml, texto e extensões de imagem, não serão compatíveis com visualização. Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificações para usuários no mecanismo de novas tentativas

Netskope A integração tentará novamente o número configurado de vezes em caso de falhas de API durante a ingestão de incidentes do DLP.

Quando o limite máximo de novas tentativas for excedido, Netskope A integração envia uma notificação por e-mail para os usuários que têm a função de administrador do DLP (sn_dlir.admin).

Depois de concluir a instalação e a configuração da integração, forneça a função Administrador do DLP (sn_dLIR.admin) aos usuários que devem ser notificados quando o limite máximo de novas tentativas exceder.

Quando o limite máximo de novas tentativas for excedido, o perfil ignorará a ingestão por uma duração de até uma hora. O máximo de novas tentativas é configurado usando a propriedade: Número máximo de novas tentativas a serem realizadas para falhas de API . Para obter mais informações, consulteConfigurar Netskope Configurações de integração do DLP.

Notificações por e-mail na expiração de credenciais

Quando o token é usado em ServiceNow a instância expira, Netskope A integração envia uma notificação por e-mail para os usuários com a função de administrador do DLP (sn_dlir.admin).

Após a conclusão da configuração da integração, forneça a função de administrador do DLP (sn_dlir.admin) aos usuários que devem ser notificados se o token expirou.

Se o token expirar, a ingestão de dados dos perfis associados ficará em espera até que a configuração de integração do Netskope seja atualizada com um token válido.

Você deve criar um token ou renovar o antigo em Netskope e atualize o token no ServiceNow instância. . Se você renovar o token estendendo o tempo de expiração, o Netskope a aplicação detecta automaticamente a renovação e continuará com a coleta de dados. Se você criar um token, deverá atualizar o token na configuração.

Domain Separation em Netskope Integração do DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com Netskope Integração do DLP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute Netskope Procedimentos de integração do DLP no domínio apropriado.

Integração do Protocolo de Adaptação de Conteúdo da Internet (ICAP) para DLP IR

A integração DLP do Protocolo de adaptação de conteúdo da Internet (ICAP) oferece suporte à ingestão de Data Loss Prevention Incident Response Permite a busca de conteúdo de correspondência e arquivos de evidência do Amazon S3 criados no ICAP compatível Data Loss Prevention Incident Response implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que os alertas são ingeridos, você pode usar o espaço do DLP para exibir as principais informações necessárias, como conteúdo de correspondência, gravidade do alerta e várias funcionalidades de gestão de incidentes para corrigir os incidentes do DLP.

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

A integração do Protocolo de Adaptação de Conteúdo da Internet (ICAP) ajuda você a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Esta integração inclui os seguintes recursos principais:

- Ingestão de alertas de DLP: Os usuários poderão configurar e programar a ingestão de alertas de DLP de buckets especificados do Amazon S3. Isso inclui a capacidade de executar importações delta para garantir que somente novos dados sejam ingeridos.
- Exibir alertas ingeridos no Espaço do DLP: Depois que os alertas são ingeridos, eles devem ser exibidos no espaço do DLP, fornecendo detalhes importantes sobre cada alerta, como conteúdo de correspondência, gravidade do alerta e metadados relevantes.
- Corresponder conteúdo: Registros de informações confidenciais são criados durante a ingestão, o conteúdo de correspondência é obtido quando o registro é aberto.
- Download de arquivo de evidência: O sistema permite que os usuários baixem arquivos de evidência associados diretamente do espaço do DLP para investigação ou revisão adicional.
- Capacidade de personalizar e definir o mapeamento de gravidade entre incidentes de DLP ICAP com incidentes da ServiceNow.

Introdução à integração do DLP ICAP para prevenção contra perda de dados

Antes de usar a integração, você deve baixá-la do ServiceNow® Store

Check-list

Revise as informações a seguir antes de começar a configurar a integração ICAP DLP do provedor para prevenção contra perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu o necessário ServiceNow AI Platform, Funções da aplicação de prevenção de perda de dados.	As seguintes funções são usadas na integração do ICAP DLP no ServiceNow AI Platform: • O administrador (administrador) instala as aplicações do ServiceNow® Store E atribui o administrador de prevenção contra perda de dados (sn_dLIR.admin).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
	• O usuário com a função sn_dLIR.admin pode configurar a integração e configurar os perfis de incidente. • Os usuários com a função sn_dLIR.analyst terão funções de leitura nas configurações de integração.
Verifique se você atribuiu as políticas de bucket necessárias do Amazon S3.	Você pode seguir a documentação oficial da AWS para criar e gerenciar usuários, políticas e permissões do IAM por meio dos seguintes links: • Criando um usuário do IAM • Criando políticas de IAM • Permissões do Amazon S3 **Nota:** Usando os links acima, você pode saber mais sobre as instruções detalhadas e outras opções para gerenciar usuários do IAM e permissões do S3 na AWS, além de como criar um usuário do IAM em sua conta da AWS - AWS Identity and Access Management e a visão geral básica do processo usado para criar um usuário do IAM e credenciais no AWS Identity and Access Management.
Verifique isso ServiceNow® A aplicação principal necessária para oferecer suporte à integração do ICAP DLP é instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative no aplicativo . • Security Support Common • Componentes comuns do espaço do Gestão de casos de segurança. • Data Loss Prevention Incident Response

Instale e configure a integração do ICAP DLP

Instale e configure a#integração do provedor ICAP DLP do ServiceNow® Store em seu ServiceNow AI Platform instância. Comece a investigar incidentes de DLP usando os#dados de incidente de DLP ICAP do provedor.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Baixe a#integração ICAP DLP do provedor doServiceNow® Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.

Tradução automática

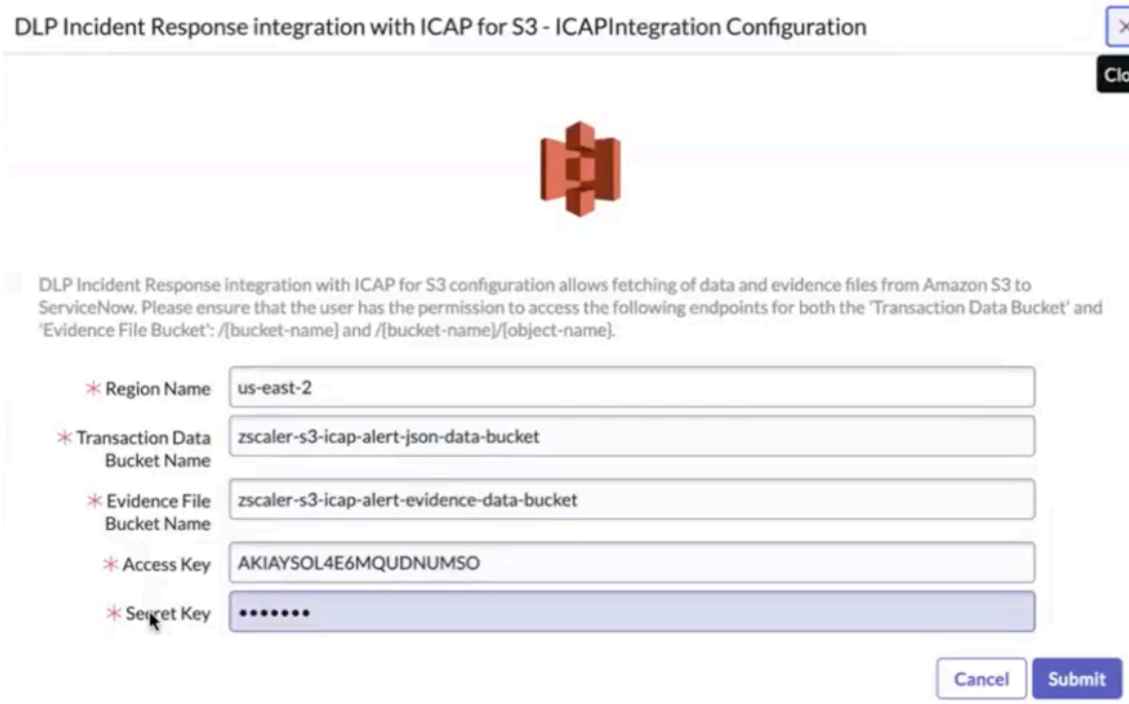
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. PESQUISE o#bloco Integração de resposta a incidentes do DLP com ICAP e clique em **Configurar** .

4. No formulário, preencha os campos.

Formulário Configuração de integração do DLP ICAP

Campo	Descrição
Nome da região	Nome da região do nome do bucket do Amazon S3.
Nome do bucket de dados de transação	O nome do bucket de dados da transação é o bucket em que ocorreu uma transação de violação do DLP.
Nome do bucket do arquivo de evidências	O nome do bucket do arquivo de evidência é o bucket em que você pode encontrar o arquivo DLP que causou a violação.
Chave de acesso	Chave de acesso do AWS IAM para a configuração do ICAP.
Chave Secreta	Chave secreta do AWS IAM para a configuração do ICAP.



5. Clique em **Enviar**.

Resultado

Nota: Conecte o subproduto ICAP ao subproduto da ServiceNow. Mantenha todos os nomes de usuário e senhas em sincronia nas instâncias para evitar que as contas sejam desconectadas.

Depois de validar e enviar a configuração com sucesso, as configurações de integração do ICAP DLP serão salvas.

Crie um perfil para integração do ICAP DLP

Crie um perfil de incidente em seu ServiceNow AI Platform instância. Determine os#alertas de DLP ICAP adequados para criar incidentes de DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa
Configure o NowPlatform para buscar os alertas do DLP da configuração do Amazon S3. Armazene esses alertas em sua instância da ServiceNow como incidentes de DLP.

Procedimento
1. Navegar até **Tudo** > **Integração DLP com ICAP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

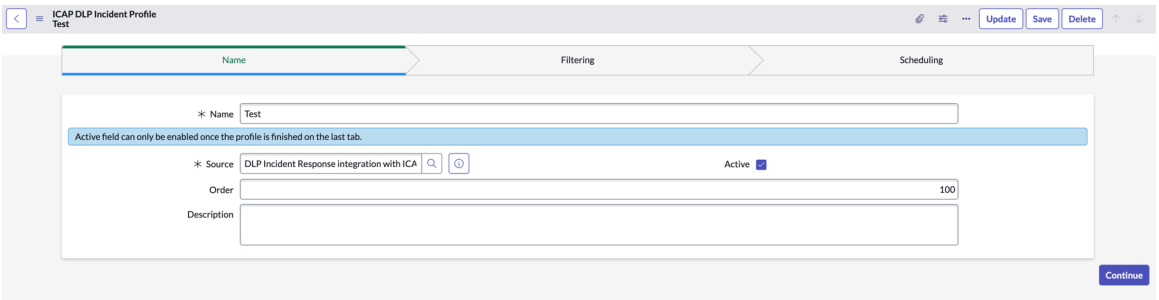
Crie um perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	Configuração do Amazon S3 que você configurou para ingerir incidentes. Se você tiver várias origens configuradas, selecione a origem apropriada para o tipo de incidente que você planeja ingerir para o perfil. **Nota:** Somente uma única origem é permitida para o perfil ativo.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois que você clicar em **Concluir** Na seção Programação. Quando o perfil está ativo, isso implica que ServiceNow AI Platform Está pesquisando ativamente alertas de DLP do ICAP. Os alertas de DLP correspondentes são criados no#DLP#quando as condições de filtragem são correspondidas com base nos parâmetros de programação que você forneceu.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição deste perfil.



O que Fazer Depois

Para ir para a seção Filtragem,#clique em **Continuar** .

Defina filtros a serem aplicados à criação do incidente

Defina e defina condições de filtro para filtrar os##alertas de DLP de entrada. Determine os alertas que devem ser criados como incidentes de DLP na ServiceNow.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

A filtragem ajuda a isolar alertas de DLP e limitar o número de alertas de DLP criados. Se critérios de filtragem adicionais forem definidos, somente os alertas que corresponderem às condições serão criados.

Procedimento

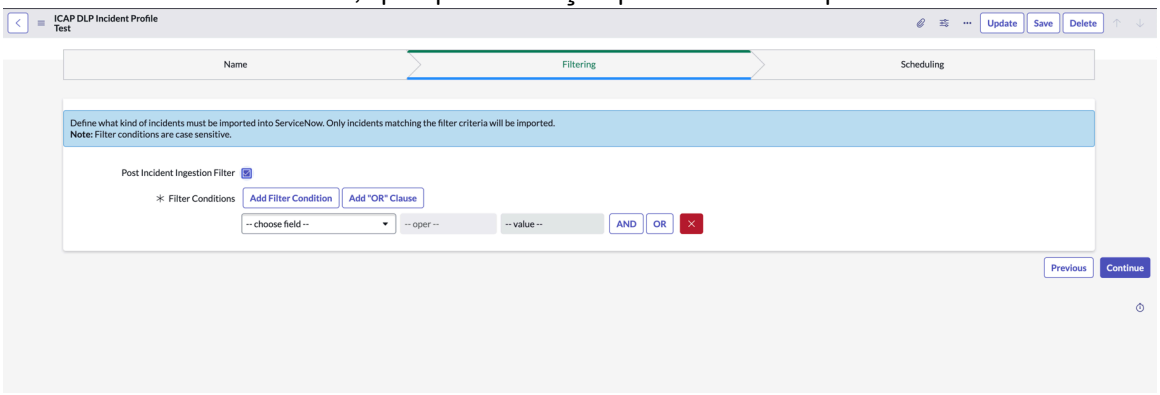
1. Selecione **Filtro de ingestão pós-incidente** caixa de seleção para aplicar os filtros de ingestão pós-incidente e recuperar os incidentes que correspondem aos critérios de filtro.
2. Selecione **Filtro com base em condições** E defina os critérios que um incidente de DLP de ICAP de entrada deve atender para que um incidente de DLP seja criado.
3. Defina os filtros em **Condições de filtro** campo.

   As opções no menu suspenso **Condições de filtro** corresponda os campos que estão disponíveis em **Importação de incidentes do DLP ICAP** tabela. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
4. Clique em para adicionar mais condições **E.** #ou**OU** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **E.** #selecionado, todas as condições devem ser correspondidas.
- Se **OU** #está selecionado, qualquer condição pode ser correspondida.



O que Fazer Depois

Para configurar a programação, clique em **Continuar** .

Programe a recuperação de incidentes de DLP ICAP

Defina uma programação para recuperar alertas de DLP ICAP que correspondam aos critérios no perfil.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que pesquisará novos incidentes ICAP líquidos que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer recuperação única usando **Recuperação única** caixa de seleção.

Procedimento

1. Configure a programação para definir como e quando você extrai incidentes do ICAP.
2. No formulário, preencha os campos.

Programe os incidentes de DLP ICAP

Campo	Descrição
Adição de incidentes em andamento	Ingestão de incidentes em andamento que você ServiceNow AI Platform A instância extrai do#ICAP novos incidentes. Se forem encontrados incidentes acionados que correspondam aos critérios de filtragem de incidentes, os incidentes do DLP serão criados.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos. Este valor padrão é definido como **5** .
Definir horário de adição do incidente inicial	Opção para definir a ingestão de incidente inicial com base na data e hora configuradas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora especificadas para a ingestão do incidente.
Horário de adição do incidente inicial	A primeira vez em que os dados são ingeridos. **Nota:** O valor ficará visível somente se **Defina o tempo de ingestão do incidente inicial** a opção está selecionada.
Horário de adição do próximo incidente (estimado)	O próximo tempo estimado de ingestão de incidente.
Recuperação Única	Opção para habilitar extração única de dados históricos. **Nota:** Se selecionado, os dados históricos serão extraídos do ICAP DLP de acordo com a data adicionada **A partir da data** .
Nome de Pasta	Nome da pasta da qual você deseja recuperar os dados. Todas as pastas cujos nomes são lexicograficamente maiores do que o nome da pasta fornecido serão ingeridas na recuperação única.

3. Clique em **Concluir**.
4. No pop-up, salve a configuração de perfil criada clicando em **Concluir** .
5. Ative o perfil.
   a. Abra o perfil criado.
   b. Definido **Ativo** . **verdadeiro** .
   c. Clique em **Atualizar**.

Resultado
Após a ativação bem-sucedida da criação do perfil, os incidentes serão obtidos periodicamente de acordo com a configuração definida no perfil. Os alertas serão adicionados à tabela de incidentes do DLP.

Exiba informações confidenciais para alertas de DLP

Exiba as informações confidenciais detectadas para alertas de DLP.

Antes de Iniciar
Determinadas regras e políticas configuradas na respectiva integração e, se você violar as políticas definidas, um incidente de DLP será criado e o conteúdo de correspondência será exibido que violou as informações na seção Informações confidenciais desse registro de incidente de DLP.

Função necessária: sn_dLIR.analyst

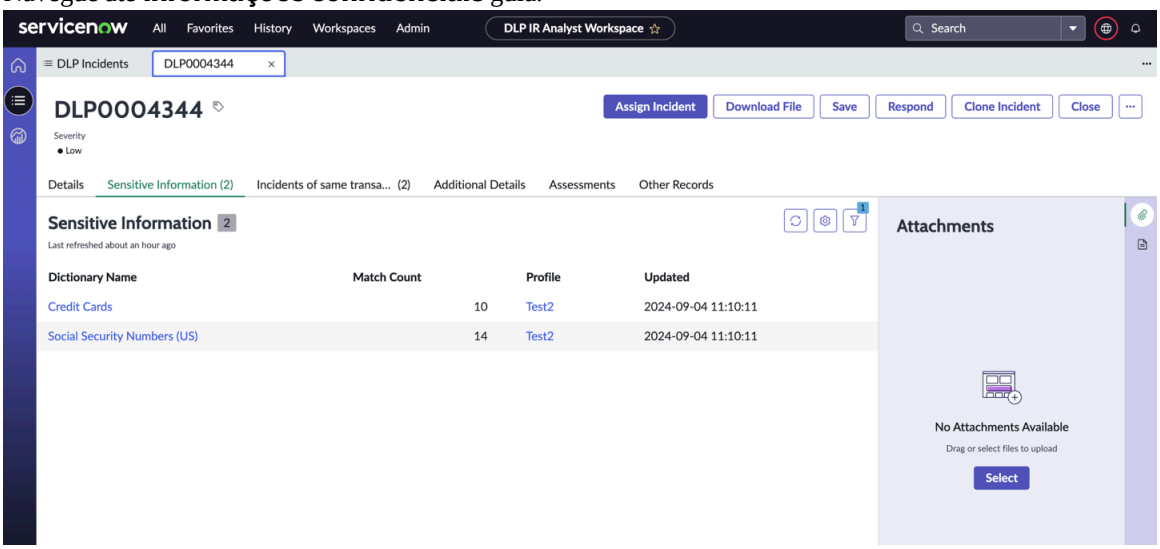
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

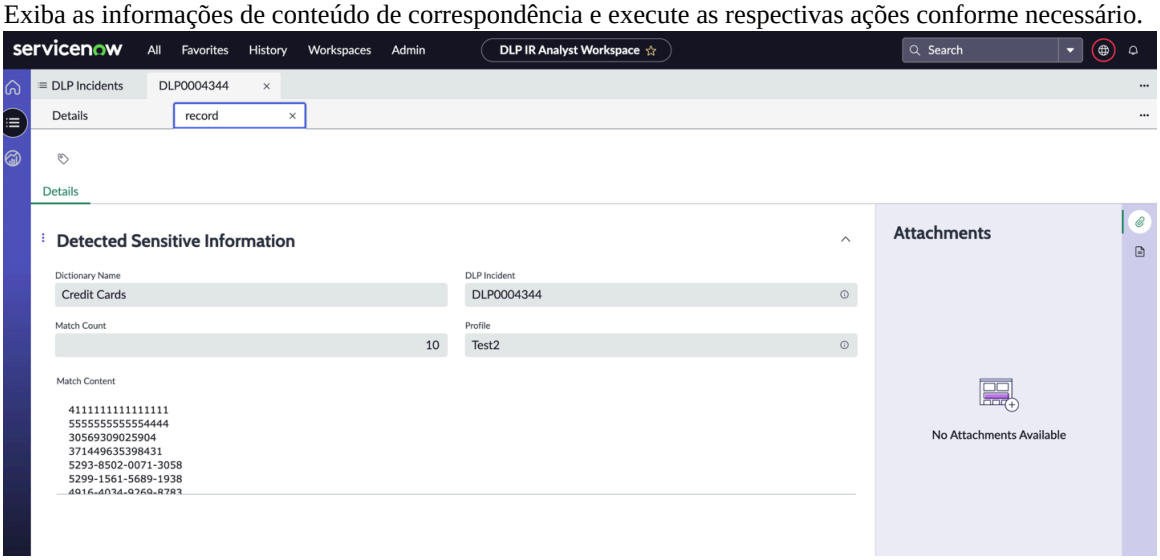
Nota: Os usuários finais também podem exibir as informações confidenciais fazendo login no Espaço do usuário do DLP.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
   A página Espaço do DLP - Meus incidentes é exibida no Espaço do analista do DLP para os analistas.
2. Abra qualquer incidente do DLP.
3. Navegue até **Informações confidenciais** guia.



4. Clique no registro violado.
5. Exiba as informações de conteúdo de correspondência e execute as respectivas ações conforme necessário.



Baixe arquivos de evidência para alertas de DLP

Baixe arquivos que violam a política de DLP no provedor compatível com ICAP. Baixe este arquivo em sua máquina local do espaço Analista do DLP IR e do espaço do usuário final do DLP IR para aprovadores.

Antes de Iniciar

Função necessária:

- sn_dlir.analista e aprovadores podem baixar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você precisa habilitar o download de arquivo para ICAP antes de prosseguir.

Procedimento

1. Navegar até **Tudo** > **Integração DLP com ICAP** > **Configurações**.
2. Habilite a propriedade sn_icap_dlp.enable_file_download **Habilitar esta propriedade permite baixar o arquivo de evidência do incidente ICAP relatado** .
   Você poderá ver **Download do arquivo** No Espaço do analista do DLP IR e no espaço do usuário final do DLP IR.
3. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
4. Abra um registro de incidente do DLP que é ingerido da origem do provedor ICAP.
5. Clique em **Download do arquivo** .

> **Nota:** O administrador do DLP pode controlar o acesso de **Download do arquivo** ação para todas as integrações desabilitando o. **O download do arquivo de violação do incidente relatado deve ser permitido** . **Configurações avançadas** Página de Administração do DLP. Para obter mais informações, consulte Definir configurações avançadas.

Visualizar arquivos de evidência para ICAP

Visualize arquivos de evidência de incidente do DLP no espaço Analista de IR do DLP.

Antes de Iniciar

- Navegar até **Tudo** > **Administração da DLP** > **Configurações avançadas**.
- Certifique-se de **sn_icap_dlp.enable_evidence_file_preview** a propriedade já está habilitada.

> **Importante:** Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado pela duração que você selecionou usando **sn_dlir.preview_temp_files_cleanup_interval** propriedade do **Configurações avançadas** página. Você pode desabilitar **Arquivos de evidência** Visualize o recurso se você não quiser armazenar dados no banco de dados da ServiceNow. Para obter mais informações, consulte Definir configurações avançadas.

Função necessária: sn_dLIR.analyst

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Selecione **Arquivos de evidência** ícone, que está disponível no menu contextual.
   É aberta uma guia que busca todos os arquivos de evidência. Quando o download estiver concluído, você poderá exibir todos os arquivos de evidência no **Arquivos de evidência** guia.
4. Selecione **Arquivo de evidência** cartão que você deseja visualizar.
   O recurso de visualização é diferente para cada tipo de arquivo.
5. Visualize PDF e documentos do Office no visualizador de documentos selecionando **Expandir** ícone no canto superior direito do arquivo de evidência para abrir o pdf em tela cheia.
   Extensões do Office para as quais o visualizador de documentos abre os arquivos de evidência: Doc, docx, ppt, pptx, xls, xlsx.

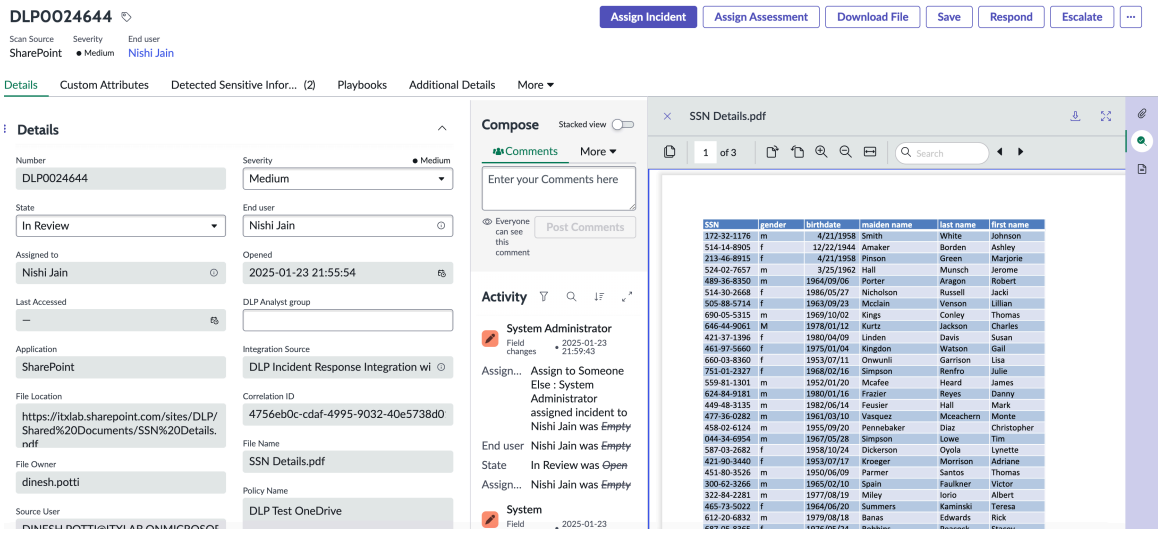
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Localize a barra de pesquisa e insira a palavra-chave que você está procurando.

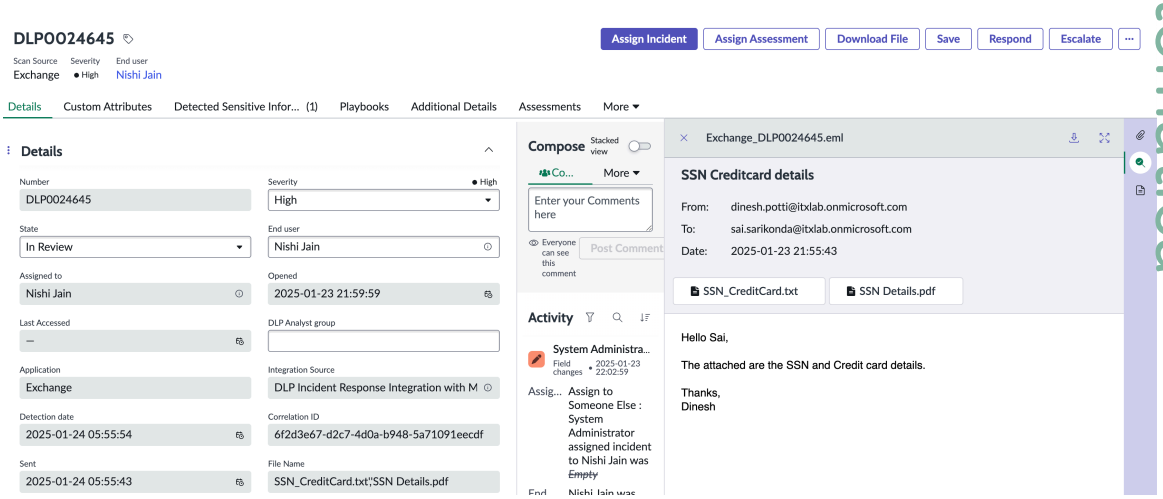
b. Use os recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade.

c. Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.
Essas opções de controle aprimoram sua capacidade de entender o arquivo de evidências de forma abrangente. Somente o pdf tem opções de controle no cabeçalho.



6. Visualizar arquivos eml.
Selecione os anexos no e-mail e visualize-os.

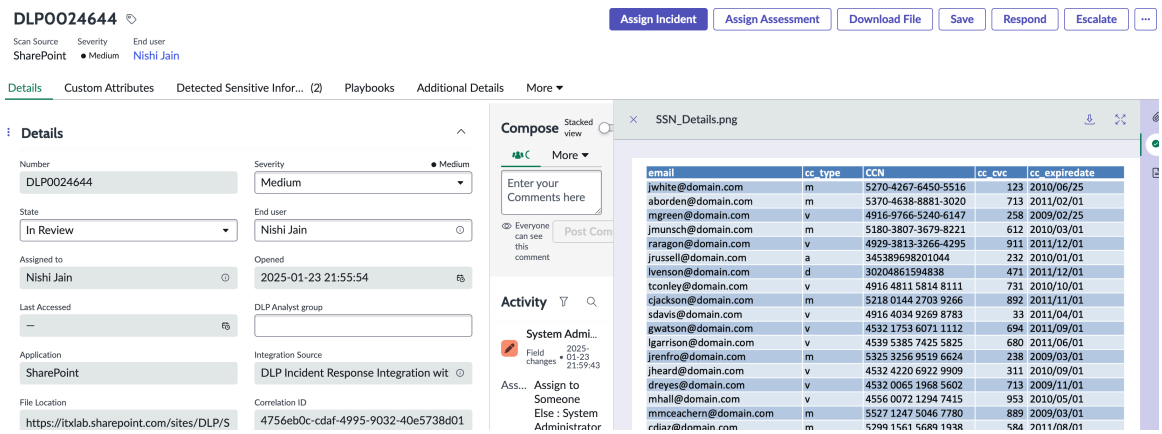
Nota: Se o arquivo de evidência selecionado exceder o limite de 5 MB, ele não poderá ser visualizado no espaço do analista. Você precisa baixar o arquivo para visualizar seu conteúdo. Este limite é somente para arquivos .eml.



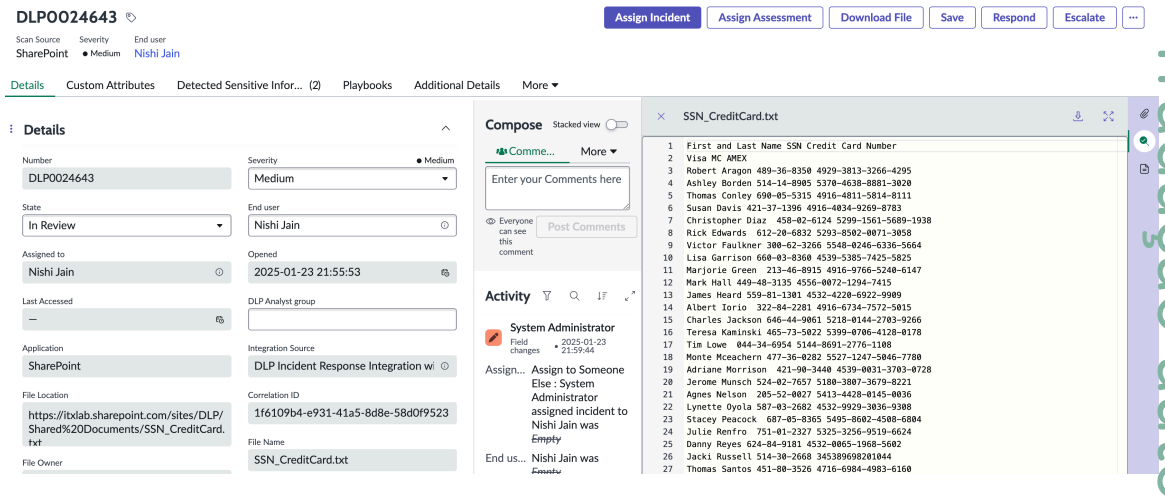
7. Visualize imagens no espaço do analista do DLP.
Imagens somente com .bmp, .gif, .ico, .jpeg, .jpg, as extensões .png, .svg e .webp são compatíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Visualize arquivos de texto no editor de texto selecionando **Expandir** ícone no canto superior direito do arquivo de evidência.



Nota: Arquivos de evidência, além dos documentos do Office, arquivos eml, texto e extensões de imagem, não serão compatíveis com visualização. Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Revise as configurações de integração do ICAP DLP

Revise as configurações de integração ICAP DLP do provedor e modifique as propriedades do sistema padrão para se adequar ao seu ambiente.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Navegar até **Tudo** > **Integração DLP com ICAP** > **Configurações**.
2. Revisar e modificar as configurações são necessárias.

Nome da propriedade	Descrição
sn_icap_dlp.maximum_retry	Opção para escolher o número máximo de novas tentativas a serem realizadas para falhas de objeto AWS GET.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade	Descrição
sn_icap_dlp.logging.detalhamento	Defina o nível de emissão de relatórios dos logs gerados pela integração. O valor padrão é definido como 4.
sn_icap_dlp.enable_file_download	A opção para habilitar esta propriedade permite baixar o arquivo de evidência do incidente ICAP relatado. Por padrão, esta opção está habilitada.
sn_icap_dlp.presigned_file_expiry_time	Especifique a duração em segundos para a qual o arquivo pré-assinado estará disponível para download ou visualização. O arquivo só estará acessível dentro deste intervalo de tempo. Este campo é definido automaticamente como 300.

Data Loss Prevention Incident Response com Microsoft

. Data Loss Prevention Incident Response com Microsoft Fornece uma estrutura principal para importar incidentes de prevenção de perda de dados (DLP) de várias fontes, como Microsoft visualizar apps (Microsoft Exchange Online, SharePoint Online, OneDrive for Business) e outros tipos de evento. Os dispositivos de endpoint permitem o fluxo de trabalho de correção que envolve usuários finais, gerentes e##equipe de operações de DLP com atribuição e escalações automatizadas de incidentes.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Use os principais recursos desta integração para executar as seguintes ações:

- Crie vários perfis para contas diferentes.
- Automatizar a criação de DLP IR incidentes.
- Mapeie o. Microsoft DLP IR campos de evento para DLP IR campos de incidente.
- Filtro Microsoft DLP IR eventos.
- Programe a ingestão de DLP IR eventos que criam DLP IR incidentes periodicamente.
- Armazene o conteúdo correspondente de cada evento do Microsoft DLP no armazenamento em nuvem externo.
- Exclua o conteúdo correspondente no armazenamento em nuvem externo após a exclusão de DLP IR incidente em ServiceNow.
- Baixar arquivos para DLP IR Incidentes do tipo Exchange, OneDrive e SharePoint.

Conheça esta integração

Identificador do documento	Título do documento
Microsoft site de documentação do produto	Site de documentação do produto da Microsoft
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução à Microsoft DLP IR integração para prevenção contra perda de dados

Revise as informações a seguir antes de começar a configurar seu Microsoft DLP IR integração para prevenção contra perda de dados.

Check-list

Configuração de tarefa	Descrição
Obtenha as credenciais do Microsoft Purview para buscar os dados do evento e as credenciais da conta de armazenamento do AWS/Azure para armazenar o conteúdo correspondente Registre uma aplicação na plataforma de identidade da Microsoft	Registre uma aplicação na plataforma Microsoft Azure de aqui Para obter o ID do cliente, o segredo do cliente e o ID do locatário. Para obter informações sobre as funções necessárias para criar uma aplicação, consulte Pré-requisitos . Para obter informações sobre as permissões/funções de API necessárias em um aplicativo do Microsoft Azure para configurá-lo ServiceNow Integração do Microsoft DLP, consulte a tabela a seguir.
Permissões necessárias para que o usuário do Azure obtenha acesso ao blob de leitura/gravação/exclusão no Armazenamento do Azure	O usuário do Azure deve ter a função **Colaborador de dados de blob de armazenamento** Para ler, gravar e excluir blobs no Armazenamento do Azure.
Permissões necessárias para que o usuário da AWS obtenha acesso ao objeto de leitura/gravação/exclusão no AWS Storage	Uma política deve ser criada que forneça acesso de lista, leitura, gravação e exclusão ao objeto no AWS S3 Storage.

Atribua e verifique se você tem as funções necessárias para ServiceNow AI Platform E Administração de perda de dados.	As seguintes funções são necessárias para configuração e verificação dos resultados esperados:
	• A função de administrador instala a integração do ServiceNow Store e atribui a função sn_dlir.admin.
	• A função sn_dLIR.admin executa as seguintes tarefas:
	  ○ Configura a integração.
	  ○ Configura os perfis de incidente.

Verifique se o ServiceNow Principais aplicações necessárias para oferecer suporte ao Microsoft DLP IR as integrações são instaladas e ativadas antes de configurar esta integração.	Verifique o seguinte DLP IR aplicações e aplicações comuns de suporte de segurança são instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative no aplicativo . • Security Support Common • Data Loss Prevention Incident Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure

Você precisa das seguintes permissões/funções de API em um aplicativo do Microsoft Azure para configurá-lo **ServiceNow** *Integração do Microsoft DLP.*

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
API de gestão do Office 365	Feed de atividades.ReadDlp	Aplicação	Leia eventos de política de DLP, incluindo dados confidenciais detectados.	Para ingerir os eventos de DLP da finalidade do MSFT para ServiceNow. **Nota:** Esta permissão é obrigatória para obter os dados do MSFT ServiceNow.	Sim
Microsoft Graph API	Files.Read.All	Aplicação	Leia arquivos em todos os conjuntos de sites que você pode acessar.	Baixar arquivo: Para baixar o anexo na instância da ServiceNow que causou o evento DLP do OneDrive ou SharePoint **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o anexo que causou o evento DLP.	Sim
	E-mail.Leitura	Aplicação	Ler e-mail em todas as caixas de correio.	Baixar arquivo: Para baixar o conteúdo do e-mail (corpo e anexo) na instância da ServiceNow que causou o evento DLP do Exchange. **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o conteúdo do e-mail (corpo, anexo) que causou o evento DLP.	Sim

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure
Você precisa das seguintes permissões/funções de API em um aplicativo do Microsoft Azure para configurá-lo **ServiceNow** *Integração do Microsoft DLP.*

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
	User.Read	Delegado	Entre e leia o perfil do usuário.	Esta é a permissão padrão que estará disponível para todas as novas aplicações.	Não

Detectadas informações confidenciais (opcional)

O conteúdo de correspondência é armazenado externamente no Armazenamento de blob do Azure ou no bucket do Amazon S3 e será extraído do armazenamento externo quando o usuário exibir um incidente.

Qualquer uma das seguintes permissões será necessária se os usuários quiserem exibir conteúdo de correspondência/informações confidenciais detectadas na aplicação DLP Core:

1. Se você for um Microsoft Azure Usuário, você deve ter a função Colaborador de dados de blob de armazenamento para ler, gravar e excluir blobs no Armazenamento do Azure.
2. Se você for um usuário do Amazon S3, deverá criar uma política que forneça acesso de lista, leitura, gravação e exclusão para o objeto no Amazon S3 Storage.

Instale e configure a integração do Microsoft DLP

Instale e configure a#integração de resposta a incidentes do DLP com Microsoft DLP do ServiceNow® Store em seu ServiceNow AI Platform instância. Comece a investigar incidentes de DLP usando Microsoft Dados de evento do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Baixe o. Microsoft Integração do DLP do ServiceNow® Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Configure o. Microsoft Integração do DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Pesquisar **Integração de resposta a incidentes do DLP com a Microsoft** lado a lado e clique **Configurar** .



b. No formulário, preencha os campos.

Formulário Configuração de integração do Microsoft DLP

Campo	Descrição
Nome	Nome do Microsoft Configuração de integração do DLP.
ID de cliente	ID do cliente do aplicativo criado no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente do aplicativo criado no portal do Microsoft Azure.
ID de locatário	ID do locatário do usuário.

c. Clique em **Enviar**.

Depois de validar e enviar a configuração com êxito, o Microsoft A integração do DLP é salva na página Integrações de segurança como um bloco.

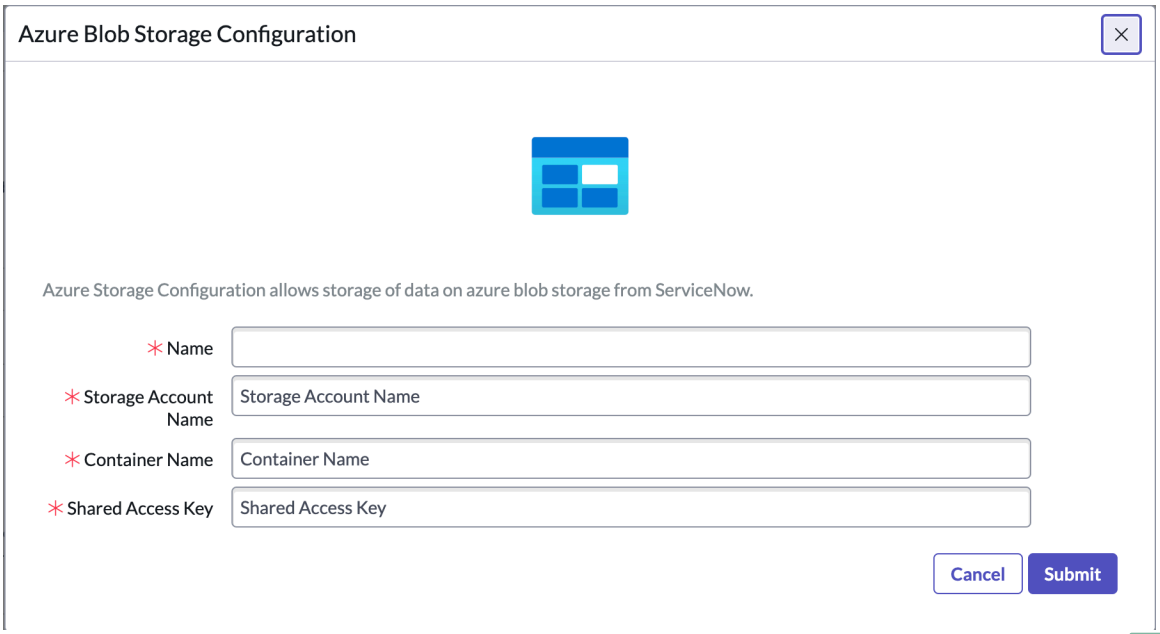
4. Atualize a Configuração de armazenamento do Azure.

a. Na página Integrações de segurança, pesquise **Configuração de armazenamento do Azure** lado a lado.

b. No bloco Configuração de armazenamento do Azure, clique em **Atualização** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. No formulário, preencha os campos.

Formulário Configuração de armazenamento do Azure

Campo	Descrição
Nome	Nome da configuração de Armazenamento do Azure.
Nome da conta de armazenamento	Nome da conta de armazenamento criado no portal do Azure
Nome do contêiner	Nome do contêiner criado na conta de armazenamento no portal do Azure.
Chave de acesso compartilhada	Chave de acesso compartilhada para a conta de armazenamento.

d. Clique em **Enviar**.

Depois de validar e enviar a configuração com êxito, a Configuração de armazenamento do Azure será salva na página Integrações de segurança como um bloco.

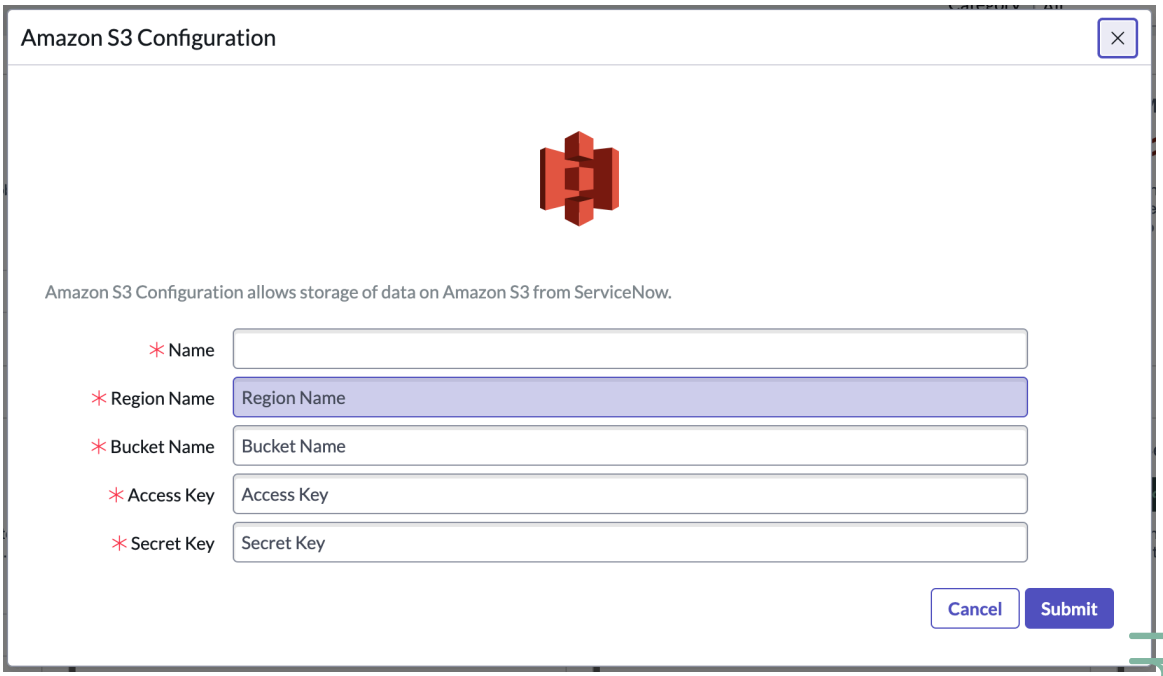
5. Atualize a Configuração de armazenamento da AWS.

a. Na página Integrações de segurança, pesquise **Configuração de armazenamento da AWS** lado a lado.

b. No bloco Configuração de armazenamento da AWS, clique em **Atualização** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. No formulário, preencha os campos.

Formulário Configuração de armazenamento da AWS

Campo	Descrição
Nome	Nome da configuração do armazenamento da AWS.
Nome da região	Nome da região da conta de armazenamento da AWS.
Nome do Bucket	Nome do bucket criado no portal da AWS.
Chave de acesso	Chave de acesso com acesso de leitura, gravação e exclusão.
Chave Secreta	Chave compartilhada com acesso de leitura, gravação e exclusão

d. Clique em **Enviar**.

Resultado

Depois de validar e enviar a configuração com sucesso, a Configuração do AWS S3 será salva na página Integrações de segurança como um bloco.

Crie um novo perfil de incidente para Microsoft Integração do DLP

Crie um perfil de incidente em seu ServiceNow AI Platform Instância para recuperar os dados do Microsoft Purview e adicionar os dados ao ServiceNow DLP IR tabela de incidentes.

Antes de Iniciar

Função necessária: sn_dLIR.admin(criar, editar e excluir)

sn_dLIR.analyst - Exibir (somente leitura)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Configure o. ServiceNow AI Platform®para recuperar os eventos do Microsoft Escopo. Armazene esses eventos no DLP IR Tabela de incidentes em seu ServiceNow® instância.

Procedimento

1. Navegar até **Integração do Microsoft DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

Formulário Criar um perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	. Microsoft DLP IR instância que você configurou para ingerir incidentes. Se você tiver várias configurações de integração, selecione o registro de configuração de integração apropriado para os tipos de incidente que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois que você clicar em **Concluir** Na seção Programação. Quando o perfil está ativo, isso implica que ServiceNow AI Platform está pesquisando ativamente Microsoft DLP IR eventos baseados na configuração definida no perfil.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição exclusiva do perfil.

O que Fazer Depois

Para ir para a seção Filtragem,#clique em **Continuar** .

Configuração de armazenamento de endpoint do Microsoft purview

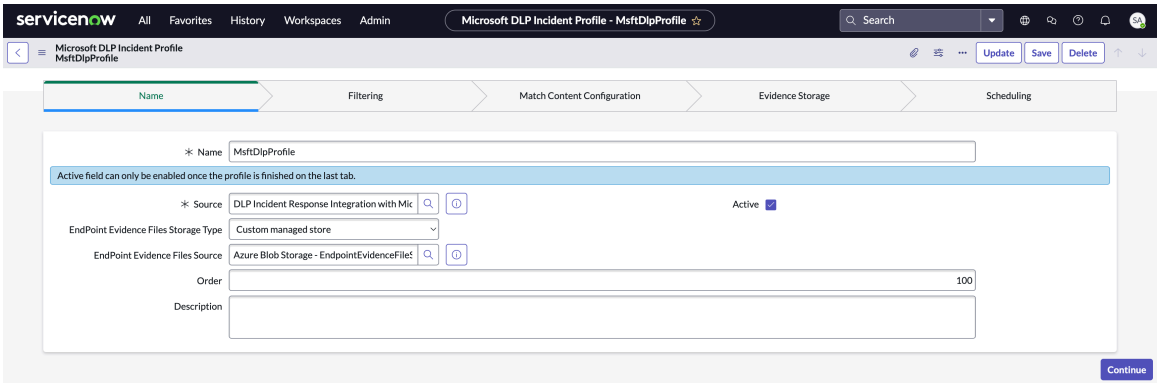
A configuração de armazenamento de arquivos de evidência do endpoint do Microsoft purview informa onde os arquivos de evidência do endpoint estão sendo armazenados pelos ambientes de armazenamento gerenciado personalizado ou armazenamento gerenciado pela Microsoft.

No caso de armazenamento gerenciado pela Microsoft, a própria Microsoft armazena os arquivos de evidência em algum local e, para armazenamento gerenciado personalizado, você precisa especificar o contêiner no qual os arquivos de evidência serão armazenados pela finalidade quando um alerta for gerado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione um dos dois tipos de armazenamento com base no que está sendo configurado no final do escopo para que o sistema busque os arquivos de evidência dos incidentes de DLP de endpoint correspondentes.



Nota: Recomendamos o uso do **Armazenamento gerenciado personalizado** Atualmente, a Microsoft não fornece APIs para recuperar arquivos de evidência do **Microsoft Managed Store** . Como resultado, a funcionalidade de visualização e download não é compatível com evidências armazenadas na Microsoft Managed Store. Levantamos um caso com a Microsoft sobre essa limitação.

Defina filtros a serem aplicados à criação do incidente

Defina e defina condições de filtro para filtrar os##eventos de entrada do Microsoft DLP. Controle qual desses eventos deve ser criado como DLP IR incidentes em seu ServiceNow instância.

Antes de Iniciar

Função necessária: sn_dLIR.admin(criar, editar e excluir)

sn_dLIR.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda você a isolar#eventos do Microsoft DLP para limitar o número de DLP IR incidentes que você cria. Se os critérios de filtragem estiverem definidos, somente os eventos que corresponderem às condições serão criados como incidentes DLP.

Procedimento

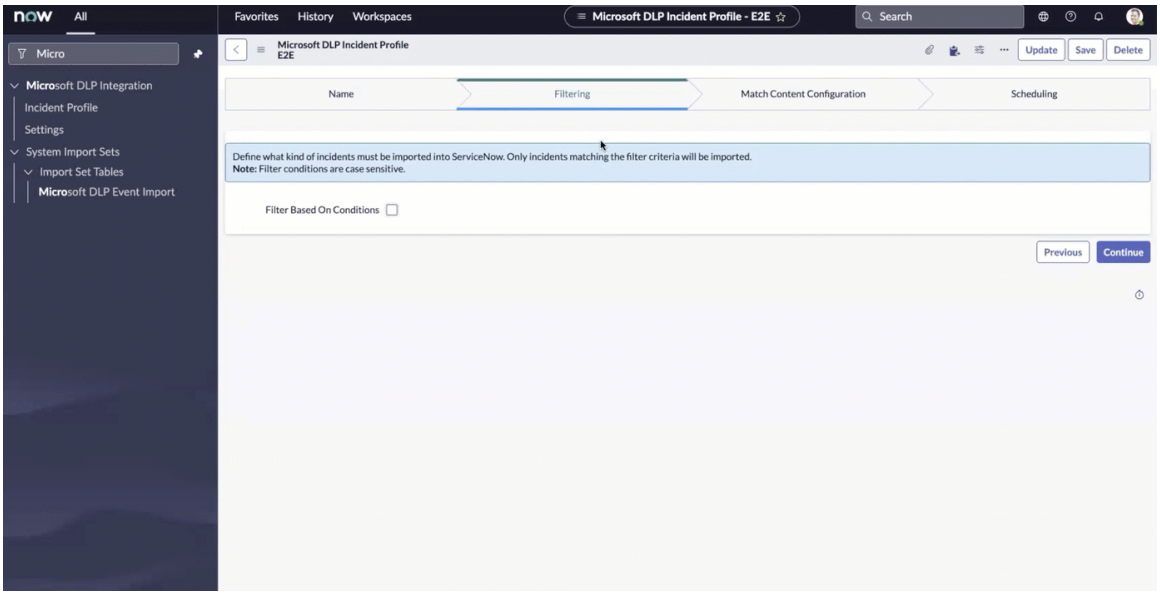
1. Selecione **Filtro com base em condições** opção.
2. Usando as listas e os campos do construtor de condições, defina os filtros no **Condições de filtro** campo.

   Defina os critérios que um de entrada Microsoft O evento do DLP deve satisfazer para que um incidente do DLP seja criado.

   As opções no primeiro campo em **Condições de filtro** Corresponda os campos que estão disponíveis no evento do Microsoft DLP. Os critérios inseridos diferenciam maiúsculas de minúsculas. Verifique se os critérios definidos correspondem aos valores do evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em para adicionar mais condições **E.** #ou**OU** .
   - Se **E.** #selecionado, todas as condições devem ser correspondidas.
   - Se **OU** #está selecionado, qualquer condição pode ser correspondida.
4. Clique em **Continuar** E mover para a seção Corresponder configuração de conteúdo.
   UserID era mapeado somente para o campo Usuário de origem, mas o campo UserID está disponível como um atributo de pesquisa para todos os eventos de finalidade, incluindo eventos de endpoint.

Configure o conteúdo de correspondência do incidente

Forneça a configuração para armazenar as informações confidenciais no armazenamento em nuvem externo, como Armazenamento do Azure ou bucket do AWS S3, para recuperar esse conteúdo em uma carga ao acessar o Incidente de IR do DLP.

Antes de Iniciar

Função necessária: sn_dLIR.admin(criar, editar e excluir)

sn_dLIR.analyst - Exibir (somente leitura)

Procedimento

1. Na barra de andamento, clique em **Corresponder à configuração de conteúdo** etapa.
2. No formulário, preencha os campos.

Corresponder configuração de conteúdo

Campo	Descrição
Armazenar conteúdo de correspondência	Opção para armazenar o conteúdo correspondente no armazenamento em nuvem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Importante: Se esta opção não estiver selecionada, o conteúdo de correspondência de política para incidentes do DLP não poderá ser visto no espaço do DLP. Habilitar esta opção garante que o conteúdo correspondente retornado nos incidentes do DLP seja armazenado no armazenamento em nuvem externo (por exemplo, Azure, AWS). Você também pode recuperar e exibir o conteúdo de correspondência sempre que um incidente do DLP for aberto no espaço. Para obter informações sobre a configuração do Armazenamento externo em nuvem, consulte Instale e configure a integração do Microsoft DLP.
Excluir conteúdo de correspondência na exclusão do incidente	Opção para excluir o conteúdo de correspondência do incidente do armazenamento em nuvem externo. Esta opção fica visível somente quando **Armazenar conteúdo de correspondência** o campo está selecionado.
Credenciais de acesso à nuvem externas	O armazenamento externo em nuvem onde o conteúdo correspondente é armazenado. Você pode consultar Credenciais de nuvem externas adicionadas para a configuração de armazenamento. Esta opção fica visível somente quando **Armazenar conteúdo de correspondência** o campo está selecionado.

3. Clique em **Continuar** E mover para a seção Programação.

Programe o. DLP IR Recuperação de incidentes da Microsoft

Defina uma programação para recuperar os dados do incidente e ingerir Microsoft DLP IR incidentes que correspondem aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Microsoft.

Antes de Iniciar
Função necessária: sn_dLIR.admin(criar, editar e excluir)

sn_dLIR.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer recuperação única usando **Recuperação única** caixa de seleção. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho do Microsoft DLP IR integração de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

incidentes. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Procedimento

1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

Formulário de incidente do DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidente em andamento que o ServiceNow AI Platform A instância extrai da Microsoft novos incidentes. DLP IR os incidentes serão criados se incidentes acionados forem encontrados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa da Microsoft. Este campo é definido automaticamente como 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa. Esta opção fica visível somente quando **Ingestão de incidentes em andamento** o campo está selecionado.
Horário de entrada de adição do incidente inicial	Data e hora especificadas para a ingestão do incidente. ○ Se o valor estiver definido, a recuperação de dados da Microsoft começará na data futura adicionada. ○ Este campo fica visível somente quando **Defina o tempo de ingestão inicial** selecionado.
Horário de adição do incidente inicial	Primeira vez quando os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	O próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar extrações de dados históricos únicas. Se este campo for selecionado, os dados históricos serão extraídos da Microsoft DLP IR de acordo com a data adicionada em **A partir da data** campo.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Microsoft.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este campo pode ser definido como no máximo 7 dias.

3. Salve a configuração de perfil criada clicando em **Concluir** na janela pop-up.
4. Ative o perfil.
   a. Abra o perfil criado.
   b. Habilite o. **Ativo** opção.
   c. Clique em **Atualizar**.

Resultado

Após a criação e ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela Incidentes do DLP.

Configurar o Microsoft DLP IR configurações de integração

Modifique o. Microsoft DLP IR#propriedades do sistema padrão de integração.

Antes de Iniciar

Função necessária: sn_dLIR.admin

Procedimento

1. Navegar até **Integração Microsoft com DLP** > **Configurações**.
2. Modifique as propriedades a seguir conforme necessário.

Configurações de integração do Microsoft DLP

Campo	Descrição
Tempo limite máximo para chamadas HTTP (sn_pp_dlp.maximum_http_time_out)	Tempo limite máximo para chamadas HTTP (em segundos). ○ Tipo: inteiro ○ Valor padrão: 30
Nível de emissão de relatórios dos logs gerados pela integração (sn_pp_dlp.logging.verbosity)	O nível de logs de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** ○ **desativado** Por padrão, o valor é **informações** .
Destino do relatório dos logs gerados pela integração (sn_pp_dlp.logging.destination)	O destino dos logs gerados pela integração. Você também pode atualizar o valor para as seguintes opções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **banco de dados** ○ **arquivo** ○ **nenhum** Por padrão, o valor é **banco de dados** .

3. Clique em **Salvar**.

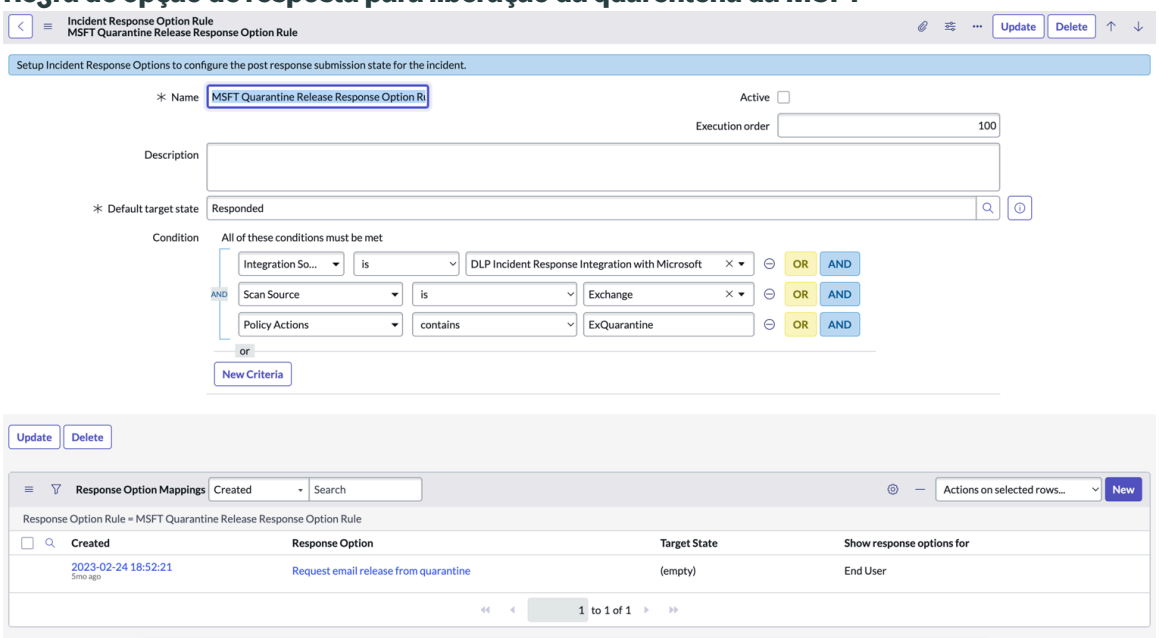
Resultado
Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Solicitar e-mail de liberação da quarentena

Use este recurso para liberar o e-mail que está em quarentena do portal de conformidade do Microsoft Purview.

Antes de Iniciar
Por padrão, o sistema de base fornece o. **Solicitar liberação de e-mail da quarentena** opção de resposta e. **Regra de opção de resposta da versão de quarentena do MSFT** para liberar o e-mail da quarentena. Este registro padrão também tem **Regra de aprovação da versão de quarentena** configurado com ele para aproveitar a funcionalidade de aprovação desta ação. Para obter mais informações, consulte Criar regras de opção de resposta a incidentes, Configure a opção de resposta para seus incidentes de DLP e Criar regras de aprovação.

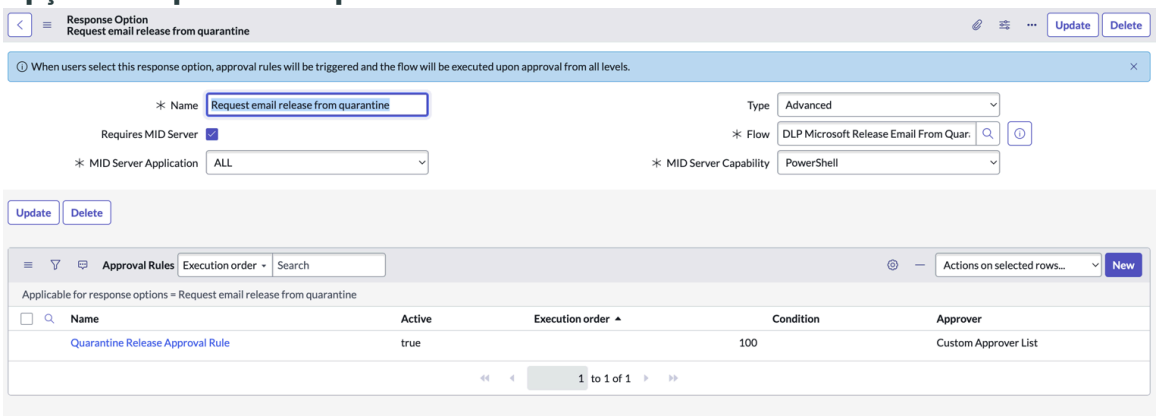
Regra de opção de resposta para liberação da quarentena da MSFT



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção de resposta MSFT padrão



Pré-requisitos :

1. O módulo PowerShell do Exchange Online precisa ser instalado no MID Server. Para obter mais informações, consulte Instale e mantenha o PowerShell do Exchange Online .
2. O MID Server precisa se comunicar com o servidor Exchange, que também é um serviço em nuvem. Portanto, o MID Server requer acesso contínuo à Internet.

Nota: Se você estiver usando esta opção de resposta, certifique-se de que o MID Server esteja instalado e em execução com o recurso PowerShell. Se um MID Server não estiver instalado e em execução e não tiver o recurso PowerShell, o usuário final não poderá selecionar **Solicitar liberação de e-mail da quarentena** Ação do espaço Usuários do DLP. Para obter mais informações, consulte Criar regras de opção de resposta a incidentes e Configure a opção de resposta para seus incidentes de DLP.

- Se você quiser um MID Server específico da lista, será necessário configurar o aplicativo MID e torná-lo visível na lista e, em seguida, pelo menos um MID Server configurado deve estar ativo e em execução nas aplicações MID selecionadas e deve ter o recurso Power Shell.
- Para você usar a opção Liberar da quarentena, você precisa de permissões de API. Na página Permissões de API da Microsoft, verifique **Exchange Online do Office 365** > **Exchange.ManageAsApp** está listado e contém os seguintes valores:
  - **Tipo** : **Aplicação** .
  - **Consentimento do administrador necessário** : **Sim** .
  - **Status** : O valor incorreto atual é **Não concedido para o <Organization>** para **Exchange Online do Office 365** > **Exchange.ManageAsApp** e mude o valor do status. Para obter mais etapas sobre as permissões de API, consulte Atribua permissões de API à aplicação No site de documentação da Microsoft.

    Nota: Esta etapa é necessária para se conectar ao Exchange on-line usando o princípio de serviço.

- Você também deve precisar **Administrador de segurança** Princípio de função no serviço,
  - Pesquisar **Funções e administradores do Microsoft Entra ID** No portal do Microsoft Azure, adicione a atribuição ao aplicativo registrado (princípio de serviço) e siga o procedimento explicado na Documentação da Microsoft sobre como fazer atribua uma função .
- Esta opção é aplicável somente a incidentes do Microsoft Exchange que têm **Ação de política** opção como **ExQuarentena** na exibição do formulário de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

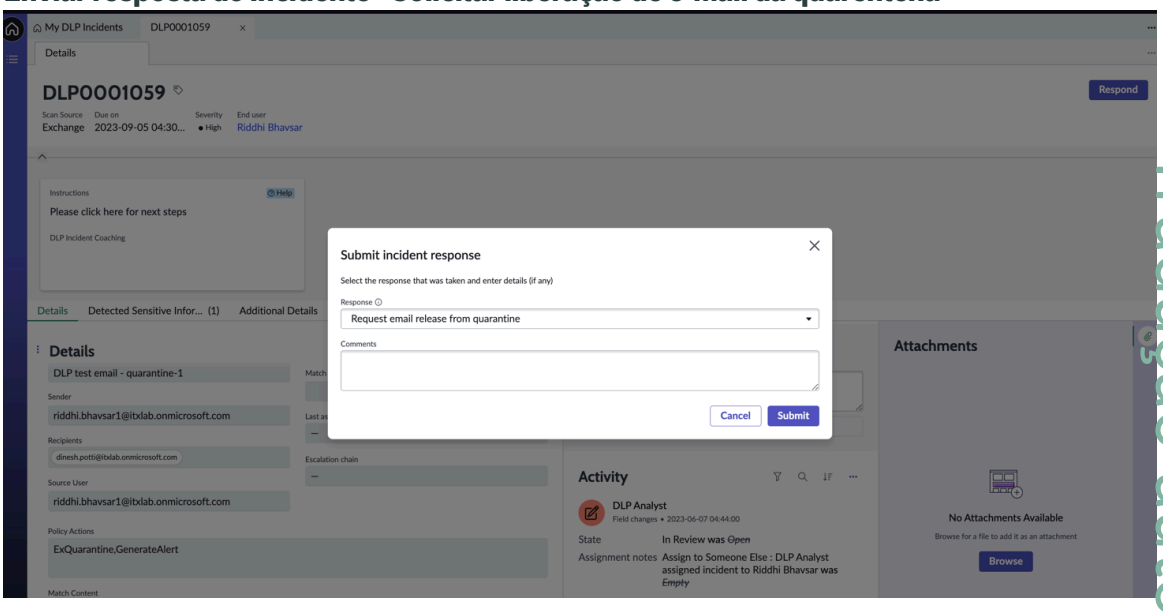
Função necessária: Usuário final

O procedimento a seguir explica como enviar esta ação do Espaço do usuário do DLP.

Procedimento

1. Navegar até **DLP** > **Espaço do usuário do DLP**.
2. Abra qualquer incidente do Microsoft Exchange DLP.
   Verifique se o incidente **Ação de política** Está definido como ExQuarentena.
3. Clique em **Responder** .
4. Selecione **Solicitar e-mail de liberação da quarentena** Opção da lista suspensa Resposta.

Enviar resposta do incidente - Solicitar liberação de e-mail da quarentena



5. Clique em **Enviar**.

> **Nota:** Quando uma regra de aprovação é configurada para esta ação, o fluxo de aprovação será acionado primeiro e, depois de receber todas as aprovações, a solicitação de liberação de e-mail do fluxo de quarentena será acionada e o e-mail será liberado da quarentena. O estado do incidente do DLP será atualizado para **Liberado da quarentena** após a versão bem-sucedida.

Baixe arquivos para incidentes de DLP do tipo Exchange Online, OneDrive e SharePoint

Baixe arquivos ou e-mail que violem a política de DLP no Microsoft Purview. Baixe este arquivo ou e-mail para sua máquina local do DLP IR Exibição de incidentes. Você pode baixar os arquivos para DLP IR Incidentes do tipo Verificar origem do Exchange Online, OneDrive e SharePoint.

Antes de Iniciar

Função necessária:

- sn_dlir.admin, sn_dlir.analyst
- Qualquer aprovador válido

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP do tipo Verificar origem do Exchange Online, OneDrive ou SharePoint que é ingerido da origem da Microsoft.
3. Clique em **Download do arquivo** .
   O arquivo ou e-mail que violou a política de DLP no lado do perfil da Microsoft será baixado para a máquina local do usuário.

> **Nota:** O administrador do DLP pode controlar o acesso de **Download do arquivo** desabilitando o. **O download do arquivo de violação do incidente relatado deve ser permitido** Configuração na página Configurações avançadas. Para obter mais informações, consulte Definir configurações avançadas.

Visualize arquivos de evidência para incidentes de DLP do tipo Exchange Online, OneDrive e SharePoint

Visualização Data Loss Prevention Incident Response Arquivos de evidência no espaço Analista de IR do DLP.

Antes de Iniciar

> **Importante:** Ao usar a ação Arquivos de evidência no espaço do analista do DLP, os arquivos de evidência são armazenados temporariamente no banco de dados da ServiceNow em um formato não criptografado. Se você não quiser armazenar os arquivos de evidência, desabilite o recurso de visualização de arquivos de evidência. Para obter mais informações, consulte Definir configurações avançadas.

Função necessária: sn_dLIR.analyst

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes da DLP** > **DLP Analyst Workspace**.
2. Abra um registro de incidente do DLP.
3. Na barra lateral contextual, selecione o ícone Arquivos de evidência ( ).
4. Em **Arquivos de evidência** , selecione **Arquivo de evidência** cartão para visualizar os arquivos de evidência no visualizador de documentos.

   O recurso de visualização é diferente para cada tipo de arquivo, conforme listado na tabela a seguir.

Formato do arquivo	Extensão de arquivo
Imagem	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg e .webp. Arquivos de imagem são abertos no modo de visualizador de documentos.
Microsoft Arquivos do Office	.doc, .docx, .ppt, .pptx, .xls, e .xlsx Os arquivos do Office são abertos no modo de visualizador de documentos.
Arquivos de texto	.txt

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formato do arquivo	Extensão de arquivo
	Arquivos de texto são abertos no modo de editor de texto.
Arquivos de e-mail	.eml **Nota:** O tamanho do arquivo deve ser inferior a 5 MB. Primeiro, você deve baixar o arquivo para visualizar seu conteúdo.
Arquivos PDF	.pdf ○ Insira uma palavra-chave para pesquisar o documento. ○ Recursos de zoom-in e zoom-out para ajustar a exibição para melhor legibilidade. ○ Gire a página no sentido horário ou anti-horário para exibir o conteúdo com mais clareza.

Nota:

Os arquivos binários não serão renderizados e precisam ser baixados para visualizar seu conteúdo. O recurso de visualização de arquivo de evidências também funciona para incidentes arquivados.

Domain Separation em Microsoft Integração do DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com Microsoft Integração do DLP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com função necessária no respectivo domínio.
- Execute Microsoft Procedimentos de integração do DLP no domínio apropriado.

Operações de segurança funcionalidade comum

Qualquer um dos plug-ins para o principal Operações de segurança aplicações (Resposta a incidentes de segurança, Resposta a vulnerabilidades, Inteligência contra ameaças Ou Conformidade de configuração) estão ativados, o. Security Support Common o plug-in está ativado. Este plug-in carrega vários módulos que fornecem funcionalidade que é comum em todos Operações de segurança aplicações.

Nota: Somente usuários com [sn_sec_cmn.admin] podem exibir e usar o. Operações de segurança módulo. Esta função é herdada quando você recebe uma função administrativa em qualquer um dos Operações de segurança aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos de operações de segurança

Recurso	Descrição
Referência do Security Operations Integrations, Integrações do Inteligência contra ameaças, Integrações do Resposta a vulnerabilidades	Várias integrações estão incluídas com Operações de segurança aplicações (Resposta a incidentes de segurança, Inteligência contra ameaças e Resposta a vulnerabilidades). Esta seção fornece instruções para ativar os plug-ins e configurar ambos ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.
Operações de segurança processamento de e-mail	Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.
Grupos	• **Grupos de filtros** Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores pelo mesmo fabricante. Você também pode filtrar itens de configuração (ICs) que têm vulnerabilidades semelhantes ou que se enquadram em um intervalo de endereços IP de sub-rede específico. • **Escalações** Você pode criar um caminho de escalação de incidentes de segurança para problemas que exigem mais atenção ou conhecimento especializado. Quando um grupo de escalação existe, um botão aparece em qualquer incidente de segurança nesse grupo.
Marcadores de Segurança	**Marcadores** : As regras de marcador de segurança fornecem filtragem para acesso a marcador de segurança.
Fluxos de trabalho	• **Exibir Fluxos de Trabalho de Segurança** Você pode exibir os muitos fluxos de trabalho incluídos com as aplicações Operações de segurança. Você pode criar fluxos de trabalho a partir de modelos e no Editor de fluxo de trabalho. • **Gatilhos de fluxo de Trabalho**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
	Operações de segurança os gatilhos de fluxo de trabalho contêm uma condição em uma tabela. Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.
Utilitários	• **Mapeamento de Dados de Aprimoramento** Mapeamento de Dados de AprimoramentoTransforma dados de XML, JSON ou Propriedadesarquivos para ServiceNow registros. Operações de segurança os fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança. • **Transformações de Valores de campos** Transforma valores de campo do cliente exclusivos em valores de campo reconhecidos por Operações de segurança análise de e-mail, aprimoramento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de escolha, referências e alinha dados externos à terminologia e ao formato padrão do seu novo registro. • **Mapeamento de campo** Operações de segurança as tabelas podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do Operações de segurança sistema. Por exemplo, você pode integrar um plug-in a um Resposta a incidentes de segurança tarefa. • **Orquestração sob Demanda** Durante Resposta a incidentes de segurança um analista de segurança pode querer executar uma tarefa orientada por um fluxo de trabalho de incidente de segurança. Por exemplo, execute um despejo de processo em um IC específico. Isso pode ser feito com orquestração sob demanda. • **Grupos de sistemas operacionais** N/D. • **Registro da aplicação SecOps** N/D.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
CMDB	**Regras de Identificador de IC** Identificadores de IC são regras usadas para pesquisar um item de configuração (IC) no CMDB que contém informações correspondentes de uma integração de terceiros. Essas regras definem os campos que contêm dados correspondentes e a ordem de precedência pela qual eles são avaliados. O mais baixo **Pedido** o valor é avaliado primeiro.

Criar e definir grupos de filtros em Operações de segurança

Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores pelo mesmo fabricante. Você também pode filtrar itens de configuração (ICs) que têm vulnerabilidades semelhantes ou que se enquadram em um intervalo de endereços IP de sub-rede específico.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Os grupos de filtros podem conter registros atualizados dinamicamente, uma série de registros estáticos que não são filtrados usando condições ou uma combinação de registros estáticos e atualizados dinamicamente. Alguns grupos de filtros estão incluídos no sistema de base, por exemplo, exclusões de IC.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Grupos** > **Grupos de filtros**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome do grupo de filtros.
Ativo	Para ativar o grupo.
Descrição	Descrição do grupo de filtros.
Endereço IP da Rede	O endereço IP de rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo. Este campo aparecerá somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no **Tabela** campo.
Máscara de sub-rede	A sub-rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo, por exemplo, 255.255.255.0. Este campo aparecerá somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no **Tabela** campo.
Tabela	A tabela a ser filtrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Use construtor de condições para definir os critérios a serem filtrados.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   Um **Condições avançadas** é exibida.

   Mais guias são exibidas dependendo do tipo de tabela especificado em **Tabela** , da seguinte forma:

Tabela	Guias exibidas
Item de configuração [cmdb_ci] ou uma tabela que estende a tabela de item de configuração	**ICs adicionados manualmente** e. **ICs correspondentes**
Tarefa [task] ou uma tabela que estende a tabela de tarefas	**Tarefas adicionadas manualmente** e. **Tarefas correspondentes**
Uma tabela não relacionada a um IC ou tarefa	**Registro Adicionado Manualmente**

5. Para definir mais condições para o seu grupo de filtros:

   a. Clique em **Condições avançadas** .

   b. Insira uma nova linha no **Condições adicionais do grupo de filtros** lista integrada para selecionar outros grupos de filtros pré-criados que você deseja combinar com o grupo de filtros que está sendo atualizado.
   Se você quiser que o grupo de filtros selecionado filtre registros com base em um campo de referência, um campo mapeado será selecionado automaticamente quando o registro atual for salvo.

   Nota: . **Campo mapeado** o valor não pode ser editado no **Condições adicionais do grupo de filtros** lista integrada. Para mudar o campo, clique no ícone de informações para abrir o registro.

   c. Clique em **Atualizar**.

6. Para adicionar manualmente mais ICs ou tarefas ao grupo de filtros:

   a. Clique em **ICs adicionados manualmente** ou **Tarefas adicionadas manualmente** guia.

   b. Clique em **Editar**.

   c. Selecione os ICs ou tarefas que você deseja adicionar.

   d. Clique em **Salvar**.

7. Para exibir os ICs ou tarefas que correspondem aos seus critérios de seleção:

   a. Clique em **ICs correspondentes** ou **Tarefas correspondentes** guia.

   b. Se você alterou os critérios, atualize a lista clicando com o botão direito do mouse no cabeçalho do formulário e selecionando **Atualizar lista** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transformação de dados compartilhados

. Resposta a incidentes de segurança, Resposta a vulnerabilidades e Inteligência contra ameaças os plug-ins compartilham recursos comuns, para dados de relacionamento e regras de duplicação, usados para importar informações externas e internas para Operações de segurança.

Análise de E-mails, Regras de Duplicaçãoe Mapeamento de campoPegue os dados de entrada (um e-mail, arquivo JSON ou XML ou um registro) e transforme esses dados no formato correto para criar um novo registro. Cada um desses recursos extrai dados de sua própria maneira, mas é transformado no novo registro usando muitos dos mesmos processos.

Dados de relacionamento

Ao adicionar informações a uma lista relacionada (como um observável associado em um incidente de segurança), você pode criar um registro de relacionamento que consiste em uma tabela m2m. Às vezes, há dados adicionais sobre esse registro de relacionamento a serem definidos. Por exemplo, um observável é um IP de origem (em oposição a um IP de destino). Essas informações vão para **Dados de relacionamento** . **Transformação de campo** formulário usado por **Análise de e-mail** ou um **Campos de mapeamento de campo** lista relacionada em **Mapeamento de campo** formulário.

. **Dados de relacionamento** o campo geralmente está vazio. É mais comumente usado para endereços IP em observáveis em **Análise de e-mail** .

Você pode transformar dados de qualquer ServiceNow grave em qualquer outro ServiceNow registre usando **Campos de mapeamento de campo** em **Mapeamento de campo** recurso. Por exemplo, para transformar dados de um incidente em um incidente de segurança ou um incidente de segurança em um PRB.

Regras de duplicação de Operações de segurança

Usar Regras de DuplicaçãoPara lidar com registros duplicados para segurança, vulnerabilidade, IOCs e assim por diante.

As regras de duplicação têm duas finalidades. Eles impedem que muitos registros duplicados sejam criados e, quando uma duplicata é detectada, especificam quais campos no registro são atualizados. São pesquisadas somente duplicatas ativas. Se o registro não estiver ativo, por exemplo, se o incidente estiver encerrado, qualquer novo problema idêntico se tornará um novo incidente.

Regras de duplicação são usadas por **Análise de e-mail** , **Mapeamento de campo** e **Mapeamento de dados de aprimoramento** .

Tópicos relacionados

Crie analisadores de e-mail em Operações de segurança

Mapeie tabelas para tabelas com mapeamento de campo Operações de segurança

Crie regras de duplicação em Operações de segurança

Você pode usar Regras de Duplicaçãopara identificar novos e-mails, dados de aprimoramento ou mapas de campo com registros duplicados ativos e processá-los adequadamente.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Regras de Duplicação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado:

Regra de duplicação

Campo	Descrição
Nome	O nome da regra de duplicação.
Tabela	Tabela em que os registros são criados e usados para determinar a duplicação.
Campos de identificação	Selecione um conjunto de campos que indicam um incidente de segurança duplicado, observável, vulnerabilidade e assim por diante, quando os valores nesses campos forem idênticos.
Ação duplicada	Controla como lidar com e-mails duplicados. As opções são: **Criar como secundário** Cria um registro como secundário do original. O campo que vincula o secundário ao primário é **Primário** campo. **Não criar nem atualizar registros** (Padrão) não faz nada. Ignora duplicatas. **Atualizar registro duplicado** Atualiza os campos no registro existente conforme especificado em **Ações de duplicação.** **Nota:** Se você escolher **Atualizar registro duplicado** . **Ações de duplicação** a lista relacionada é exibida.
Ativo	Marque esta caixa de seleção para ativar a regra.
Descrição	Descreve a finalidade e a aplicação desta regra de duplicação; quando ela deve ser usada, por exemplo, uma regra projetada para observável baseado em IP ou incidentes de segurança do firewall.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar** ou clique em **Atualização** .
5. Para definir ações de duplicação, se você tiver escolhido **Atualizar registro duplicado** clique em **Novo** para criar ações de duplicação para cada campo que você deseja atualizar no incidente.
6. Preencha ou edite os campos no formulário para descrever como atualizar o campo:

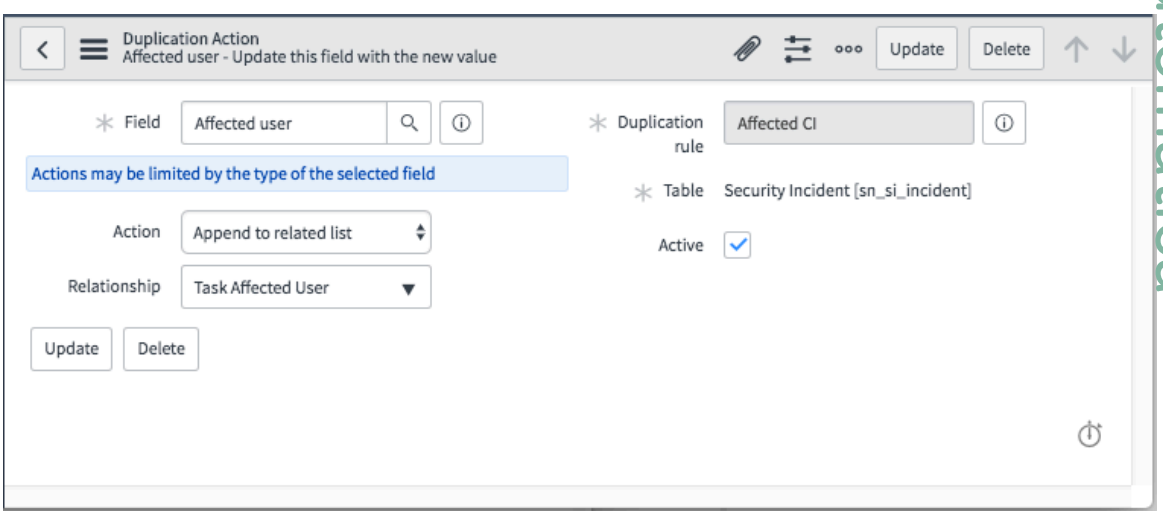
Ações de duplicação

Campo	Descrição
Campo	O nome do campo a ser usado para a ação de duplicação.
Ação	As ações compatíveis variam de acordo com o tipo de campo. As opções são: **Atualizar este campo com o novo valor** Substitui o valor anterior no registro existente por este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

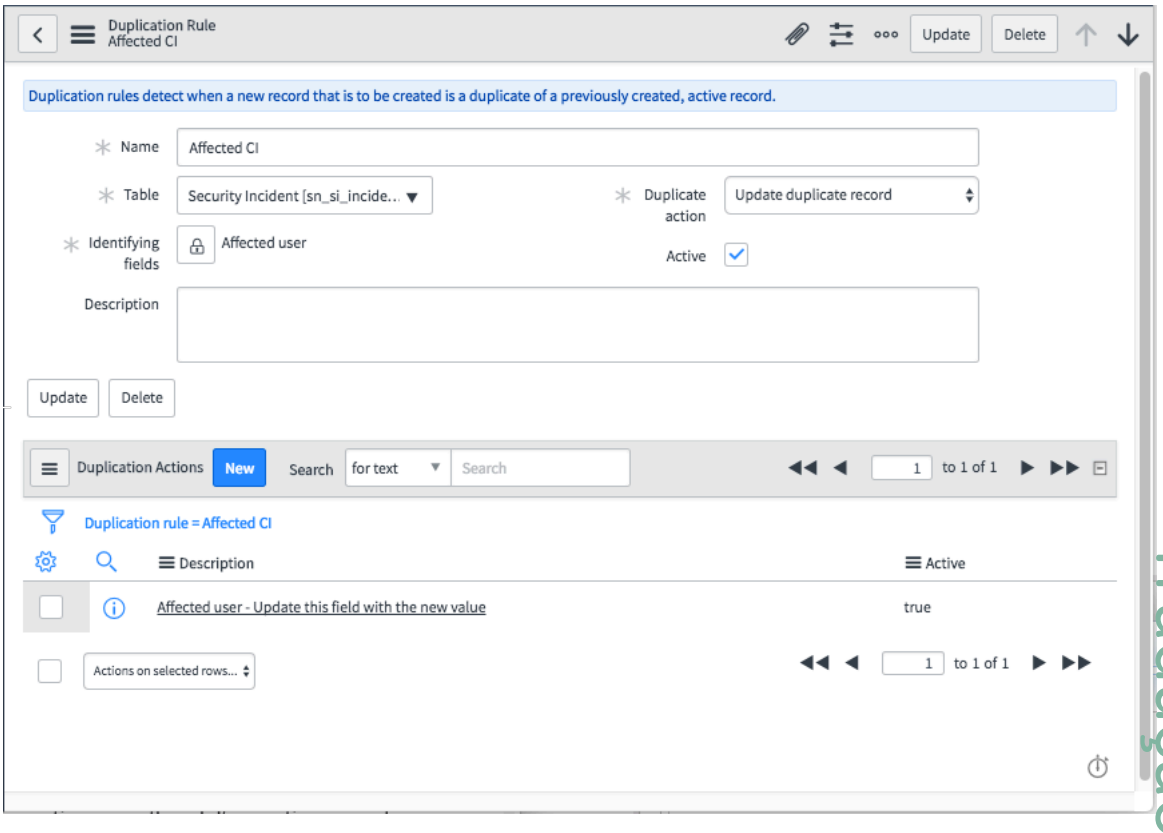
Campo	Descrição
	Anexar o novo valor a uma lista separada por vírgulas, se exclusivo Trata o valor como uma entrada em uma lista separada por vírgulas e adiciona os novos dados (se houver) como uma nova entrada nessa lista. Se os dados já estiverem na lista, eles não serão adicionados duas vezes. **Anexar o novo valor a este campo** Anexa o novo valor ao final do texto existente no campo. **Adicionar um a um campo de contador** Adiciona um ao campo numérico. **Definir o campo como hoje** Define o campo como a data e a hora atuais. **Anexar à lista relacionada** Adiciona o registro relacionado com este valor à lista relacionada do registro atual. Aparece quando há uma tabela muitos para muitos, com uma coluna do mesmo tipo, vinculada à tabela que está sendo atualizada. Por exemplo, **IC afetado** ou **Usuário afetado** .
Relacionamento	[Opcional] Este campo aparece somente quando **Anexar à lista relacionada** a ação foi escolhida. É o nome da lista relacionada que você deseja associar a esta regra.
Regra de duplicação	Regra da qual esta ação faz parte.
Tabela	Tabela em que os registros são criados. Exibido somente como informações.
Ativo	Marque esta caixa de seleção para ativar a ação.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.



Operações de segurança processamento de e-mail

Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.

Processamento de E-mails consiste nestes recursos:

Recurso	Descrição
Análise de E-mails	Gerar novo Operações de segurança registros de e-mails do sistema externo.
Regras de Duplicação	Identifica novos e-mails com incidentes conhecidos e os processa adequadamente.
Propriedades	Especifica as contas usadas como entrada no Análise de E-mailsPara segurança, vulnerabilidade e IOCs. Fornece granularidade no processamento Operações de segurança registros.
E-mails Incompatíveis	Lista e-mails que não correspondem a nenhum Operações de segurança registro.

Operações de segurança propriedades de e-mail

E-mail Propriedadesespecifique quais caixas de entrada são usadas como entrada no Análise de E-mailsPara importar informações de sistemas de detecção externos para criar registros de segurança, vulnerabilidade e IOCs. Você pode configurar uma conta geral para todos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os sistemas de detecção externos usarem ou contas de e-mail individuais para Resposta a incidentes de segurança, Inteligência contra ameaças ou Resposta a vulnerabilidades.

Criar Operações de segurança propriedades de e-mail

Você pode especificar endereços de e-mail para relatórios e controlar comportamentos de e-mail automáticos usando e-mail Propriedades.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Configure ferramentas de detecção externas para enviar e-mails para sua caixa de entrada de análise de e-mail.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Processamento de E-mails** > **Propriedades**.
2. Insira as caixas de correio do destinatário conforme apropriado:
   Endereços de e-mail de entrada a serem processados por **Análise de e-mail** , em vez de **Ações de entrada** .

Propriedades de análise de e-mail

Campo	Descrição
Caixa de entrada para Operações de segurança ferramentas	Endereço de e-mail completo para Operações de segurança. Por exemplo, secops_support@yourcompany.com.
Caixa de entrada para ferramentas de Incidente de segurança	Endereço de e-mail completo para Resposta a incidentes de segurança. Por exemplo, sir_support@your.company.com.
Caixa de entrada para Resposta a vulnerabilidades ferramentas	Endereço de e-mail completo para Resposta a vulnerabilidades. Por exemplo, vuln_resp@yourcompany.com.
Caixa de entrada para Inteligência contra ameaças ferramentas	Endereço de e-mail completo para Inteligência contra ameaças. Por exemplo, threat_intel@yourcompany.com.

3. Clique em **Salvar**.

Operações de segurança análise de e-mail

Gerar novo Operações de segurança registros de sistemas de detecção externos usando Análise de E-mails. Este recurso fornece um método para integrar informações de ferramentas externas, como detecção de malware, detecção de vulnerabilidades, firewalls, inteligência contra ameaças e muito mais.

Como os e-mails são analisados

Qualquer sistema que possa enviar um e-mail, pode criar Operações de segurança registros, por exemplo, incidentes de segurança, solicitações, itens vulneráveis, observáveis de incidentes de segurança, métodos de ataque e muito mais.

Todos Operações de segurança plug-ins (Resposta a incidentes de segurança, Inteligência contra ameaças e Resposta a vulnerabilidades) têm uma propriedade (**email_to**) que define o endereço de e-mail para o qual as integrações externas devem enviar e-mails, a ser analisado pelos analisadores de e-mail. Confira **Processamento de E-mails** > **Propriedades** para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail enviado para qualquer um dos Operações de segurança os endereços de e-mail são armazenados em uma tabela de eventos de e-mail. Esses e-mails são processados para determinar se correspondem a qualquer analisador de e-mail.

Os e-mails que têm uma correspondência são sinalizados e as regras de transformação e duplicação criam ou atualizam um Operações de segurança registro. O e-mail está vinculado a esse registro e sinalizado como `correspondido` .

Os e-mails que não correspondem são listados em E-mails Incompatíveis. Operações de segurança registro. Eles podem ser revisados para ajudar a criar analisadores de e-mail para lidar com esses e-mails. Uma ação de reprocessar permite executar o e-mail incompatível por meio dos analisadores novamente. O log de e-mail original está vinculado a esse registro.

As regras de duplicação para a transformação de e-mail gerenciam vários e-mails relacionados ao mesmo problema. Essas regras definem o que faz um registro duplicado e podem impedir que registros duplicados sejam criados. Quando uma duplicata é detectada, a regra especifica qual ação executar: nenhuma ação (não criar um novo registro), criar o novo registro como um registro secundário do registro existente ou atualizar o registro existente. Ao atualizar a regra duplicada, especifica quais campos no registro existente serão atualizados.

Nota: . Operações de segurança o analisador de e-mail funciona em conjunto com as ações de entrada da plataforma e não as substitui. Não é compatível com a definição de valores em campos indiretos, por exemplo, **sys_journal_field** entradas.

Por padrão, os eventos de e-mail são excluídos após 30 dias.

Vários registros

Os sistemas de detecção externos (detectores de malware, vulnerabilidade e assim por diante) podem enviar e-mails que relatam vários itens de uma só vez. O analisador de e-mail oferece suporte a separadores no e-mail.

Por exemplo, um detetor de malware pode enviar um relatório por e-mail sobre todos os sistemas da sua rede infectados por um malware específico com informações sobre o malware primeiro, seguido por uma lista dos sistemas afetados.

Exemplo de e-mail mal-intencionado

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Neste exemplo, quando **Separador de registro** está definido em seu **Transformação de e-mail** . . ele divide o e-mail em quatro seções que são avaliadas separadamente. Isso cria um Incidente de segurança para cada um dos três sistemas afetados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A seção do cabeçalho foi detectada, mas não tem nenhum sistema afetado, portanto, ela é usada em todos os três registros e não cria um quarto registro.

Transformações de campo extraia dados de cada seção. Se algo no cabeçalho ou rodapé do e-mail se aplicar a todos os registros, como hash de malware, nome do malware e tipo neste exemplo, a transformação de campo para eles deverá ser definida **Pesquisar valor** para um valor que pesquisa no corpo do e-mail **No início de uma linha no corpo do e-mail** ou **Em qualquer lugar no corpo do e-mail** .

Transformação de campo s deve ser definido para pesquisa **No início de uma linha na seção de registro** ou **Seg** Para dados definidos em cada seção, como Sistema, Endereço IP ou Status. As opções da seção de registro só estão disponíveis quando há um separador de registro definido na transformação de e-mail.

Ao analisar um e-mail com um separador definido, os registros são criados somente para seções com pelo menos um pedaço de dados específicos da seção.

Três registros são criados, embora haja quatro seções definidas. A primeira seção é um cabeçalho e não tem nada específico para apenas um sistema. Se qualquer um dos campos na primeira seção for preenchido (Sistema, IP ou Status), um registro também será criado para essa seção.

Tópicos relacionados

Crie analisadores de e-mail em Operações de segurança

Operações de segurança mapeamento de dados de aprimoramento

Operações de segurança mapeamento de campo

Crie analisadores de e-mail em Operações de segurança

Análise de E-mailscria Operações de segurança registros do seu e-mail para segurança, vulnerabilidade e observáveis para agilizar a resposta e correção de ameaças.

Antes de Iniciar

- Configure ferramentas de detecção externas para enviar e-mails para um endereço de e-mail central.
- Defina o endereço de e-mail em Propriedades de operações de segurança. Para obter mais informações, consulte Criar Operações de segurança propriedades de e-mail.
- Atribua uma conta de usuário a este endereço de e-mail e conceda a esse usuário controles de acesso de segurança para criar e atualizar os registros de eventos de e-mail.
- Tenha uma cópia do e-mail relevante da sua ferramenta de detecção externa à sua frente.
- Decida que tipo de registro você deseja criar, um incidente de segurança, registro de vulnerabilidade, tarefa e assim por diante. Esta opção determina a tabela selecionada.

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Análise de E-mails**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se mais de um campo for especificado, todos os campos deverão corresponder ao e-mail para criar um registro.

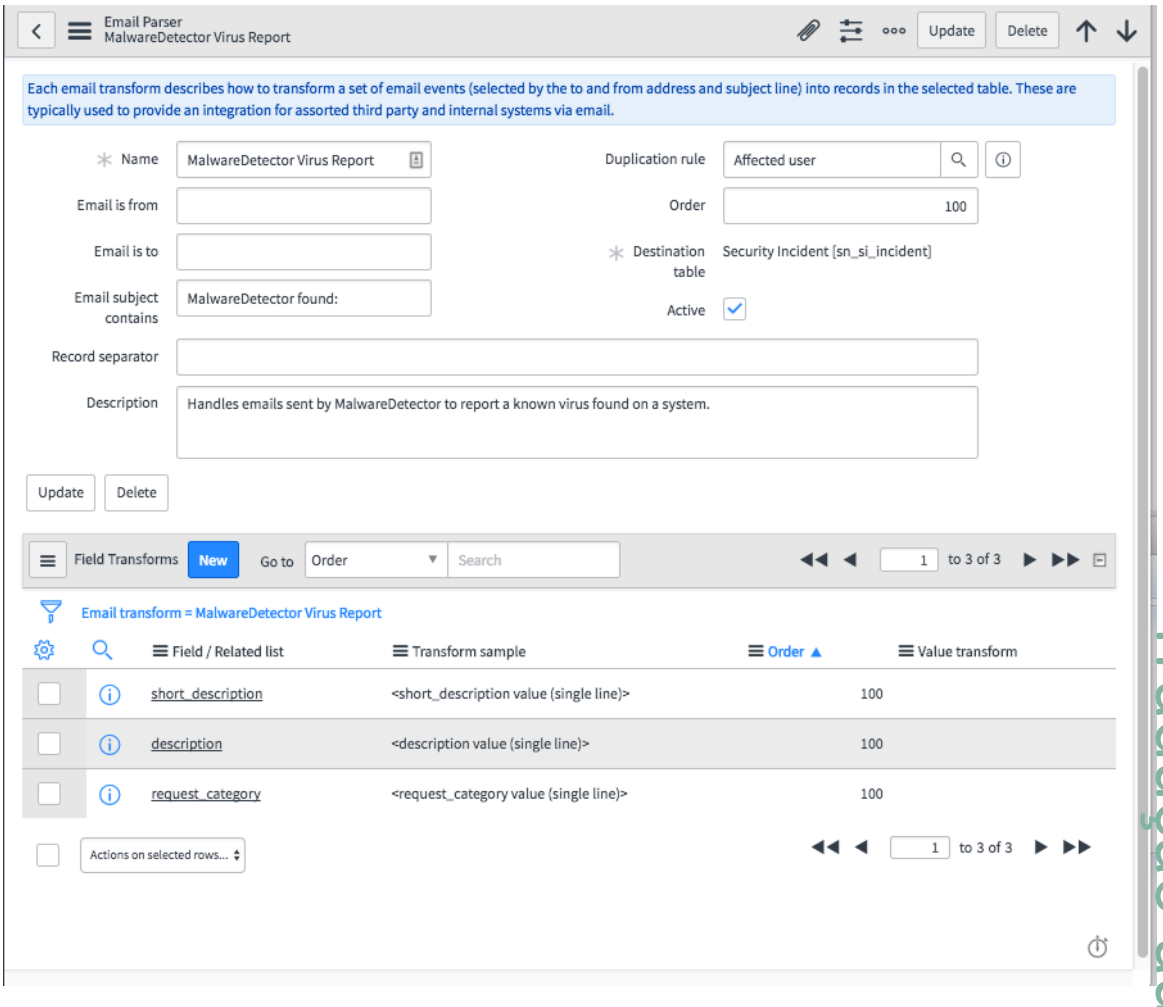
Analisador de e-mail

Campo	Descrição
Nome	O nome do analisador de e-mail.
O e-mail é de	Se preenchido, somente os e-mails deste endereço serão transformados por este analisador de e-mail.
O e-mail é para	Se preenchido, somente os e-mails deste endereço serão transformados por este analisador de e-mail.
O assunto do e-mail contém	Se preenchido, somente os e-mails em que o assunto contém esta frase serão transformados por este analisador de e-mail.
Regra de duplicação	Controla como lidar com e-mails duplicados para qualquer e-mail manipulado por esta transformação. Para obter mais informações, consulte Transformação de dados compartilhados.
Ordem	Em que ordem considerar as transformações. A primeira transformação de e-mail correspondente é usada. Normalmente, você deseja configurar os analisadores de e-mail mais específicos nos números mais baixos, com algum fallback. Dê analisadores de e-mail catchall mais altos **Pedido** para que eles sejam executados se nada mais corresponder. O padrão é 100. Quando tudo corresponde, o analisador de e-mail mais específico (corresponde **de** , **.** e **assunto**) é usado.
Tabela de destino	A tabela em que você deseja criar registros.
Ativo	Se esta transformação está ativa, em uso ou não. Se desmarcado, nenhum e-mail será transformado com este código.
Separador de registro	Quando os e-mails manipulados por este analisador de e-mail criam vários registros, este campo contém o separador entre as informações desses registros. Para obter mais informações, consulte Operações de segurança análise de e-mail.
Descrição	Descrição deste analisador de e-mail, com qual ferramenta ele funciona, a finalidade e assim por diante.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar** .
. **Transformações de campo** é exibida. Esta guia mostra como os campos individuais na tabela de destino são definidos com base no conteúdo do e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para adicionar **Transformações de campo** execute estas etapas.

a. Em **Transformações de campo** clique em **Novo** .

b. Preencha os campos no formulário, conforme o apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem: ○ Armazene o valor em um campo no novo registro ○ Vincular a este valor a uma lista relacionada ○ Vincular a este valor, criando um novo registro se um registro correspondente não existir **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Selecione o campo a ser preenchido com este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Para campos de seleção, são feitas correspondências com as escolhas existentes usando o rótulo ou valor de escolha subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção . Para campos de referência, uma entrada é definida somente quando um valor corresponde ao nome de exibição do registro ou é válido `sys_id` encontrado. Para obter mais informações, consulte Campos de referência .
Lista relacionada	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica a lista relacionada à qual adicionar informações.
Campo de valor	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica o campo na tabela exibida na lista relacionada. Ele é usado para pesquisar e encontrar um registro existente. Por exemplo, se sua lista relacionada for **ICs afetados** este campo pode conter **Nome** ou **Nome de domínio totalmente qualificado** Ou qualquer outro campo no registro de IC a ser usado para pesquisar o IC adicionado ao **ICs afetados** lista.
Dados de relacionamento	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** Um registro é criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um observável e assim por diante). Este campo especifica todas as informações adicionais (pares de campo e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	valor) que devem ser adicionadas ao registro de vinculação. Por exemplo, ao adicionar um observável a um IP de origem, especifique que este IP é a origem, em vez de o IP de destino. Para vários valores, use um separador, por exemplo, digite IP de origem ativo verdadeiro.
Novos dados de registro	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor, criando um novo registro se um registro correspondente não existir** se nenhum registro relacionado correspondente ao valor analisado for encontrado, um registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Para **IC afetado** Se nenhum ICs correspondente for encontrado, um registro de IC será criado). Quando isso acontece, o valor encontrado no e-mail é definido como **Valor** Campo no registro de IC. Você pode definir dados adicionais - uma anotação indicando por que o IC foi criado, algumas informações sobre o tipo de ICs com os quais você está trabalhando e assim por diante. Uma amostra seria: Descrição: Criado pelo analisador de e-mail do scanner de malware.
Pesquisar valor	Selecione o local no e-mail a ser pesquisado. As opções incluem: ○ **No início de uma linha do corpo do e-mail** ○ **Em qualquer parte do corpo do e-mail** ○ **Na linha de assunto do e-mail** ○ **Sempre o valor estático** Quando você tiver definido um **Separador de registro** mais opções (**Em qualquer lugar na seção de registro** e. **No início de uma linha na seção de registro)** Permite que você pesquise somente na seção atual, em vez de em todo o corpo do e-mail (consulte Operações de segurança análise de e-mail para obter mais informações. As informações que estão em um cabeçalho ou rodapé, aplicadas a todos os registros, são pesquisadas em todo o corpo do e-mail. As informações que diferem entre os registros são pesquisadas somente na seção .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Separador de valores	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica o separador a ser usado para listas de itens. Por exemplo, uma vírgula ou ponto-e-vírgula quando os dados do e-mail são uma lista de endereços IP.
Prefixo de valor	O texto que sempre precede o valor inserido neste campo a ser extraído.
Final do valor	Selecione o que indica o fim do valor. As opções incluem: **Fim da linha** , **Fim do e-mail** (traz todo o texto restante no e-mail), ou **Até** (para quando encontra o texto especificado), ou **Até** (para quando encontra o texto especificado).
Sufixo de valor	. **Fim do valor** está definido como **Até** este campo especifica qual texto sempre segue o valor inserido neste campo. Por exemplo, procurar um valor que vem depois de "O computador afetado é" e antes de "." Analisará "AB123" de "The department bunny vírus has found. O computador afetado é AB123. O tempo estimado de infecção foi 3:45" em um e-mail.
Transformação de valor	Escolha a entrada de transformação de campo a ser aplicada. Converte o valor encontrado no e-mail em um valor diferente, usado para preencher campos de escolha, referência ocasionalmente e outros campos .
Ordem	A ordem em que as transformações de campo são executadas, da menor para a maior. Uma transformação de campo com uma entrada de pedido de 100 é tentada primeiro. Uma transformação de campo com uma ordem superior (200) no mesmo campo será executada somente se essa transformação de campo não conseguir encontrar um valor.
Transformação de e-mail	A transformação à qual esta transformação de campo pertence.
Tabela de destino	Tabela de destino da transformação de e-mail. Ele contém dados informativos da transformação de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Ativo	O padrão é marcado. Quando marcado, a transformação de campo é ativada. Desmarque esta caixa para desativar a transformação de campo.

a. Clique em **Enviar**.
O novo registro é usado para analisar as informações no e-mail em um novo registro.

Tópicos relacionados

Crie regras de duplicação em Operações de segurança

Criar Operações de segurança transformações de valor do campo

Definir Resposta a vulnerabilidadesnotificações por e-mail

Edite registros de e-mail em Operações de segurança

Adicione ou crie transformações em seus registros de eventos de e-mail existentes.

Antes de Iniciar

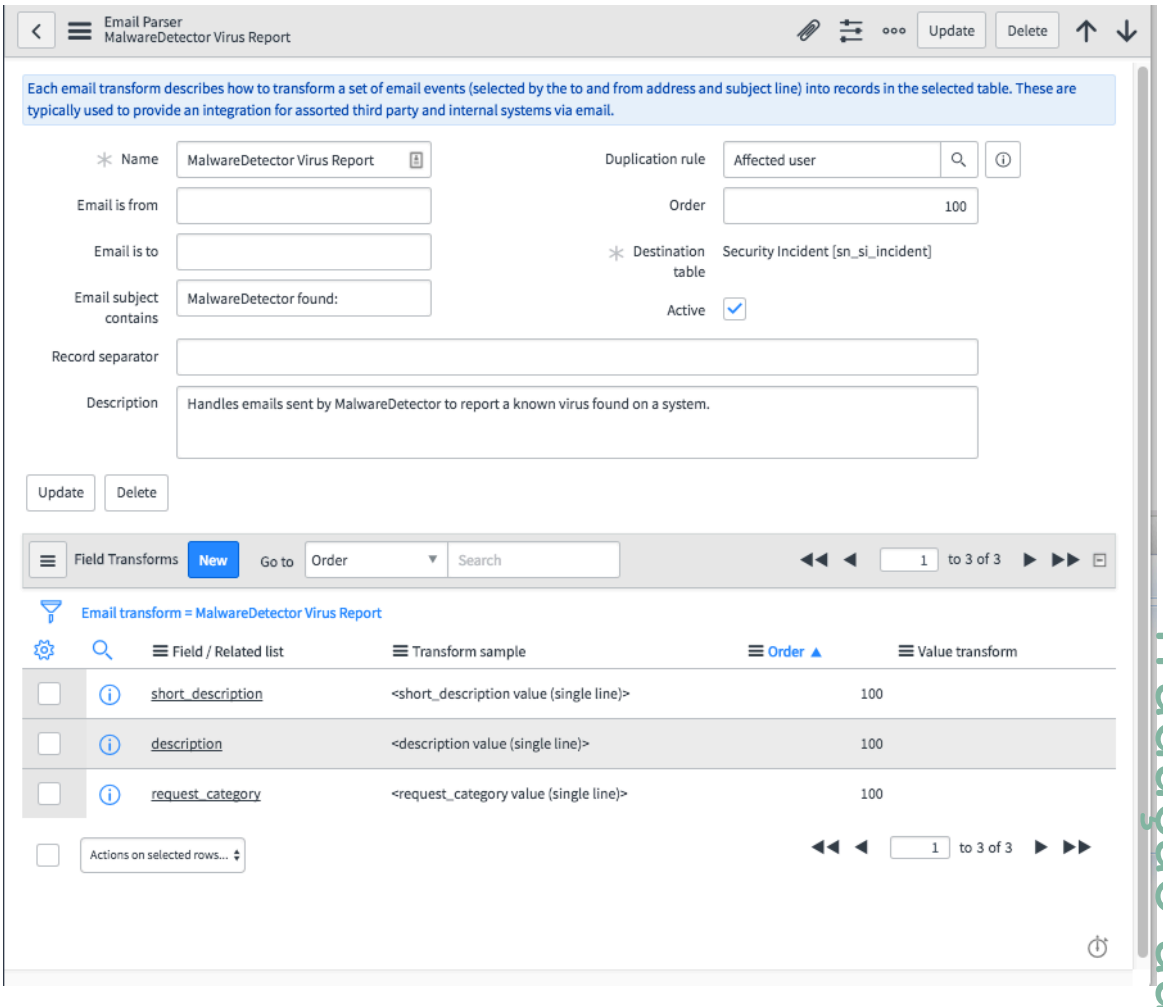
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Análise de E-mails**.
2. Clique no analisador de e-mail para editar.
   Se o registro for somente leitura, clique em aqui link na mensagem do cabeçalho.
   Você será direcionado para o formulário editável da transformação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Edite os campos conforme apropriado.
4. Para editar **Transformações de campo** , clique no campo e mude conforme apropriado.
5. Clique em **Atualizar.**

Incompatível Operações de segurança eventos de e-mail

Os eventos de e-mail que não correspondem a um analisador de e-mail têm o sinalizador "Correspondente" desdefinido. Você pode exibir esses registros de eventos de e-mail no E-mails Incompatíveispara revelar sistemas de detecção externos cujos e-mails ainda não foram analisados.

Ao criar analisadores de e-mail, você pode tentar reprocessar o evento de e-mail (do formulário ou da lista) para validar um novo analisador de e-mail.

Exibir e reprocessar e-mails de operações de segurança incompatíveis

Você pode revisar E-mails Incompatíveispara filtros descontinuados ou como candidatos a um novo filtro para manter ou melhorar a taxa em que você captura ameaças de e-mail.

Antes de Iniciar
Função necessária: sn_sec_cmn.read

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **E-mails Incompatíveis**.
   Se algum e-mail incompatível tiver sido encontrado, eles serão listados.
2. Os campos no formulário são os seguintes:

Eventos de e-mail de segurança

Campo	Descrição
De	Endereço de e-mail do remetente.
Para	Endereço de e-mail dos destinatários.
Assunto	Linha de assunto no e-mail.
Corpo da mensagem	Conteúdo do corpo do e-mail.
Correspondido	Indica se este evento de e-mail foi correspondido.

3. Para reprocessar este e-mail, crie um registro de e-mail ou edite um registro de e-mail existente para corresponder às informações neste e-mail.
   Consulte Crie analisadores de e-mail em Operações de segurança.
4. Navegue de volta para **Operações de segurança** > **E-mails Incompatíveis**.
5. Clique em **Reprocessar evento de e-mail** para tentar processar este e-mail.
   Você retorna para E-mails Incompatíveislista principal. Se o novo registro de e-mail corresponder, o evento de e-mail não estará mais na lista. Uma mensagem indica se foi correspondida ou não.

Operações de segurança mapeamento de campo

Operações de segurança as tabelas podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do Operações de segurança sistema.

Mapeamento de campo define o mapeamento usado quando um registro da tabela de origem é usado para criar um novo registro na tabela de destino. Normalmente usados para criar um incidente de segurança a partir de outro registro, esses mapas definem quais campos em um incidente de segurança são inseridos em um novo problema ou quais campos de um incidente de cliente existente preenchem um novo incidente de segurança.

Mapeie tabelas para tabelas com mapeamento de campo Operações de segurança

Operações de segurança fornece granularidade de mapeamento de campo mais fina para que você possa mapear um Operações de segurança tabela para qualquer outra tabela.

Antes de Iniciar

Função necessária: Sec_cmn.write

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Mapeamento de Campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

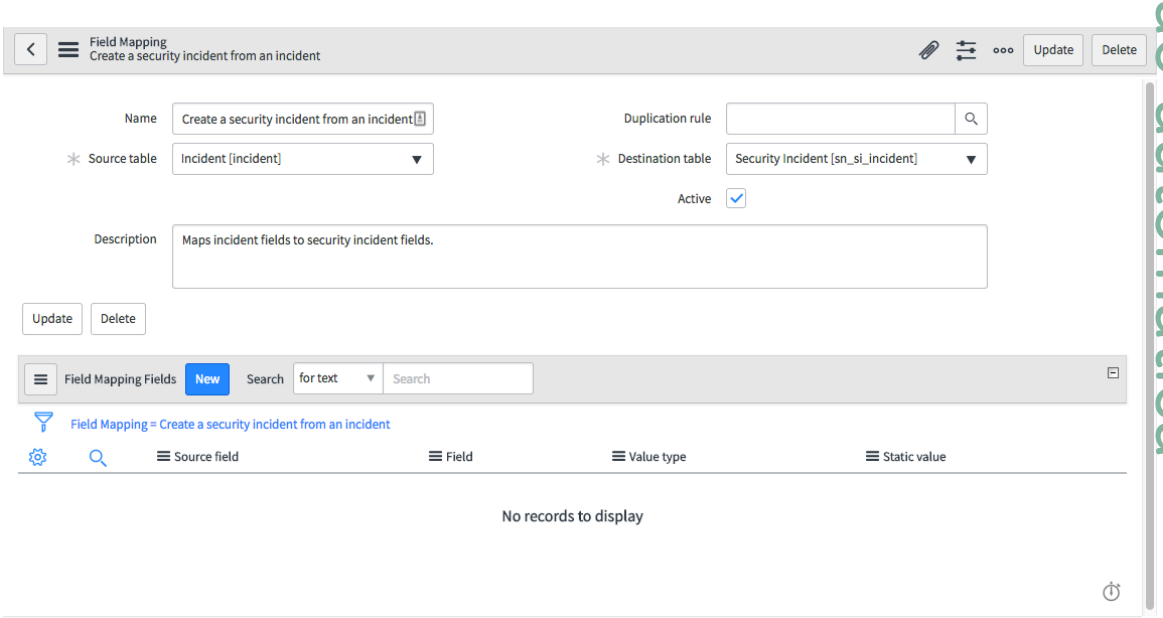
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de campo

Campo	Descrição
Nome	O nome do mapa de campo.
Tabela de origem	A tabela que fornece os dados a serem usados para criar um registro na tabela de destino.
Regra de duplicação	Controla como lidar com registros de origem que gerariam um registro duplicado. Para obter mais informações, consulte Transformação de dados compartilhados.
Tabela de destino	A tabela em que novos registros são criados.
Ativo	Marque esta caixa de seleção para ativar o mapeamento. **Nota:** Somente um mapeamento entre tabelas pode estar ativo por vez. Se dois mapas contiverem as mesmas tabelas, a versão mais antiga será desativada automaticamente.
Descrição	Descrição do mapa de campo.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar** .
Campos de mapeamento de campo é exibida. Este registro define quais dados são colocados no campo de destino, em registros criados por esta transformação de campo.



5. Clique em **Nova**.

6. Preencha os campos no formulário, conforme o apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Adicionar novo valor a um campo no registro ○ Vincular a este valor a uma lista relacionada ○ Link para este valor, criando um registro se um registro correspondente não existir **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Adicione um novo valor a um campo no registro** este campo especifica o campo a ser preenchido. **Nota:** Para campos de seleção, são feitas correspondências com as escolhas existentes usando o rótulo ou valor de escolha subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção . Para campos de referência, uma entrada é definida somente quando um valor corresponde ao nome de exibição do registro, ou é válido sys_id encontrado. Para obter mais informações, consulte Campos de referência .
Lista relacionada	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica a lista relacionada à qual adicionar informações.
Campo de valor	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica o campo na tabela exibida na lista relacionada, que é usado para pesquisar e localizar um registro exis–

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	tente. Por exemplo, se sua lista relacionada for **ICs afetados** este campo pode conter **Nome** ou **Nome de domínio totalmente qualificado** Ou qualquer outro campo no registro de IC que deve ser usado para pesquisar o IC é adicionado ao **ICs afetados** lista.
Dados de relacionamento	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** Um novo registro é criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um observável e assim por diante). Este campo especifica todas as informações adicionais (pares de campo e valor) que devem ser adicionadas a esse registro de vinculação. Por exemplo, ao adicionar um observável para um IP de origem, você pode especificar que este IP é o IP de origem, em vez de o IP de destino. Para vários valores, use um separador, por exemplo, digite IP de origem ativo verdadeiro.
Novos dados de registro	**Store valor em um campo ou lista relacionada** está definido como **Link para este valor, criando um novo registro se um registro correspondente não existir** se um registro relacionado correspondente ao valor analisado não for encontrado, um novo registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Por exemplo, para **ICs afetados** Se não for possível encontrar o IC, esta configuração indica que um novo IC foi criado). O valor encontrado no registro de origem é definido como **Valor** Campo no registro de IC. Você pode definir dados adicionais - uma anotação indicando por que este IC foi criado, algumas informações sobre com que tipo de ICs você está trabalhando. Uma amostra seria: Criado por tipo de relatório de incidente de malware: Detecção automática
Separador de valores	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Link para este valor em uma lista relacionada** ou **Link para este valor, criando um novo registro se um registro correspondente não existir** este campo especifica o separador a ser usado para listas de itens, geralmente uma vírgula ou ponto-e-vírgula.
Tipo de valor	Quando **Armazene o valor em um campo ou lista relacionada** está definido como **Adicione**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	um novo valor a um campo no registro este campo especifica o tipo de valor. As opções incluem: ○ **Registro do campo de origem** ○ **Anexar ao campo como uma nova linha** ○ **Valor estático** ○ **Valor estático mais o valor do campo de registro de origem**
Campo de origem	Escolha o campo de origem que contém o valor a ser colocado no campo de destino ou na lista relacionada selecionada.
Campo estático	Valor estático do campo.
Transformação de valor	Escolha a entrada de transformação do valor do campo a ser aplicada. Ele é usado para mapear campos de seleção entre registros, por exemplo, convertendo o conjunto de **Categoria** opções para um incidente de segurança no apropriado **Tipo** Campo para uma solicitação de mudança.
Tabela de destino	Preenchido automaticamente com a tabela de destino.
Mapeamento de Campos	Preenchido automaticamente com o mapa de campo primário.
Tabela de origem	Preenchido automaticamente com a tabela de origem.

7. Clique em **Enviar**.

Operações de segurança transformações de valor do campo

Transforma valores de campo do cliente exclusivos em valores de campo reconhecidos por Operações de segurança análise de e-mail, aprimoramento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de escolha, referências e alinha dados externos à terminologia e ao formato padrão do seu novo registro.

Você pode mapear dados de campos como Categoria, Estado ou Grupo de atribuição para os valores usados na tabela Operações de segurança. Por exemplo, mapeie "Em análise" para "Trabalho em andamento.

Criar Operações de segurança transformações de valor do campo

Transformações de valor do campo define uma transformação entre os dados de origem fornecidos e o valor de substituição a ser usado.

Antes de Iniciar

Função necessária: sn_sec_cmn.basic ou sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa

Defina cada entrada de transformação a ser aplicada quando houver uma correspondência com o valor de pesquisa, quando o valor de pesquisa estiver contido nos dados de origem fornecidos ou quando nenhuma correspondência for encontrada. Defina um valor padrão para quando nenhuma correspondência for encontrada. Se nenhum valor padrão for

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

definido e nenhuma correspondência for encontrada, os dados de origem originais serão usados.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Transformações de Valores de campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Transformações de valor do campo

Campo	Descrição
Nome	O nome da transformação de valor do campo.
Descrição	Descrição do mapa de campo.
Entradas de Transformação de Valor de Campo	A lista de entradas da tabela. **a.** Em **Substituir dados** Clique duas vezes em "Inserir uma nova linha". **b.** Escolha uma das seguintes opções: Quando a data deste campo corresponde Quando os dados para este campo contêm Quando nenhuma outra entrada de transformação corresponde aos dados (padrão) **c.** Clique na marca de seleção verde. **d.** Clique duas vezes em **Valor da pesquisa** , adicione o valor da pesquisa. **e.** Clique na marca de seleção verde. **f.** Clique duas vezes em **Valor de substituição** adicione ServiceNow valor correspondente. **g.** Se necessário, repita.
Ativo	Marque esta caixa de seleção para ativar a transformação.
Aplicação	Escopo da aplicação.

4. Clique em **Enviar**.

Operações de segurança mapeamento de dados de aprimoramento

Mapeamento de Dados de AprimoramentoTransforma dados de XML, JSON ou Propriedadesarquivos para ServiceNow registros. Operações de segurança os fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança.

Operações de segurança inclui vários mapas de dados de aprimoramento, acionados por vários fluxos de trabalho, por exemplo, Integrações de operações de segurança - Obter fluxo de estatísticas de rede e. Integração de comando do sistema de operações de segurança- Obter fluxo de processos em execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Saída do mapa de dados de aprimoramento de Operações de segurança os fluxos de trabalho são exibidos no **Dados de aprimoramento** no formulário de incidente de segurança.

Crie um Operações de segurança mapa de dados de aprimoramento

Transformar dados de JSON, XML ou Propriedadesformato de arquivo para ServiceNow registros que usam mapas de dados de aprimoramento.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Os mapas de dados de aprimoramento existentes são usados pelos fluxos de trabalho fornecidos em Operações de segurança. Você pode exibir a lista em **Mapeamento de dados de aprimoramento** . Para usar um mapa, você precisa de um gatilho, uma regra de negócios ou um fluxo de trabalho.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Mapeamento de Dados de Aprimoramento**.
2. Clique em **Nova**.
3. Preencha os campos, se for o caso.

Criando um mapa de dados de aprimoramento

Campo	Descrição
Nome	Nome deste mapa de dados de aprimoramento.
Formato de entrada	Escolha um formato na lista: JSON (padrão) XML Formato do arquivo de propriedades

Chave de prefixo	Use para limitar o conjunto de dados de entrada a uma chave especificada. A raiz do conjunto de dados de entrada é definida como esta chave. Neste exemplo, se você inseriu file_info, os valores de entrada serão limitados aos valores em file_info.
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<malware>`
	`<version>2.0</version>`
	`<file_info>`
	`<malware>yes</malware>`
	`<sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>`
	`<filetype>PE</filetype>`
	`<sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256>`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	<md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Aplicação	Escopo da aplicação.
Regra de duplicação	Regra que define quando um registro é considerado duplicado e quais ações executar com registros duplicados.
Tabela de destino	Escolha uma tabela na lista.
Ativo	Marque esta caixa de seleção para ativar o mapa.
Descrição	Insira uma descrição do mapa de dados de aprimoramento.

4. Clique em **Enviar**.
   A guia Campos de mapeamento de dados de aprimoramento é exibida.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme o apropriado.

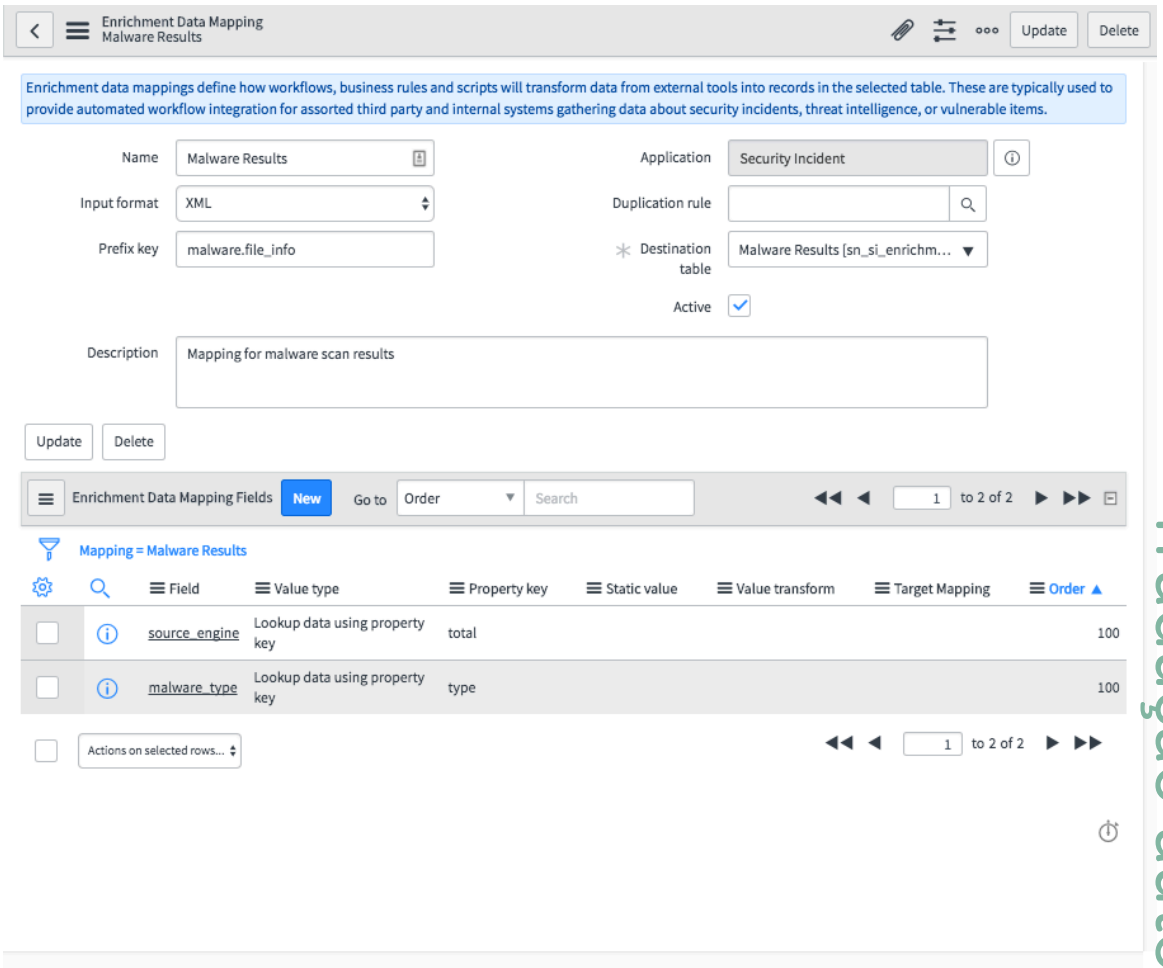
Campos de mapeamento de dados de aprimoramento

Campo	Descrição
Campo	Nome do mapa de dados de aprimoramento.
Tipo de valor	Escolha na lista: Pesquisar dados usando a chave de propriedade Valor estático Valor estático e dados da chave de propriedade Um campo é uma matriz ou objeto (aninhamento de dados brutos) Cada opção tem entradas diferentes. Valores de campo e matrizes ou objetos exigem uma chave de propriedade.
Chave de propriedade	Determina a chave para a pesquisa de dados de entrada e o valor gravado no campo de destino.
Transformação de valor	A transformação de valor do campo que mapeia um valor para outro.
Aplicação	Escopo da aplicação.
Ordem	Em que ordem considerar o mapeamento. A primeira correspondência é usada. O padrão é 100.
Mapeamento	Nome do mapa de dados de aprimoramento.
Tabela de destino	A tabela para a qual os campos a serem mapeados estão indo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.
A seguir está um exemplo de um mapa de dados de aprimoramento.



Operações de segurança escalação definida pelo usuário

Você pode criar um caminho de escalação de incidentes de segurança para problemas que exigem mais atenção ou conhecimento especializado. Quando um grupo de escalação existe, um botão aparece em qualquer incidente de segurança nesse grupo.

Crie um Operações de segurança grupo de escalação definido pelo usuário

Escale um incidente de segurança para qualquer grupo associado ao incidente usando escalações.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Grupos** > **Escalações**.

2. Clique em **Novo**.

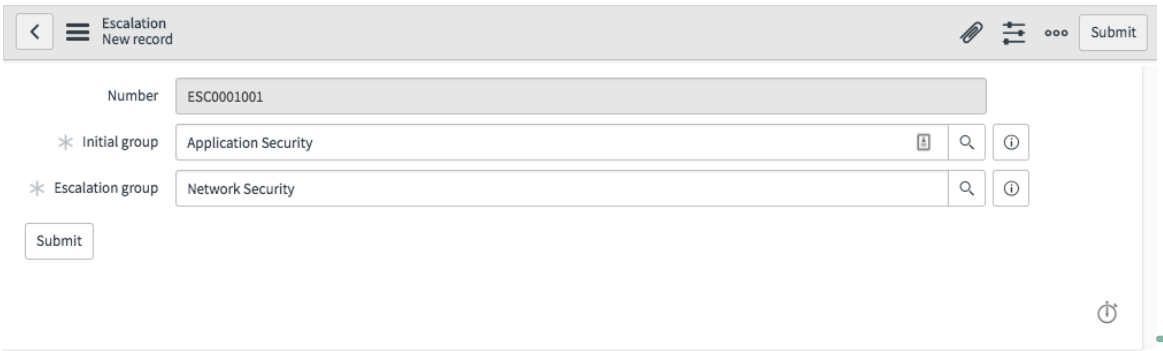
3. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

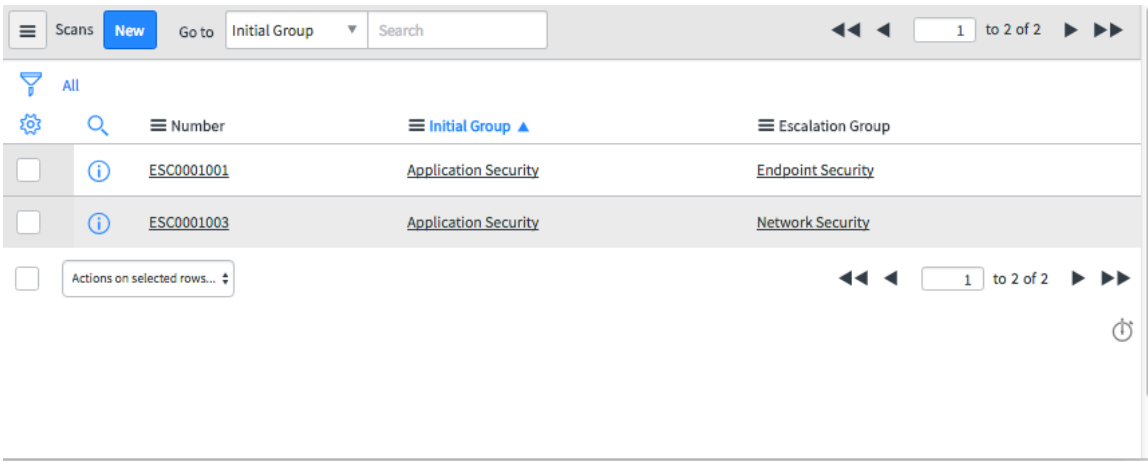
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Escalações

Campo	Descrição
Número	Número do incidente de escalação (o campo é gerado automaticamente).
Grupo inicial	Selecione o grupo ao qual este incidente de segurança pertence.
Grupo de escalação	Selecione o grupo para o qual escalar o incidente de segurança.



4. Clique em **Enviar**.
   Um grupo de escalação está disponível para todos os incidentes de segurança no grupo inicial. Você pode criar vários grupos.



Tradução automática

Crie substituições de propriedade separadas por domínio

Ao usar Domain Separation, você pode criar substituições nas propriedades existentes do Security Operations que permitem personalizar as funções das aplicações em cada um dos seus domínios.

Antes de Iniciar

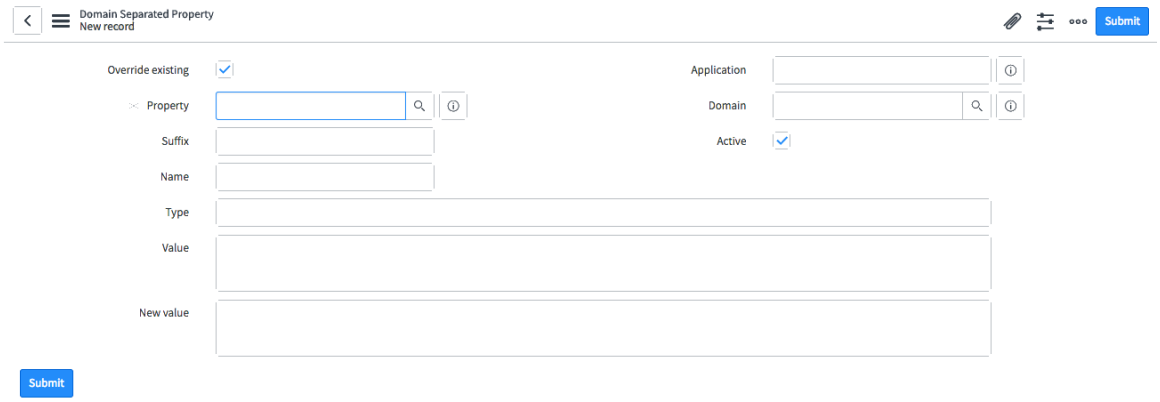
Requer isso Suporte de domínio - Extensões de domínio ser ativado. Você também pode aprender mais sobre Visualizador de substituição de domínio .

Função necessária: administrador

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Propriedades Separadas de Domínio**.
2. Clique em **Nova**.



3. No formulário, preencha os campos.

Formulário Propriedade de Separação de domínios

Campo	Descrição
Substituir existente	Marque esta caixa de seleção para criar um valor específico de domínio para uma propriedade existente.
Aplicação	Selecione a aplicação que contém a propriedade que você deseja substituir.
Propriedade	Selecione a propriedade da aplicação selecionada para a qual você deseja criar uma substituição específica do domínio.
Domínio	Selecione o domínio para o qual você está criando esta substituição de propriedade.
Ativo	Ativar ou desativar a substituição.
Sufixo	Exibe o sufixo da propriedade.
Nome	Exibe o nome da propriedade.
Tipo	Exibe o tipo de propriedade.
Valor	Exibe o valor atual definido para a propriedade.
Novo valor	Insira um novo valor para a propriedade a ser aplicada a este domínio.

4. Clique em **Enviar**.
   A substituição de propriedade é aplicada à propriedade selecionada no domínio especificado. Quando a lógica desta propriedade é acionada, o sistema verifica se há substituições de propriedade separadas por domínio. Se uma substituição para o domínio for encontrada, o novo valor será usado. Caso contrário, o valor do domínio padrão será usado.

Tópicos relacionados

Noções básicas sobre o Domain Separation

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um grupo de sistemas operacionais

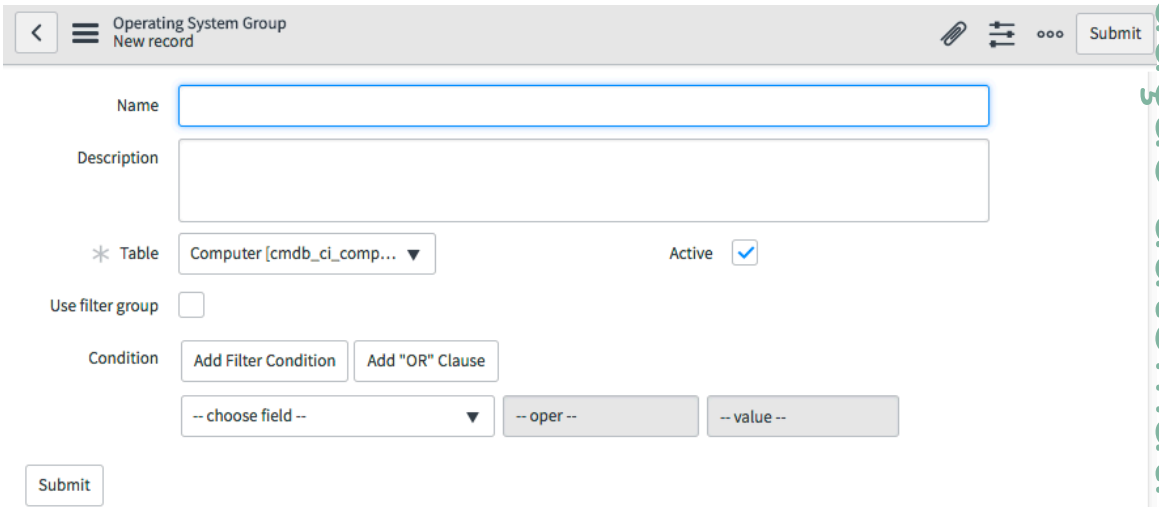
Grupos de sistemas operacionais são usados para mapear um sistema operacional para tipos de processo e scripts específicos no Resposta a incidentes de segurança fluxos de trabalho. Os scripts definem como os processos em execução dos grupos de sistemas operacionais definidos são recuperados. Novos sistemas operacionais podem ser adicionados conforme necessário.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Grupos de Sistemas Operacionais**.
   O sistema de base inclui scripts para três sistemas operacionais:
   - SO baseado em BSD
   - SO baseado em POSIX
   - SO Windows
2. Clique em **Nova**.



3. Preencha os campos, conforme necessário.

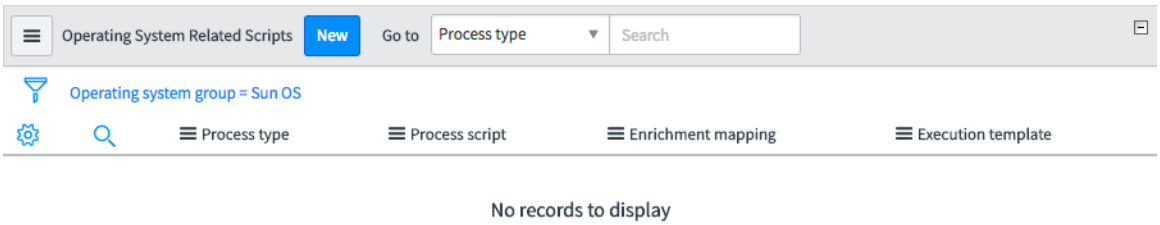
Campo	Descrição
Nome	O nome do grupo de sistemas operacionais.
Descrição	Uma descrição do grupo de sistemas operacionais.
Tabela	A tabela afetada.
Ativo	Marque esta caixa de seleção para ativar o grupo de sistemas operacionais.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros para localizar registros correspondentes na tabela selecionada.
Grupo de filtros	Selecione o grupo de filtros para localizar registros correspondentes na tabela selecionada. Este campo será exibido somente se você tiver selecionado **Usar grupo de filtros** caixa de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	O construtor de condições os campos serão exibidos somente se você não selecionou **Usar grupo de filtros** caixa de seleção.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada Scripts relacionados ao sistema operacional é aberta.



5. Clique em **Nova**.
6. Selecione scripts que correspondam aos fluxos de trabalho que você está usando para obter processos em execução, serviços e/ou estatísticas de rede.
7. Clique em **Enviar**.

Tópicos relacionados

Anexar um arquivo de script a um MID Server sincronizado

Configurar grupos de marcadores de segurança e marcadores

Você pode atribuir marcadores a incidentes de segurança, tarefas de resposta, itens vulneráveis, observáveis, IOCs, e casos de segurança para criar metadados no registro de resposta e definir quem deve ter acesso a tipos específicos de conteúdo de segurança. Os marcadores podem ser adicionados a grupos de segurança para organizá-los.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Marcadores de Segurança** > **Grupos**.
   Três grupos de classificação padrão estão incluídos no sistema de base.
   - **Lista de permissões/lista de proibições de aprimoramento** : Este grupo define se um registro deve ser tratado como um registro de lista de permissões ou de lista de proibições. Registros da lista de permissões geralmente são menos significativos, portanto, podem ser ignorados. Registros da lista de proibições geralmente são de maior interesse.
   - **Metatag** : Este grupo é fornecido como dados de demonstração. Você pode usá-lo para criar marcadores de classificação personalizados que são usados por aplicações de operações de segurança.
   - **Protocolo de semáforo** : Este grupo é usado para garantir que informações confidenciais sejam compartilhadas com o público correto. Ele emprega quatro cores (Branco, Verde, Amarelo e Vermelho) para indicar diferentes graus de sensibilidade. Para cada cor, você pode atribuir as funções de acesso de leitura/gravação apropriadas. Ao compartilhar observáveis com um círculo de segurança confiável, o marcador atribuído ao perfil de círculo de segurança confiável determina quais observáveis marcados com TLP podem ser compartilhados com o círculo, da seguinte forma:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **TLP: BRANCO:** Somente observáveis com TLP: BRANCO podem ser compartilhados com um TLP: Perfil BRANCO.
- **TLP: VERDE:** Observáveis com TLP: VERDE e TLP: BRANCO podem ser compartilhados com um TLP: Perfil VERDE.
- **ÂMBAR: ÂMBAR:** Observáveis com TLP: ÂMBAR, TLP: VERDE e TLP: BRANCO podem ser compartilhados com um perfil TLP: ÂMBAR.
- **TLP: VERMELHO:** Todos os observáveis, independentemente do marcador TLP, podem ser compartilhados com um perfil TLP: VERMELHO, já que TLP: VERMELHO é o marcador TLP mais bem classificado.

Nota: Você pode adicionar outras cores TLP, mas qualquer uma além das quatro cores incluídas é considerada inválida pelo Fórum para equipes de resposta a incidentes e segurança (PRIMEIRO).

2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Insira o nome do grupo de segurança.
Permitir várias seleções	Marque esta caixa se quiser atribuir vários marcadores de segurança a um registro que compartilha um grupo.
Ativo	Ative ou desative o grupo.
Descrição	Insira uma descrição deste grupo.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada Marcadores de segurança é exibida.
5. Na lista relacionada Marcadores de segurança, clique em **Novo** .
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome do marcador de classificação.
Grupo de marcadores de segurança	Se o marcador foi criado usando **Novo** na lista relacionada ao grupo, este campo é padronizado para o grupo atual. Se necessário, você pode adicionar o marcador a um grupo diferente, mas isso é opcional.
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista.
Cor	Selecione a cor deste marcador.
Impor acesso restrito	Marque esta caixa de seleção para atribuir funções de leitura e/ou gravação necessárias para que os usuários leiam ou gravem em registros que tenham este marcador de segurança.
Ativo	Ativar ou desativar o marcador.
Descrição	Uma descrição deste marcador.
Função (acesso de leitura)	Para atribuir acesso de leitura a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	novamente. Este campo aparecerá somente se você selecionou **Impor acesso restrito** caixa de seleção.
Funções (acesso de gravação)	Para atribuir acesso de gravação a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado novamente. Este campo aparecerá somente se você selecionou **Impor acesso restrito** caixa de seleção.

7. Repita conforme necessário para criar mais marcadores de segurança.
8. Clique em **Atualizar**.

Nota: Você também pode criar novos marcadores navegando até **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**. O procedimento é o mesmo.

Criar regras de marcador de segurança

As regras de marcador de segurança fornecem filtragem para acesso a marcador de segurança.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança .
3. Em **Regras de marcador de segurança** guia relacionado, clique em **Novo** .
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da regra de marcador de segurança.
Marcador de segurança	O marcador de segurança a ser anexado à regra.
Ativo	Ative ou desative o marcador de segurança.
Descrição	Uma descrição desta regra.

5. Determinar **Filtragem de registro.**
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Usar grupo de filtros	Associa o grupo de filtros à regra.
Tabela	A tabela que contém a regra.
Condição	Adicione uma ou mais condições de filtro.

7. Clique em **Enviar**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar regras de marcador de segurança

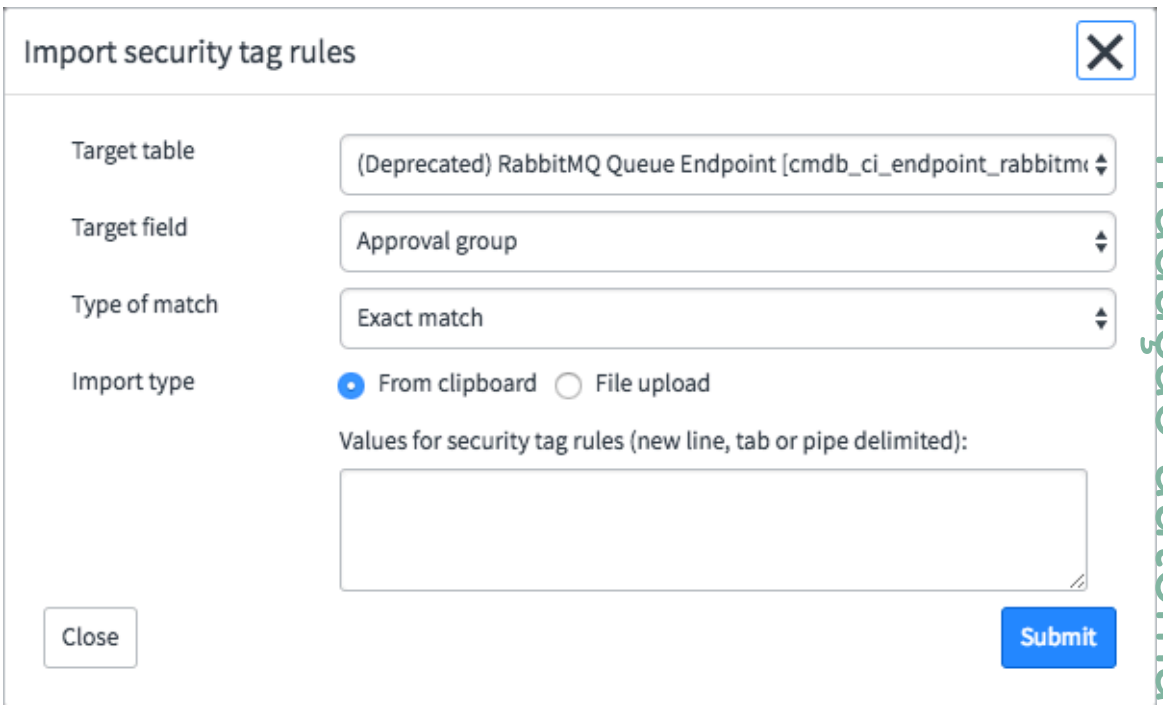
Você pode importar regras de marcador de segurança de outras tabelas em sua implantação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança .
3. Clique em **Regras de marcador de segurança de importação** link relacionado.



4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Tabela de destino	Escolha a tabela a ser usada para importar regras.
Campo de destino	Escolha o campo a ser usado para importar regras.
Tipo de correspondência	Escolha como corresponder as regras importadas **Marcadores de segurança** de: Correspondência exata (padrão) Contém Começa com Termina com Expressão regular
Tipo de importação	Escolha: **Da área de transferência**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Copie uma lista de valores delimitados para a área de texto. Os valores são analisados em marcadores de segurança. **Do carregamento do arquivo** Carregue um arquivo com valores delimitados. Os valores são analisados em marcadores de segurança. Adicione valores para as regras de marcador de segurança usando uma nova linha ou delimitadores de tubo rígido.

5. Clique em **Enviar**

Anotações de segurança

Uma anotação de segurança é uma anotação de explicação ou comentários adicionados a um item de configuração, observável ou uso em um incidente de segurança.

Várias anotações de segurança estão disponíveis para usuários e observáveis (requer Inteligência contra ameaças plug-in). Relatórios sobre anotações de segurança também estão disponíveis.

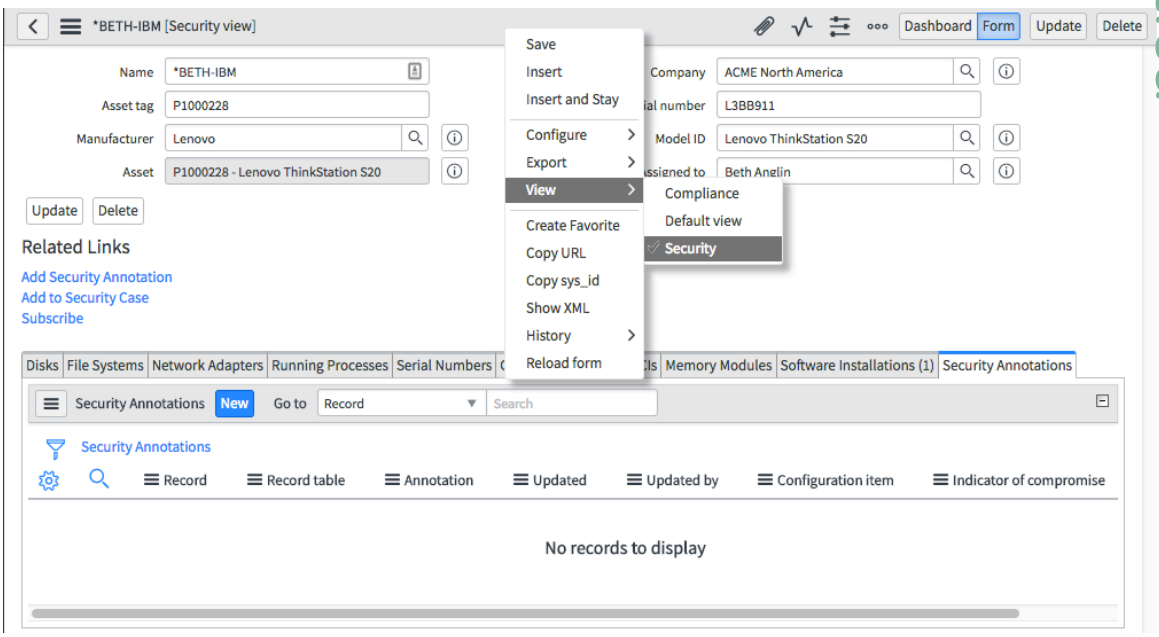
Criar anotações de segurança para ICs

Anotações em ICs permitem rastrear a atividade entre incidentes. Você pode adicionar anotações a um ou vários ICs.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Em um incidente de segurança ou na tabela Item de configuração, abra um IC.
2. Clique com o botão direito do mouse no cabeçalho e escolha **Exibição** > **Segurança**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Anotações de segurança** lista relacionada, clique em **Novo** .
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

> **Nota:** Você pode adicionar a mesma anotação a vários ICs selecionando ICs na lista, escolha **Adicionar anotação de segurança** insira uma anotação em qualquer formato de texto e clique em **Enviar** .

Criar anotações de segurança para observáveis

Você pode selecionar um ou vários observáveis e aplicar anotações de segurança a eles usando **Ações nas linhas selecionadas** menu de seleção.

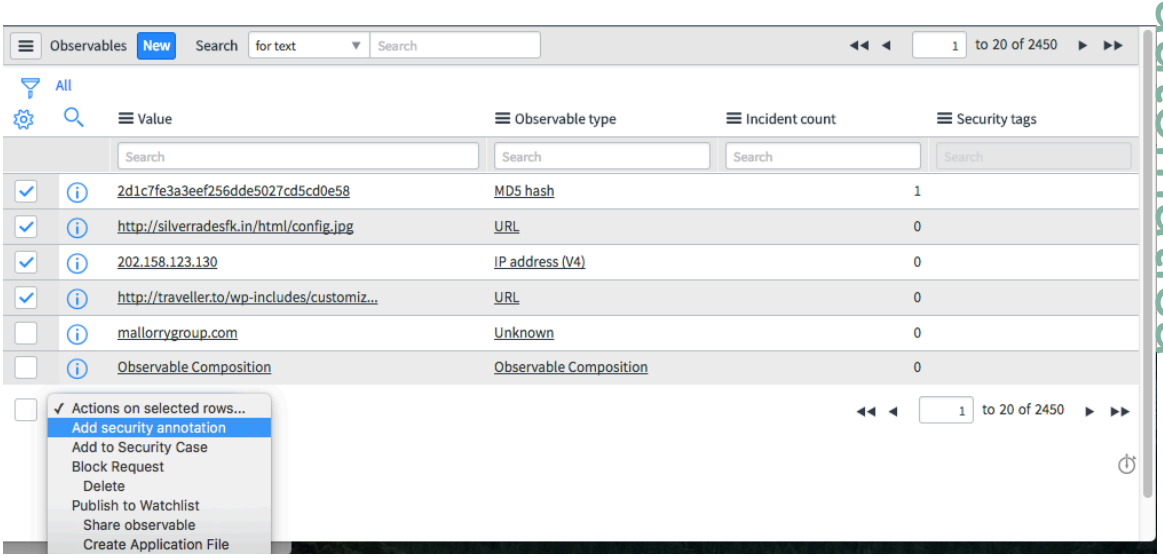
Antes de Iniciar

- Requer Inteligência contra ameaças plug-in e ativação. . Inteligência contra ameaças o plug-in está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Inteligência contra ameaças** > **Observáveis**
2. Selecione um ou mais observáveis na lista.
3. Em **Ações nas linhas selecionadas** menu suspenso, escolha **Adicionar anotação de segurança** .



4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Criar anotações de segurança para usuários

Você pode selecionar um ou vários usuários e aplicar anotações de segurança a eles usando **Ações nas linhas selecionadas** menu de seleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Requer Inteligência contra ameaças plug-in e ativação. . Inteligência contra ameaças o plug-in está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Administração de Usuários** > **Usuários**
2. Selecione um ou mais usuários na lista.
3. Em **Ações nas linhas selecionadas** menu suspenso, escolha **Adicionar anotação de segurança** .
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Exibir relatórios de anotações de segurança

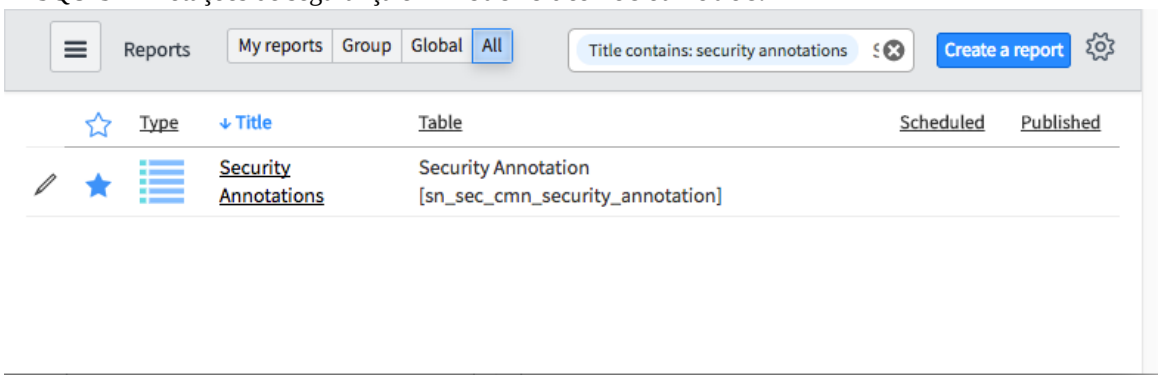
O relatório Anotações de segurança apresenta detalhes armazenados na tabela Anotações de segurança [sn_sec_cmn_security_annotations]. Você pode personalizar as colunas no relatório e agrupar os dados da maneira que mais lhe convier.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Relatórios** > **Exibir/Executar**.
2. PESQUISE Anotações de segurança em **Meus relatórios** ou **Todos.**



Tópicos relacionados

Exiba a lista Relatórios

Componentes instalados com Security Support Common

Vários tipos de componentes são instalados com Security Support Common. Eles fornecem funcionalidade comum para uso em várias aplicações de segurança, como Resposta a incidentes de segurança.

Localizar e exibir componentes instalados

Consulte Exibir componentes instalados com Security Support Common mais informações sobre como localizar e exibir componentes instalados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir componentes instalados com Security Support Common

Vários tipos de componentes são instalados quando você ativa o. Security Support Common plug-in, incluindo, entre outros, tabelas, funções de usuário e módulos.

Localizando componentes

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Se você quiser limitar a lista de componentes instalados a funções, trabalhos agendados e tabelas da aplicação Common Support de segurança, siga estas etapas:

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, trabalhos agendados e tabelas instaladas com uma aplicação sejam exibidas. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o Construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação.
3. No Construtor de condições, para adicionar um segundo filtro, clique em **E.** e, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função** , **Trabalho agendado** ou **Tabela** .
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Pesquisar Operações de segurança

Você pode encontrar informações rapidamente em qualquer Operações de segurança aplicação usando o ícone de pesquisa no cabeçalho da tela. Zing é o mecanismo de indexação de texto e pesquisa que executa todas as pesquisas de texto em sua instância.

Antes de Iniciar

Função necessária: sn_si.read ou superior

Procedimento

1. Clique no ícone de pesquisa ( ) no canto superior direito da tela.
2. Digite os critérios pelos quais você deseja pesquisar e pressione **Insira** .
   . Resposta a incidentes de segurança Plug-in ativado, os critérios de pesquisa inseridos apresentam qualquer texto de descrição resumida, ICs, endereços IP ou URLs correspondentes em seus incidentes de segurança, Resposta a incidentes de segurança tarefas ou solicitações de segurança. . Resposta a vulnerabilidades ou Inteligência contra ameaças Plug-ins ativados, os resultados da pesquisa incluem vulnerabilidades, itens vulneráveis, entradas vulneráveis, observáveis, IOCs, e modos/métodos de ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Introdução à pesquisa

Zing pesquisa de texto

Referência do Security Operations Integrations

Os desenvolvedores e os parceiros da ServiceNow podem usar as informações nesta seção para entender a funcionalidade básica das integrações de terceiros, incluindo diretrizes de desenvolvimento, recursos de integração e fluxos de trabalho.

ServiceNow Operações de segurança diretrizes de desenvolvimento de integração

. ServiceNow a plataforma fornece vários mecanismos para desenvolver integrações com sistemas externos. . ServiceNow Operações de segurança o pacote de produtos adiciona recursos de integração destinados a simplificar o processo de integração com sistemas externos focados em segurança.

A maioria dos conceitos neste guia pressupõe alguma familiaridade com o padrão ServiceNow funcionalidade. Para integrar com Operações de segurança pacote, no mínimo, conhecimento do seguinte ServiceNow conceitos são necessários:

- Inclusões de script
- Serviços web de entrada/saída
- Fontes de dados
- Conjuntos para importação
- Mapas de transformação

Programa de parceiros de tecnologia

Quaisquer requisitos para certificação de aplicações ou diretrizes fornecidos na literatura do Programa de parceiros de tecnologia substituem todas as informações contidas neste guia. Este guia não substitui a literatura do Programa de parceiros de tecnologia e serve apenas como um complemento à documentação existente.

Para obter mais informações, consulte Publicação do blog do curso de treinamento do Programa de parceiros de tecnologia .

Tipos de ServiceNow integrações fornecidas

. Operações de segurança aplicações (Resposta a incidentes de segurança, Inteligência contra ameaças e Resposta a vulnerabilidades) pode ser perfeitamente integrado com outros ServiceNow para aprimorar sua funcionalidade.

As integrações a seguir são fornecidas no Operações de segurança sistema de base.

Integração Resposta a incidentes de segurança - Gestão de eventos

Os recursos do Gestão de eventos a aplicação foi expandida para oferecer suporte a Resposta a incidentes de segurança. . Resposta a incidentes de segurança Gestão de eventos o plug-in de suporte analisa automaticamente o conteúdo de eventos em Gestão de eventos para preencher campos em incidentes de segurança.

Caso de uso coberto:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação de eventos de segurança no Gestão de eventos Sistema de Informações de segurança e. Gestão de eventos(SIEM)

Recursos úteis fornecidos:

- Funcionalidade de gestão de eventos - correlação de eventos, regras de evento e regras de alerta
- Mapeamento automático de valores additional_information para o incidente de segurança resultante

Recursos:

Documentação de suporte da Gestão de eventos de incidentes de segurança

Documentação da Gestão de eventos

Resposta a incidentes de segurança - Integração da API do conjunto de importação

Além de usar Gestão de eventos para enviar eventos relacionados à segurança por push, o Resposta a incidentes de segurança A aplicação fornece uma API de conjunto de importação que permite a criação direta de incidentes de segurança. O endpoint REST do Conjunto de importação de incidentes de segurança é http://localhost:8080/api/now/import/sn_si_incident_import.

Esta técnica de integração é útil quando a) Gestão de eventos Não está instalado, ou b) É desejável simplesmente criar Incidentes de segurança sem passar pelo fluxo Evento > ALERT > Incidente de segurança necessário ao usar Gestão de eventos.

Caso de uso coberto:

Criação de incidentes de segurança diretamente de ferramentas SIEM.

Recursos úteis fornecidos:

Correspondência automática de IC na criação de incidente de segurança com base em IP, NetBIOS ou nome de domínio totalmente qualificado.

Recursos:

Documentação da API do conjunto de importação da plataforma

Documentação do conjunto de importação de serviços web de incidentes de segurança

Integração de origem de pesquisa - Inteligência contra ameaças

As fontes de pesquisa fornecem a capacidade de enviar dados para fontes de pesquisa externas para determinar se esses dados são mal-intencionados. Esses dados são um endereço IP, URL, arquivo ou hash de arquivo.

Caso de uso coberto:

PESQUISE um endereço IP, URL, arquivo ou hash com um serviço de pesquisa externo.

Recursos úteis fornecidos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Maneira consistente de solicitar pesquisas de itens do catálogo e incidentes de segurança.
- Limitação de taxa e recursos de limitação fornecidos com pouca/nenhuma codificação.
- Criação automática de entradas observáveis de indicadores de comprometimento (IOC) para quaisquer problemas encontrados por fontes de pesquisa.

Inteligência contra ameaças - Integração de origem da ameaça

As origens de ameaça fornecem a capacidade de extrair dados de repositórios externos de inteligência contra ameaças. Esses dados são importados para os vários indicadores de tabelas de comprometimento existentes no sistema. Coleções TAXII e blocklists simples são compatíveis nativamente. Para adicionar novas coleções TAXII (ou perfis baseados em um serviço de descoberta ou gestão de coleções), basta adicionar uma entrada. Da mesma forma, adicionar uma nova lista de bloqueios simples de coluna única é uma questão de inserir um novo registro e fornecer a URL da lista de bloqueios. Para conjuntos de dados mais complicados, uma integração personalizada pode ser fornecida para fazer uma chamada para um URL e analisar a resposta.

Caso de uso coberto:

Recupere dados de uma fonte de inteligência contra ameaças para carregar nas tabelas IOC.

Recursos úteis fornecidos:

- Suporte para blocklists simples e coleções TAXII sem codificação.
- Mecanismo simples para executar mensagens REST para recuperar dados.
- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processar dados de passagem retornados para fontes de dados (e conjuntos de importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes

Recursos:

Defina uma origem de ameaça

Vulnerability Response - Integração de invocação do scanner

A invocação do verificador de vulnerabilidades é um ponto de entrada de integração leve que oferece suporte à invocação de verificações de vulnerabilidade da instância. Um verificador de vulnerabilidades de terceiros é chamado de forma assíncrona para programar uma verificação de itens de configuração ou endereços IP.

Caso de uso coberto:

Faça uma solicitação ao scanner de terceiros para verificar um IC (usando informações de host derivadas de IC) ou endereço IP/endereços IP.

Recursos úteis fornecidos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Estrutura simples para definir implementações de scanner.
- Maneira consistente de solicitar verificações de itens do catálogo, incidentes de segurança e itens vulneráveis.
- Atualização automática de tarefas com resultado da invocação de verificação.

Vulnerability Response - integração de dados

As integrações de dados de vulnerabilidade destinam-se a recuperar dados de vulnerabilidade de sistemas de vulnerabilidade de terceiros. As saídas esperadas dessas integrações são entradas de vulnerabilidade e itens vulneráveis. Esta integração permite que os scanners de vulnerabilidades de terceiros funcionem de forma independente, com a expectativa de que as vulnerabilidades possam ser trabalhadas e rastreadas na instância.

Casos de uso cobertos:

- Recupere bibliotecas de vulnerabilidades
- Recupere emparelhamentos de vulnerabilidade/IC
- Sincronizar ICs com o sistema de gestão de vulnerabilidades

Recursos úteis fornecidos:

- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processar dados de passagem retornados para fontes de dados (e conjuntos de importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes.

Recursos:

Documentação de integração de dados de vulnerabilidade

Operações de segurança Configurações de integração

Muitas das integrações incluídas no sistema de base exigem pouca ou nenhuma configuração e operam da mesma maneira. Determinadas integrações, como Qualys Cloud Platform, no entanto, exigem etapas separadas para configurar a integração. Outros são compatíveis com diferentes conjuntos de tipos de verificação e pesquisa e diferentes limites de taxa.

Esta seção descreve as diferenças entre as integrações compatíveis e direciona você para mais documentação, conforme necessário.

- Integração do Carbon Black: Permite que você investigue e responda a incidentes de segurança usando as APIs Carbon Black para consultar e interagir com endpoints associados a incidentes de segurança.
- Antibot Check Point - Integração do analisador de e-mails: Usa um analisador de e-mail que consome notificações por e-mail do Check Point Anti-bot para criar incidentes de segurança.
- Integração de aprimoramento de incidentes do Elasticsearch: pesquisa seus logs e adiciona informações de vista relevantes aos incidentes de segurança.
- Have I been pwned? integração: Permite que a lista de contas violadas (endereços de e-mail e nomes de usuário) seja pesquisada rapidamente por meio de um serviço RESTful.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- HPE Security ArcSight ESM - Integração do analisador de e-mail: Usa um analisador de e-mail que consome notificações por e-mail do HPE ArcSight ESM para criar incidentes de segurança.
- HPE ArcSight Logger Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de vista relevantes aos incidentes de segurança.
- IBM QRadar - Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de vista relevantes aos incidentes de segurança.
- McAfee ESM - Integração do analisador de e-mail: Usa um analisador de e-mail que consome notificações por e-mail do McAfee ESM para criar incidentes de segurança.
- McAfee ESM - Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de vista relevantes aos incidentes de segurança.
- OPSWAT Metadefender visão geral da integração: Permite que os dados da ameaça, detectados pelo scanner Metadender de terceiros, sejam baixados para Inteligência contra ameaças aplicação para acompanhamento, priorização e resolução.
- Palo Alto Networks - AutoFocus integração: O foco automático da Palo Alto Networks, um serviço em nuvem de inteligência contra ameaças, permite pesquisar informações de sessão relacionadas a observáveis de incidentes de segurança.
- Palo Alto Networks - Firewall integração: O Firewall da Palo Alto Networks permite configurar e manter firewalls para evitar ameaças conhecidas e desconhecidas na rede, na nuvem e nos endpoints.
- Palo Alto Networks - WildFire integração A integração do Wildfire permite que você consulte programaticamente trabalhos de análise no Wildfire e recupere resultados históricos por meio de uma interface de API XML simples.
- Noções básicas do Qualys Vulnerability Integration: Qualys Cloud Platformé usado em Resposta a vulnerabilidades.
- Splunk - Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de vista relevantes aos incidentes de segurança.
- Integração do VirusTotal: usado em Inteligência contra ameaças. Para usar esta origem de pesquisa, você deve Ative o plug-in VirusTotal Integration .
- Configuração de integração da API WhoisXML: Fornece dados consistentes e bem estruturados de uma pesquisa do Whois. Mantém os dados precisos do Whois acessíveis 24 horas por dia, 7 dias por semana.

Tradução automática

Ativar e configurar integrações de terceiros

Você pode ativar os plug-ins para integrações de terceiros e configurá-los para uso na mesma tela.

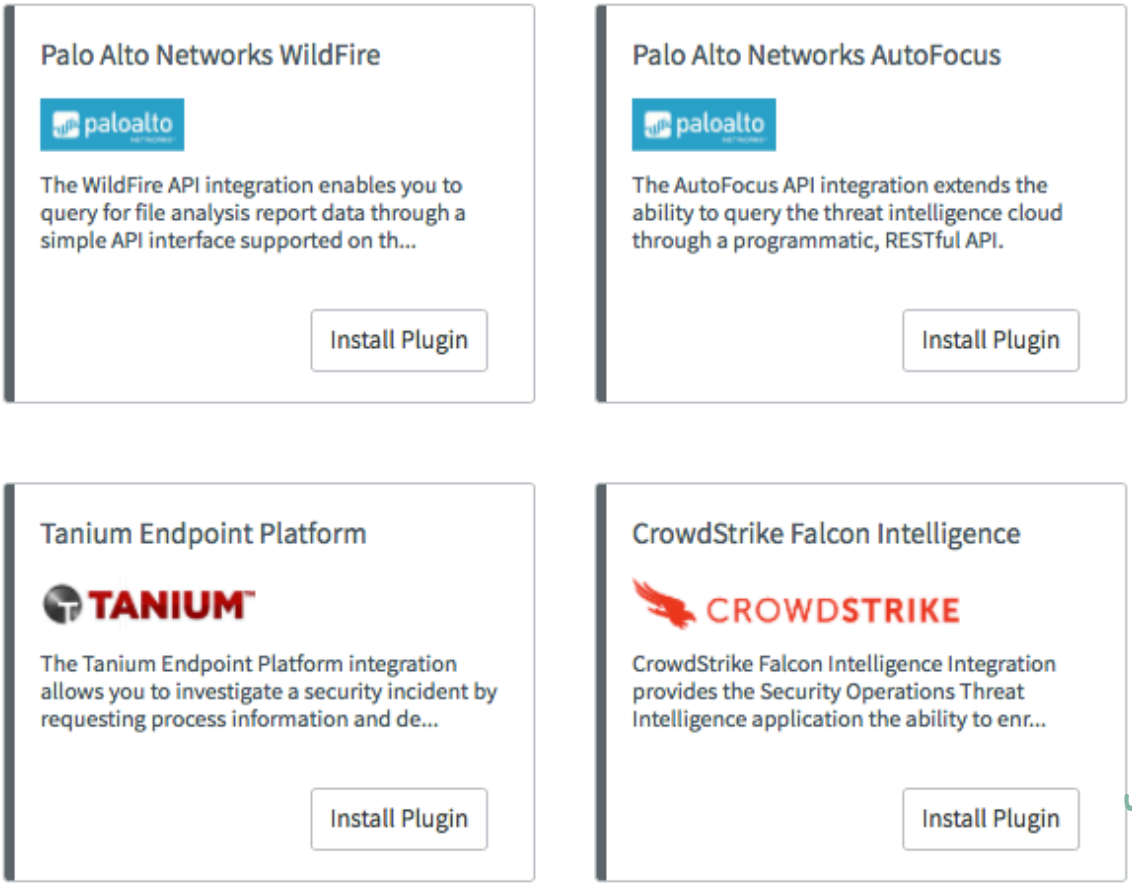
Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões, semelhante ao grupo de cartões a seguir. Você pode apontar para qualquer cartão para obter uma descrição da integração.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

2. Para instalar o plug-in para uma determinada integração, clique em **Instale o plug-in** .

   a. No formulário Plug-in do sistema, revise os detalhes do plug-in e clique em **Fazer upgrade/upgrade** link relacionado.

   b. Clique em **Ativar**.
   Quando a ativação estiver concluída, a tela Integração de segurança será reaberta e o botão da integração que você ativou será rotulado **Configurar** .

3. Clique em **Configurar**.

   Nota: Se você estiver configurando o. Qualys Vulnerability Integration, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

4. Insira **Chave de API** .

5. Clique em **Enviar**.

Crie uma integração

Você pode criar uma integração e adicionar o cartão de integração associado à tela Integrações de segurança. Este procedimento se destina a parceiros que criam integrações de terceiros.

Antes de Iniciar
Função necessária: sn_sec_cmn.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Público: Parceiros que criam integrações de terceiros.

Procedimento

1. No filtro de navegação, digite sn_sec_core_integration_item.list e pressione **Insira** chave.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da integração.
ID do plug-in	O plug-in que deve ser ativado para usar a integração.
Ordem	Indica a ordem em que este cartão de integração aparece.
Texto da faixa	Clique no link, selecione uma imagem ou logotipo para aparecer no cartão de integração e clique em **OK** .
Instalado	Campo somente leitura que indica se o plug-in já foi instalado.
Configurável	Indica se você pode configurar a integração.
Categorias	Usado para filtrar os cartões de integração.
Descrição resumida	Uma descrição da integração que aparece na dica de dica da ferramenta do cartão.
Descrição	Uma descrição mais longa da integração.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
. **Integração e configurações** a lista relacionada é exibida. Você pode usar esta lista relacionada para definir opções de configuração para a integração. Essas opções aparecem quando você clica em **Configuração** botão no cartão de integração associado.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Rótulo	O nome do item de integração.
Nome	O plug-in que deve ser ativado para usar a integração.
Integração	Exibe a integração para a qual você está definindo itens de integração
Ordem	Indica a ordem em que este item de integração aparece.
Tipo	Na lista, selecione o tipo de campo: ○ Cadeia de caracteres ○ Inteiro ○ Decimal ○ Data ○ Booliano ○ Senha

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ IPv4 ○ IPv6 ○ URL
Valor	Insira o valor associado ao **Tipo** selecionado. Se for um valor inválido para o selecionado **Tipo** inserido, nenhum registro é recuperado quando a integração é executada. Por exemplo, se você selecionar o tipo de URL e inserir um valor de 12.32.23.10, nenhum registro será recuperado.

7. Clique em **Enviar**.

Dicas para escrever integrações

Siga estas diretrizes para evitar algumas das armadilhas que você pode encontrar ao escrever suas próprias integrações.

Use a funcionalidade da plataforma ServiceNow sempre que possível

Principalmente, os recursos de integração integrados no Operações de segurança aplicações (Resposta a incidentes de segurança, Inteligência contra ameaças e Resposta a vulnerabilidades) destinam-se a aprimorar ou simplificar os existentes ServiceNow funcionalidade de integração da plataforma. Ao escrever integrações, sempre use a funcionalidade da plataforma quando ela existir. Aqui estão alguns comuns ServiceNow funcionalidades que podem ser usadas em vez de "rolar por conta própria".

- Serviços da Web de saída - Para a maioria das interações com sistemas de terceiros, a comunicação ocorre por meio de serviços da Web. Nesses casos, utilize serviços web de saída da plataforma (REST e SOAP são compatíveis).
- Fontes de dados/conjuntos de importação/mapa de transformação - para processar dados e inserir em ServiceNow, o mecanismo preferencial é usar fontes de dados e componentes associados.

Use estruturas de integração do Operações de segurança sempre que possível

Porque Operações de segurança os mecanismos de integração resolveram muitos problemas comuns, não é necessário reimplementar funcionalidades básicas para cada integração. Por exemplo, as estruturas de dados de vulnerabilidade e de origem de ameaça são compatíveis com o processamento de várias páginas e a transmissão desses dados para fontes de dados/transformações/conjuntos de importação. Da mesma forma, a estrutura de origem de verificação ou pesquisa fornece funcionalidade configurável de limitação de taxa. Como regra, ao implementar um recurso ou conjunto de recursos, verifique se o existe Operações de segurança a estrutura de integração cobre seu caso de uso. Em caso afirmativo, use essa estrutura.

Estenda as estruturas de integração de Operações de segurança existentes conforme necessário

A maioria das tabelas e scripts usados por Operações de segurança as estruturas de integração deveriam ser estendidas para atender às necessidades futuras. Se um caso de uso for encontrado enquanto você estiver escrevendo uma integração, estenda uma tabela ou script de integração para melhor atender a esse caso de uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Forneça feedback à ServiceNow sobre problemas encontrados durante a integração

Como uma integração está sendo desenvolvida ou testada, certifique-se de fornecer feedback quando problemas forem encontrados. Mesmo que uma solução alternativa seja necessária, Suporte e atendimento ao cliente a equipe pode fornecer uma melhoria em versões futuras que pode aliviar o problema para integrações futuras.

Teste sob carga razoável

Um problema comum com integrações é que elas não estão equipadas para lidar com cargas realistas. Como cada integração é uma aplicação com escopo, há mais limitações impostas pela plataforma para garantir a estabilidade do sistema. Essas limitações podem resultar em trabalhos de execução longa ou chamadas de API encerrados. Você pode garantir que os processos de execução longa ou processos que processam muitos dados sejam tratados corretamente, reduzindo o tempo necessário para cada chamada ou processo (geralmente fornecendo um meio de paginar solicitações de API ou agrupar grandes conjuntos de dados).

Solução de problemas de integração

Essas sugestões de solução de problemas podem ajudar você a resolver problemas comuns que você pode encontrar ao configurar ou executar integrações.

Substitua um certificado SSL de terceiros não confiável ou expirado

Quando uma conexão SSL é necessária em uma integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Você pode substituí-lo ou adicionar um novo certificado.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereços do navegador.
   Por exemplo: `https://<3rdparty>/` .

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e clique em **Segurança** guia.

   d. Clique em **Exibir certificado** e clique em **Detalhe** guia.

   e. Clique em **Exportação** Para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Deve começar com `------ INICIAR CERTIFICADO------` e termine com `------ CERTIFICADO FINAL-------` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e. crie um novo registro para a integração.
4. Em **Certificado PEM** cole o certificado baixado e copiado para a área de transferência anteriormente.
5. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Estrutura de capacidades de integrações 2,0

O novo Integration Capabilities Framework 2,0 foi reprojetado para permitir a implementação de integrações de maneira simples e consistente. Isso garante uma experiência consistente para tipos semelhantes de integrações (por exemplo: Pesquisa de reputação observável).

A nova estrutura tem recursos implementados usando Fluxos .

Os benefícios da implementação da estrutura aprimorada incluem:

- Os fluxos de capacidade que incluem somente componentes de nível de negócios sem lógica específica de implementação.
- Os fluxos de capacidade agora aceitam uma ampla matriz de entradas e formatos para máxima flexibilidade (por exemplo, referências observáveis, referências de IC, tarefas, qualquer tabela ou combinações de sys_id).
- A limitação de taxa ou limitação em execuções de integração agora são fáceis de configurar (removendo a necessidade de fazer isso usando código personalizado ou mudanças nos fluxos de trabalho de implementação).
- Auditoria aprimorada e recursos de acompanhamento de execução agora permitem relatórios melhores e solução de problemas mais fácil.
- Funções robustas de tratamento de erros são integradas aos fluxos de capacidade para evitar a duplicação de rotinas de implementação.
- Capacidade de configurar o acionamento condicional dos recursos ou das integrações. Isso fornece flexibilidade para iniciar automações automaticamente com base na categoria de incidente.
- Uma condição de filtro padrão foi introduzida em todos os recursos para filtrar Permitir observáveis listados antes que as entradas sejam fornecidas para as integrações.

Nota: Esta nova estrutura de capacidade não atualiza a estrutura de capacidade atual. Ambas as estruturas podem funcionar em paralelo. Para obter instruções sobre como aproveitar a nova estrutura de recursos, consulte Usando a nova Estrutura de capacidade com uma integração instalada e. Usando a nova Estrutura de capacidade com um fluxo.

Integrações e componentes compatíveis

O plug-in Resposta de incidentes de segurança inclui todos os fluxos de capacidade listados na Estrutura de capacidades de integração 2,0 e filtros de alto nível padrão que você pode habilitar ou desabilitar dependendo de seus requisitos.

Nota: Se você quiser usar a nova Estrutura de integração de capacidades com a versão New York, instale o plug-in do ServiceNow IntegrationHub Starter Pack Installer. Entre em contato com o Suporte ao cliente para obter assistência com a instalação.

Versões da aplicação compatíveis

A partir do Security Incident Response 10,0, as seguintes integrações são compatíveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Versão mínima necessária
Integração de análise híbrida de operações de segurança	10.0.0
Integração do PhishTank de operações de segurança	10.0.0
Integração ThreatCrowd de operações de segurança	10.0.0
Integração de Inteligência do CrowdStrike de Operações de segurança	10.0.0
Operações de segurança "Eu fui pwned?" Integração	10.0.0
Integração do Metafender de operações de segurança	10.0.0
Integração Futura Registrada de Operações de Segurança	10.0.0
Integração VirusTotal de operações de segurança	10.0.0
Integração WHOIS reversa de operações de segurança	10.0.0

A partir do Security Incident Response 10,4, as seguintes integrações são compatíveis:

Aplicação	Versão mínima necessária
Integração RiskIQ de operações de segurança	10.0.0
Integração do Shodan de operações de segurança	10.0.0
Integração do WHOIS de operações de segurança	10.0.0
Integração Carbon Black de operações de segurança	10.3.1
Integração do Splunk Search de operações de segurança	10.3.0
Integração do Logger do ArcSight para operações de segurança	10.3.0
Integração do Security Operations McAfee ESM	10.3.0
Integração do Elasticsearch de operações de segurança	10.3.0
Integração do IBM QRadar de operações de segurança	10.3.1
Host do CrowdStrike Falcon de operações de segurança	10.3.0

Componentes incluídos

A nova Estrutura de integração de capacidades inclui os seguintes componentes:

- .: Todos os seguintes recursos que existem no produto hoje como fluxos de trabalho foram reprojetados usando Fluxos :
  - **Solicitação de bloqueio** : Fornece uma maneira de bloquear observáveis associados a um incidente de segurança em um firewall, proxy da web ou algum outro ponto de controle. Esta capacidade é usada durante as investigações de resposta do incidente para conter uma ameaça identificada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Pesquisa e exclusão de e-mail** : Fornece uma maneira de pesquisar um servidor de e-mail durante uma investigação de segurança e, se necessário, excluir e-mails do servidor.
- **Enriquecer Item de Configuração** : Fornece uma maneira geral de enriquecer itens de configuração com informações adicionais de várias origens. Este recurso é usado durante as investigações de resposta a incidentes para enriquecer os dados associados a um incidente de segurança.
- **Enriquecer o observável** : Fornece uma maneira geral de enriquecer observáveis com informações adicionais de uma variedade de fontes. Esta capacidade é usada durante as investigações de resposta do incidente para conter uma ameaça identificada.
- **Ingestão de evento** : Fornece uma maneira geral de criar um incidente de segurança mapeando eventos de uma origem de integração para um incidente de segurança.
- **Obter estatísticas de rede** Recupera uma lista de conexões de rede ativas de um endpoint ou host. Essa funcionalidade é usada para enriquecer o incidente durante as investigações.
- **Obter processos em execução** Recupera uma lista de processos em execução de um endpoint ou host. Essa funcionalidade é usada para enriquecer o incidente durante as investigações.
- **Isolar host** : Fornece uma maneira de isolar um endpoint ou um host associado a um incidente de segurança. Isolar host é executado em relação a um item de configuração (IC).
- **Publicar na Lista de observação** : Fornece uma maneira de adicionar observáveis associados a um incidente de segurança a uma lista de observação que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.
- **Pesquisa de vistas** : Pesquisa vários SIEMs ou outros armazenamentos de log para instâncias de observáveis. Este recurso é usado para determinar a presença de IOCs mal-intencionados em seu ambiente.
- **Pesquisa de ameaças** Executa pesquisas de inteligência contra ameaças para determinar se um determinado observável está associado a uma ameaça à segurança conhecida. Essa capacidade é usada como parte da resposta do incidente durante as investigações.

- **Novas tabelas** :
  - sn_sec_cmn_capability: Capacidade e fluxo que implementa a capacidade.
  - sn_sec_cmn_capability_implementation: O fluxo de implementação real que fornece os serviços da capacidade.
  - sn_sec_cmn_capability_execution: O registro de execução de uma capacidade no tempo de execução.
  - sn_sec_cmn_capability_implementation_execution: O registro de execução de uma implementação de capacidade no tempo de execução.
  - sn_sec_cmn_filter_condition: As condições de filtro que podem ser aplicadas no tempo de execução à capacidade ou a uma implementação de capacidade.
- **Incluir script** CapabilityProcessor: Manipula todo o código de processamento da estrutura.
- **Limite de taxa** Capacidade máxima de solicitação simultânea por período: Define quantas integrações podem ser executadas em paralelo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Implementação da capacidade de processo de trabalho programado** : É executado a cada 15 segundos e pode ser desabilitado na página Propriedades de administração de segurança (**Incidente de segurança** > **Administração** > **Propriedades**.
  - Habilita ou desabilita o trabalho agendado, Implementações de capacidade de processo: Este trabalho agenda e gerencia automaticamente os fluxos de execução de implementação de capacidade.
  - Habilita ou desabilita pesquisas automatizadas ou aprimoramentos: Configuração que ativa ou desativa o trabalho agendado que executa a pesquisa automatizada de ameaças ou o aprimoramento de observáveis quando observáveis são adicionados a incidentes de segurança na estrutura de capacidade atual.
  - Habilita ou desabilita o trabalho agendado, Pesquisar observáveis de incidentes de segurança: Este trabalho agenda automaticamente um trabalho Pesquisa de ameaças ou Enrich observables quando observáveis são adicionados a um incidente de segurança.

Configurações na nova Estrutura de capacidade

Esta seção descreve as configurações disponíveis na nova estrutura.

Antes de Iniciar

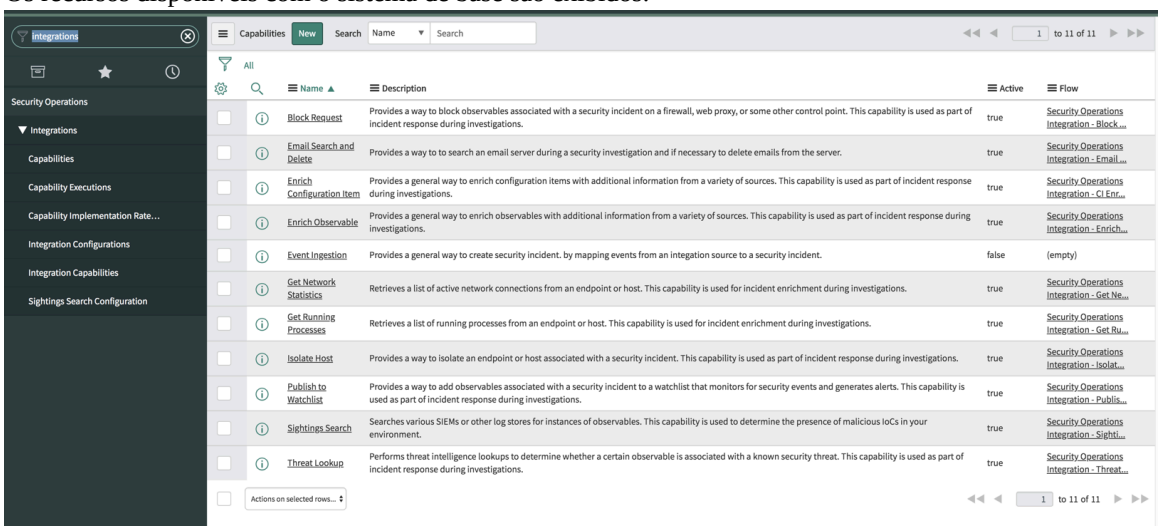
Função necessária: sn_si.admin, flow_designer, action_designer

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Capacidades**.

Nota: Versão 10,4: Começando com Resposta de incidente de segurança 10,4, o nome do menu . foi alterado para **Capacidades de integração (fluxos)** .

2. Os recursos disponíveis com o sistema de base são exibidos.



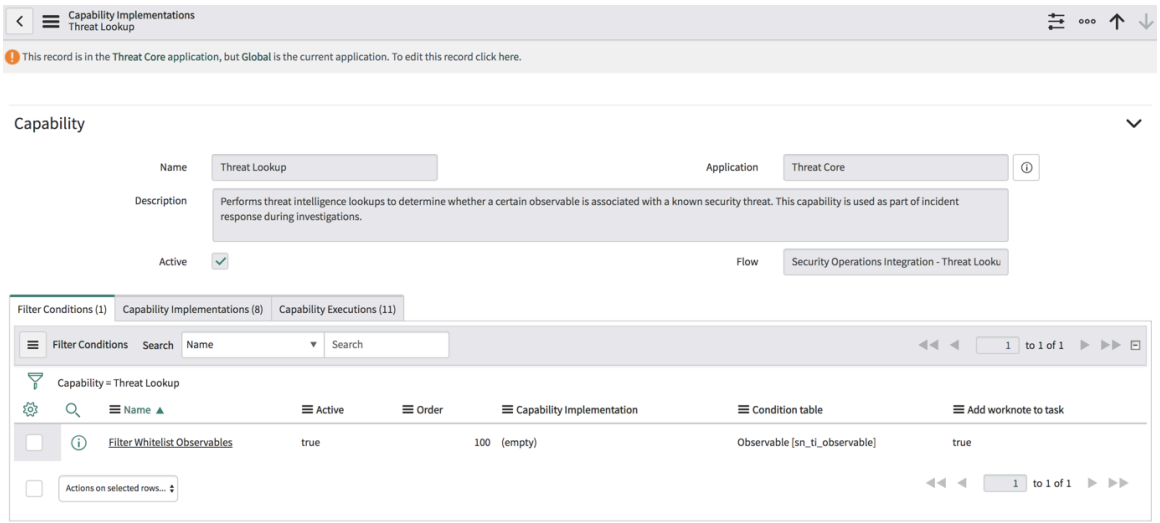
Nota:

Esses são os recursos fornecidos com o sistema de base. Você pode usar os recursos ou personalizá-los conforme necessário. As etapas a seguir descrevem como configurar um recurso e as integrações implementadas para o recurso.

3. Clique no link na coluna Nome para configurar uma capacidade.
Nome, Aplicação, Descrição e Fluxo que a capacidade implementa são exibidos.

Tradução automática

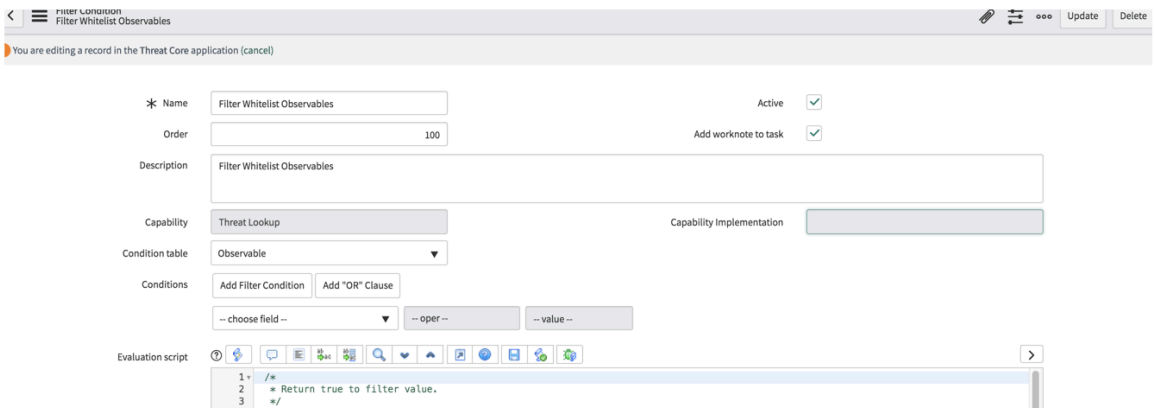
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione **Ativo** caixa de seleção para ativar a capacidade.

   - **Condições de filtro no nível de capacidade** : Quando um recurso de integração implementa um fluxo, as condições de filtro associadas ao fluxo serão executadas antes que o fluxo de capacidade seja iniciado. Por exemplo, o recurso Pesquisa de ameaças inclui a condição de Observáveis na lista de permissões de filtro, conforme mostrado acima. Clique no link Nome para editar a condição do filtro.

     Nota: Selecione **Adicionar anotação de trabalho à tarefa** caixa de seleção para adicionar anotações de trabalho para incluir informações sobre as condições de filtro usadas.



     Você pode definir condições de filtro ou um script ou uma combinação de ambos. No exemplo acima, um script é usado para definir as condições do filtro. Quando o fluxo de capacidade é executado, o script pesquisa observáveis na lista de permissões e os remove da tabela.

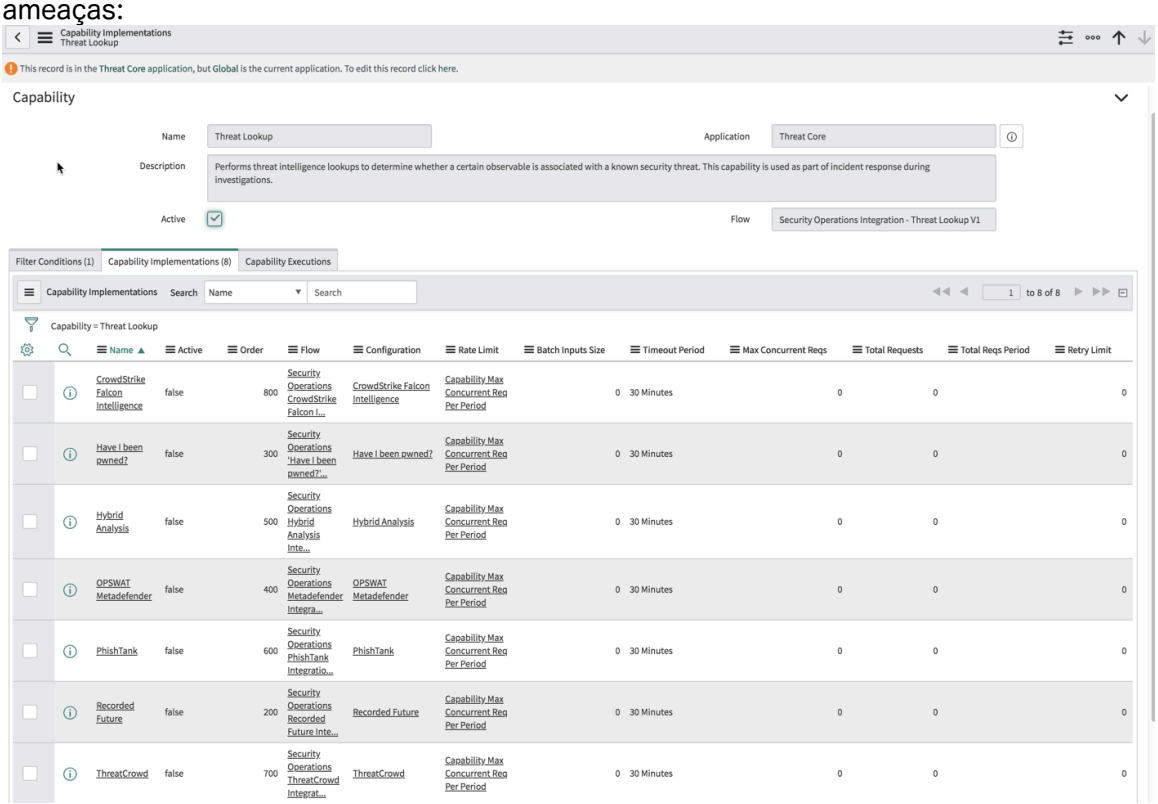
     Nota: As condições de filtro definidas aqui são aplicáveis a todas as integrações ativas definidas em **Implementações de capacidade** guia.

   - **Implementações de capacidade** : Clique em **Implementações de capacidade** guia. As implementações (integrações) que foram configuradas para o recurso são exibidas.

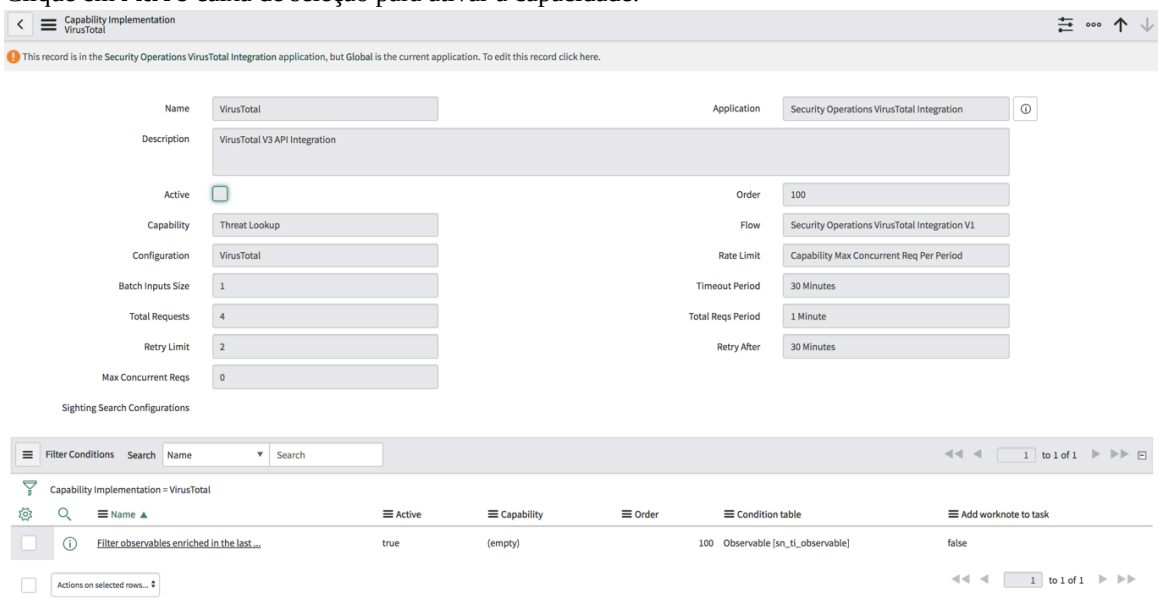
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo abaixo mostra as integrações configuradas para o recurso Pesquisa de ameaças:



5. Clique no link Nome para exibir a implementação de capacidade.
   Nome, Aplicação, Descrição e Fluxo que a capacidade implementa são exibidos.
6. Clique em **Ativo** caixa de seleção para ativar a capacidade.



Você pode especificar os seguintes detalhes:

Nome do Campo	Descrição
Ativo	Marque esta caixa de seleção para habilitar a desativação desta integração.

Tradução automática

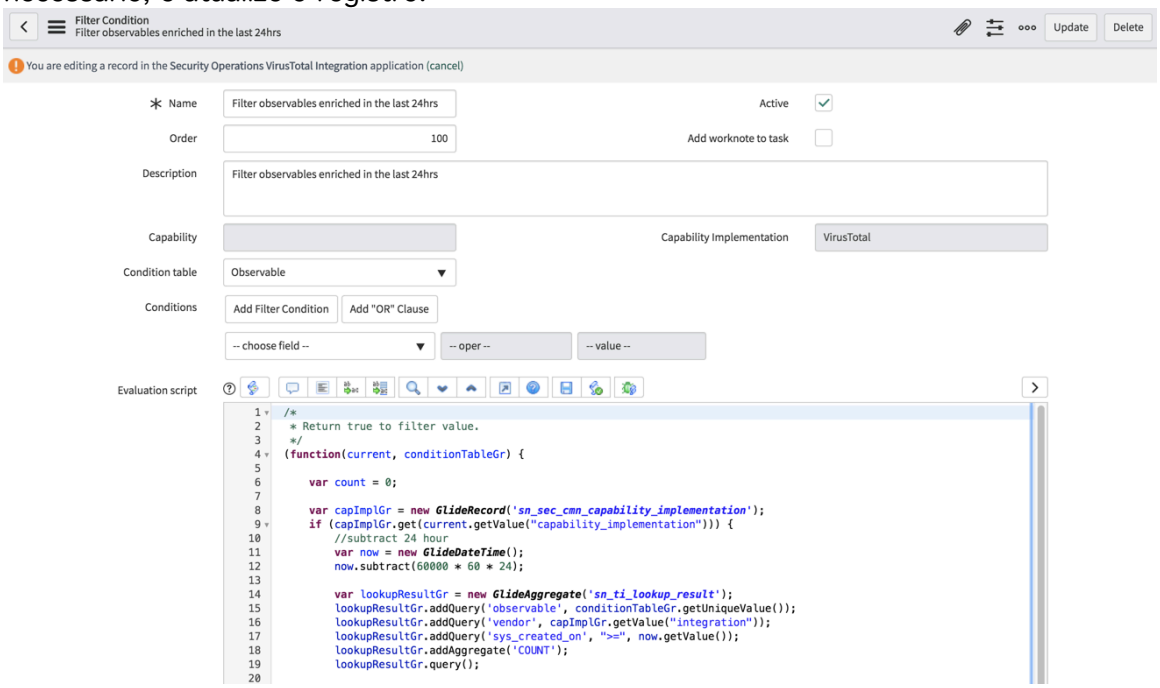
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
	Nota: Se você configurar esta integração usando o bloco de integração no **Operações de segurança** > **Integrações** > **Configurações de integrações**, este sinalizador é definido automaticamente como **Ativo** .
Ordem	Indica a ordem na qual as integrações são executadas.
Capacidade	A capacidade implementada por esta integração.
Fluxo	O subfluxo que implementa a capacidade.
Configuração	A configuração de integração desta capacidade. **Nota:** Inicialmente, isso é definido para a configuração padrão fornecida com o sistema de base. Quando uma integração está sendo configurada usando o bloco de integração no **Configurações de integração** , este valor é redefinido automaticamente para a nova configuração criada.
Limite de Taxa	Indica o número de integrações que podem ser executadas em tempo de execução (em paralelo ou por unidade de tempo).
Tamanho das Entradas em Lote	O tamanho de entrada do lote para cada execução. Por exemplo, para uma integração de Pesquisa de vistas, você pode agrupar os observáveis em lotes de 50 para que as consultas geradas não se tornem muito grandes. 0 indica que não há limite.
Período de tempo limite	A duração máxima antes que o fluxo de implementação de capacidade seja cancelado. 0 indica que não há período de tempo limite.
Total de solicitações	O número total de solicitações de execução de implementação. Este campo, em conjunto com o campo Período total de solicitações, pode ser usado para limitar o número de solicitações para o serviço. Por exemplo, você pode limitar o número a 4 solicitações por minuto.
Período de solicitações total	O número total de solicitações de execução permitidas por período.
Limite de novas tentativas	O número de novas tentativas permitidas para uma solicitação de execução com falha. Este limite será aplicável se **Tente novamente** o sinalizador é definido em sua integração para tentar novamente uma solicitação de execução quando uma condição é atendida. Por exemplo, uma solicitação de nova tentativa é feita quando você excede o limite de licença para esse serviço por um período de tempo ou o serviço está inativo.
Tente novamente após	O período após o qual é feita uma tentativa de tentar novamente uma solicitação de execução com falha.
Máximo de Solicitações Simultâneas	O número máximo de solicitações de execução de implementação simultâneas. 0 indica que não há limite.
Configurações de Pesquisa de detecções	As consultas de pesquisa de vistas padrão que podem ser executadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique no link Nome na seção Condições de filtro para configurar as condições definidas para a implementação. Adicione ou exclua condições de filtro, modifique o script, se necessário, e atualize o registro.



Usando a nova Estrutura de capacidade com uma integração instalada

Esta seção descreve como usar a nova estrutura de capacidade para uma integração existente.

Use as etapas abaixo para habilitar uma integração já instalada e configurada (consulte a lista de integrações compatíveis em Integrações e componentes compatíveis) para usar a nova estrutura de capacidade.

Nota: Integration Capability Framework 2,0 disponível com o Security Incident Response 10.0.2 oferece suporte a implementações do **Pesquisa de ameaças** e. **Enriquecer o observável** . Implementações para outros recursos serão disponibilizadas em uma versão futura.

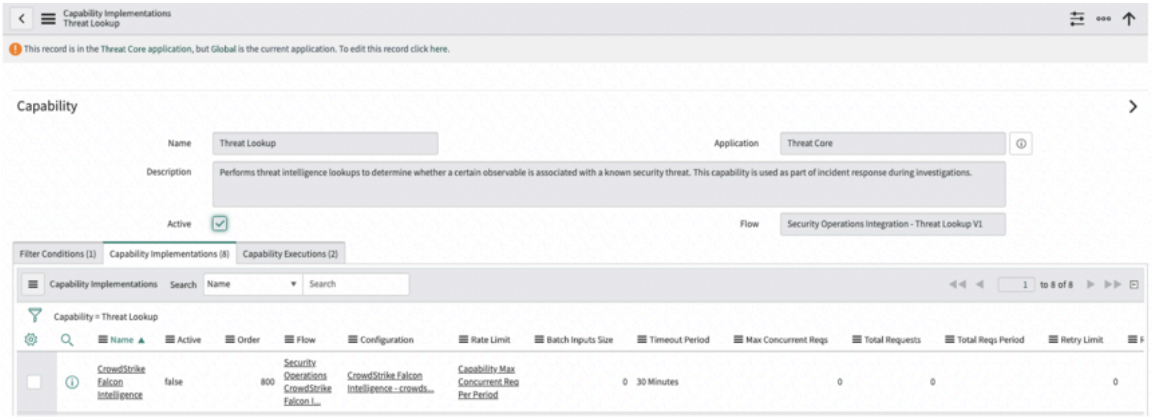
Antes de começar

- Função necessária: sn_si.admin
- Resposta a incidentes de segurança 10.0.2

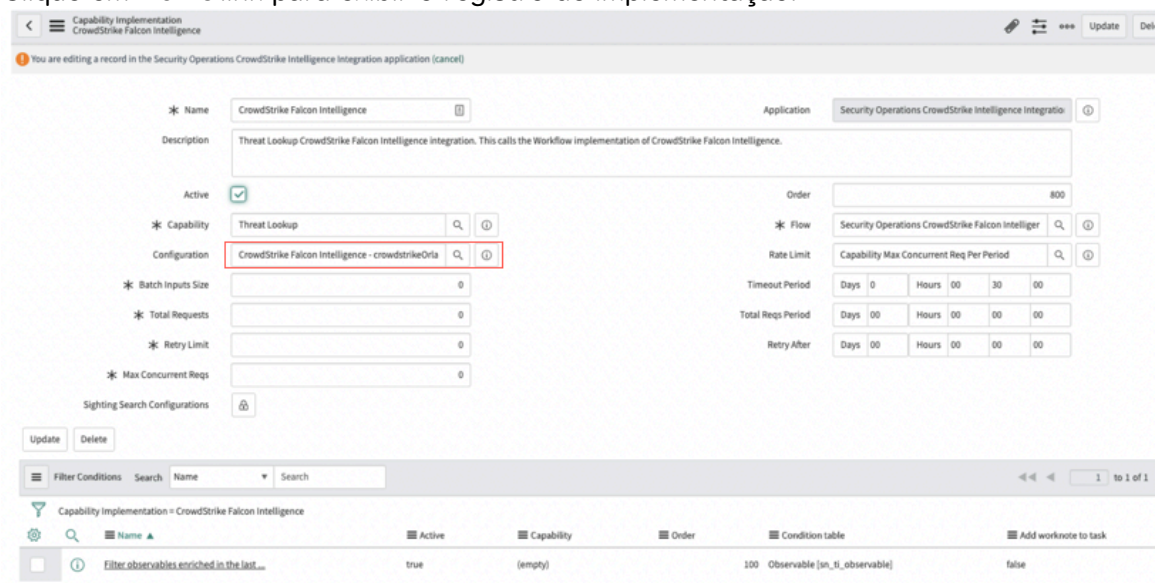
1. Navegar até **Operações de segurança** > **Integrações** > **Capacidades**.
2. Clique em **Pesquisa de ameaças** capacidade.
3. Clique na guia Implementação de capacidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



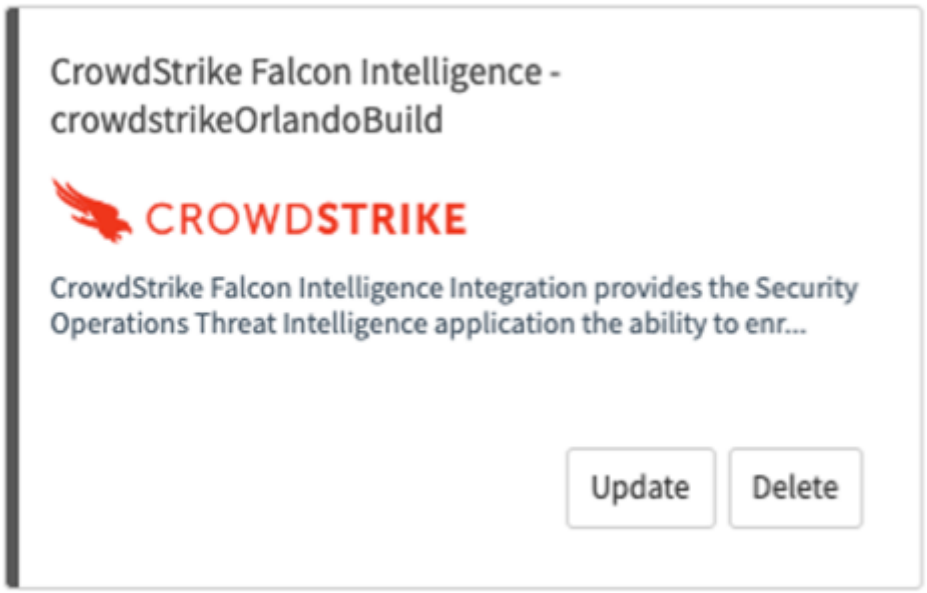
4. 4. Exiba o registro de implementação de capacidade para a integração de interesse (exemplo: Crowdstrike Falcon Intelligence). . **Ativo** a coluna deve ter o valor como **Falso** .
5. Clique em **Nome** link para exibir o registro de implementação.



6. Marque a caixa de seleção **Ativo**.
7. Certifique-se de que o registro de implementação aponte para o registro de configuração correto (o nome do bloco da integração em **Configurações de Integração** > **Mostrar configurações (Sim)**).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. A implementação está habilitada para uso com a nova estrutura.

Nota: Quando instaladas com o Security Incident Response 10.0.2, todas as integrações compatíveis serão habilitadas automaticamente na nova estrutura de capacidade de integração.

Usando a nova Estrutura de capacidade com um fluxo

Use as etapas abaixo para criar um fluxo e chamar o subfluxo fornecido pela nova estrutura de capacidade.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer, action_designer
- Instale uma das integrações compatíveis (consulte Integrações e componentes compatíveis)

As etapas abaixo descrevem como criar um fluxo de amostra e chamar um dos subfluxos fornecidos com a nova estrutura de capacidade.

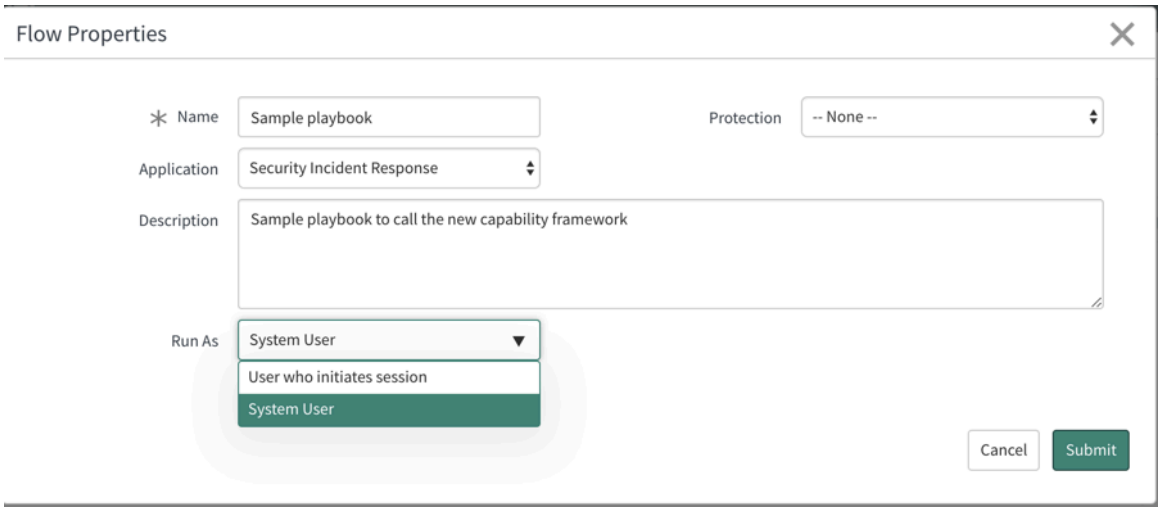
Procedimento

1. Navegar até **Tudo** > **Flow Designer** > **Designer**.

2. Clique em **Novo** para criar um novo fluxo e fornecer as informações necessárias para as propriedades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

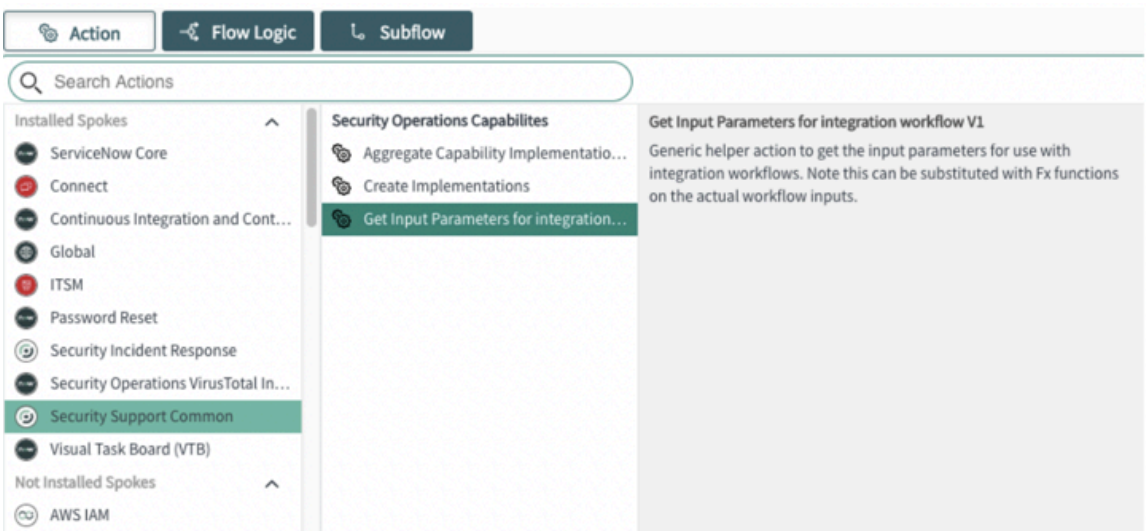


Nota: Selecione **Usuário do sistema** Na lista de seleção Executar como, conforme mostrado na imagem acima.

3. Selecione uma Condição de gatilho para o fluxo (um gatilho comum é a criação de um registro de incidente de segurança para uma determinada categoria de incidente).



4. Na etapa 1 do fluxo, selecione uma ação para obter entradas do incidente de segurança (por exemplo, observáveis).
   Você pode selecionar uma ação nas ações fornecidas com o sistema de base com o spoke comum do Suporte de segurança.



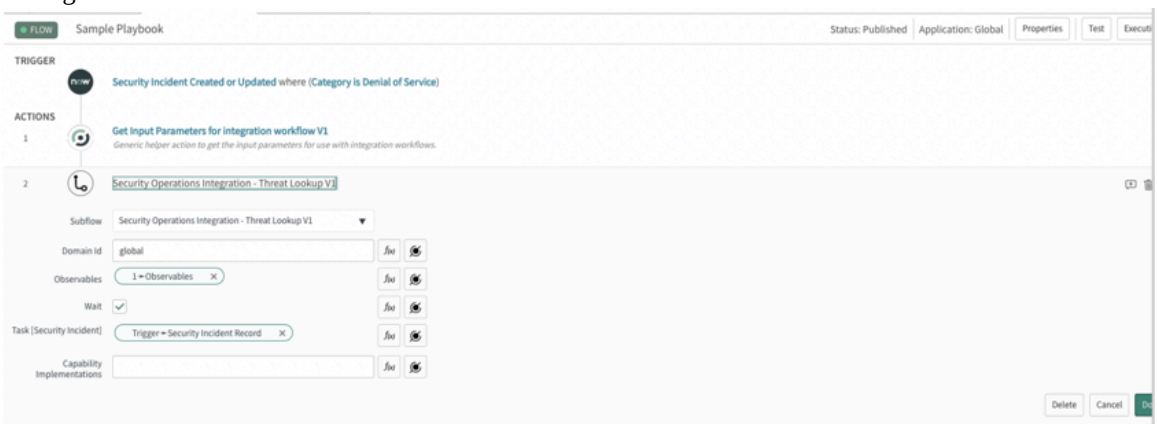
5. Na etapa 2, selecione um subfluxo (por exemplo, Pesquisa de ameaças).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Configure o subfluxo selecionado conforme mostrado abaixo:



7. Salve e publique o fluxo.

Solução de problemas de fluxos de capacidade de integração

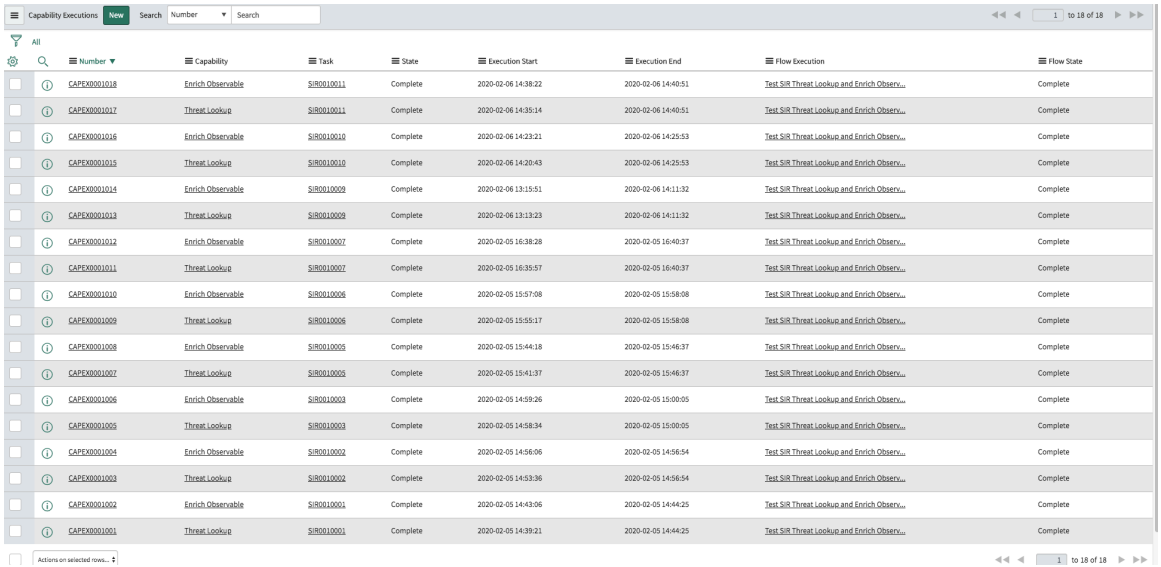
A opção Execuções de capacidade fornece informações detalhadas sobre cada capacidade que foi executada.

Nota: Execuções concluídas são arquivadas após 30 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Operações de segurança** > **Integrações** > **Execuções de capacidade.**.



2. Clique no link Execuções de capacidade para exibir detalhes adicionais.

`Anotações de trabalho de registro de incidente de segurança`

Quando observáveis são adicionados a um incidente de segurança e a condição de gatilho do fluxo é atendida, os subfluxos Pesquisa de ameaças e Enrich observable são iniciados e as seguintes anotações de trabalho são adicionadas ao incidente de segurança:

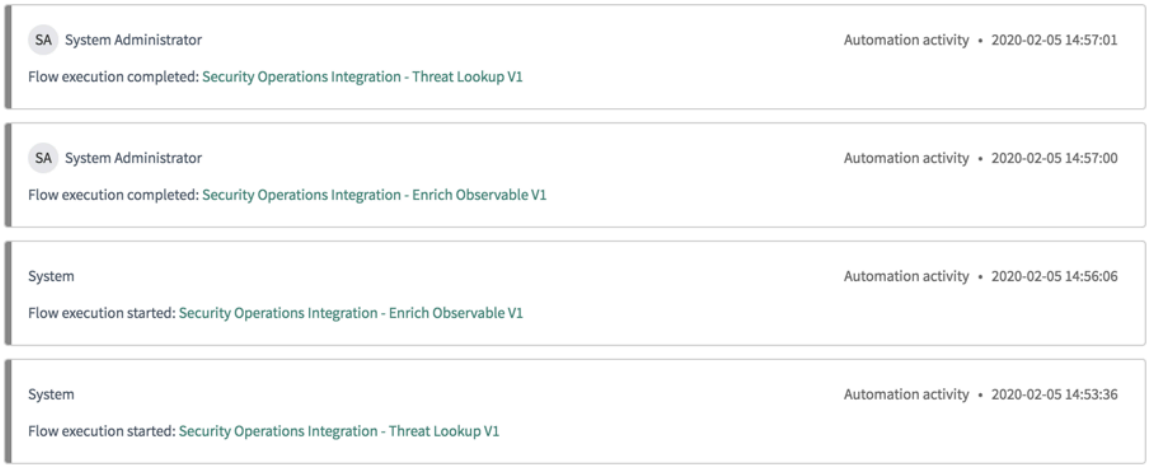
- Execução de fluxo iniciada: Integração de operações de segurança - enriquecer observável V1
- Execução de fluxo concluída: Integração de operações de segurança - enriquecer observável V1
- Execução de fluxo iniciada: Integração de operações de segurança - Pesquisa de ameaças V1
- Execução de fluxo concluída: Integração de operações de segurança - Pesquisa de ameaças V1

Para exibir essas anotações de trabalho, faça login como um usuário com *`sn_si.admin`* ou *`sn_si.analista`* e *`flow_designer`* e *`action_designer`* funções.

Navegue até a página de registro de incidente de segurança e clique nessas anotações de trabalho para exibir os detalhes da execução do fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



REST APIs para integração de terceiros com Operações de segurança

. Operações de segurança O sistema de base inclui uma série de REST APIs com script que permitem que clientes e parceiros se integrem facilmente a um existente Operações de segurança implantação. As APIs permitem coletar dados de fora do seu sistema (por exemplo, um script Python é usado para receber dados do VirusTotal) e enviá-los de volta para sua instância.

Scripts escritos em quase qualquer linguagem (Python, por exemplo) podem ser usados com as APIs para executar processos específicos do cliente. Os scripts devem ser escritos em um idioma capaz de fazer uma chamada HTTP POST externa. Por exemplo, se você tiver uma aplicação Java, deverá usar uma biblioteca, como java.net.HttpUrlConnection Pacote, para construir uma chamada HTTP e passar uma cadeia de caracteres JSON como corpo para a mensagem.

A API é usada exclusivamente para adicionar dados que foram coletados fora do nosso sistema. Por exemplo, se você inseriu o script Python de VT e recebeu dados de VT, poderá enviar esses dados de volta para a instância de SN.

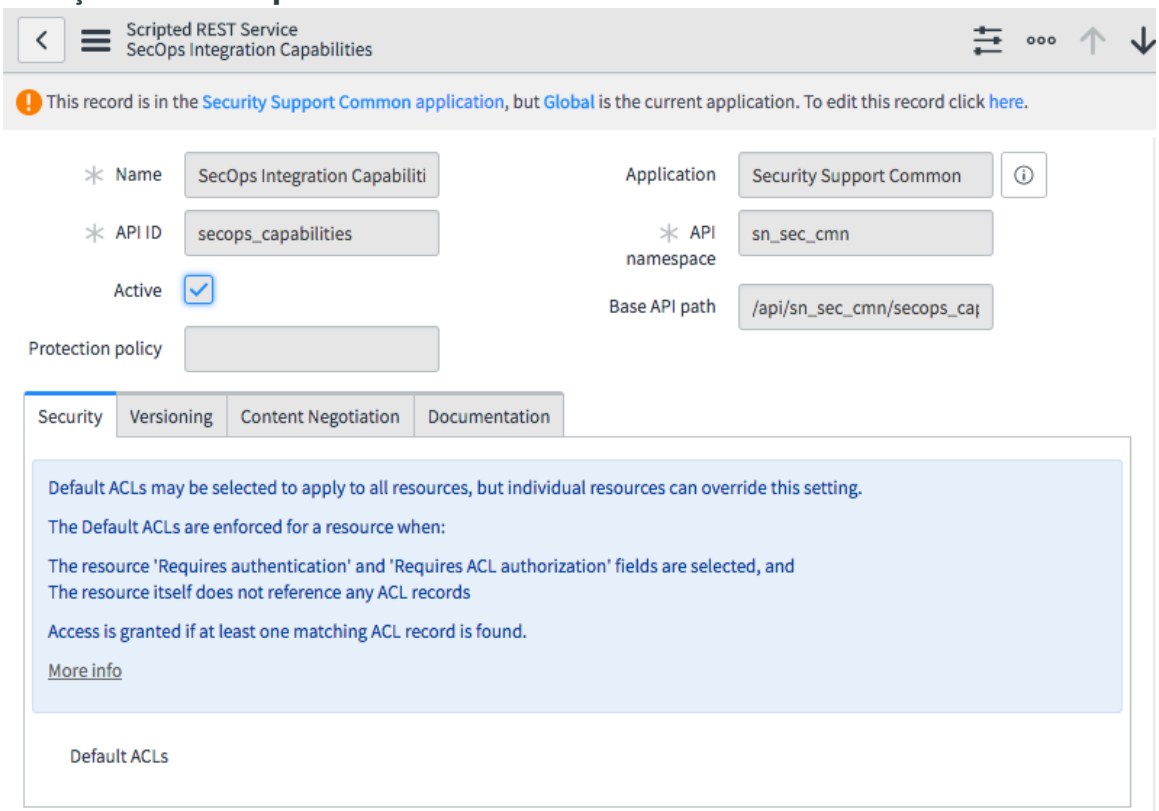
Autenticação

Todas as operações nas definições de API usam autenticação de plataforma fornecida pelo REST APIs com script recurso de operação. Para acessar, navegue até **Serviços web do sistema** > **Serviços web com script** > **Scripted REST APIs** e localize **Capacidades de integração SecOps** API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Serviço REST de Script



O usuário e o domínio do usuário estão prontamente disponíveis no contexto da API. Os registros podem ser vinculados a um usuário, um caminho de auditoria a ser estabelecido e a separação de domínio realizada. Como você está autenticado como um usuário específico, você pode usar Usando GlideRecordSecure impedir qualquer acesso não autorizado aos dados.

Autorização

Proteger o processo de criação de registro de usuários fora do Operações de segurança, você deve ter sn_sec_cmn.api_write função. Somente usuários com esta função podem acessar as APIs.

Parâmetros de solicitação de configuração

Os seguintes parâmetros de solicitação estão disponíveis.

Nome	Padrão	Descrição
ignore_mandatory_fields	falso	Se definido como verdadeiro, o registro persiste mesmo se os campos obrigatórios não estiverem preenchidos.
include_wrap	falso	Se definido como verdadeiro, a resposta incluirá o wrapper padrão fornecido pela instância para REST APIs com script.
simple_response	falso	Se definido como verdadeiro, a resposta incluirá somente se a operação foi bem-sucedida.

Respostas de erro

As seguintes respostas de erro podem ocorrer.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de erro	Quando isso ocorre?	Solução
Acesso insuficiente	O usuário não tem a função sn_sec_cmn.api_write.	Adicione a função ao usuário.
Corpo de publicação inválido	O corpo da solicitação está vazio ou é um objeto vazio.	Em conformidade com a definição da API.
Nenhum campo fornecido	Os campos de dados fornecidos para persistir estão vazios.	Em conformidade com a definição da API.
Campos obrigatórios ausentes: X,y,z	Os campos obrigatórios estão ausentes.	Em conformidade com a definição da tabela ou conjunto de destino **ignore_mandatory_fields** para verdadeiro.
Não é possível manter o registro	Não é possível persistir o registro analisado.	GlideRecord insert() falhou, análise adicional é necessária.
Erro desconhecido	Ocorre se nenhum caminho de erro conhecido tiver sido seguido.	Uma análise mais detalhada é necessária.

Caso de uso de aprimoramento de IC

Usando scripts de terceiros, você pode gravar na tabela Aprimoramento do item de configuração [sn_sec_cmn_ci_enrichriment_result] para aprimoramento de IC. Os registros de aprimoramento são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma origem de terceiros.

Solicitações e respostas de amostra para o caso de uso de aprimoramento de IC são mostradas aqui.

Create-request para aprimoramento de IC

```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Create-Response para aprimoramento de IC


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Caso de uso de aprimoramento de observável

Usando scripts de terceiros, você pode gravar no resultado de aprimoramento do observável [sn_ti_observable_enrichment_result] tabela para aprimoramento de observável. Os registros de aprimoramento são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma origem de terceiros.

Solicitações e respostas de amostra para o caso de uso de aprimoramento de observável são mostradas aqui.

Create-request para aprimoramento de observável


```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Create-Response para aprimoramento do observável


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```


Nota: Além de enriquecer os registros existentes, você também pode usar Operações de segurança mapeamento de dados de aprimoramento para adicionar novos registros a tabelas aprovando um **enrichment_mapping_id** para um mapeamento de aprimoramento existente e um correspondente **raw_data** cadeia de caracteres que pode ser analisada pelo processo de mapeamento.

Caso de uso da pesquisa de ameaças

Usando scripts de terceiros, você pode gravar na tabela Resultado da pesquisa de ameaças [sn_ti_lookup_result] para obter resultados da pesquisa de ameaças. Os registros de pesquisa são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma origem de terceiros.

Solicitações e respostas de amostra para o caso de uso de pesquisa de ameaças são mostradas aqui.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Create-request para pesquisas de ameaças


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Create-Response para pesquisas de ameaças


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Capacidades de integração

. Capacidades de integraçãoa estrutura fornece uma arquitetura consistente para oferecer suporte à interoperabilidade com integrações de terceiros. Esta interface abstraída e modelo de dados isola as integrações de mudanças na aplicação principal e garante uma experiência consistente para tipos semelhantes de integrações.

Cada capacidade de integração persiste na capacidade de integração [sn_sec_cmn_integration_capability] tabela. Os fluxos de capacidade de integração não podem ser executados sozinhos e exigem a inicialização de um fluxo de implementação. Qualquer plug-in que forneça uma implementação da capacidade adiciona sua implementação à tabela secundária: Implementação da capacidade de integração [sn_sec_cmn_integration_capability_implementation] .

A implementação especifica o fluxo a ser executado, a integração relacionada (ID do plug-in) e a capacidade que ela implementa. Esses fluxos podem ser executados em paralelo usando o inicializador de fluxo paralelo; no entanto, a execução sequencial é o padrão no sistema de base. Se necessário, você pode mude a ordem de execução .

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integração de operações de segurança - capacidade de solicitação de bloqueio

O recurso Bloquear ação bloqueia observáveis associados a um incidente de segurança em um firewall, proxy da web ou outro ponto de controle usando fluxos de implementação. Esta capacidade é usada durante as investigações de resposta do incidente para conter uma ameaça identificada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O recurso Solicitação de bloco tem um fluxo, Integração de operações de segurança - Bloquear fluxo de solicitação, que executa a solicitação para bloquear. Este fluxo aceita uma lista de observáveis, encontra todos os recursos de implementação e executa a solicitação com base no fluxo configurado.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Executar bloqueio de solicitação

Bloqueia a comunicação com observáveis associados a um incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

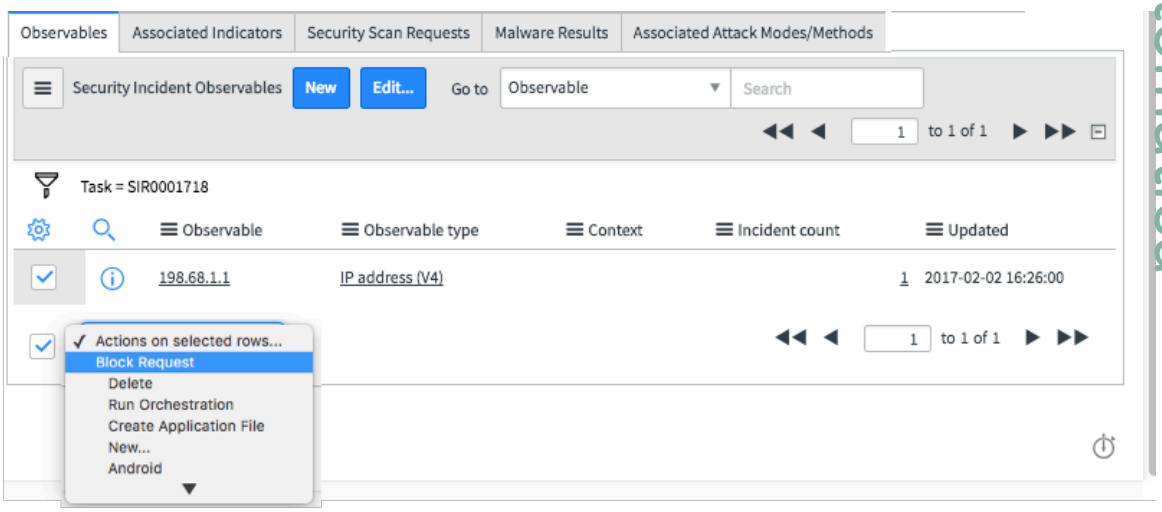
Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

. **Integração de operações de segurança - Solicitação de bloqueio** o fluxo pode ser acionado a partir de um formulário observável ou do **Observáveis de incidentes de segurança** lista relacionada em um incidente de segurança.

Este exemplo mostra uma solicitação de bloqueio de um incidente de segurança.

Procedimento

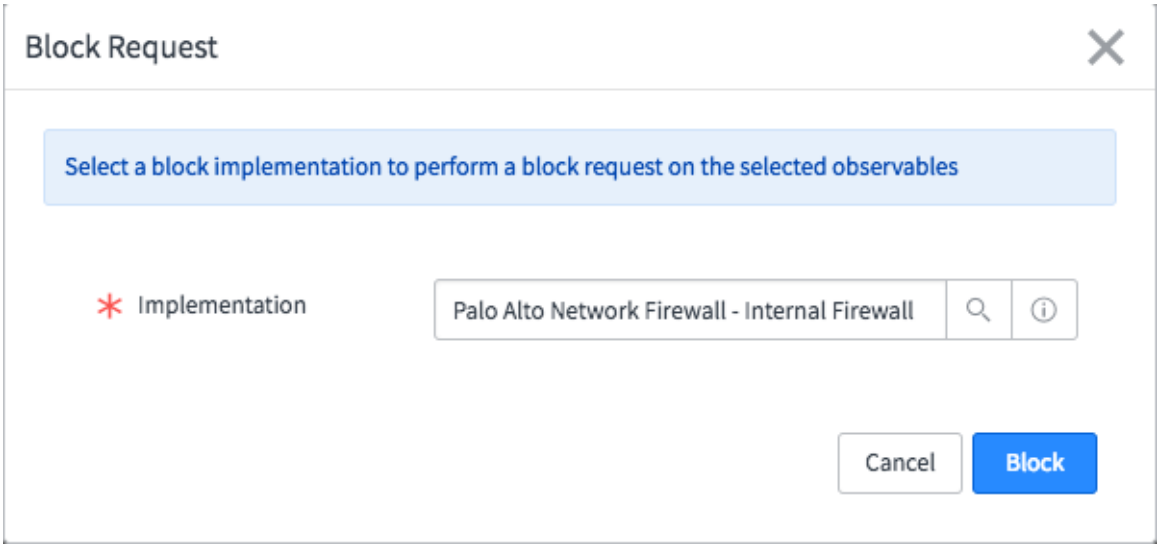
1. Navegue até um incidente de segurança.
2. Selecione Observáveis no **Lista relacionada** guia.
3. Clique em **Solicitação de bloqueio** em **Ações nas linhas selecionadas...** menu suspenso.



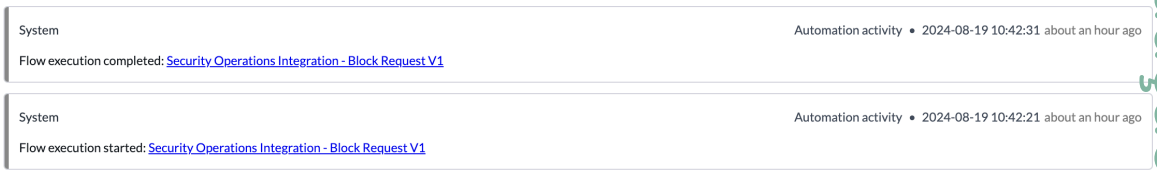
A caixa de diálogo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Escolha a implementação.
5. Clique em **Bloco** .
   A auditoria de execução de fluxo é exibida na seção Anotações de trabalho.



Integração de operações de segurança - Bloquear fluxo de solicitação

O fluxo Integração de operações de segurança - Solicitação de bloco é um fluxo de alto nível independente de integrações. Bloqueia observáveis associados a um incidente de segurança. Use-o para executar uma integração como Palo Alto Networks - Firewall.

. **Integração de operações de segurança - Solicitação de bloqueio** o fluxo pode ser acionado em um formulário observável ou a partir de **Observáveis de incidentes de segurança** lista relacionada em um incidente de segurança. Em uma lista, ele está no menu de ação suspenso. Em um formulário, é um link relacionado. O bloqueio de uma solicitação está disponível somente quando você tem uma implementação instalada para o recurso de solicitação de bloqueio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitação de bloqueio



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração de operações de segurança - Recurso de pesquisa e exclusão de e-mail

O recurso Pesquisa e exclusão de e-mail retorna o número de e-mails de ameaças de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

O recurso Pesquisa e exclusão de e-mail tem um fluxo que executa os processos de pesquisa e exclusão de e-mail.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto. Se nenhum dos **Pesquisa e exclusão de e-mail** as implementações de capacidade estão ativas, o. **Pesquisa de e-mail** o link relacionado em um incidente de segurança não é exibido.

Integração de operações de segurança - Fluxo de pesquisa e exclusão de e-mail

O fluxo Integração de operações de segurança - Pesquisa e exclusão de e-mail retorna o número de e-mails de ameaças de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

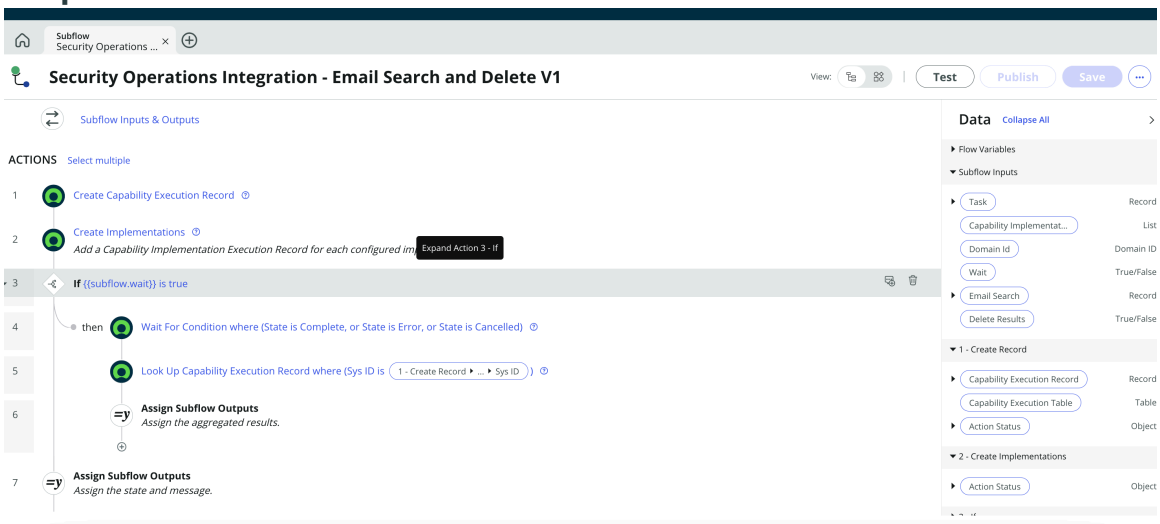
A consulta de pesquisa pode levar algum tempo para ser concluída. Depois que a contagem é recebida, a aprovação é necessária para excluir e-mails de um servidor de e-mail.

Este fluxo é acionado pelo **Excluir do(s) servidor(es) de e-mail** e. **Pesquisar em servidor(es) de e-mail** botões no **Pesquisa de e-mail** em um incidente de segurança. Para obter mais informações, consulte PESQUISE e exclua e-mails de phishing.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa e exclusão de e-mails



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As atividades do processo de fluxo incluem:

Acompanhamento da execução Iniciar ação (pesquisa de e-mail)

A ação de execução do recurso Acompanhamento de execução - Iniciar (Pesquisa de e-mail) cria um registro de acompanhamento de execução e marca o estado do registro como Iniciado. Esta ação é usada por todos os fluxos de capacidade e implementação para acompanhar seu estado.

Resultados

Os resultados possíveis para esta ação são:

Resultados

Resultado	Descrição
Êxito	O registro de acompanhamento de execução foi criado.
Falha	Não foi possível criar o registro de acompanhamento de execução.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
ImplementationId	Identificador do sistema da implementação da capacidade de integração que está sendo executada.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo.
Id_do_contexto_do_fluxo	Identificador do sistema do registro de contexto de fluxo associado. Fornecido pelo sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
FlowName	Nome do fluxo. Fornecido pelo sistema.
ID de ExcutionCapabilityParentCapability	Identificador do sistema do registro de auditoria que iniciou o fluxo de implementação. Necessário somente para fluxos de implementação de capacidade de integração, como Splunk, Elasticsearch.
EmailsearchId	O SYSID do registro de pesquisa de e-mail na tabela Pesquisa de e-mail [sn_sec_cmn_email_search].

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema do registro de acompanhamento de execução.

- Ação Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - Nenhuma ação de impls

Integração de operações de segurança- Enrich a capacidade de IC

O recurso Enrich IC permite enriquecer dados para itens de configuração associados a um incidente de segurança.

. **Enriquecer IC** a capacidade tem um fluxo, Integração de operações de segurança - Fluxo de aprimoramento de IC. Quando o fluxo de capacidade é executado, ele executa fluxos adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o aprimoramento nos ICs selecionados ou executar o aprimoramento usando todas as implementações.

Nota: Esses dados aprimorados não são o tipo de dados que você deseja armazenar no CMDB, pois são dados forenses específicos de uma determinada investigação - por exemplo, executar um memdump de um IC. Em vez disso, os dados são armazenados na tabela Aprimoramento do item de configuração [sn_sec_cmn_ci_enrichment_result].

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integração de operações de segurança - Fluxo de aprimoramento de IC

O fluxo Integração de operações de segurança - Aprimoramento de IC permite enriquecer dados em itens de configuração (IC) associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado a partir de Resposta a incidentes de segurança de duas maneiras.

- Selecionando um ou mais ICs do **Itens de configuração** (em **Itens afetados** link relacionado) e selecionando **Executar aprimoramento de IC** em **Ações nas linhas selecionadas** lista de seleção.
- Abrindo um registro de IC e clicando em **Executar aprimoramento de IC** link relacionado.

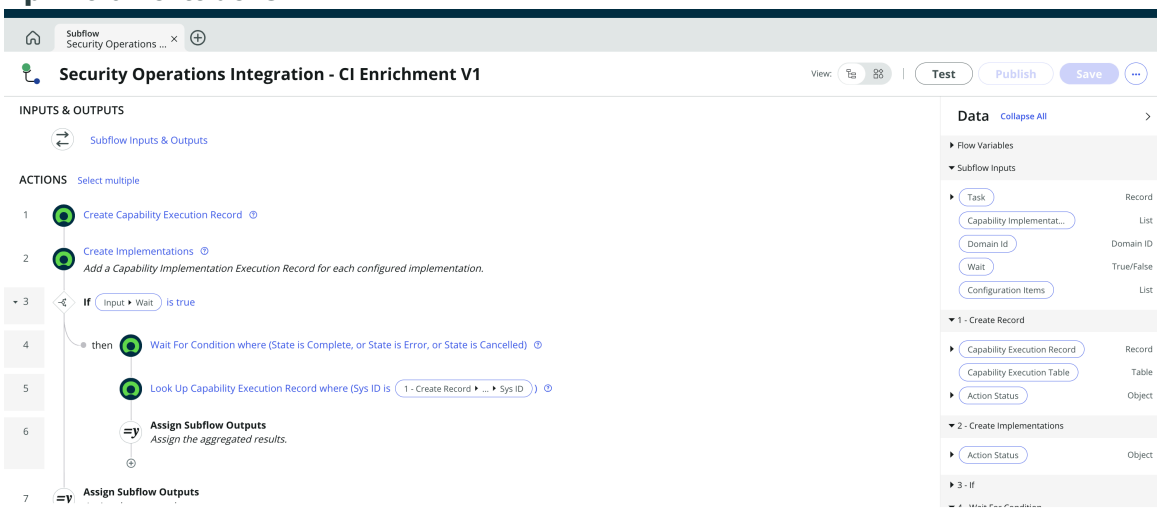
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualquer método permite especificar quais implementações serão usadas para enriquecer os ICs selecionados. Os fluxos de implementação associados são executados para executar o aprimoramento.

Nota: O sistema de base não inclui um fluxo de implementação para esta capacidade. Para enriquecer ICs, você deve criar sua própria implementação fluxo .

Aprimoramento de IC



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As ações do processo de fluxo incluem:

- Acompanhamento da execução - Iniciar ação de fluxo
- Integração de operações de segurança - Fluxo de aprimoramento de IC
- Acompanhamento de execução de capacidade - Nenhuma ação de impls
- Ação Obter capacidades de segurança compatíveis

Integração de operações de segurança- Enrich a capacidade observável

O recurso Enrich observable permite enriquecer observáveis com informações adicionais de uma variedade de fontes usando fluxos de implementação. Esta capacidade é usada durante as investigações de resposta do incidente para conter uma ameaça identificada.

A capacidade Observável Enrich tem um fluxo, Integração de operações de segurança - Enrich o fluxo observável. Quando o fluxo de capacidade é executado, ele executa fluxos adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o aprimoramento nos observáveis selecionados ou executar o aprimoramento usando todas as implementações que correspondam aos tipos de observáveis compatíveis.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integração de operações de segurança - Enrich o fluxo observável

O subfluxo Integração de operações de segurança - Enrich observable permite enriquecer observáveis com informações adicionais de uma variedade de fontes usando o designer de fluxo de implementação.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

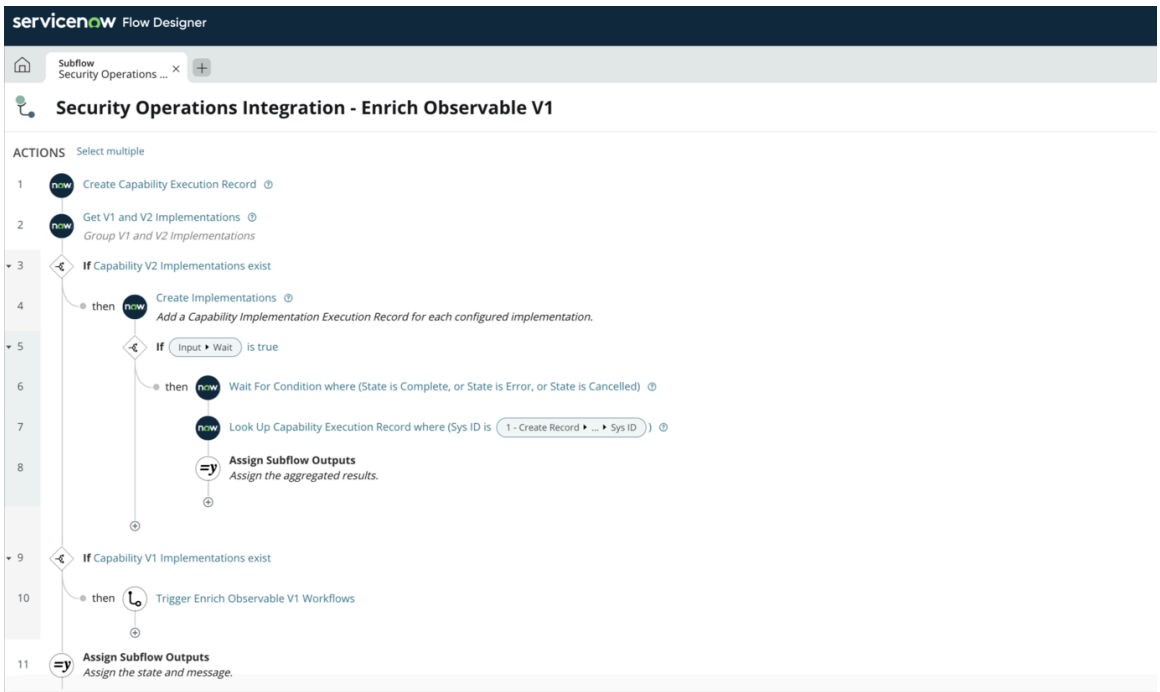
Por Que e Quando Desempenhar Esta Tarefa

Este fluxo pode ser acionado a partir de qualquer um Resposta a incidentes de segurança ou Inteligência contra ameaças de duas maneiras.

- Selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar aprimoramento de observável** em **Ações nas linhas selecionadas** lista de seleção.
- abrindo um registro observável e clicando em **Executar aprimoramento de observável** link relacionado.

Qualquer método permite especificar quais implementações serão usadas para enriquecer os observáveis selecionados. Os fluxos de implementação associados são executados para executar o aprimoramento.

Aprimorar observável



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As ações do processo de fluxo incluem:

- Acompanhamento de execução de capacidade - Nenhuma ação de impls
- Ação Obter capacidades de segurança compatíveisAcompanhamento de execução de capacidade - Nenhuma ação de impls

Integração de operações de segurança- Obtenha a capacidade de estatísticas de rede

O recurso Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint. Ele pode ser usado para aprimoramento de incidentes durante investigações. Este recurso é acionado automaticamente quando um item de configuração é adicionado a um incidente de segurança.

. **Obter estatísticas de rede** a capacidade tem um fluxo, Integrações de operações de segurança - Obter fluxo de estatísticas de rede Que aceita um ou mais ICs e tarefas. O fluxo itera em cada implementação e em cada IC e invoca novamente o fluxo de implementação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integrações de operações de segurança - Obter fluxo de estatísticas de rede

O fluxo Integrações de operações de segurança - Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint.

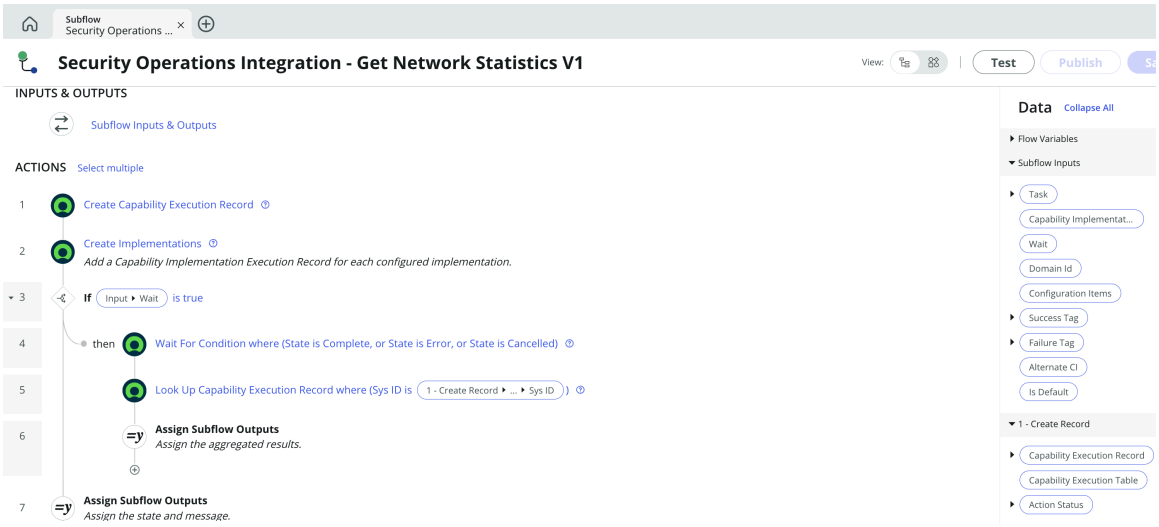
Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é executado automaticamente quando um item de configuração é adicionado a um incidente de segurança.

Obter estatísticas de rede



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As ações de fluxo incluem:

- Atividade Determine ICs
-

.

Acompanhamento de execução - Início (ICs) Ação de fluxo

. **Acompanhamento de execução - Início (ICs)** a ação de fluxo inicia o processo de auditoria de um Operações de segurança Fluxo de integração que opera em itens de configuração (ICs).

. **Acompanhamento de execução - Início (ICs)** A ação de fluxo pode ser usada com qualquer fluxo de IC para começar a registrar o andamento do fluxo em uma auditoria.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
Impl	Sinalizador que especifica se a auditoria é feita para um fluxo de capacidade de integração ou um fluxo de implementação de capacidade de integração. Os valores possíveis são: • Falso - Indica auditoria em um fluxo de capacidade de integração abstrato, como Pesquisa de vistas. (padrão.) • Verdadeiro - Indica auditoria em um fluxo de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo.

CiList	Um ou mais itens de configuração (IC) para executar a ação desejada no seguinte formato:
	`["sysId", "sysId"]`
	ou
	`"sysId"`
	Usado como uma entrada de fluxo.

Id_do_contexto_do_fluxo	Identificador do sistema do registro de contexto de fluxo associado. Fornecido pelo sistema.
FlowName	Nome do fluxo. Fornecido pelo sistema.
ID de ExcutionCapabilityParentCapability	Identificador do sistema do registro de auditoria que iniciou o fluxo de implementação. Necessário somente para fluxos de implementação de capacidade de integração, como Splunk, Elasticsearch.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema do registro de auditoria.

As ações do processo de fluxo incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ação Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - Nenhuma ação de impls

Resposta do incidente de segurança- Obter fluxo de estatísticas de rede

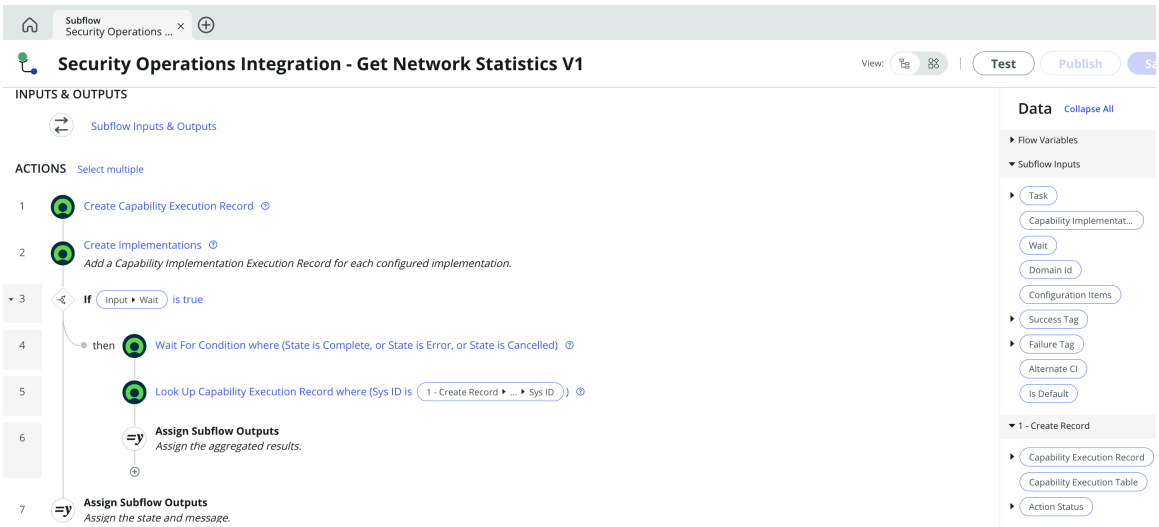
O **Resposta a incidentes de segurança** > **Obter estatísticas de rede** O fluxo recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no **Análise** estado.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança que contêm itens de configuração, o fluxo é executado automaticamente quando o estado muda para **Análise** .

Os incidentes de segurança existentes são atualizados automaticamente quando você está em **Análise** e você adiciona um novo item de configuração.

Obter estatísticas de rede



As ações do processo de fluxo incluem:

Obter ação de fluxo de FQDN do item de configuração

Determinar Shell Script por SO

Se a instrução for executada pelo PowerShell

Acompanhamento da execução - Iniciar ação de fluxo

Obter estatísticas de rede por meio da ação de fluxo netstat

Acompanhamento da execução da capacidade - Ação de fluxo de falha

Ação de fluxo Criar registros de dados de aprimoramento

Acompanhamento da execução da capacidade - Ação de fluxo de falha - Retorna o ID de aprimoramento.

Acompanhamento da execução da capacidade - Ação de fluxo concluída

Procedimento

1. Abra um incidente de segurança.
2. Atualize o. **Estado** . **Análise** , se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração de Resposta a incidentes de segurança fornece informações de estatísticas de rede no **Links relacionados** > **Melhorias de incidentes de segurança** guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração de operações de segurança- Obtenha a capacidade de processos em execução

A funcionalidade "Obter processos em execução" recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint. Essa funcionalidade é usada para enriquecer o incidente durante as investigações.

O recurso Obter processos em execução tem dois implementação fluxos:

- Integração Carbon Black de operações de segurança - Obter fluxo de processos em execução
- Integração de comando do sistema de operações de segurança- Obter fluxo de processos em execução

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

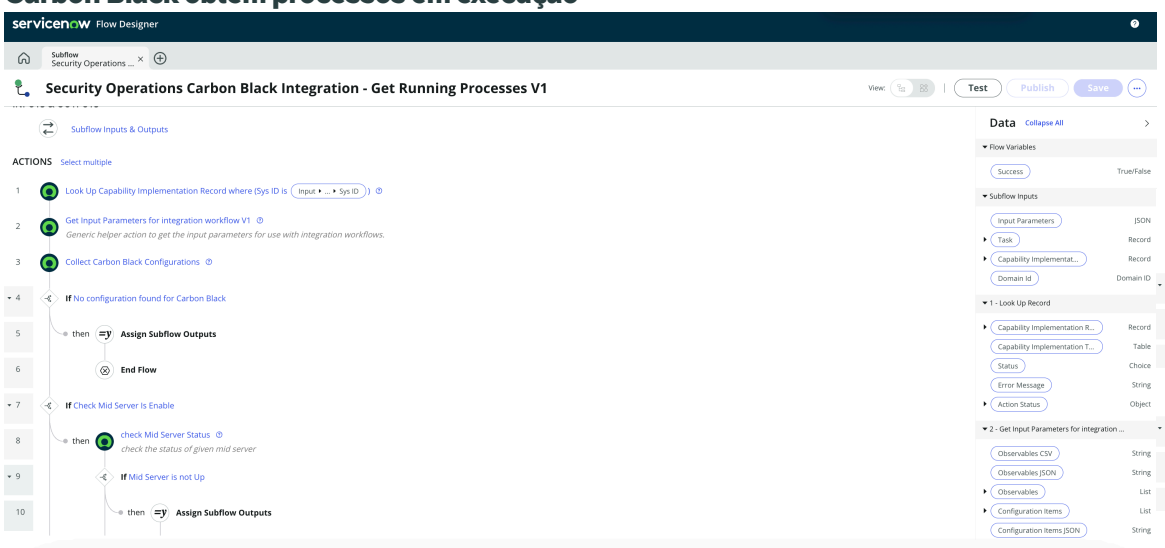
Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração Carbon Black de operações de segurança - Obter fluxo de processos em execução

Security Operations Carbon Black Integration - Obter processos em execução é a implementação da integração Carbon Black lançada pelo fluxo de processo Integração de operações de segurança - Obter em execução.

Função necessária: sn_si.analyst

Carbon Black obtém processos em execução



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coletar ação de fluxo de configurações Carbon Black

A ação de fluxo Coletar Configurações Carbon Black reúne informações de configuração para usar no fluxo.

A ação de fluxo Coletar configurações do Carbon Black reúne informações de configuração do Carbon Black para usar no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Não há variáveis de entrada para esta ação de fluxo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.
api_token	Chave de API de integração de terceiros.

Verifique o status do MID Server

Determina se o MID Server foi identificado no **Host do MID Server** o campo da configuração da integração está ativo e em execução. Se o campo estiver definido como **Qualquer** , A ação de fluxo verifica se qualquer MID Server está instalado e em execução.

A ação Verificar fluxo de status do MID Server pode ser usada com qualquer fluxo para verificar a presença de um MID Server em execução no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
ExecutitionId de capacidade	O ID da capacidade que está sendo executada.
FlowName	O nome do fluxo que está sendo executado.
mid_server_host	O MID Server identificado na configuração da integração i.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
mid_server_live	Identifica se o MID Server foi identificado em **Host do MID Server** o campo da configuração da integração está ativo e em execução. Se o campo estiver definido como **Qualquer** , A ação de fluxo verifica se qualquer MID Server está instalado e em execução.

Obter ação de fluxo de ID do sensor

A ação Obter fluxo de ID do sensor coleta identificadores do sensor para usar no fluxo.

A ação Obter fluxo de ID do sensor pode ser usada com qualquer fluxo para coletar informações do sensor a serem usadas no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensor encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ic_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Criar ação de fluxo de sessão

A ação Criar fluxo de sessão estabelece uma sessão Carbon Black a ser usada no fluxo.

A ação Criar fluxo de sessão pode ser usada com qualquer fluxo para criar uma sessão Carbon Black no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Sessão criada.
Falha	Sessão não criada. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Ação de fluxo de verificação do status da sessão

Determina o status de uma sessão Carbon Black no fluxo.

A ação de fluxo Verificar status da sessão pode ser usada com qualquer fluxo para verificar o status da sessão do Carbon Black no fluxo .

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador da sessão.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
saída	Informações sobre os processos em execução do Carbon Black.

Criar ação de fluxo de processo de comando

A ação de fluxo do processo Criar comando cria um processo de comando Carbon Black para usar no fluxo .

A ação de fluxo Criar processo de comando pode ser usada com qualquer fluxo para criar um processo de comando Carbon Black no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Processo de comando criado.
Falha	Processo de comando não criado. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador da sessão.
command_id	Identificador do comando.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Verificar status do comando e obter ação de fluxo do processo

Verifica o status do comando Carbon Black e recupera processos a serem usados no fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar status do comando e Obter ação de fluxo do processo podem ser usadas com qualquer fluxo para verificar o status de um comando Carbon Black e obter processos no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Status do comando retornado e processos criados.
Falha	Status do comando ou erro de processo. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador da sessão.
command_id	Identificador do comando.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Ação de fluxo de dados de processos de mapeamento

A ação Mapear processos de fluxo de dados mapeia os dados do processo Carbon Black no fluxo.

A ação Mapear fluxo de dados de processos pode ser usada com qualquer fluxo para mapear processos Carbon Black.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Processos mapeados
Falha	Processos não mapeados. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
affected_ci	Item de configuração afetado.
implementation_id	Identificador de implementação.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Retorna dados formatados sobre processos em execução usados pelo fluxo de trabalho abstrato.
processos	Lista de processos em uma matriz.

Acompanhamento da execução da capacidade - Ação de fluxo concluída

A ação de fluxo Acompanhamento de execução de capacidade - Concluir atualiza o registro de auditoria quando o fluxo é concluído.

A ação Acompanhamento de execução de capacidade - Concluir fluxo pode ser usada com qualquer fluxo para registrar a conclusão do fluxo.

Nota: . **Valor de retorno** matriz do **Inicializador paralelo** a ação de fluxo principal contém uma matriz de resultados de todos os fluxos de integração executados e solicita a conclusão bem-sucedida do acompanhamento da execução.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído** .

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades Iniciar auditoria.
FlowName	Nome do fluxo. Fornecido pelo sistema.
mensagem	Mensagem de conclusão.

Variáveis de saída

Não há variáveis de saída.

Fechar ação de fluxo da sessão

Fecha uma sessão Carbon Black no fluxo.

A atividade Fechar sessão pode ser usada com qualquer fluxo para fechar uma sessão Carbon Black.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Sessão encerrada.
Falha	Sessão não encerrada. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador da sessão.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
saída	Variáveis de API

Integração de comando do sistema de operações de segurança- Obter fluxo de processos em execução

O fluxo Integração de comando do sistema de operações de segurança - Obter processos em execução recupera os processos em execução de um item de configuração quando adicionado ou atualizado para um incidente de segurança baseado no Windows ou Unix no **Análise** estado.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para novos incidentes de segurança, o fluxo é executado automaticamente quando você envia o incidente com um item de configuração selecionado, quando o estado muda automaticamente para **Análise** . Se ele permanecer em **Rascunho** e, em seguida, ele não será executado.

Os incidentes de segurança existentes são atualizados automaticamente quando você está em **Análise** e você adiciona um novo item de configuração.

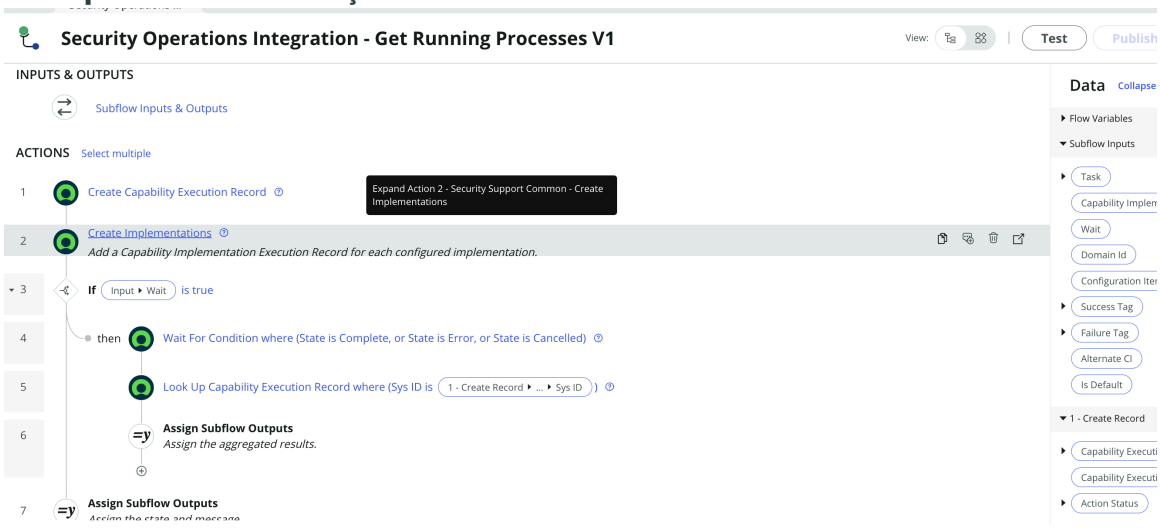
As ações do processo de fluxo incluem:

- Obter ação de fluxo de FQDN do item de configuração
- Atividade Determinar script do shell por SO
- Acompanhamento da execução - Iniciar ação de fluxo
- Obter processos em execução via PowerShell
- Atividade Executar script de shell
- Acompanhamento da execução da capacidade - Ação de fluxo de falha
- Atividade Extrair script do shell do script do MID
- Combinar resultados e retornam valores em uma matriz
- Ação de fluxo Criar registros de dados de aprimoramento
- Acompanhamento da execução da capacidade - Ação de fluxo concluída

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter processos em execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o. **Estado** . **Análise** , se necessário.
3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração de Resposta a incidentes de segurança fornece informações do processo em execução no **Link relacionado** > **Melhorias de incidentes de segurança**guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Atividade Combinar resultados

A atividade de fluxo de trabalho Combinar resultados mescla os resultados de integrações de terceiros para usar no fluxo de trabalho.

A atividade Combinar resultados pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID Server no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resultados combinados.
Falha	Combinação falhou. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
Entrada A.	Conjunto de resultados A.
Entrada B	Conjunto de resultados B
implementation_id	Identificador de implementação.
affected_ci	Item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	Conjunto de resultados A ou conjunto de resultados B com base no qual um é preenchido.

Atividade Executar script de shell

A atividade Executar fluxo de trabalho de script de shell executa um script de shell do MID Server no fluxo de trabalho.

A atividade Executar script de shell pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID Server no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Script de shell encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
target	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
ScriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Atividade Extrair script do shell do script do MID

A atividade Extrair script de shell do fluxo de trabalho de script DO MID extrai um script de shell DO MID Server para usar com no fluxo de trabalho.

A atividade Extrair script de shell do script do MID pode ser usada com qualquer fluxo de trabalho para extrair um script de shell do MID Server para incluir no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Script de shell encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sysId	Identificador do sistema

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ScriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Atividade Obter processos em execução via PowerShell

A atividade Obter fluxo de trabalho de ID do sensor reúne processos em execução usando o PowerShell para usar no fluxo de trabalho.

A atividade Obter processos em execução via fluxo de trabalho do PowerShell pode ser usada com qualquer fluxo de trabalho para recuperar processos a serem incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Processos encontrados
Falha	Nenhum processo encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
target	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
Processando Script	Script ECC executado em um sistema baseado no Windows.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

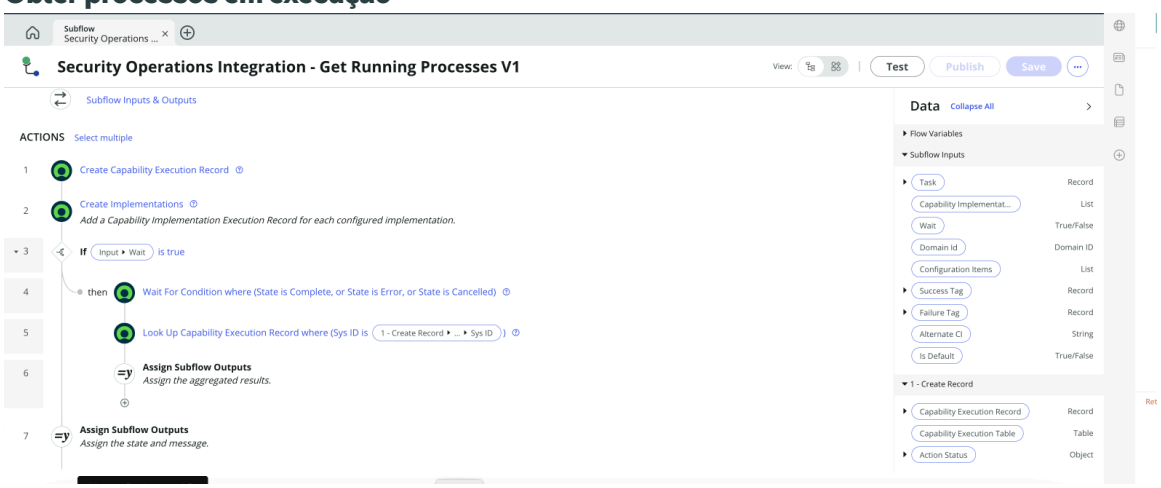
Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Operações de segurança - Obter fluxo de processos em execução

O fluxo Operações de segurança - Obter processos em execução é um fluxo de alto nível independente de integrações. Recupera uma lista de processos em execução em um item de configuração (IC) de um host. Use-o para executar uma integração, como Carbon Black, ou para um incidente de segurança baseado no Windows.

Função necessária: sn_si.analyst

Obter processos em execução



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de operações de segurança- Isolar capacidade do host

. **Isolar host** a capacidade restringe as conexões do sistema a outros dispositivos. Isolar host é executado em relação a um item de configuração (IC).

. **Isolar host** a capacidade tem um fluxo, Operações de segurança - Isolar o fluxo do host Que aceita um ou mais ICs e, opcionalmente, uma implementação. Você pode especificar uma implementação a ser usada para isolar o host ou para que o fluxo tente isolar o host usando todas as implementações.

Nota: Embora não esteja integrado a um recurso, um fluxo, Operações de segurança Carbon Black Integration - Remover fluxo de isolamento de host está disponível para orquestração para restaurar a comunicação com um host isolado.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Execute Isolar host

Isolar host restringe as conexões do sistema a outros dispositivos.

Antes de Iniciar

Função necessária: sn_si.analyst

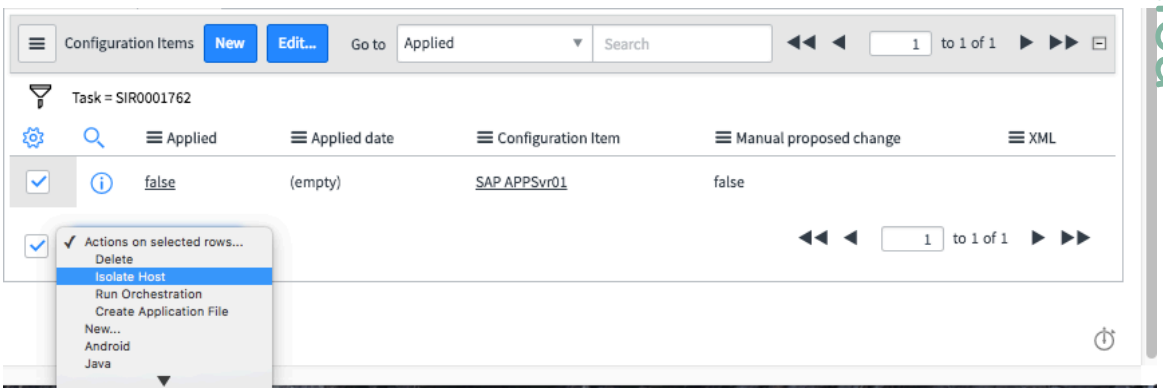
Por Que e Quando Desempenhar Esta Tarefa

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

. **Integração de operações de segurança - Isolar host ou endpoint** o fluxo pode ser acionado a partir da lista relacionada em um incidente de segurança.

Procedimento

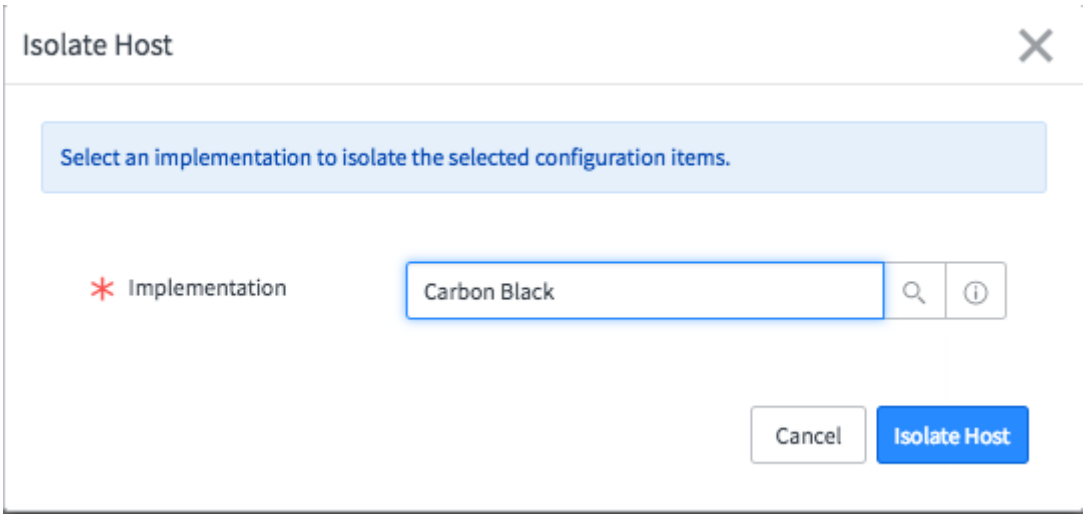
1. Navegue até um incidente de segurança.
2. Selecione **Itens de configuração** em **Lista relacionada** guia.
3. Clique em **Isolar host** em **Ações nas linhas selecionadas...** menu suspenso.



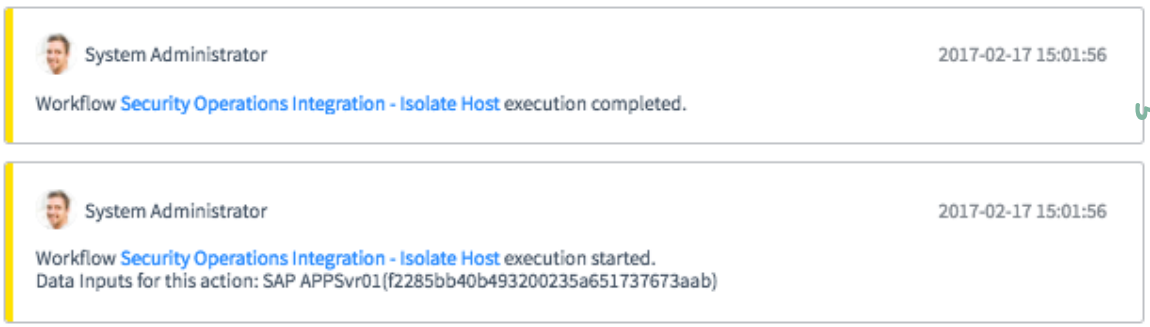
A caixa de diálogo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Escolha a implementação.
5. Clique em **Isolar host** .
   A auditoria de execução de fluxo é exibida na seção Anotações de trabalho.



Operações de segurança - Isolar o fluxo do host

. **Operações de segurança - Isolar host** o fluxo é um fluxo de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de itens de configuração. Use-o para realizar uma integração, como Carbon Black.

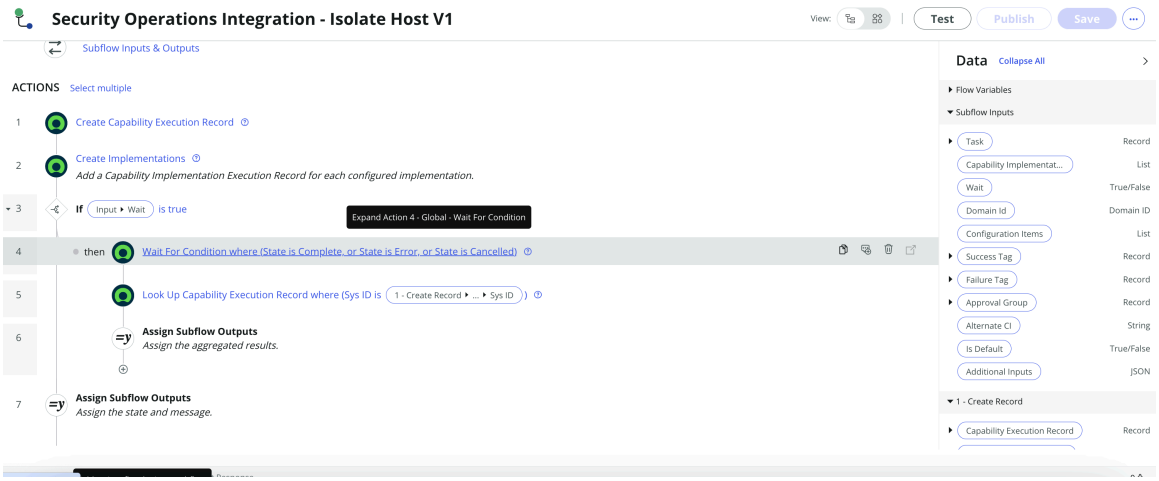
Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo é acionado a partir do **Itens de configuração** em uma lista relacionada a incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isolar Host



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração Carbon Black de operações de segurança - isolar fluxo de host

O Security Operations Carbon Black Integration - isolar host é a implementação da integração Carbon Black iniciada pelo fluxo Security Operations Integration - isolar host.

Antes de Iniciar

Função necessária: sn_si.analyst

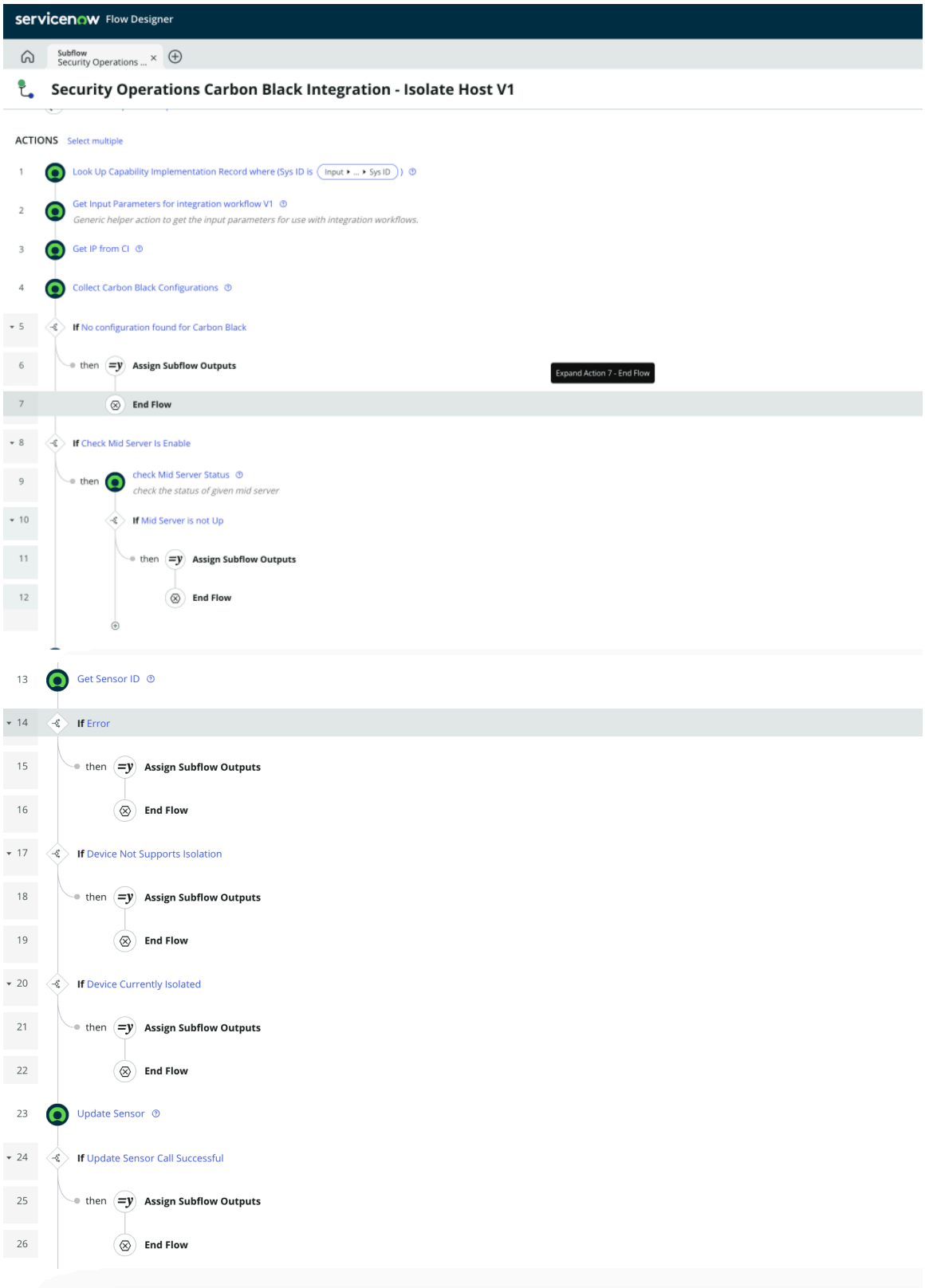
Por Que e Quando Desempenhar Esta Tarefa

As atividades do processo de fluxo incluem:

- Acompanhamento de execução - Início (ICs) Ação de fluxo
- Obter IP de IC
- Colete configurações Carbon Black
- Acompanhamento da execução da capacidade - Ação de fluxo de falha
- Obter Identificador de Sensor
- Atividade Definir isolamento de rede habilitado
- Atualizar sensor - Retorna o resultado do host isolado.
- Acompanhamento da execução da capacidade - Ação de fluxo concluída

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Obter ação de fluxo de ID do sensor

A ação Obter fluxo de ID do sensor coleta identificadores do sensor para usar no fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação Obter fluxo de ID do sensor pode ser usada com qualquer fluxo para coletar informações do sensor a serem usadas no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensor encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ic_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atividade Definir isolamento de rede habilitado

A atividade de fluxo de trabalho Definir isolamento de rede habilitado habilita o isolamento de rede.

A atividade Definir isolamento de rede habilitado pode ser usada com qualquer fluxo de trabalho para habilitar o isolamento de rede.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Isolamento de rede habilitado.
Falha	O isolamento de rede não pode ser habilitado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.
desativar	Determina se o host está isolado ou remove o isolamento do host. Desabilitar isolamento Falso: O isolamento permanece habilitado

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atividade Atualizar sensor

A atividade Atualizar fluxo de trabalho do sensor atualiza o sensor para isolar hosts ou endpoints.

A atividade Atualizar sensor pode ser usada com qualquer fluxo de trabalho para isolar hosts ou endpoints.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sensor atualizado.
Falha	Não é possível atualizar o sensor. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID Server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Operações de segurança Carbon Black Integration - Remover fluxo de isolamento de host

. **Carbon Black Integration de operações de segurança - Remover isolamento de host** O fluxo desbloqueia a comunicação com um host ou endpoint especificado em um sistema Carbon Black.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

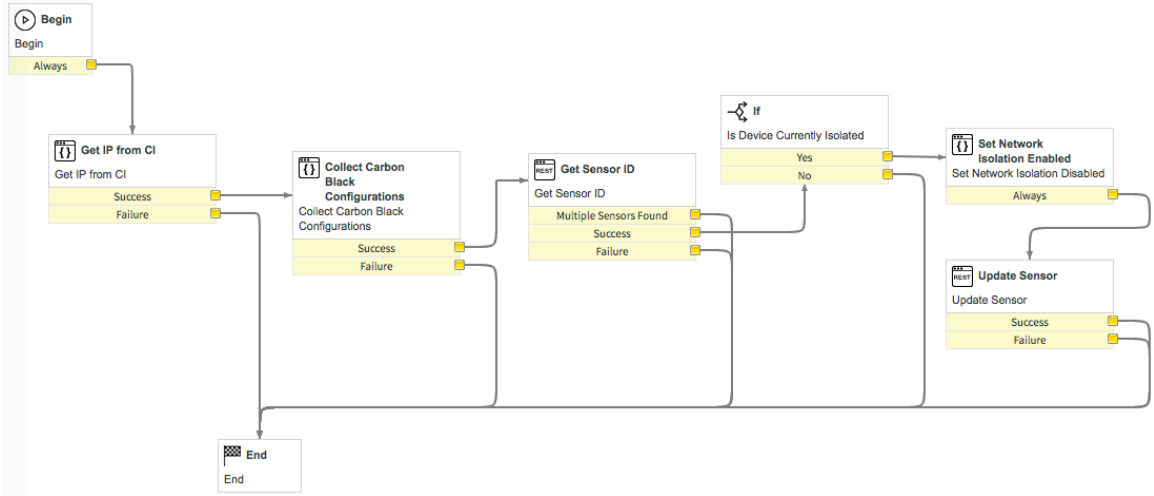
Este fluxo não faz parte de um recurso e precisa de uma orquestração personalizada para ser executado.
As atividades do processo de fluxo incluem:

- Atividade Obter IP do IC
- Se bem-sucedido- Coletar ação de fluxo de configurações Carbon Black
- Obter ação de fluxo de ID do sensorObter Identificador de Sensor
- Se- O dispositivo oferece suporte ao isolamento- e o dispositivo não está isolado para desabilitado.
- Atividade Atualizar sensor- Retorna o resultado do host isolado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Carbon Black Integration - Remover isolamento de host



Integração de operações de segurança- Publicar na lista de observação

. Publicar na Lista de observação o recurso adiciona observáveis e indicadores associados a um incidente de segurança a uma lista de observação de terceiros que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integração de operações de segurança - Publicar no fluxo da lista de observação

. **Integrações de operações de segurança - Publicar na lista de observação** o fluxo é um fluxo de alto nível independente de integrações. Ele adiciona observáveis à lista de observação de terceiros que oferecem suporte ao recurso. Use-o para realizar uma integração.

Antes de Iniciar

Função necessária: sn_si.analyst

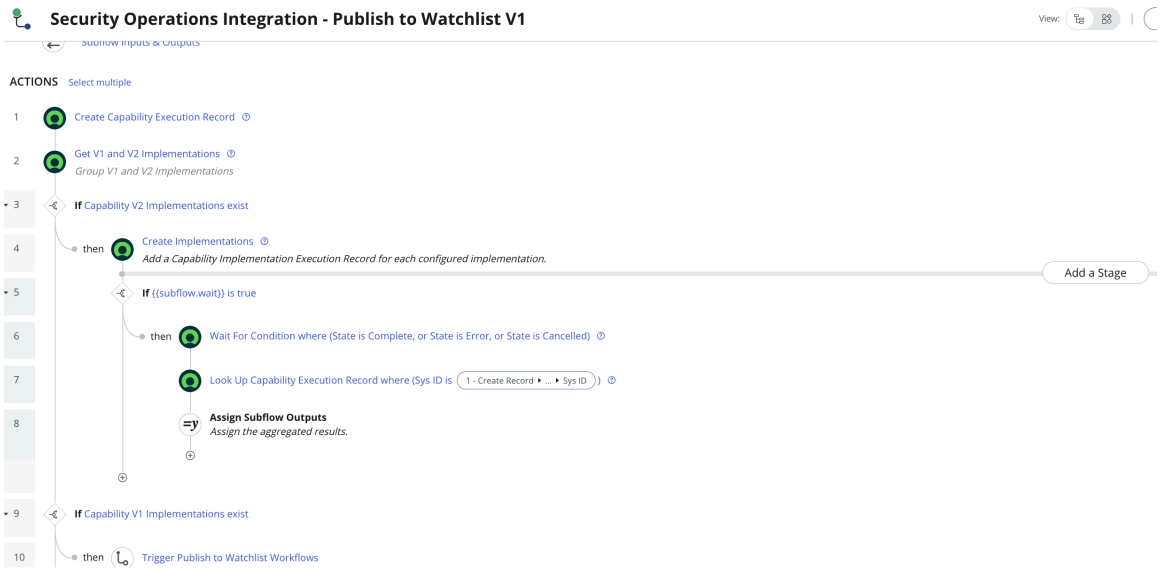
Por Que e Quando Desempenhar Esta Tarefa

Este fluxo fica visível e é executado somente quando uma integração está disponível. Ele é acionado a partir do **Observáveis** ou **Indicadores associados** em um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Publicar na lista de observadores



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração de operações de segurança - Capacidade de pesquisa de vistas

. **Pesquisa de vistas** A capacidade aceita um conjunto de observáveis, encontra todas as integrações compatíveis com uma Pesquisa de vistas e executa essas pesquisas.

O recurso de Pesquisa de vistas tem um fluxo de trabalho, Integração de operações de segurança - Fluxo de pesquisa de vistas, que executa a pesquisa de vistas. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas com base nas Configurações de pesquisa de vistas e executa as pesquisas com base no fluxo de trabalho configurado. Quando a pesquisa estiver concluída, uma anotação será adicionada às anotações de trabalho do incidente, incluindo se alguma vista foi encontrada e, em caso afirmativo, quantas.

Para exibir as Configurações de pesquisa de vistas, navegue até **Operações de segurança** > **Integrações** > **Configurações da Pesquisa de detecções**.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Criar registros de configuração de pesquisa de vistas

Crie vários registros de configuração de pesquisa de vistas e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar

Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a Integração Splunk.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode criar registros de configuração de pesquisa de vistas para invocar pesquisas salvas No armazenamento de logs do Splunk Enterprise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com CIM (Common Information Model, Modelo de informações comuns) do Splunk.

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinam vários registros de evento.
- Pesquisas eficientes e eficazes.
- Use entradas com parâmetros na pesquisa salva do Splunk.

O sistema de base inclui as configurações de amostra mostradas nesta imagem:

Configurações de pesquisa salvas

		Name	Observable type	Search	Is saved search
		Search	Search	Search	Search
☐	ⓘ	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
☐	ⓘ	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
☐	ⓘ	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração no local são consultas de exemplo e podem ser substituídas por parâmetros apropriados para seu ambiente. Crie configurações de pesquisa salvas adicionais conforme necessário. Quando você define uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à configuração salva definida em sua instância do Splunk. Se o nome e os parâmetros não forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de vistas.

Nota: Em sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique em **Permissões** Link para navegar até a página Permissões. Selecione **Todos os aplicativos** botão de opção e habilite **Permissão de leitura** opção para **Todos** . Isso mudará o valor da coluna Compartilhamento de Privado para App para sua consulta de pesquisa salva. Se isso não estiver definido, a consulta de pesquisa salva poderá não retornar resultados.

Para verificar se a configuração de pesquisa salva corresponde à configuração definida em sua instância do Splunk:

1. Navegar até **Configurações** > **Pesquisas, Relatórios e Alertas**.
2. Mudança **Contexto da aplicação** . **Todos** .

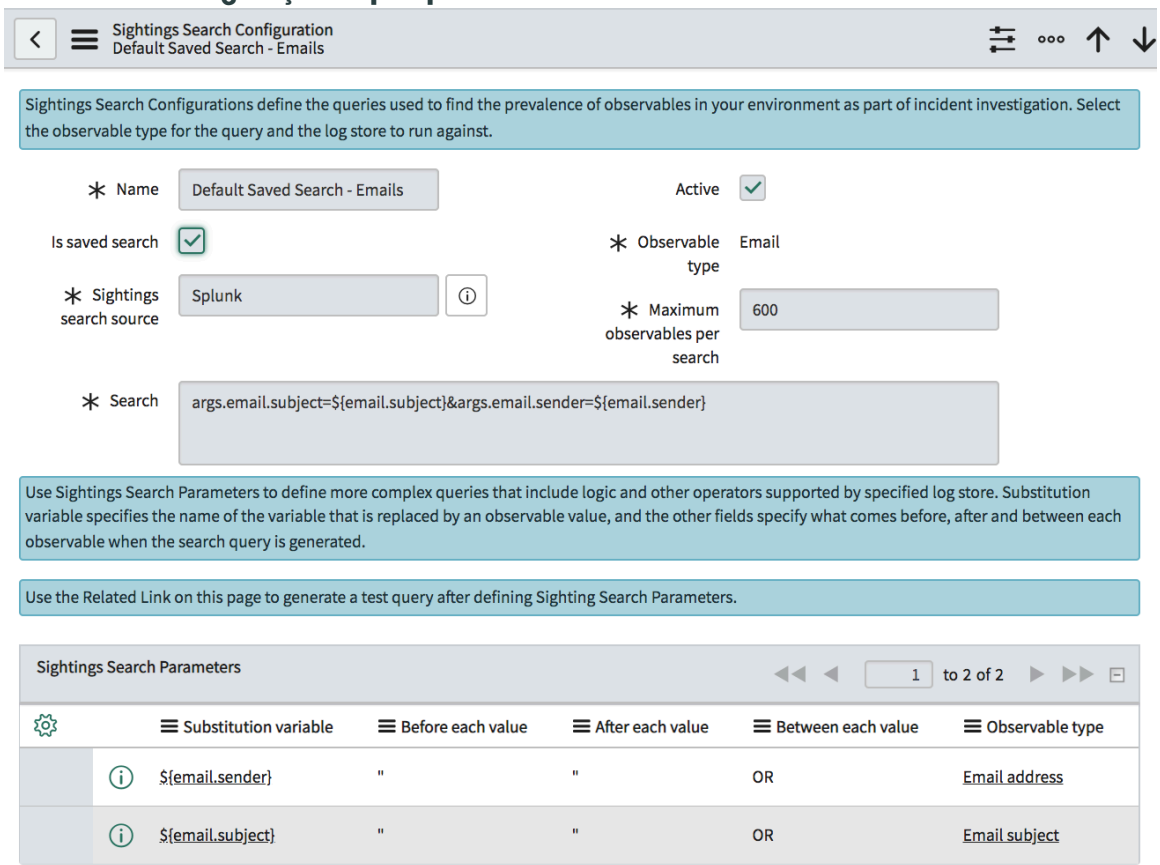
   Uma lista de relatórios de pesquisa é exibida.
3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de vistas contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração de pesquisa de vistas



Em sua instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - E-mails e os mesmos parâmetros de pesquisa para o endereço de e-mail e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem os mesmos, a pesquisa de vistas não gerará um resultado preciso.

Procedimento

1. Navegar até **Operações de segurança** > **Integrações** > **Configuração da Pesquisa de detecções** e criar um novo registro (consulte a tabela para obter descrições dos campos).

Formulário Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome da configuração.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de vistas. Selecione o armazenamento de logs do Splunk como a origem.
Ativo	Opção para o status da pesquisa salva. Somente configurações de pesquisa ativas podem ser usadas para executar uma pesquisa de vistas.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisar	A cadeia de caracteres de pesquisa padrão é `(observável)` , Mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com o armazenamento de logs do Splunk.

2. Clique em **Enviar**.

Resultado
Você criou um registro de configuração de pesquisa de vistas.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de vistas** e especificam uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Execute uma Pesquisa de vistas

Determine a prevalência de uma ameaça ao longo do tempo ou teste os esforços de correção ou erradicação. Você pode selecionar observáveis individuais ou vários observáveis e o intervalo de datas para sua pesquisa a partir de um incidente de segurança. Os resultados são incluídos em **Observáveis de incidentes de segurança** lista relacionada.

Antes de Iniciar
Função necessária: sn_si.analyst

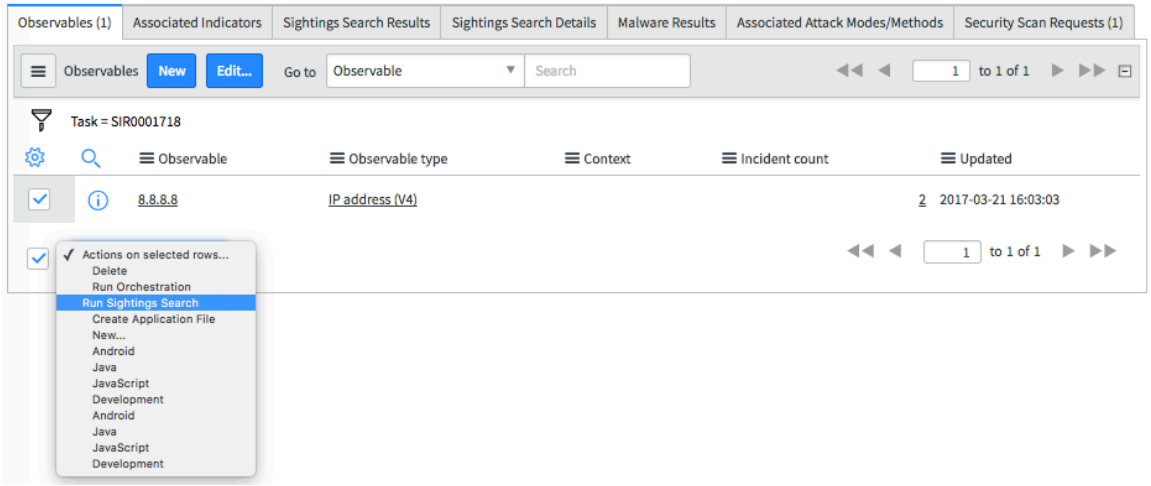
Por Que e Quando Desempenhar Esta Tarefa
O recurso de Pesquisa de vistas tem um fluxo, Integração de operações de segurança - Fluxo de pesquisa de vistas, que executa a pesquisa de vistas. Este fluxo aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas com base nas Configurações de pesquisa de vistas e executa as pesquisas com base no fluxo configurado.

Nota: Uma implementação ativa deve ser configurada. A Pesquisa de avistamentos oferece suporte ao Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger e aprimoramento de incidentes QRadar. Se nenhuma implementação estiver disponível, ações de capacidade, como **Executar Pesquisa de vistas** não são exibidos nos menus do produto.

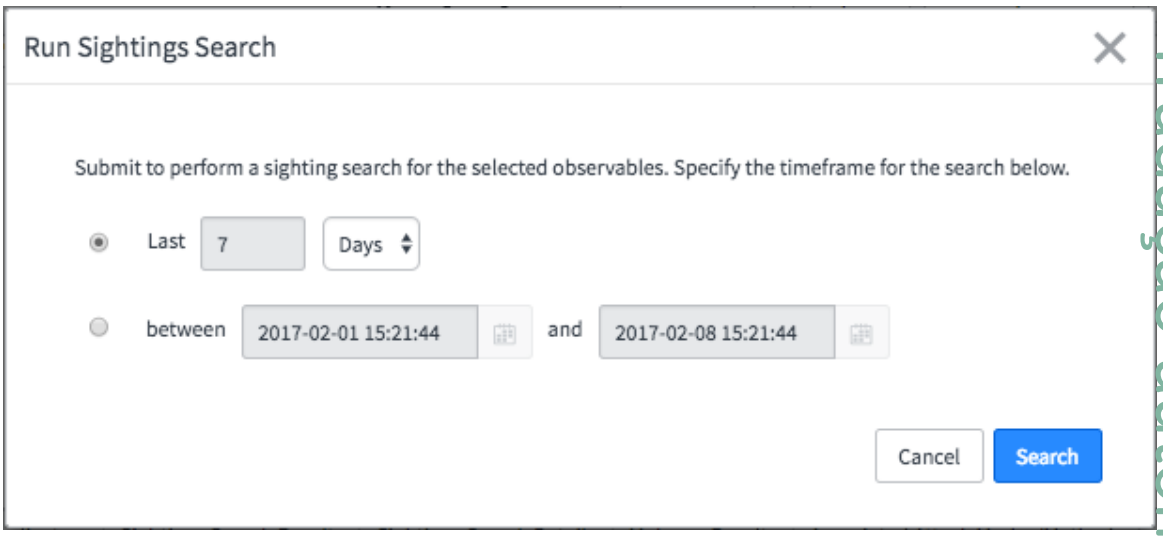
Procedimento
1. Navegue até um incidente de segurança.
2. Clique em **Mostrar IOC** link relacionado.
3. Selecione **Observáveis** Na guia Lista relacionada.
4. Selecione os observáveis nos quais você deseja executar uma pesquisa de vistas.
5. Clique em **Executar Pesquisa de vistas** em **Ações nas linhas selecionadas...** menu suspenso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo Executar pesquisa de vistas é aberta.



Nota: Os valores inseridos na caixa de diálogo substituem os valores de configuração de capacidade para esta execução.

6. Escolha o número de dias ou um intervalo de datas para pesquisar dados.

Opção	Descrição
Último	O número de horas ou dias antes da criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas para pesquisar. As datas padrão são: A data e a hora em que o incidente foi aberto. A data e a hora sete dias antes da abertura do incidente.

Nota: **Último** é o número de horas ou dias antes da criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Pesquisar**.
   Um registro de Pesquisa de vistas é criado. Os dados agregados e de vistas associados são exibidos no incidente de segurança em **Resultados da pesquisa de vistas** e. **Detalhes da pesquisa de vistas** guias.

   Nota: Os dados dos resultados da pesquisa de vistas podem ser compartilhados com Círculo de segurança confiável, com exceção de dados brutos no caso de implementações configuradas para incluir dados brutos.

Resultados da pesquisa de detecções

Resultado	Descrição
Número	O identificador da pesquisa de vistas.
Contagem de observáveis	Número de observáveis pesquisados por consulta.
Detecções internas	Contagem de vistas internas.
Vistas externas	Contagem de avistamentos externos. (Recebido do compartilhamento de ameaças.)
Itens de configuração correspondidos	Contagem de itens de configuração que corresponderam a um registro existente em seu cmdb para cada observável encontrado em seu ambiente.
Intervalo de datas de início	Hora de começar a procurar avistamentos.
Intervalo de datas de término	Hora de parar de procurar avistamentos.
Atualização em	Data e hora da última modificação.

Observação: Se a implementação usada para a pesquisa de vistas estiver configurada para incluir dados brutos e pelo menos uma vista for encontrada, um anexo contendo amostras de dados brutos aparecerá na parte superior do incidente de segurança.

Detalhes da Pesquisa de detecções

Detalhe	Descrição
Pesquisa de detecção	O identificador da pesquisa de vistas.
Observável	Observável pesquisado por consulta.
Tipo de observável	Tipo de observável pesquisado por consulta.
Detecções internas	Contagem agregada de vistas internas.
Vistas externas	Contagem agregada de vistas externas. (Recebido do compartilhamento de ameaças.)
Atualização em	Data e hora da última modificação.

Integração de operações de segurança - Fluxo de pesquisa de vistas

Integração de operações de segurança - Pesquisa de vistas o fluxo é um fluxo de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de observáveis com base nas integrações configuradas que oferecem suporte ao recurso. Use-o para executar uma integração como Splunk ou Elasticsearch.

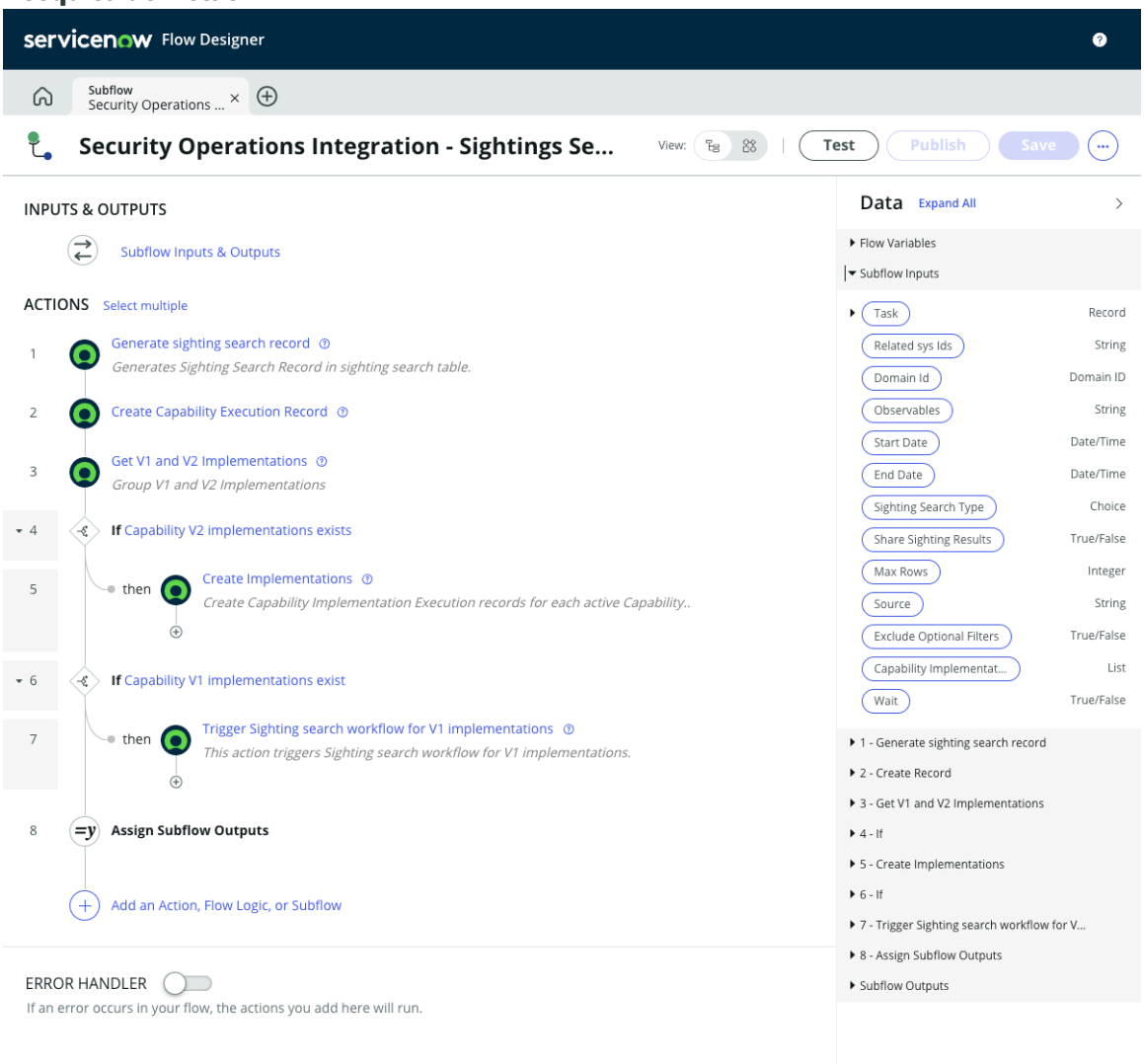
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Se um incidente de segurança tiver um observável anexado a ele, esse fluxo será acionado quando você clicar em **Executar Pesquisa de vistas** em **Ações nas linhas selecionadas...** menu suspenso em **Observáveis de incidentes de segurança** guia.

Pesquisa de vistas



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Atividade Pesquisa de vistas - Determinar observáveis

. **Pesquisa de vistas - Determine observáveis** a atividade fluxo de trabalho determina quais observáveis serão incluídos no fluxo de trabalho.

. **Pesquisa de vistas - Determine observáveis** a atividade pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador da tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.
workflow_current_sys_id	Identificador do sistema do registro atual. (Usado somente se `task_sys_id` entradas observáveis não estão disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Atividade Observáveis Persistentes

. **Observáveis persistentes** a atividade de fluxo de trabalho recupera observáveis da integração de terceiros.

. **Observáveis persistentes** a atividade pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
sightingsResponse	
taskId	Identificador da tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	

Atividade Obter consultas de vistas observáveis

. **Obter consultas de avistamentos observáveis** a atividade de fluxo de trabalho recupera consultas da configuração de integração.

. **Obter consultas de avistamentos observáveis** a atividade pode ser usada com qualquer fluxo de trabalho para obter consultas a serem enviadas para a implementação especificada usando **Inicializador de fluxo paralelo** .

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consultas encontradas.
Falha	Ocorreu um erro ao tentar obter consultas. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis filtrados.
Capacidades	Lista de capacidades compatíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

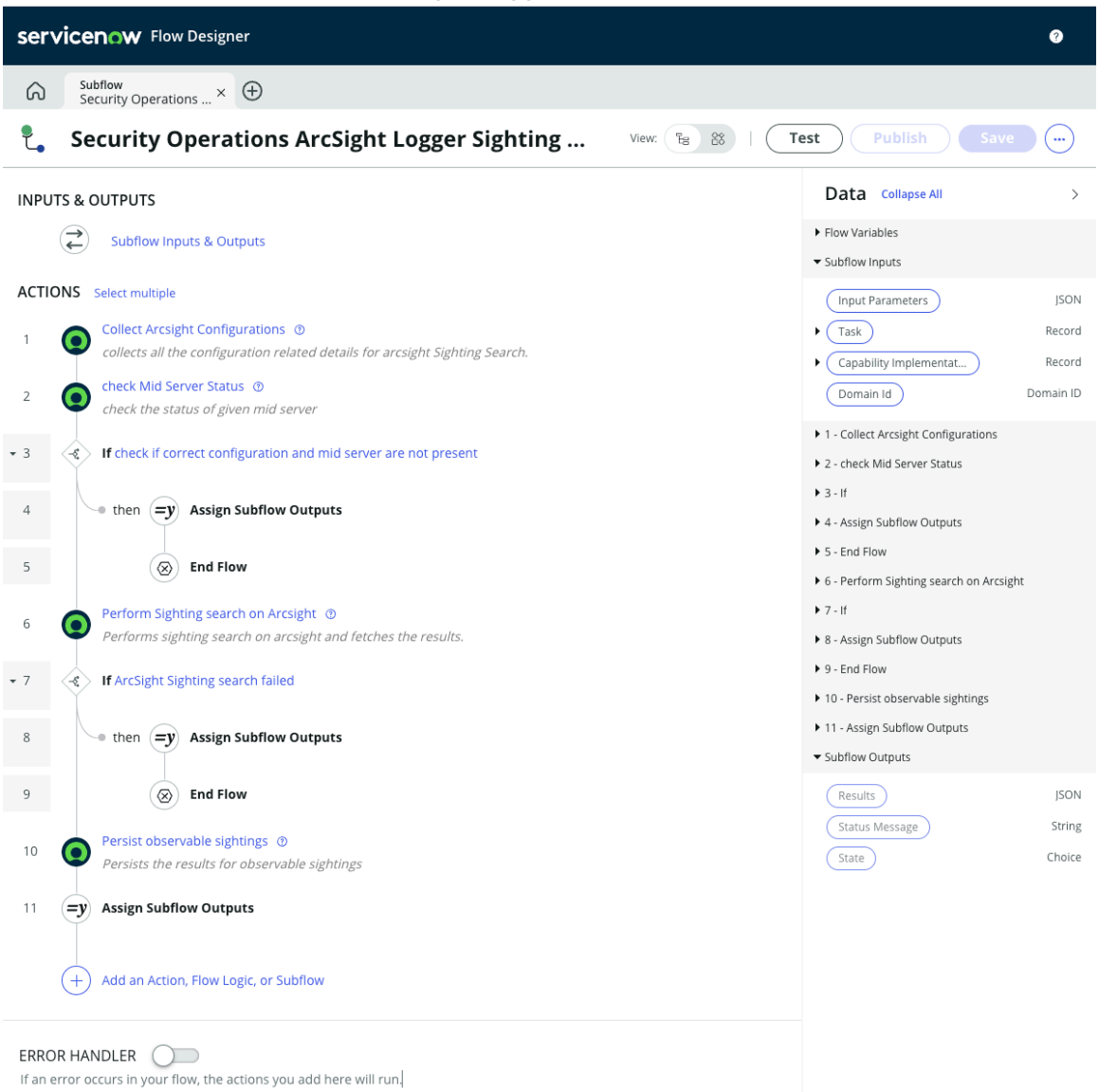
Variável	Descrição
consultas	Cadeia de caracteres de pesquisa.
QueryCount	Número de consultas a serem executadas.

Operações de segurança - Fluxo de pesquisa de vistas do Arcsight Logger

Operações de segurança - Pesquisa de avistamentos do ArcSight Logger Flow é a implementação da integração do Splunk iniciada pelo **Integração de operações de segurança - Fluxo de pesquisa de vistas** .

Função necessária: sn_si_analyst

Pesquisa de avistamentos do ArcSight Logger



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Tradução automática

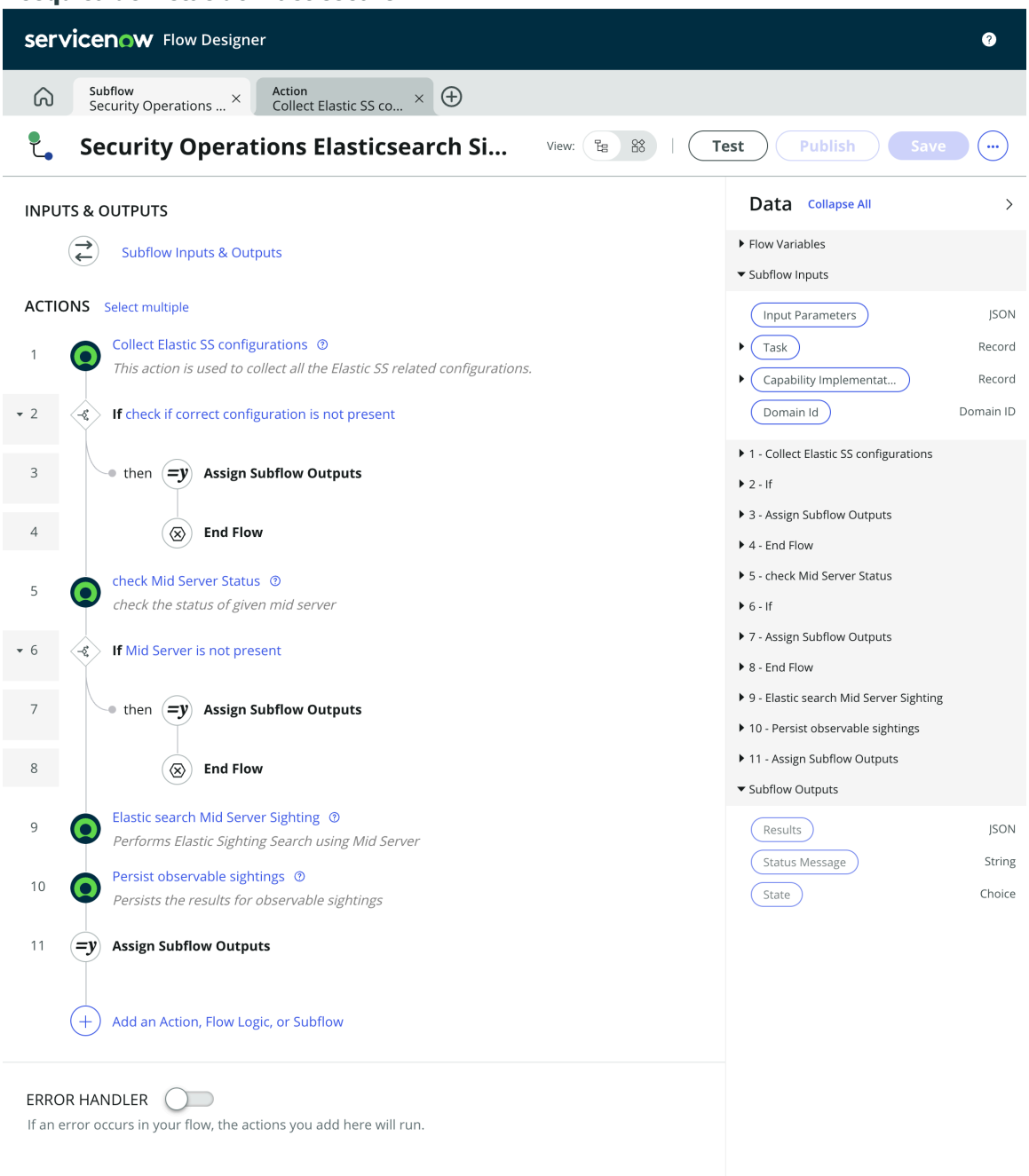
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança - Fluxo de pesquisa de vistas do Elasticsearch

Operações de segurança - Pesquisa de vistas do Elasticsearch Flow é a implementação do Elasticsearch iniciada pelo **Integração de operações de segurança - Pesquisa de vistas** fluxo.

Função necessária: sn_si.analyst

Pesquisa de vistas do Elasticsearch



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

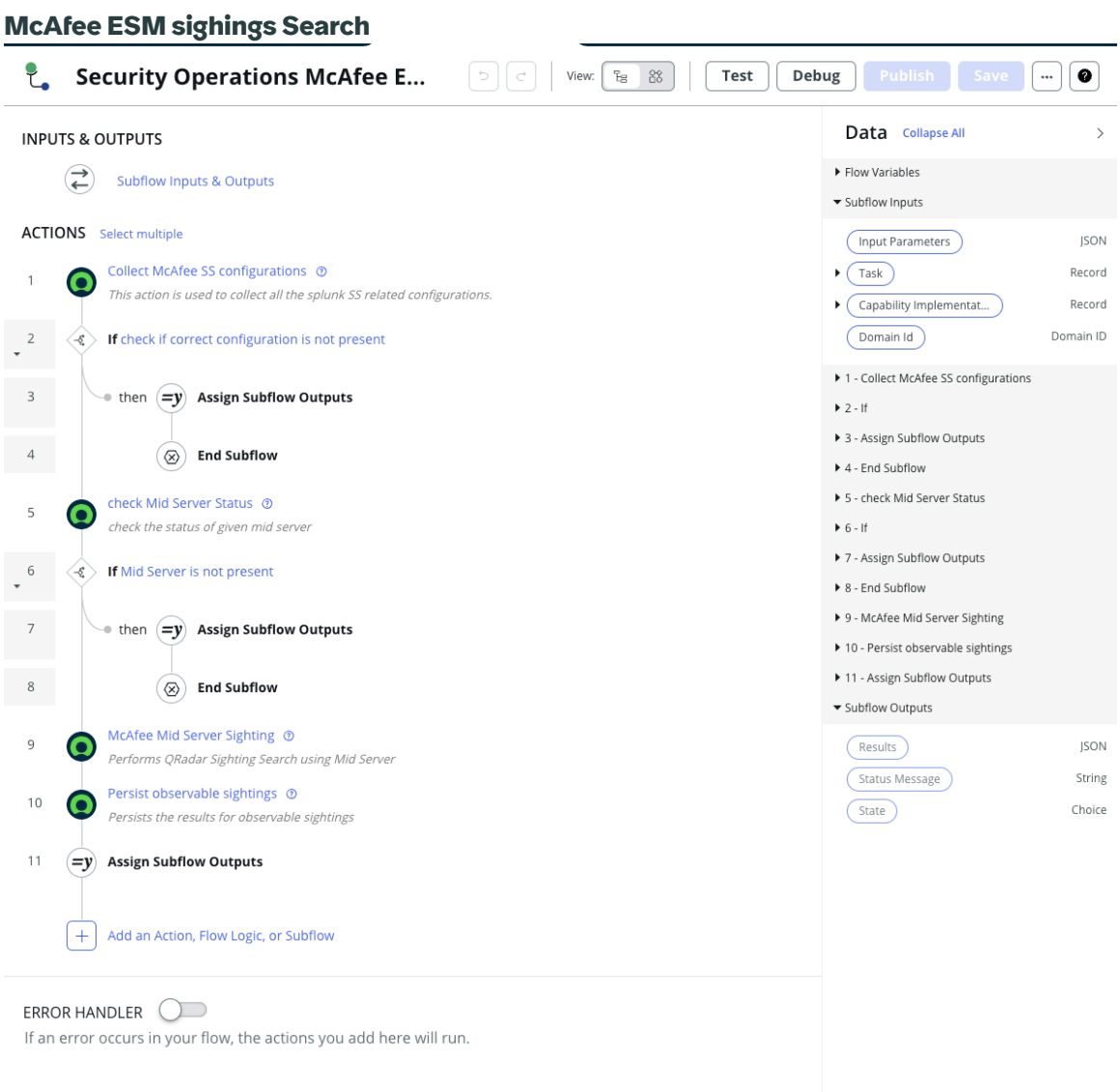
Operações de segurança - Fluxo de pesquisa de detecções do McAfee ESM

Operações de segurança - Pesquisa de avistamentos do McAfee ESM Flow é a implementação da implementação do McAfee Sighting Search iniciada pelo **Integração de operações de segurança - Fluxo de pesquisa de vistas** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si_analyst



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Operações de segurança - Fluxo de pesquisa de vistas do QRadar

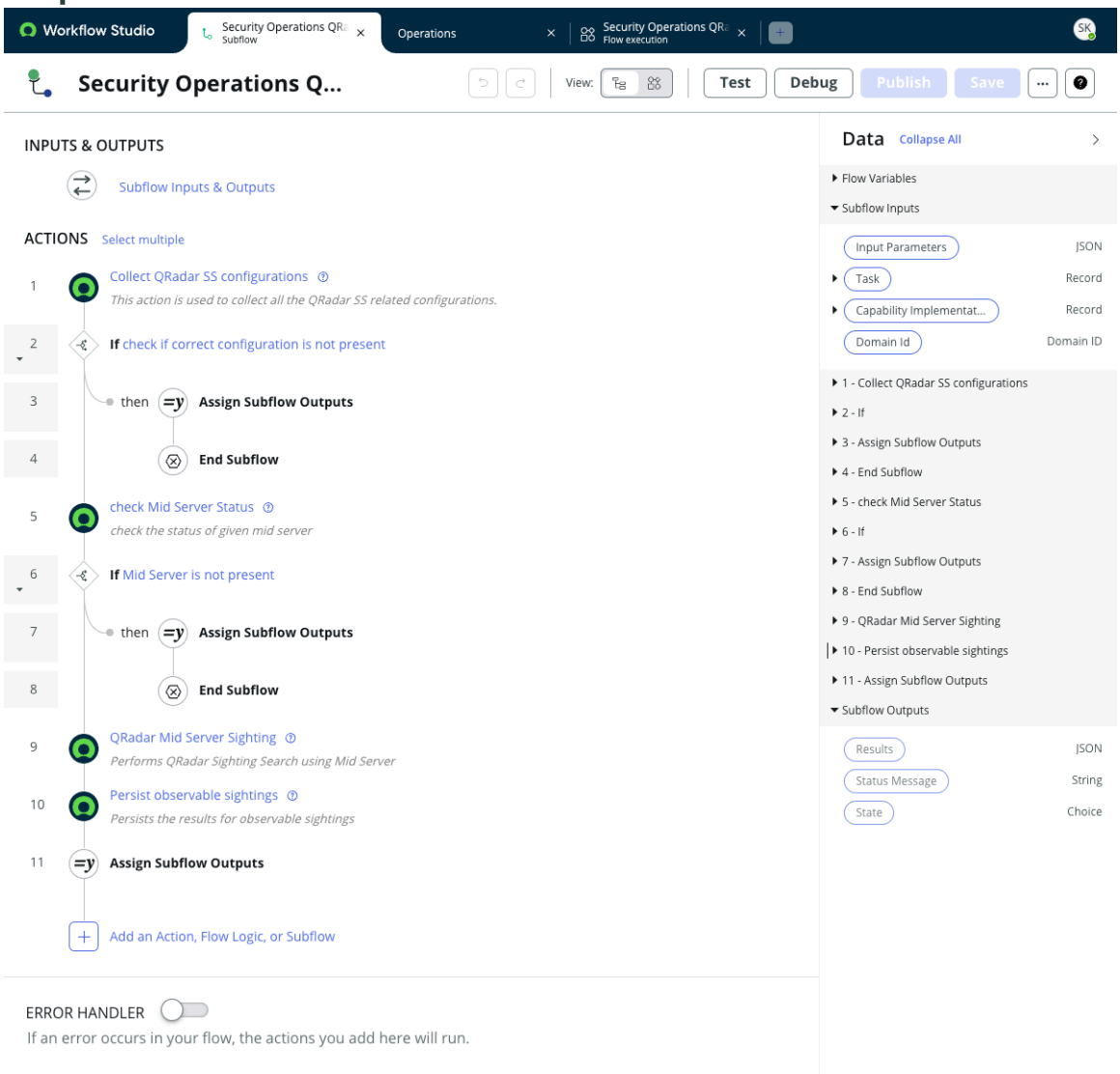
Operações de segurança - Pesquisa de avistamentos do QRadar Flow é a implementação da integração do IBM QRadar lançada pelo **Integração de operações de segurança - Fluxo de pesquisa de vistas** .

Função necessária: sn_si_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de avistamentos do QRadar



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Integração de operações de segurança - Fluxo de pesquisa de vistas do Splunk

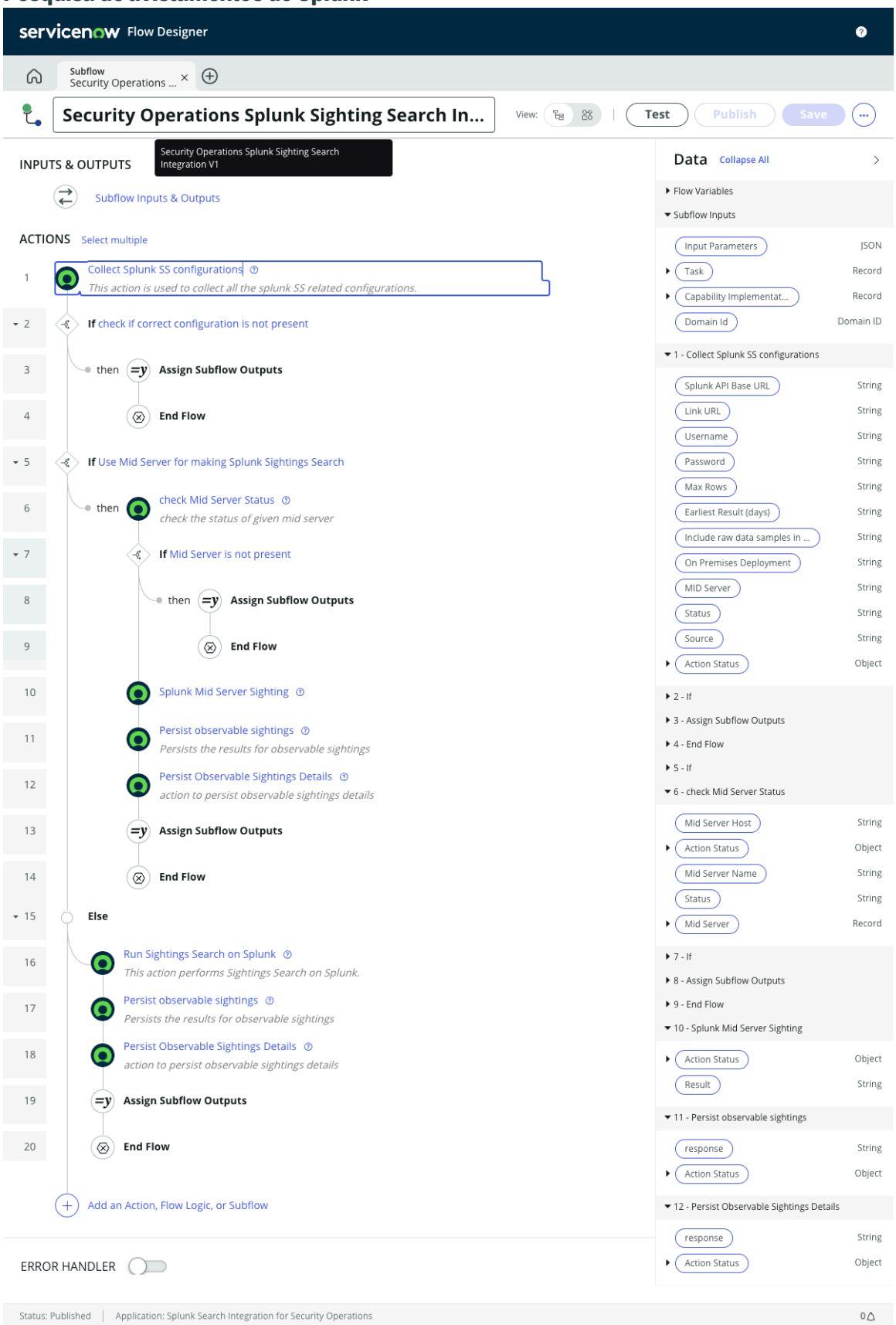
Operações de segurança - Pesquisa de avistamentos do Splunk Flow é a implementação da integração do Splunk iniciada pelo **Integração de operações de segurança - Fluxo de pesquisa de vistas** .

Função necessária: sn_si_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de avistamentos do Splunk



As atividades específicas deste fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir resultados da pesquisa de vistas

Você pode revisar os resultados da Pesquisa de vistas para indicadores mal-intencionados internos e externos.

Antes de Iniciar

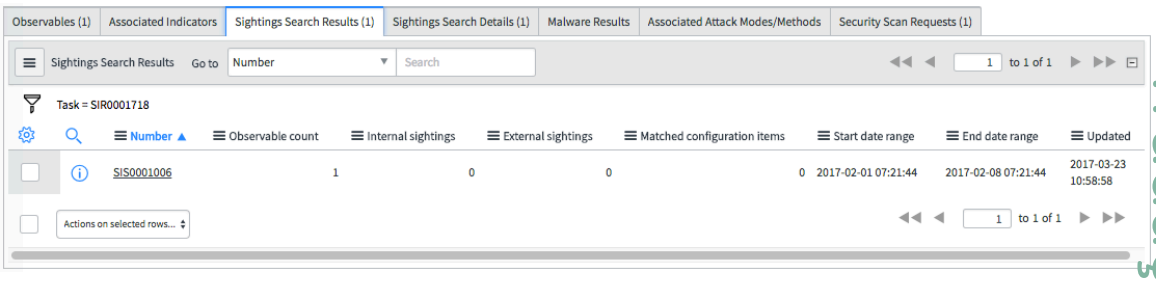
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Resultados da pesquisa de vistas** guia de **Mostrar IOC** Grupo Lista relacionada para exibir a lista de pesquisas de vistas.



Nota: Esses dados podem ser compartilhados com Círculo de segurança confiável.

Resultados da pesquisa de detecções

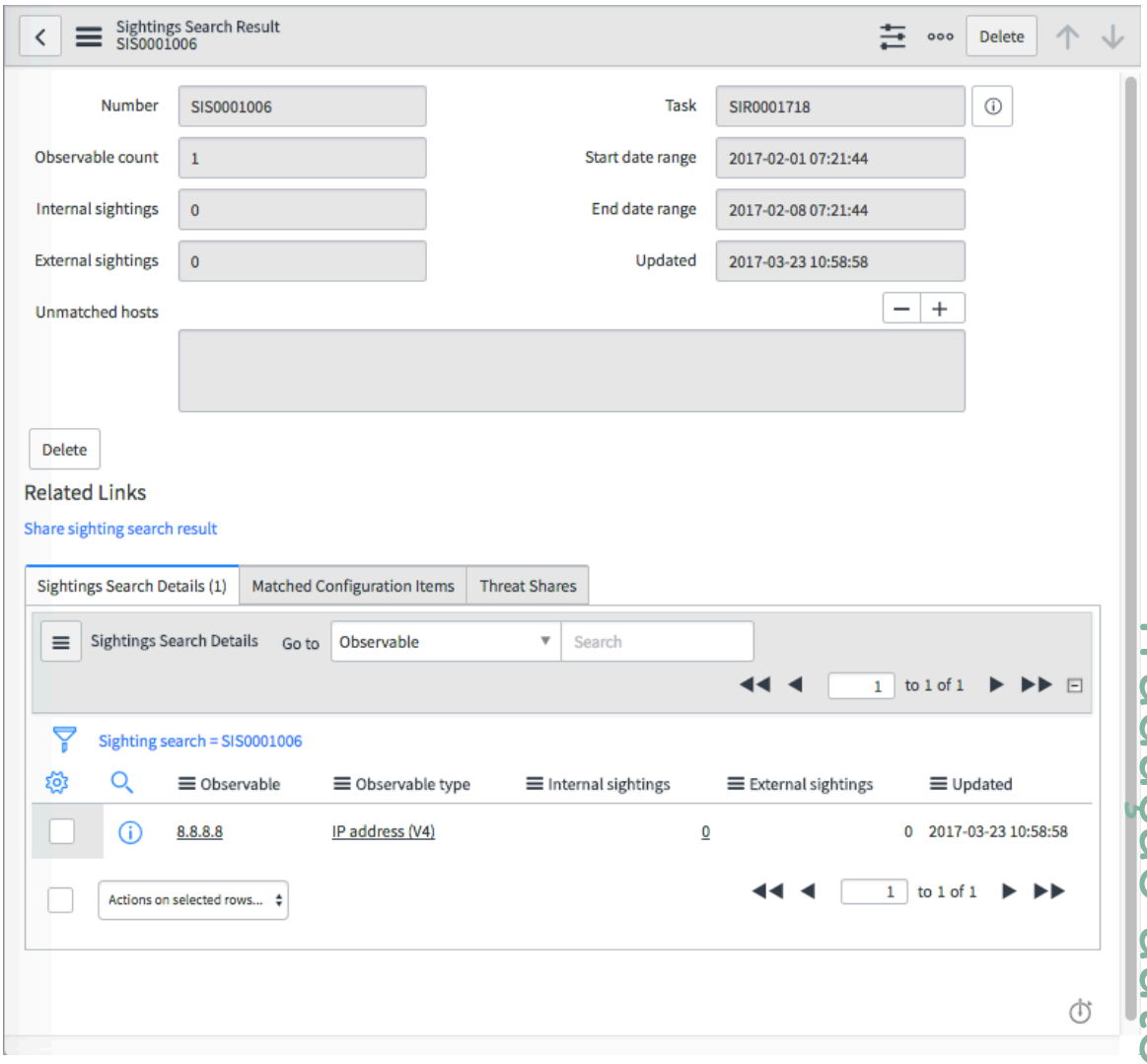
Resultado	Descrição
Número	Identificador de pesquisa de vistas.
Contagem de observáveis	Número de observáveis pesquisados.
Vistas Internas	Contagem agregada de vistas internas.
Vistas Externas	Contagem agregada de vistas externas. (Recebido do compartilhamento de ameaças.)
Itens de configuração correspondidos	Contagem agregada de itens de configuração que corresponderam a um registro existente em seu `cmdb` .
Intervalo de datas de início	Hora de começar a procurar avistamentos.
Intervalo de datas de término	Hora de parar de procurar avistamentos.
Atualização em	Data e hora da última modificação.

Para exibir os detalhes de uma única pesquisa:

3. Clique em uma Pesquisa de vistas no **Resultados da pesquisa de vistas** lista.
O formulário Resultado da pesquisa de vistas é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Formulário Resultados da pesquisa de vistas

Detalhe	Descrição
Número	Identificador de pesquisa de vistas internas.
Contagem de observáveis	Contagem de observáveis pesquisados por esta consulta.
Detecções internas	Contagem de vistas internas para esta pesquisa.
Vistas externas	Contagem de vistas externas para esta pesquisa. (Recebido de Círculo de segurança confiável.)
Hosts incompatíveis	Lista de possíveis itens de configuração para esta pesquisa que não foram correspondidos a nenhum registro em seu `cmdb` .
Tarefa	Identificador da tarefa de incidente de segurança.
Intervalo de datas de início	Hora em que a pesquisa de vistas foi iniciada.
Intervalo de datas de término	Hora em que a pesquisa de vistas parou.
Atualização em	Data e hora da última modificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhe	Descrição
Detalhes de Pesquisa de detecções	Número de vistas e data de modificação.
Itens de configuração correspondidos	Contagem de itens de configuração que corresponderam a um registro existente em seu `cmdb` . Lista o IC e a vista.
Compartilhamentos de ameaças	Lista de ameaças compartilhadas com Círculo de segurança confiável.

Compartilhar resultados da pesquisa de vistas

Você pode compartilhar detalhes ou resultados de vistas locais que estão associados a uma pesquisa específica com seu Círculo de segurança confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O compartilhamento pode ser automatizado usando a seguinte Resposta de incidente de segurança **Propriedades** .

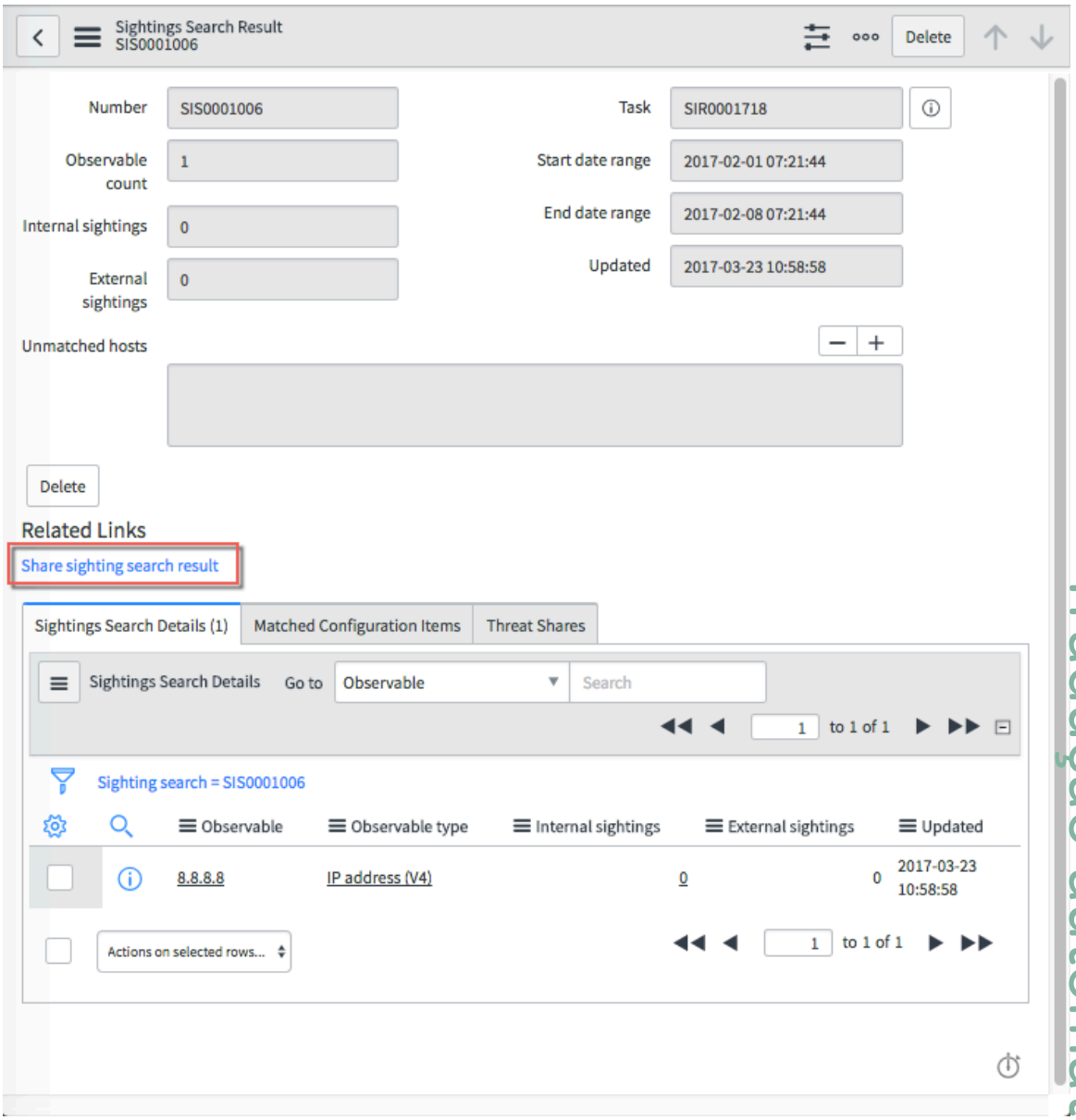
- Compartilhe automaticamente os resultados de uma pesquisa de vistas com o círculo confiável da ServiceNow padrão
- Incluir observáveis sem vistas locais ao compartilhar automaticamente os resultados da pesquisa de vistas
- Responda com vistas locais sempre que um compartilhamento de ameaça for recebido de um círculo confiável

Procedimento

1. Navegue até um incidente de segurança.
2. Clique em **Mostrar IOC** lista relacionada e selecione **Resultados da pesquisa de vistas** para exibir a lista de pesquisas de vistas.
3. Clique em um resultado de pesquisa de vistas.

Tradução automática

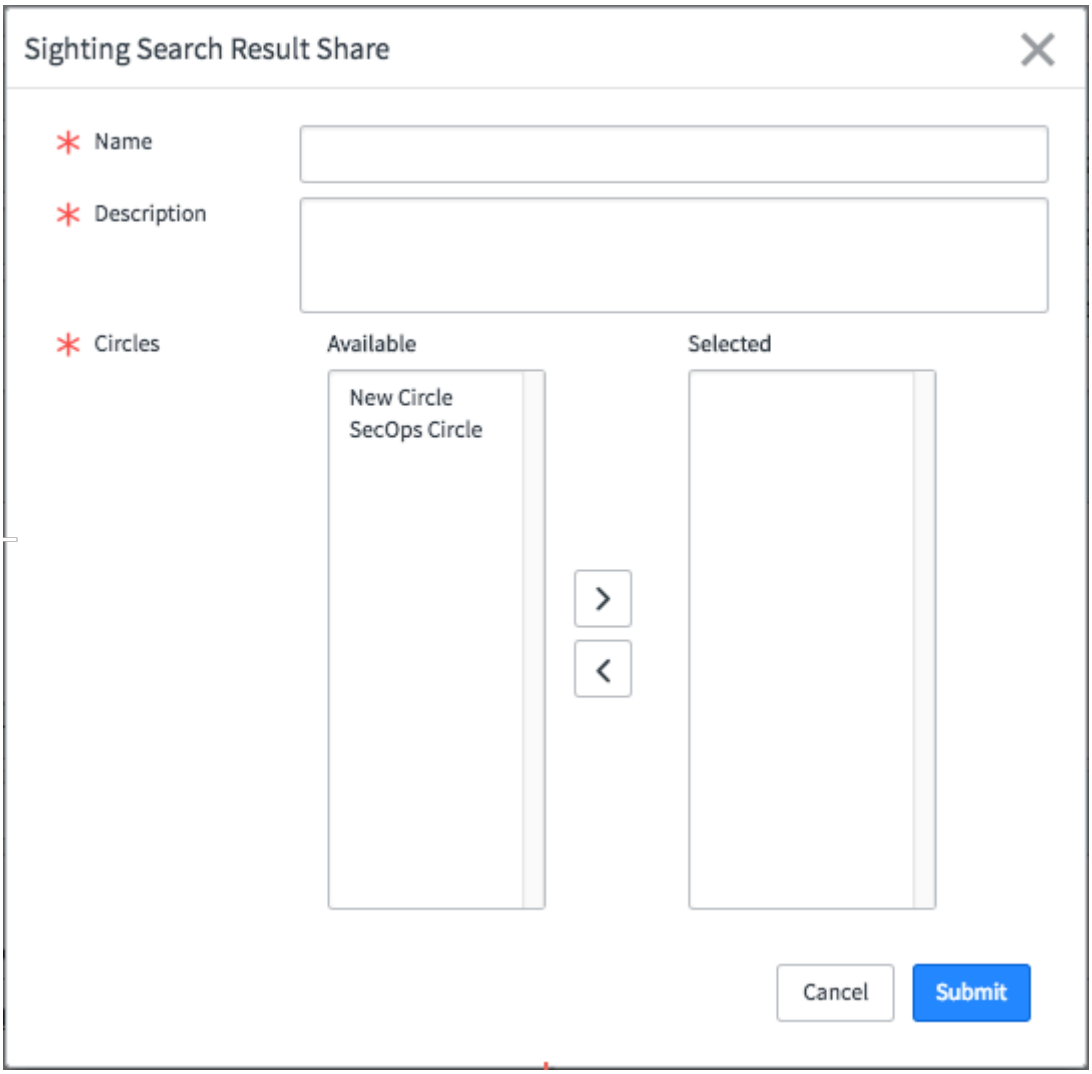
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Em **Resultado da pesquisa de vistas** , clique em **Compartilhar resultado da pesquisa de vistas** link relacionado.
   A caixa de diálogo Compartilhamento do resultado da pesquisa de vistas é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Insira um **Nome** para este registro de compartilhamento observável.
6. Insira um **Descrição** dos observáveis a serem compartilhados.
7. Escolha **Círculos** para compartilhar os observáveis com.
8. Clique em **Enviar**.
   Os observáveis são compartilhados com o Círculo confiável especificado.

Compartilhar observáveis de um incidente de segurança

Observáveis podem ser compartilhados a partir de um incidente de segurança em Resposta a incidentes de segurança para membros em seu círculo confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

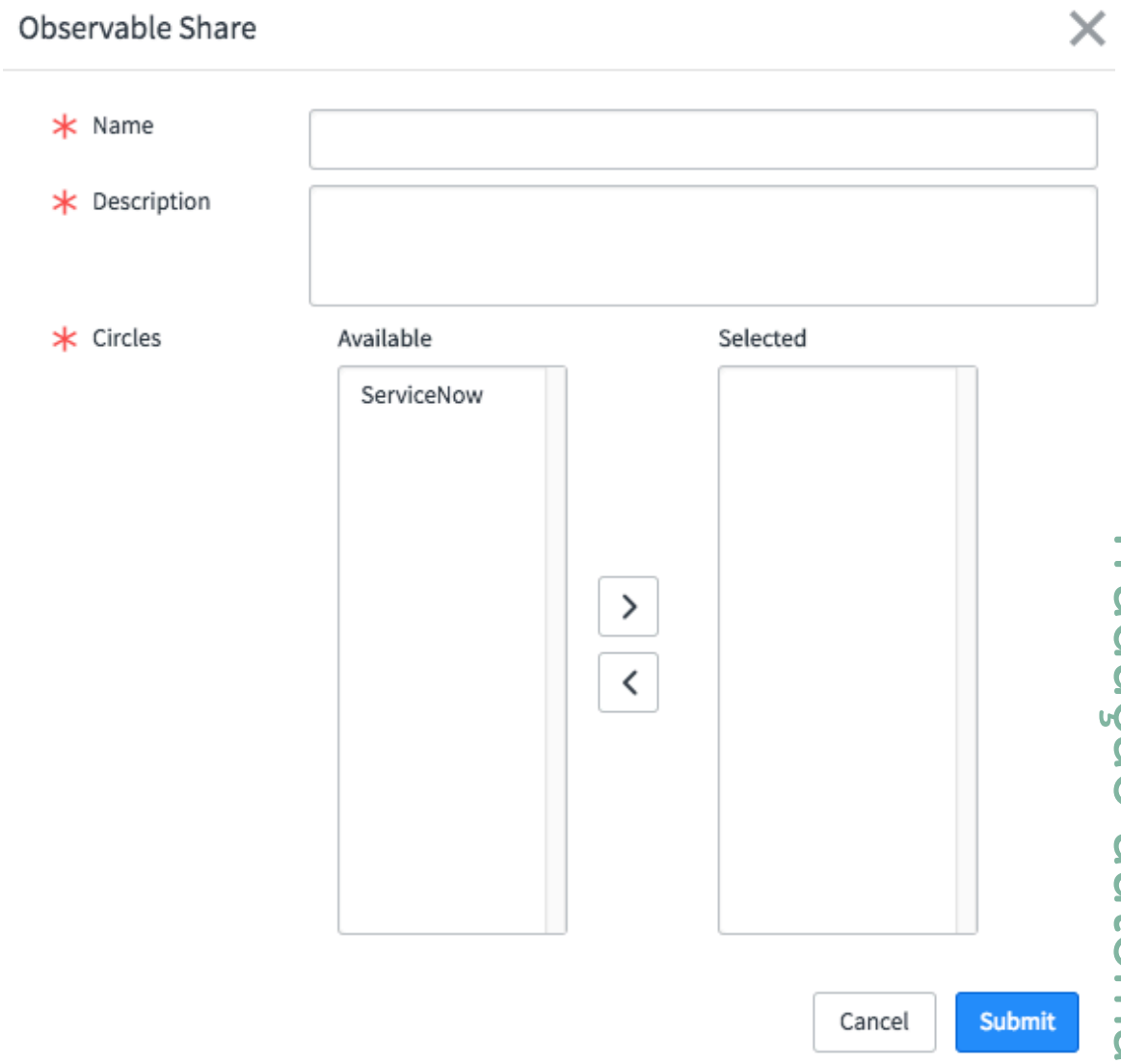
Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** guia de **Mostrar IOC** Grupo de lista relacionada.
3. Clique em um observável.
4. Em **Observável** formulário clique em **Compartilhar observável** link relacionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A caixa de diálogo Compartilhamento do Observável é exibida.



5. Insira um **Nome** para este registro de compartilhamento de ameaça.
6. Insira um **Descrição** dos observáveis selecionados.
7. Escolha **Círculos** para compartilhar os observáveis com.
8. Clique em **Enviar**.
   Os observáveis são compartilhados com o Círculo confiável especificado.
9. Você pode exibir os registros de compartilhamento de ameaças clicando em **Compartilhamentos de ameaças** guia.
10. Se algum dos observáveis compartilhados contiver vistas, as vistas também serão compartilhadas e poderão ser exibidas clicando em **Vistas** guia.

Exibir detalhes da pesquisa de vistas

Revise os detalhes agregados de todas as pesquisas de vistas.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Detalhes da pesquisa de vistas** guia de **Mostrar IOC** Grupo Lista relacionada para exibir a lista de pesquisas de vistas.

Nota: Esses dados podem ser compartilhados com Círculo de segurança confiável.

Detalhes de Pesquisa de detecções

Detalhe	Descrição
Observável	Lista de todos os observáveis pesquisados por consulta.
Tipo de observável	
Detecções internas	Contagem de vistas internas para todas as pesquisas.
Vistas externas	Contagem de vistas externas para todas as pesquisas. (Recebido do compartilhamento de ameaças.)
Pesquisa de detecção	Identificador de pesquisa de vistas.
Atualização em	Data e hora da última modificação.

Exibir dados de pesquisa de vistas

Revise os dados agregados de todas as pesquisas de vistas.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Dados de pesquisa de vistas** guia de **Mostrar todas as listas relacionadas** Grupo Lista relacionada para exibir a lista de pesquisas de vistas.

Nota: Esses dados podem ser compartilhados com Círculo de segurança confiável.

Dados de pesquisa de vistas

Resultado	Descrição
Intervalo de datas de término	Hora de parar de procurar avistamentos.
Vistas Externas	Contagem agregada de vistas externas. (Recebido do compartilhamento de ameaças.)
Vistas Internas	Contagem agregada de vistas internas.
É local	Indica se as vistas vieram do ambiente atual ou compartilhado.
Observável	Lista de todos os observáveis pesquisados por consulta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado	Descrição
Contagem de detecções	Número de vistas pesquisadas.
Pesquisa de detecção	Identificador de pesquisa de vistas.
Detalhe da pesquisa de detecção	Detalhe agregado da pesquisa de vistas.
Link de pesquisa de detecção	Link que aponta para o portal de pesquisa de vistas. A consulta de pesquisa é aplicada automaticamente ao clicar no link de pesquisa de vistas.
Consulta de pesquisa de detecções	Consulta para identificar a instância. 172.10.0.171 é substituível e é substituído no observável selecionado. (pesquisa 172.10.0.171 | cabeça 10) **Nota:** A seleção de dias não será aplicável à pesquisa salva.

Integração de operações de segurança - Recurso de pesquisa de ameaças

. **Pesquisas de ameaças** a capacidade executa pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

. **Pesquisas de ameaças** a capacidade tem um fluxo de trabalho, Integração de operações de segurança - Fluxo de pesquisa de ameaças. Quando o fluxo de trabalho de capacidade é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar uma pesquisa nos observáveis selecionados ou executar a pesquisa usando todas as implementações.

Nota: Se nenhuma implementação estiver disponível, as ações de capacidade não serão exibidas nos menus do produto.

Integração de operações de segurança - Fluxo de pesquisa de ameaças

. **Integração de operações de segurança - Pesquisa de ameaças** o fluxo de capacidade acessa as implementações de pesquisa de ameaças disponíveis e executa os fluxos de implementação associados a cada para executar pesquisas de ameaças de observáveis selecionados.

Antes de Iniciar
Função necessária: sn_ti.write

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo pode ser acionado dessas maneiras.

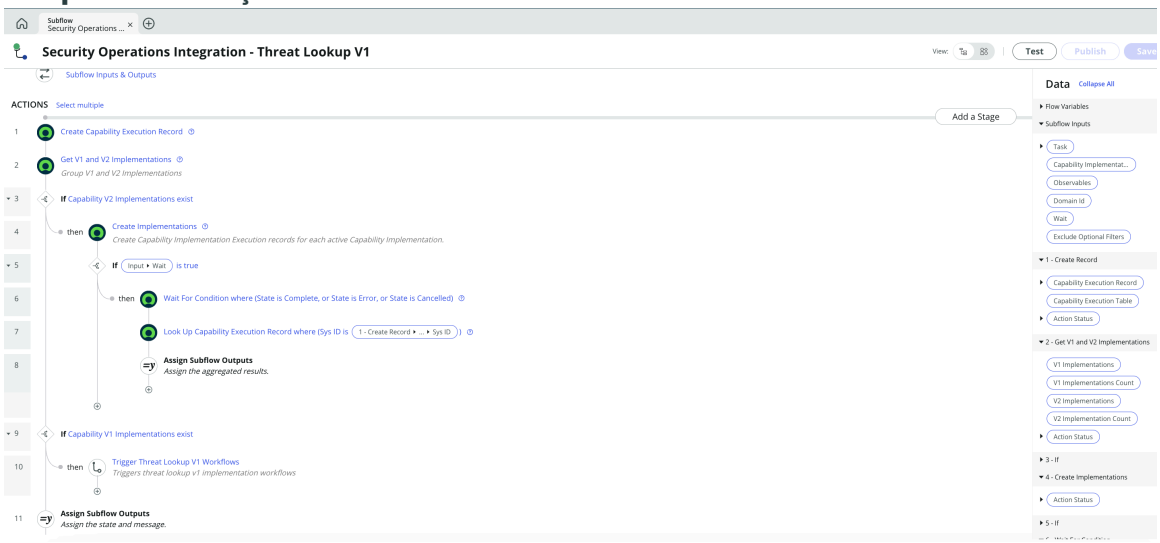
- Selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar pesquisa de ameaças** em **Ações nas linhas selecionadas** lista de seleção.
- abrindo um registro observável e clicando em **Executar pesquisa de ameaças** link relacionado.
- Na lista relacionada Observáveis em um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada método permite especificar quais implementações de pesquisa serão usadas para verificar os observáveis selecionados. Os fluxos de implementação associados são executados para executar as pesquisas.

Pesquisa de ameaças



Ações específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras ações, consulte Fluxos comuns de integração do Security Operations e atividades de orquestração.

As ações do processo de fluxo incluem:

- Ação Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - Nenhuma ação de impls

Mude a ordem de execução do fluxo

As implementações de capacidade de integração especificam o fluxo a ser executado. No sistema de base, os fluxos são executados sequencialmente, na ordem especificada na implementação. Você pode mudar a ordem conforme necessário.

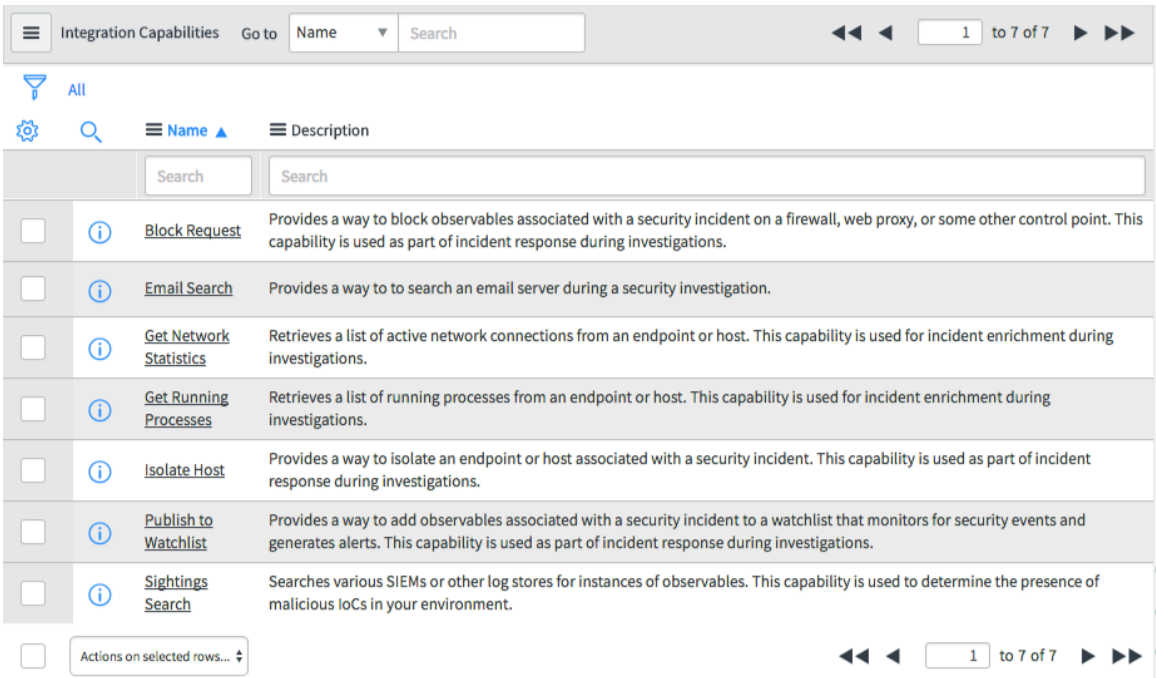
Antes de Iniciar
Função necessária: sn_sec_cmn.write

Tradução automática

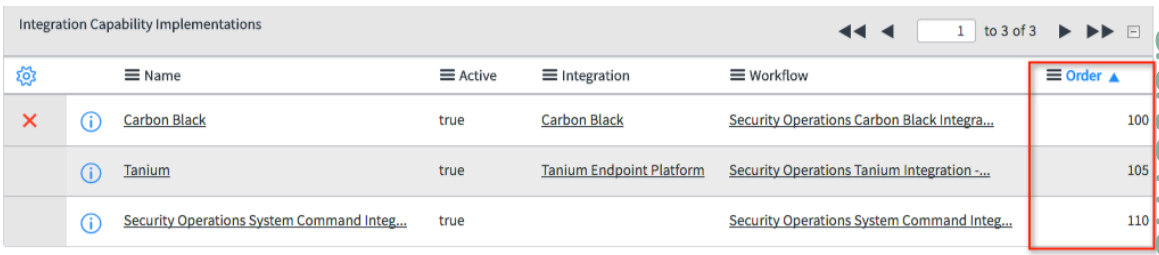
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

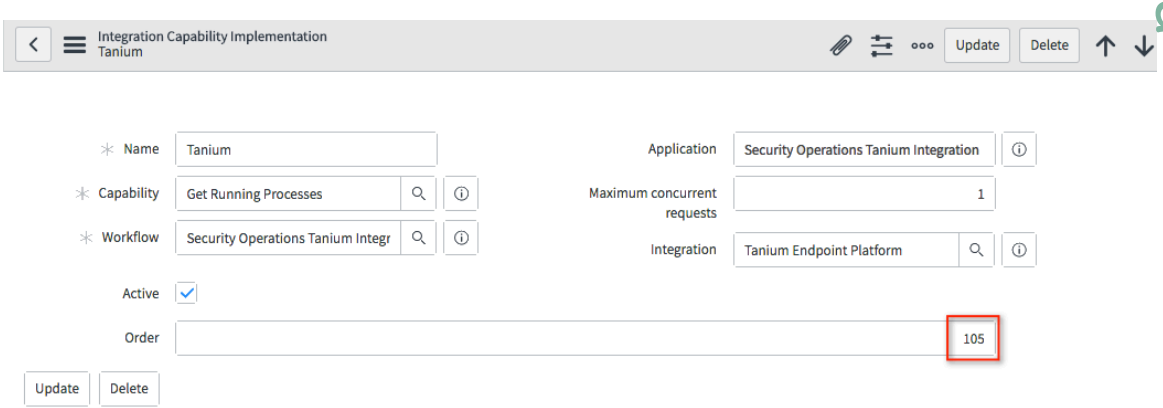
1. Navegar até **Tudo** > **Operações de segurança** > **Integrações** > **Capacidades de integração**.



2. Selecione a capacidade de integração para a qual você deseja alterar a ordem de execução.



3. Selecione a implementação que você deseja modificar.



4. Mude **Pedido** para um número maior ou menor.
Números mais baixos têm uma prioridade de execução mais alta.

5. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos comuns de integração do Security Operations e atividades de orquestração

Muitos dos fluxos associados a integrações de terceiros incluem as mesmas atividades. Por exemplo, atividades para iniciar e concluir o processamento.

Acompanhamento da execução - Iniciar ação de fluxo

A ação Acompanhamento de execução - Iniciar fluxo inicia o processo de auditoria de um Operações de segurança Fluxo de integração que opera em observáveis.

A ação Acompanhamento de execução - Iniciar fluxo pode ser usada com qualquer fluxo para começar a registrar o andamento do fluxo em uma auditoria.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
Impl	Sinalizador que especifica se a auditoria é feita para um fluxo de capacidade de integração ou um fluxo de implementação de capacidade de integração. Os valores possíveis são: • Falso - Indica auditoria em um fluxo de capacidade de integração abstrato, como Pesquisa de vistas. (padrão.) • Verdadeiro - Indica auditoria em um fluxo de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo.
ObservableList	Um ou mais SYIDs observáveis para executar a ação desejada. Usado como uma entrada de fluxo.
Id_do_contexto_do_fluxo	Identificador do sistema do registro de contexto de fluxo associado. Fornecido pelo sistema.
FlowName	Nome do fluxo. Fornecido pelo sistema.
ID de ExcutionCapabilityParentCapability	Identificador do sistema do registro de auditoria que iniciou o fluxo de implementação. Necessário somente para fluxos de implementação de capacidade de integração, como Splunk, Elasticsearch e VirusTotal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema do registro de auditoria.

- Ação Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - Nenhuma ação de impls

Acompanhamento da execução da capacidade - Ação de fluxo concluída

A ação de fluxo Acompanhamento de execução de capacidade - Concluir atualiza o registro de auditoria quando o fluxo é concluído.

A ação Acompanhamento de execução de capacidade - Concluir fluxo pode ser usada com qualquer fluxo para registrar a conclusão do fluxo.

Nota: . **Valor de retorno** matriz do **Inicializador paralelo** a ação de fluxo principal contém uma matriz de resultados de todos os fluxos de integração executados e solicita a conclusão bem-sucedida do acompanhamento da execução.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído** .

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades Iniciar auditoria.
FlowName	Nome do fluxo. Fornecido pelo sistema.
mensagem	Mensagem de conclusão.

Variáveis de saída

Não há variáveis de saída.

Acompanhamento da execução da capacidade - Ação de fluxo de falha

A ação Acompanhamento de execução de capacidade - Fluxo de falha registra uma falha no registro de auditoria.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação Acompanhamento de execução de capacidade - Fluxo de falha pode ser usada com qualquer fluxo para registrar uma condição de falha.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é definido como **Erro** e uma mensagem indicando que o erro foi registrado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema para o registro de auditoria. Esta é a saída de qualquer uma das atividades Iniciar auditoria.
errorMessage	Mensagem indicando o motivo da falha.
FlowName	Nome do fluxo. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Atividade Determine ICs

A atividade de fluxo de trabalho Capacidade - Determinar ICs determina quais itens de configuração (ICs) serão incluídos no fluxo de trabalho.

A atividade Capacidade - Determinar ICs pode ser usada com qualquer fluxo de trabalho para determinar quais ICs serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Itens de configuração encontrados.
Falha	Nenhum ICs encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia incidente de segurança para ICs).
ics_affected	Itens de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ics_affected	ICs filtrados
task_sys_id	Identificador de tarefa (mapeia incidente de segurança para ICs).

Ação de fluxo Criar registros de dados de aprimoramento

. **Criar registros de dados de aprimoramento** a ação de fluxo cria ou atualiza registros de aprimoramento para usar no fluxo.

. **Criar registros de Dados de aprimoramento** a ação de fluxo pode ser usada com qualquer fluxo para atualizar registros de aprimoramento no fluxo.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	Registro de aprimoramento atualizado.
Falha	Registro de aprimoramento não atualizado. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variável	Descrição
task_id	Identificador da tarefa.
conteúdo	Conteúdo bruto (dados de processos em execução).
enrichment_mapping_id	Identificador de mapeamento de aprimoramento.
ci_id	Identificador do item de configuração.
reference_value	Não utilizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resultado	GlideRecords criados usando o script enriquecimentUtils.

Obter ação de fluxo de FQDN do item de configuração

O **Orquestração comum de segurança** > **Obter FQDN do item de configuração** A ação de fluxo recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta ação de fluxo pode acelerar o processo de investigação e correção.

A ação de fluxo Obter FQDN do item de configuração pode ser usada com qualquer fluxo para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação de fluxo.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do item de configuração.

Observações adicionais

O campo fqdn no item de configuração deve ser preenchido.

Atividade Determine observáveis

. **Determinar observáveis** a atividade fluxo de trabalho determina qual observável incluir no fluxo de trabalho

. **Determinar observáveis** a atividade pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador da tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Ação Obter capacidades de segurança compatíveis

A ação de fluxo Obter recursos compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à capacidade solicitada.

A ação Obter capacidades compatíveis pode ser usada com qualquer fluxo para determinar quais capacidades são compatíveis.

Resultados

Os resultados possíveis para esta ação são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte à capacidade encontrada.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa compatível com o recurso. Mais informações de erro estão disponíveis no erro de saída da ação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
capabilityName	Nome da capacidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
Compatíveis	Lista de integrações compatíveis com o recurso .
CapabilityCount	Número de integrações compatíveis com o recurso.

Acompanhamento de execução de capacidade - Nenhuma ação de impls

A ação de fluxo Rastreamento de execução de capacidade - Nenhum impls cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A ação Rastreamento de execução de capacidade - Nenhum impls pode ser usada com qualquer fluxo de capacidade de integração abstrato para lidar com a condição de erro quando nenhuma implementação de capacidade configurada está disponível.

Resultados

Os resultados possíveis para esta ação são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando que o erro foi registrado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
ExecutitionId de capacidade	Identificador do sistema para o registro de auditoria. Saída da ação usada para iniciar o acompanhamento da execução.
FlowName	Nome do fluxo. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Criar ação de pesquisa de conformidade

A ação Criar pesquisa de conformidade cria uma pesquisa de conformidade para e-mails nos servidores Exchange designados usando as consultas de pesquisa definidas e retorna o nome da pesquisa de conformidade criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
search_query	Consulta de pesquisa obrigatória usada para encontrar e-mails no Exchange Server em todas as caixas de correio.
Trocar local	Campo de local obrigatório usado para pesquisar no local definido. Os valores são: • Tudo • Nome da caixa de correio específica
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Nome da pesquisa de conformidade criada.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Criação da pesquisa falhou	Quando a criação da pesquisa falha devido a uma exceção no Exchange Server.
Pesquisa criada com sucesso	Quando a criação da pesquisa é bem-sucedida.
Criação de pesquisa com falha devido a um erro de análise	Quando a criação da pesquisa falha devido a um problema de análise.
Erro	Quando ocorre uma exceção na ação de fluxo.

Atividade Obter IP do IC

Esta atividade de fluxo de trabalho determina o endereço IPV4 associado a um item de configuração (IC).

. **Obter IP do IC** A atividade pode ser usada com qualquer fluxo de trabalho para recuperar o endereço IPv4 de um IC.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
ic_sys_id [cadeia de caracteres]	Identificador do sistema do item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr [cadeia de caracteres]	Endereço IPv4. Se o endereço IP não puder ser determinado, este valor estará vazio.

Condições de Saída

Os resultados possíveis para esta atividade são:

Condições

Condição	Descrição
Êxito	Um endereço IPv4 foi retornado.
Falha	Não foi possível determinar um endereço IPv4.

Obter estatísticas de rede por meio da ação de fluxo netstat

A ação de fluxo Orquestração comum de segurança - Obter estatísticas de rede via netstat recupera as estatísticas de rede de um recurso afetado em um sistema baseado no Windows. Esta ação de fluxo pode acelerar o processo de investigação e correção.

A ação Obter estatísticas de rede via fluxo netstat pode ser usada com qualquer fluxo para recuperar estatísticas de rede de um sistema baseado no Windows. A máquina é consultada com **netstat** comando, incluindo **-a** e. **-o** parâmetros. Para aprimorar os dados de saída, **get-process** o comando também é invocado.

Resultados

Os resultados possíveis para esta ação de fluxo são:

Resultados

Resultado	Descrição
Êxito	As estatísticas de rede foram recuperadas no formato JSON.
Falha	Ocorreu um erro ao tentar recuperar estatísticas de rede. Mais informações de erro estão disponíveis no erro de saída da ação de fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução atuais na máquina de destino. Os dados JSON incluem: **PID** Identificador do processo **_port local** Porta local para a transação de rede **estado** Status da conexão TCP. **Nota:** Este campo é nulo para conexões UDP. **local_address** Nome de domínio totalmente qualificado (FQDN) local ou endereço IP **remote_address** Nome de domínio totalmente qualificado remoto (FQDN) ou endereço IP **protocolo** TCP ou UDP **remote_port** Porta remota da transação de rede **caminho** O caminho do arquivo do executável do processo **hash** O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Restrições

O MID Server deve oferecer suporte a PowerShell .

O hash SHA-256 requer o PowerShell V4.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter processos em execução por meio da atividade WMI

. **Obter processos em execução** A atividade de fluxo de trabalho recupera os processos em execução de um item de configuração em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

. **Obter processos em execução via WMI** A atividade pode ser usada com qualquer fluxo de trabalho para recuperar processos em execução em um sistema baseado no Windows.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução atuais no sistema de destino. Os dados JSON incluem: **PID** O identificador do processo **nome** O nome do processo Além disso, se disponível: **Responsável** O nome do responsável pelo processo **owner_sid** O identificador do sistema do responsável pelo processo **owner_domain** O domínio do responsável pelo processo **caminho** O caminho do arquivo do executável do processo **hash** O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrições

O MID Server deve oferecer suporte a **PowerShell** .

O hash SHA-256 requer o PowerShell V4.

Ação Verificar status da pesquisa de conformidade

A ação Verificar status da pesquisa de conformidade verifica o status da pesquisa de conformidade criada no Exchange Server e, se o status for Concluído, retorna as informações sobre a pesquisa de e-mail encontradas para a pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da ação.

Variável	Descrição
targetId	Campo de identificador do host de destino obrigatório onde o Exchange Server está localizado.
SearchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em ações subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da pesquisa de conformidade e o número de e-mails encontrados no Exchange Server para a pesquisa de conformidade.

Condições de Saída

Possíveis condições de saída para esta ação são:

Condições de Saída

Variável	Descrição
Pesquisa em andamento	Quando o status da pesquisa de conformidade está Em andamento.
Pesquisa concluída - Nenhum e-mail de ameaça encontrado	Quando o status da pesquisa de conformidade é concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Pesquisa concluída - E-mails de ameaça encontrados	Quando o status da pesquisa de conformidade é concluído e os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na ação de fluxo.

Atividade Atualizar anotações de trabalho da tarefa

. **Orquestração comum de segurança - Atualizar anotações de trabalho da tarefa** a atividade de fluxo de trabalho atualiza o. **Atividade** seção (anotações de trabalho) de um registro de tarefa. Isso é útil para registrar informações em log.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. **Atualizar anotações de trabalho da tarefa** a atividade pode ser usada com qualquer fluxo de trabalho para atualizar as anotações de trabalho de qualquer registro de tarefa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
task_id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa.
conteúdo [cadeia de caracteres]	Os dados gravados nas anotações de trabalho de uma tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Acumular informações de pesquisa para a atividade de incidente de segurança

. **Acumular informações de pesquisa para o incidente de segurança** A atividade pode ser usada com qualquer fluxo de trabalho para coletar informações de uma pesquisa de ameaças e gerar um resumo do conteúdo, bem como o ID do incidente de segurança de origem nas anotações de trabalho da tarefa.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resumo do relatório de pesquisa acumulado para incidente de segurança.
Falha	A tarefa de origem e o relatório de resumo de pesquisa estão vazios.

Variáveis de entrada

Variável	Descrição
ScanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
SIId[cadeia de caracteres]	Identificador do incidente de segurança.
resposta [cadeia de caracteres]	Resumo dos resultados da pesquisa, incluindo: Valor de IOC, resultado, motivo da falha, referência de pesquisa e assim por diante.

Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa

. **Atualize o incidente de segurança com resultados da pesquisa** o fluxo de trabalho atualiza os incidentes de segurança existentes com resultados de pesquisa.

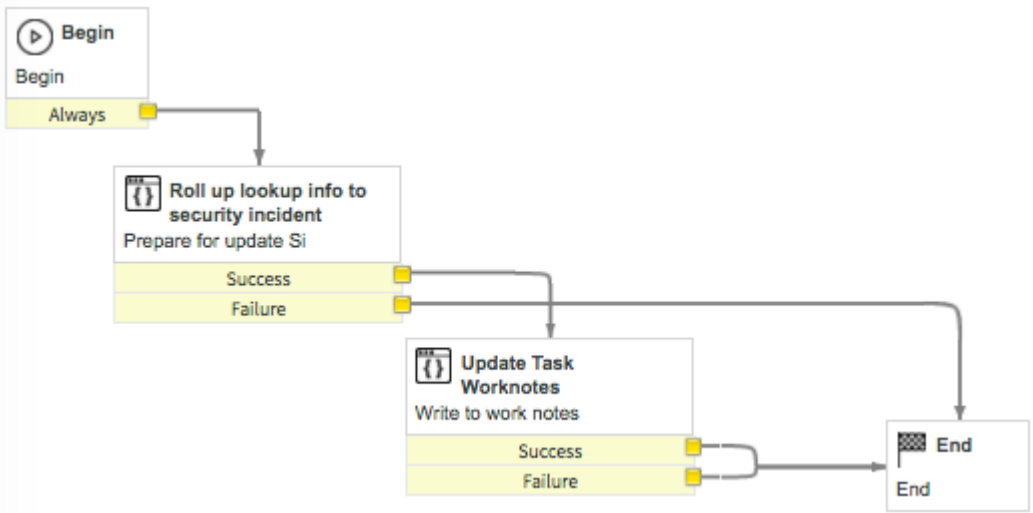
Antes de Iniciar
Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado por uma regra de negócios na tabela de pesquisa que monitora quando **Resultado** O campo muda para Falha.

As atividades do processo de fluxo de trabalho incluem:

Acumular informações de pesquisa para a atividade de incidente de segurança

Atividade Atualizar anotações de trabalho da tarefa



Atividade Filtrar observáveis permitidos

A atividade de fluxo de trabalho Observáveis na lista de permissões filtrados remove observáveis que podem ser ignorados da lista de observáveis. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Filtrar observáveis permitidos pode ser usada com qualquer fluxo de trabalho para filtrar observáveis antes de executar qualquer ação.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Lista de filtros criada.
Falha	Ocorreu um erro ao tentar filtrar os observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
FilteredObservables	Observáveis filtrados.

Gravar conteúdo para registrar como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado para um determinado registro.

. **Grave conteúdo para registrar como anexo** a atividade pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
tablename [cadeia de caracteres]	O nome da tabela do registro. Este campo de entrada é obrigatório.
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto sem formatação a ser escrito como um anexo. Este campo de entrada é obrigatório.
nomeArquivo	O nome do arquivo do anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Atividade Obter IP do IC

A atividade Obter IP do fluxo de IC reúne o endereço IP dos itens de configuração (ICs) a serem usados no fluxo.

A atividade Obter IP do IC pode ser usada com qualquer fluxo para coletar endereços IP de item de configuração (IC) a serem usados no fluxo.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Operações de segurança gatilhos de fluxo de trabalho

Operações de segurança os gatilhos de fluxo de trabalho contêm uma condição em uma tabela. Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.

Criar Operações de segurança gatilhos de fluxo de trabalho

Crie um gatilho de fluxo de trabalho que contenha uma condição em uma tabela.

Antes de Iniciar

Operações de segurança contém vários gatilhos de fluxo de trabalho no sistema de base:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mudanças de item de configuração em um Incidente de segurança ativo

Usa a integração para enriquecer os dados relacionados ao IC conforme os itens de configuração mudam.

Verificar novamente o grupo vulnerável

Nova verificação de um grupo vulnerável, usando Verificar fluxo de trabalho de vulnerabilidade, quando você **Fechar/Ignorar** o grupo.

Verificar novamente o item vulnerável

Nova verificação de um item vulnerável, usando Verificar fluxo de trabalho do item de vulnerabilidade quando você **Fechar/Ignorar** o item.

Funções necessárias:

- Para ler: sn_sec_cmn.read
- Para criar ou atualizar: sn_sec_cmn.write
- Para excluir: sn_sec_cmn.admin

Procedimento

1. Navegar até **Tudo** > **Operações de segurança** > **Utilitários** > **Gatilhos de fluxo de Trabalho**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

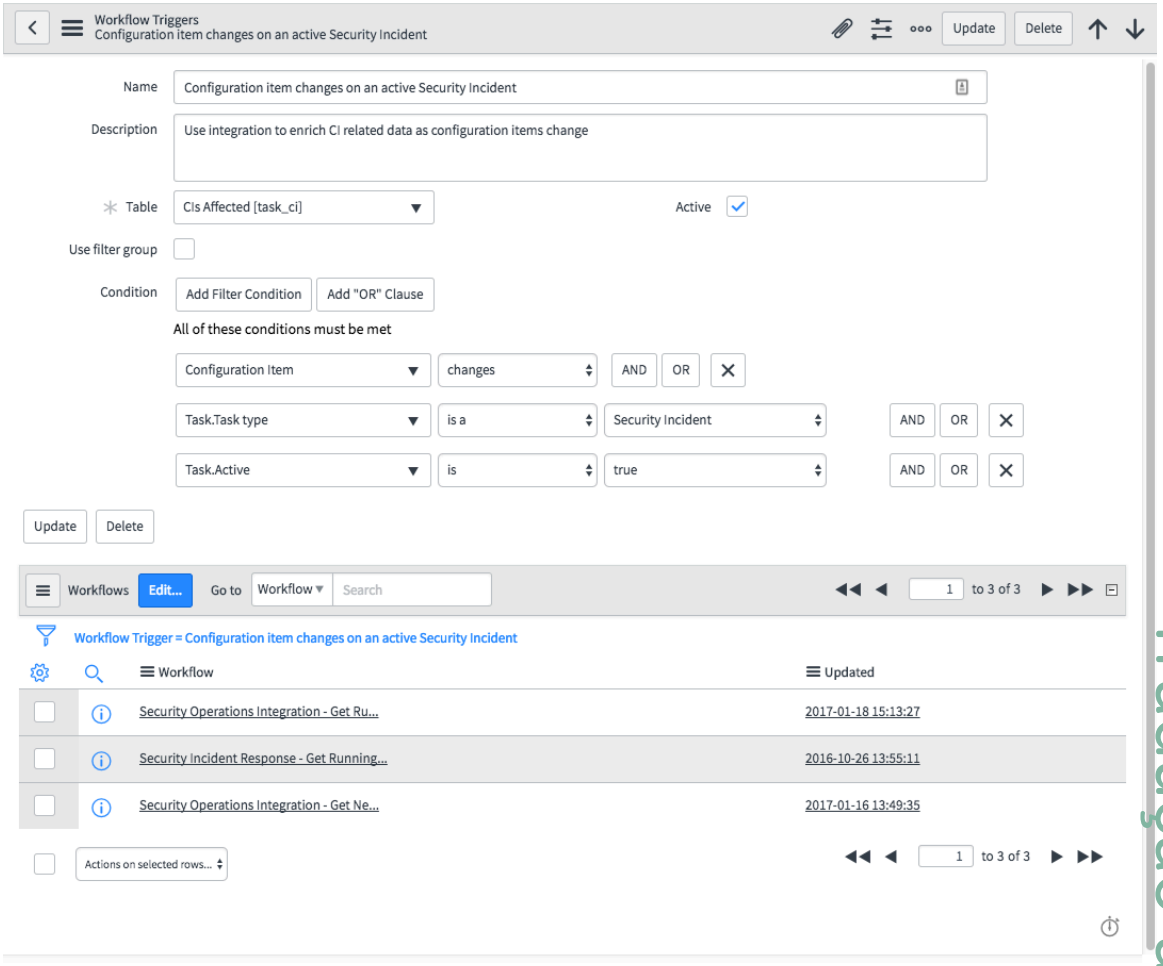
Gatilhos de fluxo de Trabalho

Campo	Descrição
Nome	O nome do gatilho de fluxo de trabalho.
Descrição	Insira uma descrição para o gatilho de fluxo de trabalho.
Tabela	A tabela que contém o gatilho de fluxo de trabalho. Se você selecionou **Usar grupo de filtros** e selecionado um grupo de filtros, este campo assume como padrão a tabela associada ao grupo de filtros selecionado.
Condição	Use o construtor de condições para definir os critérios para o gatilho de fluxo de trabalho. Se você selecionou **Usar grupo de filtros** e selecionou um grupo de filtros, o. **Condição** os campos não são exibidos.
Ativo	Marque esta caixa de seleção para ativar o gatilho de fluxo de trabalho.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou crie um novo grupo de filtros para definir os critérios do gatilho do fluxo de trabalho.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir gatilhos de fluxo de trabalho. Este campo aparecerá somente se **Usar grupos de filtros** a caixa de seleção está marcada.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



. **Fluxos de trabalho** é exibida. Ele contém fluxos de trabalho que são executados quando todas as condições de filtro ou condições de grupo de filtros são atendidas.

5. Para adicionar fluxos de trabalho, execute estas etapas.
   a. Em **Fluxos de trabalho** clique em **Editar** .
   b. Use o Construtor de condições, se necessário, para localizar os fluxos de trabalho que você deseja selecionar ou use o slushbucket para selecionar fluxos de trabalho e movê-los para a Lista de fluxos de trabalho.
   c. Clique em **Salvar**.
   Os fluxos de trabalho selecionados são adicionados.
6. Clique em **Atualizar**.

Orquestração do Security Operations

Os usuários podem interagir e recuperar dados de sistemas e ambientes baseados em Windows ou UNIX usando pacotes de atividades e fluxos de trabalho em Orquestração de Operações de segurança.

Orquestração de Operações de segurança elimina processos manuais e obtém informações contextuais para corrigir incidentes. . Operações de segurança os produtos têm pacotes de atividades padrão e fluxos de trabalho que são incluídos e ativados em cada um dos plug-ins.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar e acessar atividades de orquestração adicionais que não estão disponíveis com a oferta padrão Operações de segurança produtos, compre uma licença de orquestração completa.

- Orquestração de Resposta a incidentes de segurança fluxos de trabalho:
  - Resposta do incidente de segurança- Obter fluxo de estatísticas de rede
  - Integração de comando do sistema de operações de segurança- Obter fluxo de processos em execução
  - Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IOC
  - Integração de operações de segurança - Fluxo de pesquisa e exclusão de e-mail
- Orquestração de inteligência contra ameaças fluxos de trabalho:
  - Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IOC
  - Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa
- Orquestração de Resposta de vulnerabilidade fluxos de trabalho:
  - Verificar fluxo de trabalho de vulnerabilidade
  - Verificar fluxo de trabalho do item de vulnerabilidade

Operações de segurança e o ServiceNow Store

Começando com Madrid. todos Operações de segurança as aplicações e integrações compatíveis estão disponíveis para download no ServiceNow Store. Isso permite que você obtenha recursos novos e atualizados mais rapidamente. Antes de poder usar qualquer Operações de segurança aplicações, você deve verificar se tem direito a elas (ou seja, se você tem licenças válidas para usá-las), baixe-as do ServiceNow Store e ative-os.

A lista cada vez maior de Operações de segurança as aplicações disponíveis para download incluem:

- Resposta a incidentes de segurança (e integrações compatíveis)
- Resposta a vulnerabilidades (e integrações compatíveis)
- Inteligência contra ameaças (e integrações compatíveis)
- Conformidade de configurações
- Círculo de segurança confiável
- Data Loss Prevention Incident Response

Assista a este vídeo de cinco minutos para saber mais sobre como baixar operações de segurança e aplicações de GRC do ServiceNow Store. Este vídeo de 5 minutos descreve como baixar operações de segurança e aplicações GRC da ServiceNow Store

O processo que você usa para obter Operações de segurança as aplicações e integrações dependem de você estar baixando uma aplicação pela primeira vez, atualizando uma aplicação que você baixou anteriormente do ServiceNow Store ou atualizando de uma versão de família para a próxima.

Baixar uma aplicação do ServiceNow Store pela primeira vez

Baixando uma aplicação do ServiceNow Store pela primeira vez envolve uma série de etapas fáceis. Algumas das etapas são executadas no ServiceNow Store e alguns em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

. ServiceNow Store permite que você baixe produtos e aplicações principais. Um produto contém uma ou mais aplicações que são licenciadas como um grupo. Por exemplo, Resposta a incidentes de segurançaé um produto. O processo envolve estas etapas:

Função necessária: administrador

- Em ServiceNow Store, você deve garantir que tenha direitos (ou licenças) à aplicação e suas aplicações dependentes.

  Nota: Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

- Por fim, você pode ativar a aplicação e executá-la em sua instância.

Nota: A partir das versões anteriores de Rome e versões posteriores, os plug-ins de dependência são ativados automaticamente quando você ativa uma aplicação principal. Por exemplo, quando você ativa o. Resposta a vulnerabilidades, o. Resposta a vulnerabilidades O plug-in Dependências também está ativado. Para obter mais informações, consulte Ativar um ServiceNow Store aplicação.

Obtenha direito para um Operações de segurança produto ou aplicação

A primeira etapa na instalação de um Operações de segurança a aplicação serve para verificar se a aplicação ou o produto e suas aplicações associadas são válidas ServiceNow direitos.

Antes de Iniciar

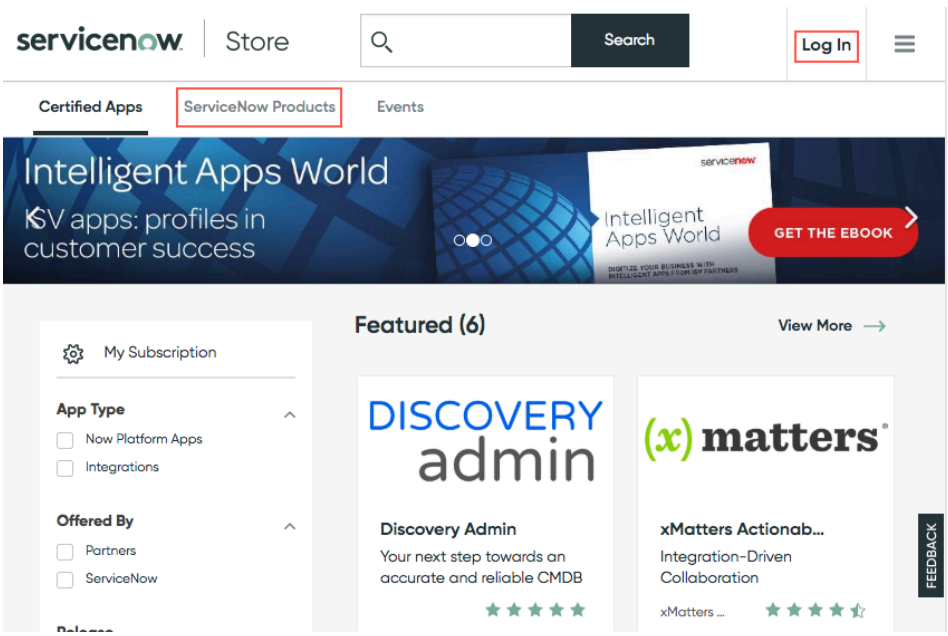
Função necessária: administrador

Os indivíduos que executam o direito devem ter um Now Support e têm permissão para solicitar aplicações para as instâncias em consideração.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar um ServiceNow Store aplicação.

Procedimento

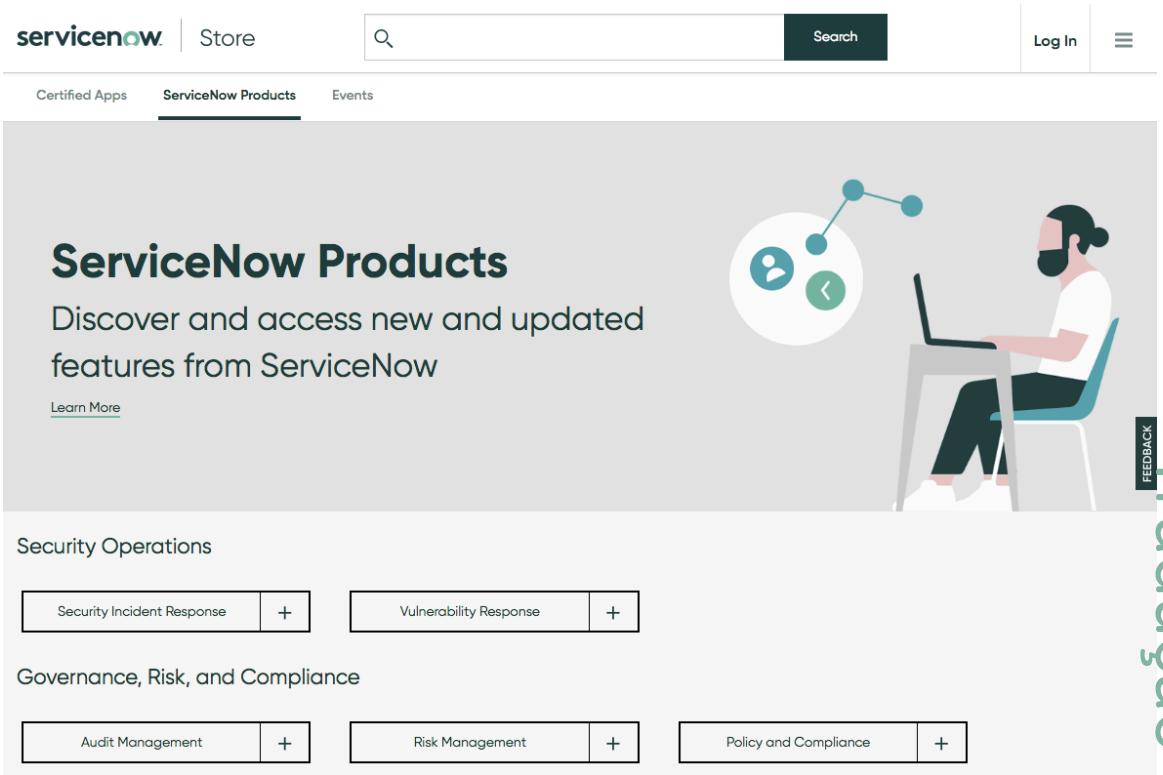
1. Navegue até ServiceNow Store .



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Clique em **Login** e faça login usando seu HI credenciais.
3. Clique em **Produtos da ServiceNow** para exibir todos os disponíveis ServiceNow produtos. Integrações e outros tipos de conteúdo são mostrados no **Aplicações certificadas** guia.



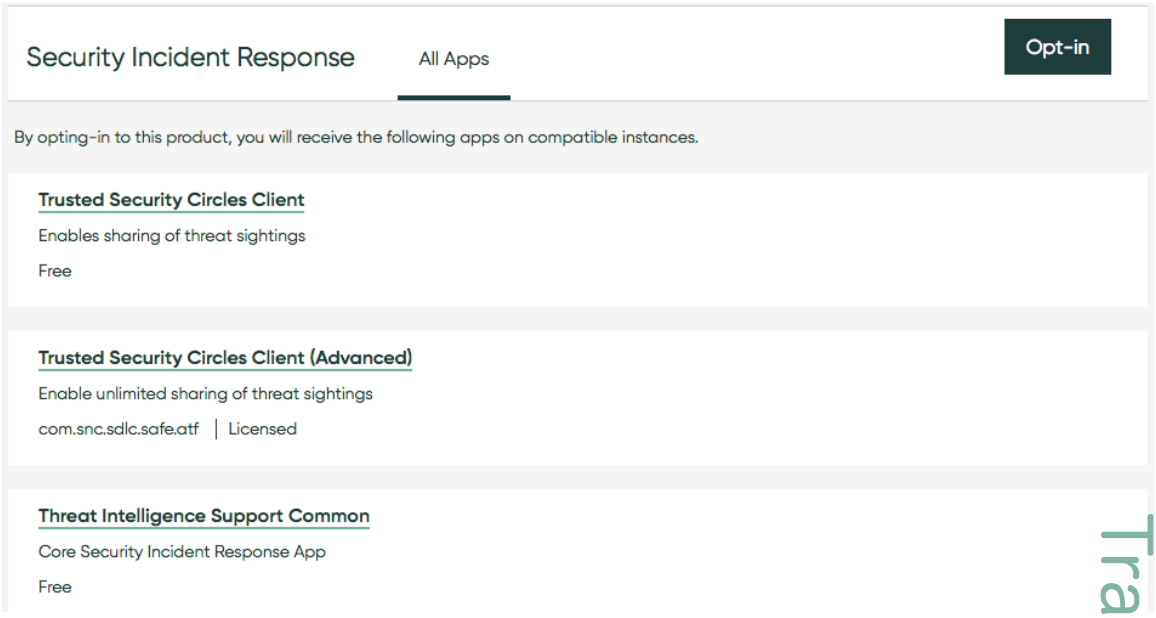
Nota: Para este exemplo, suponha que você esteja adquirindo direito para Resposta a incidentes de segurança produto.

4. Clique no sinal de adição ao lado do nome do produto ao qual você está obtendo direito.
Todas as aplicações associadas ao produto que você está qualificando são listadas. Quando você obtém o direito ao produto principal, as aplicações listadas nele também são qualificadas.

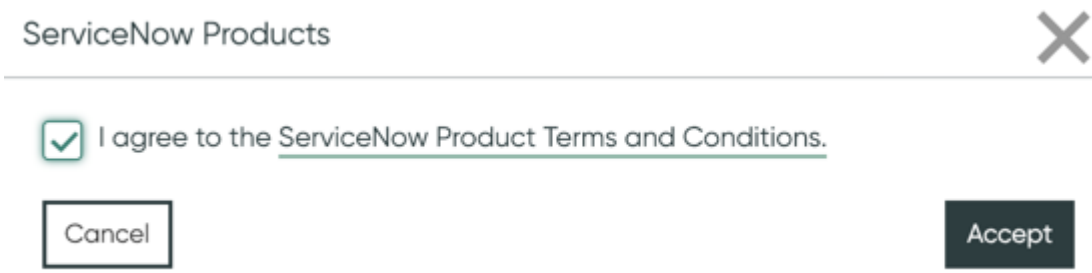
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você também pode clicar no nome do produto para exibir mais informações sobre o produto e suas aplicações associadas.



5. Clique em **Aceite** para verificar se você tem direito ao produto e às aplicações listadas. Você será solicitado a ler e aceitar ServiceNow termos e



condições.

6. Marque a caixa de seleção e clique em **Aceitar** .
7. Observe que uma marca de seleção aparece ao lado do nome do produto e o botão Gerenciar direitos é exibido.

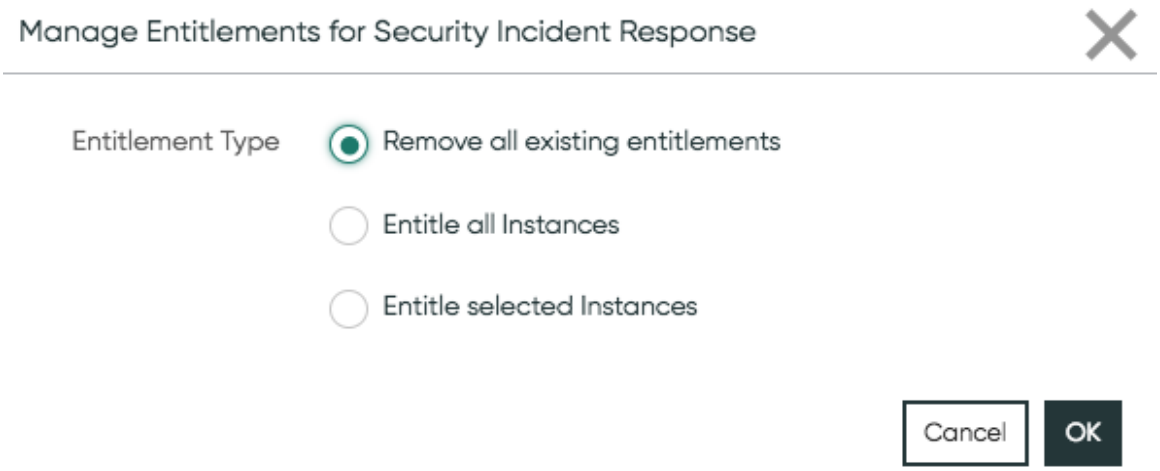


A marca de seleção indica que você assinou o produto e suas aplicações associadas. É hora de gerenciar seus direitos. Este é um processo único para este produto e quaisquer outros produtos que você deseja instalar no futuro.

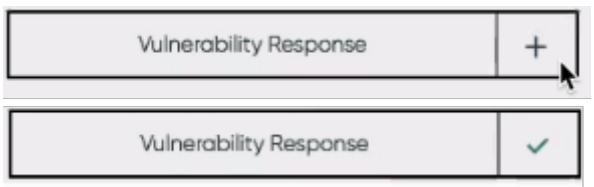
8. **Opcional:** Você pode clicar em **Gerenciar direitos** para mudar as instâncias afetadas pelas aplicações às quais você tem direito.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Depois de concordar com ServiceNow Termos e condições e Direitos gerenciados, você pode atribuir direitos a outros produtos com um único clique.



Nota: Você está pronto para ativar o produto.

Ativar um ServiceNow Store aplicação

Depois que uma aplicação receber o direito, você deve ativar o plug-in de dependências e ativar a aplicação. Este processo também se aplica a aplicações baixadas para instâncias de subprodução.

Antes de Iniciar

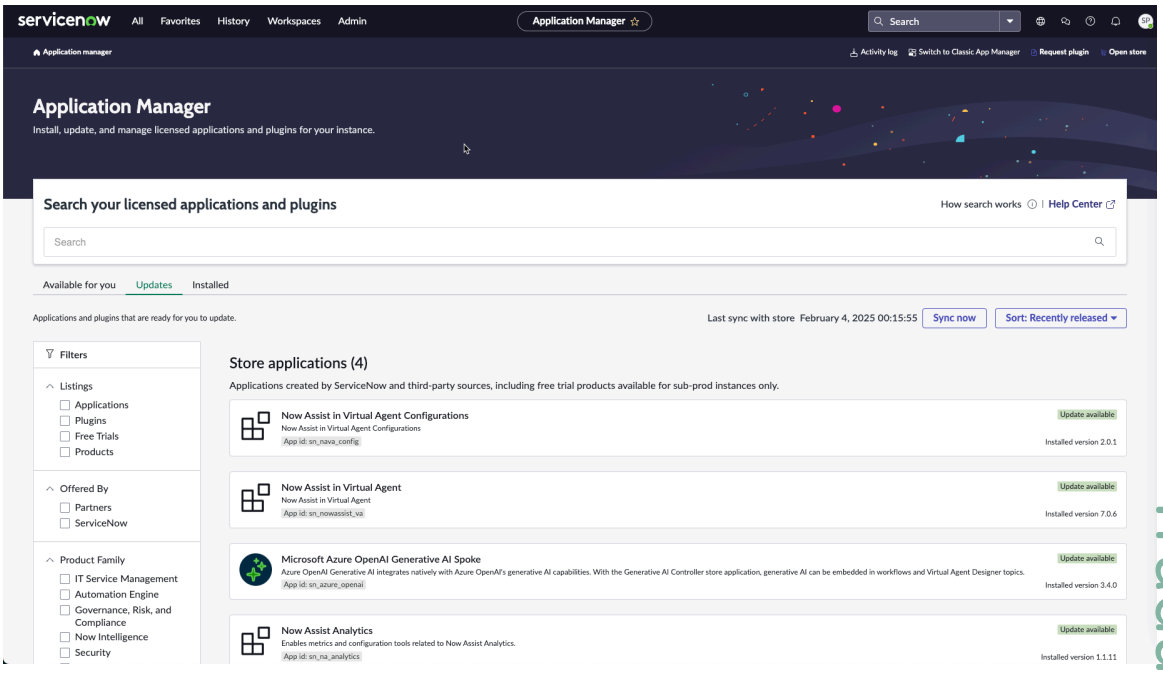
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

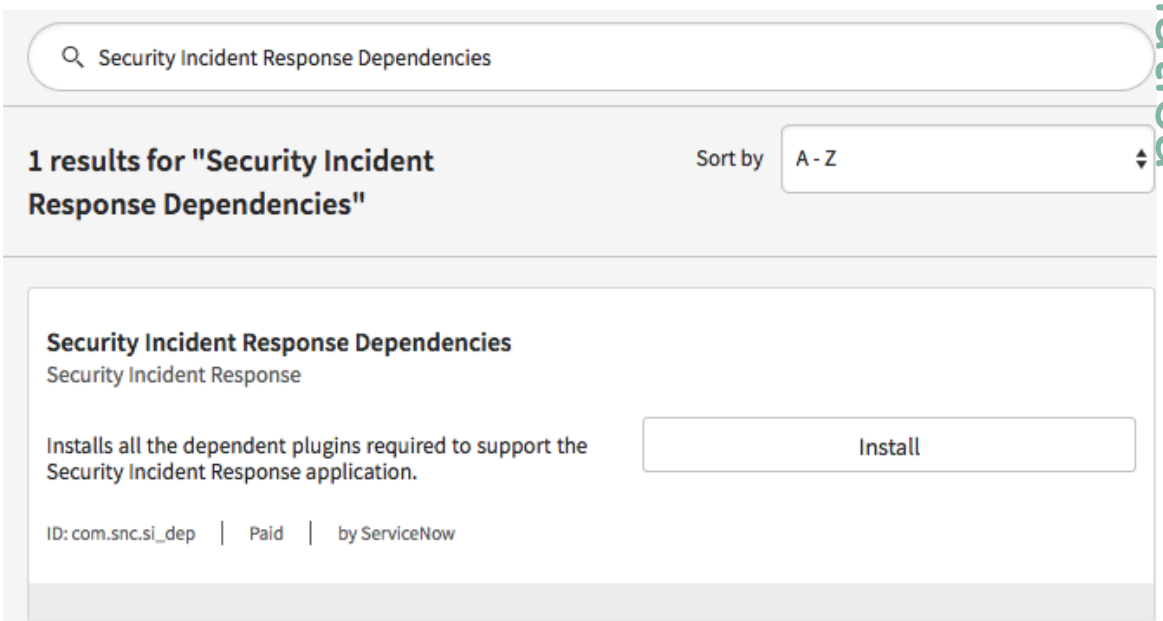
Procedimento

1. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.



> **Nota:** A partir do Orlando, os plug-ins de dependência são ativados automaticamente quando você ativa uma aplicação principal. Por exemplo, quando você ativa o. Resposta a vulnerabilidades, o. Resposta a vulnerabilidades O plug-in Dependências também está ativado. Portanto, as etapas 2 a 5 são opcionais.

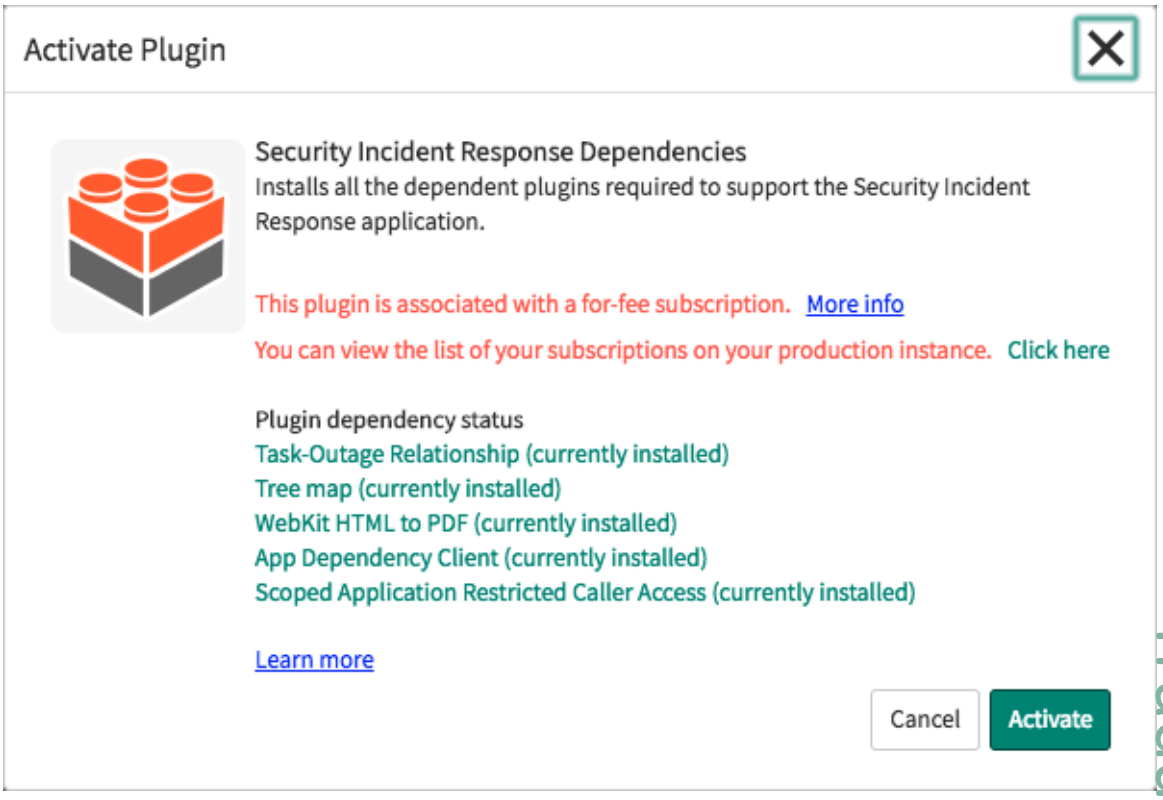
2. PESQUISE o plug-in de dependências da aplicação que você deseja ativar.
   Por exemplo, se você estiver ativando Resposta a incidentes de segurança, localize Resposta a incidentes de segurança Plug-in Dependências.



3. Clique em **Instalar**.
   A caixa de diálogo Ativar plug-in é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Em **Ativar plug-in** caixa de diálogo, clique em **Ativar** .
5. Quando a ativação estiver concluída, clique em **Formulário Fechar e recarregar** .
6. Agora localize o produto principal que você está ativando e clique em **Instalar com dados de demonstração** se quiser carregar dados de demonstração, marque a caixa de seleção e clique em **Instalar** . Sua aplicação é instalada automaticamente em sua instância.

> **Nota:** Se você não selecionar **Instalar com dados de demonstração** os dados de demonstração não estão disponíveis para instalação do **Gerenciador de aplicações** mais tarde. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] artigo no HI Base de conhecimento.

Instale um Operações de segurança integração

Todos ServiceNow as integrações estão disponíveis no ServiceNow Store. As principais aplicações, como Resposta a incidentes de segurança, estão visíveis no **Produtos da ServiceNow** na loja. Os complementos de integração estão visíveis no **Aplicações certificadas** guia.

Antes de Iniciar

Função necessária: administrador

As instalações da Store exigem um Now Support conta e permissão para solicitar aplicações para as instâncias em consideração.

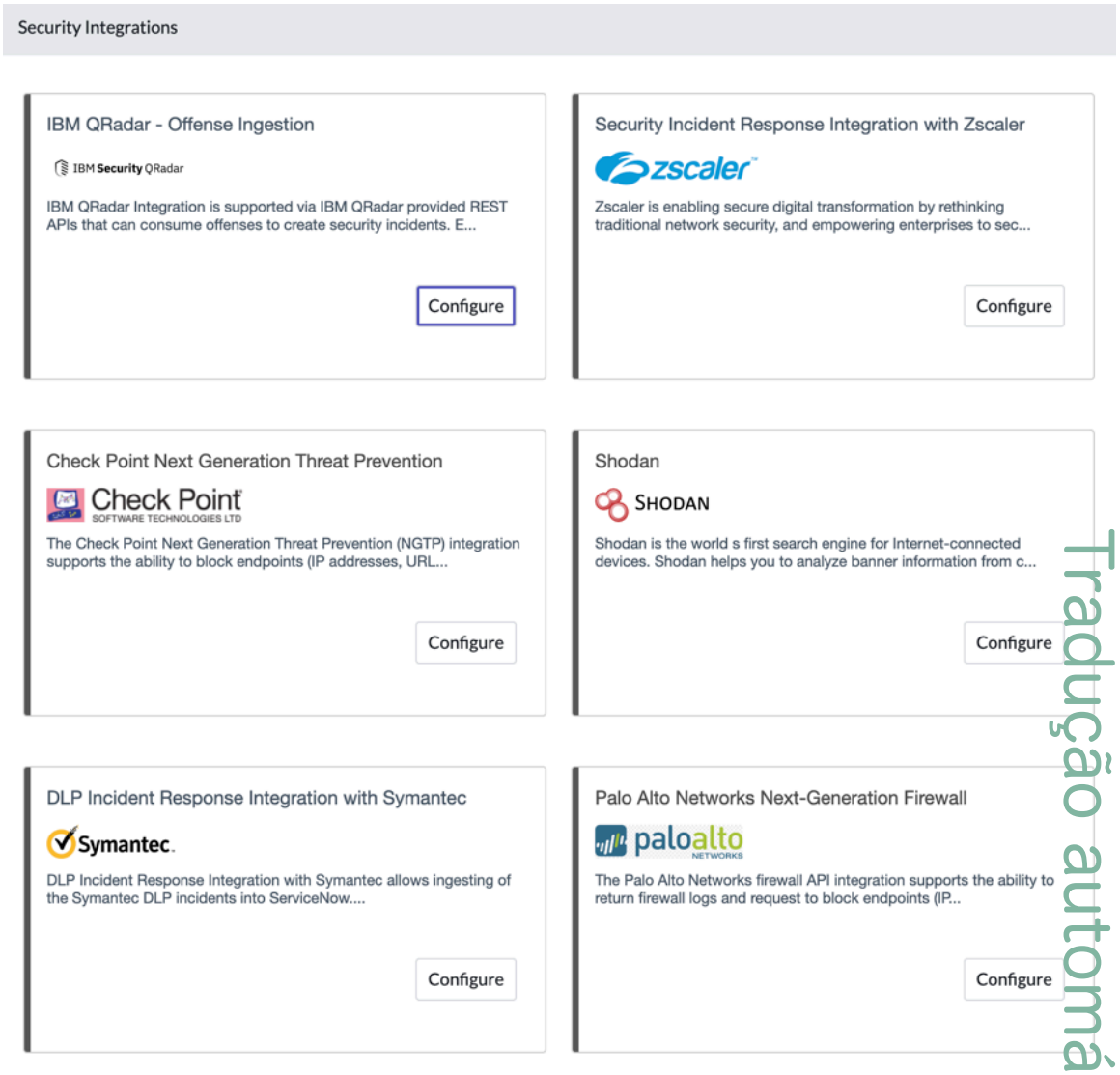
Procedimento

1. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração** Depois de instalar a aplicação da ServiceNow Store.
   Os blocos de configuração das integrações são exibidos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

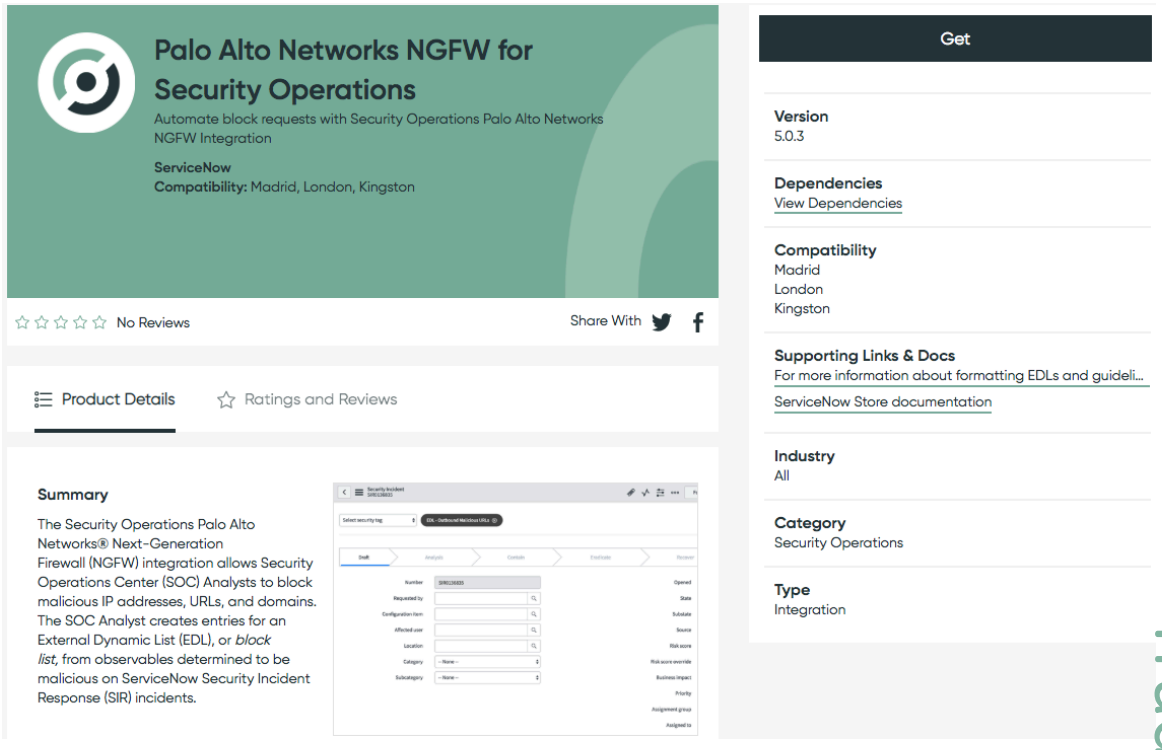
Nota:



2. Localize a integração que você deseja instalar e clique em **Configurar** .
A integração selecionada é mostrada em ServiceNow Store

Tradução automática

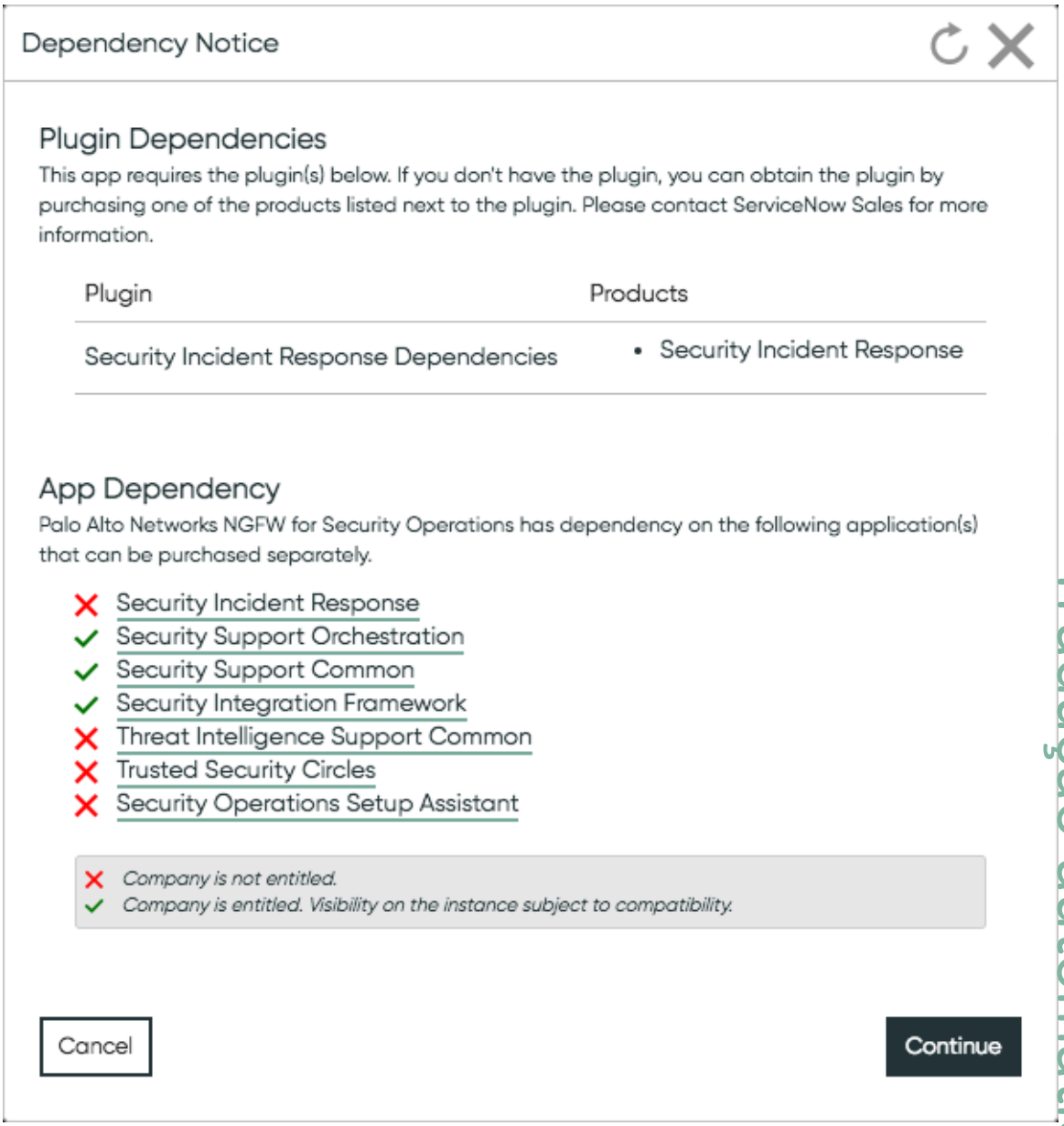
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Exibir dependências** e revise as dependências do app listadas.

Tradução automática

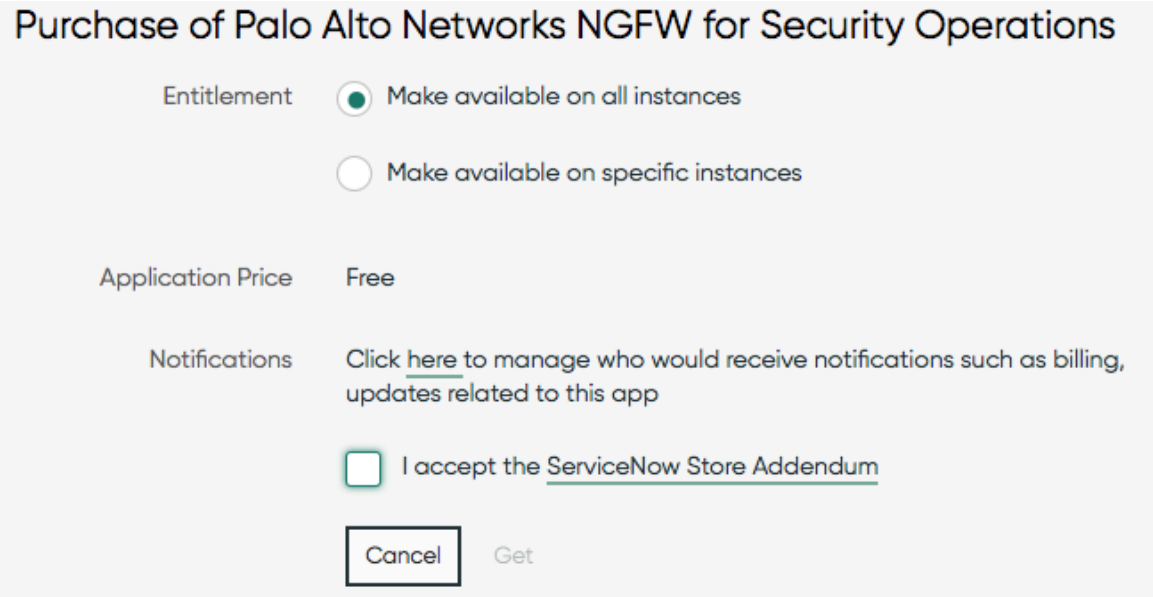
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

4. Se a integração tiver dependências de aplicação principal, como Resposta a incidentes de segurança, para o qual sua empresa ainda não tem direito:
   a. Siga estas instruções para obter direitos, baixar plug-ins de dependência e ativar as aplicações .
   b. Retorne a este procedimento.
   c. Clique em **"Continuar"**.
5. Clique em **Obter**.
   Os Termos e Condições da ServiceNow são exibidos.
6. Clique em **"Continuar"**.
   Uma tela Compra semelhante à seguinte é aberta.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Identifique em quais instâncias você deseja que a integração esteja disponível, gerencie suas notificações e selecione **Adendo da ServiceNow Store** caixa de seleção.
8. Clique em **Obter**.

   Nota: Se você estiver baixando um aplicativo para compra, clique em **Comprar** . Se você estiver baixando uma aplicação que requer aprovação prévia do fornecedor, clique em **App de solicitação** .

9. Insira o nome da instância e um motivo para a solicitação e clique em **Solicitação** .
   Você receberá um e-mail com instruções detalhadas de instalação.
10. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.
    Uma lista de aplicações disponíveis para instalação é exibida.
11. Localize a aplicação, selecione-a e clique em **Instalar** .
    Sua integração é instalada automaticamente em sua instância.

Atualize uma aplicação baixada anteriormente do ServiceNow Store

Se você baixou anteriormente um aplicativo do ServiceNow Store e uma nova versão estiver disponível, você pode atualizá-la em sua instância.

Antes de Iniciar

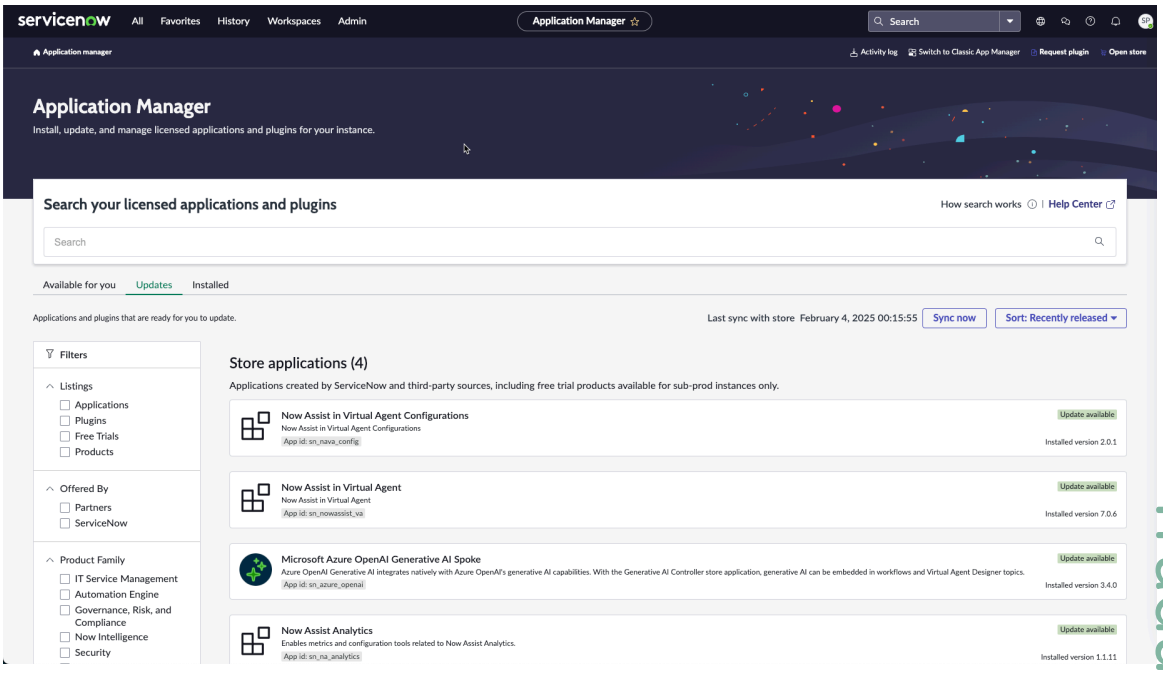
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Tudo**.



2. PESQUISE a aplicação que você deseja atualizar.
3. Selecione a versão para a qual você deseja fazer upgrade e clique em **Atualização** .
   Sua aplicação é instalada automaticamente em sua instância.

Atualize sua instância para a próxima versão da família

No momento, você estiver executando uma versão da família e quiser fazer upgrade para a próxima versão, não será necessário adquirir as aplicações do ServiceNow Store. A aplicação é atualizada automaticamente quando a plataforma é atualizada para a versão mínima necessária.

Função necessária: administrador

Para obter mais informações, consulte Utilizar as notas de versão para saber como navegar pelas notas de versão reprojetadas e encontrar as informações que você está procurando e. Obter mais informações sobre a versão Zurich para novos recursos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.